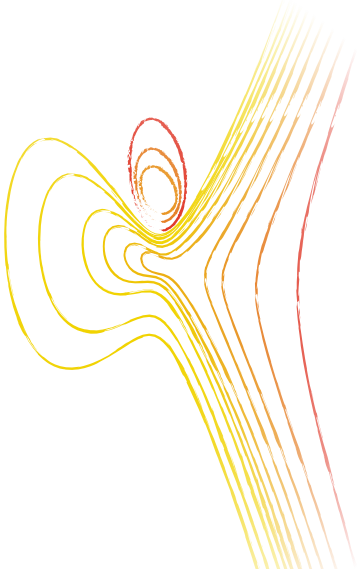
École Doctorale de Sciences Mathématiques de Paris Centre (ED 386)
Institut de Mathématiques de Jussieu - Paris Rive Gauche (UMR 7586)

THÈSE DE DOCTORAT

Discipline : Mathématiques



Analogues du théorème de Brauer-Siegel pour quelques familles de courbes elliptiques

présentée par **Richard GRIFFON**

Université Paris.Diderot (Paris 7)
Université Sorbonne Paris Cité

Dirigée par :
M. Marc HINDRY
Université Paris.Diderot

Soutenue le **4 juillet 2016**

Au vu des rapports de :
M. Michael TSFASMAN
Université de Versailles Saint-Quentin
M. Douglas ULMER
Georgia Institute of Technology

Devant le jury composé de :
M. Bruno ANGLÈS
Université de Caen Basse Normandie
M. Marc HINDRY
Université Paris.Diderot
M. David KOHEL
Université d'Aix-Marseille
M. Loïc MEREL
Université Paris.Diderot
M. René SCHOOF
Università di Roma

Lien direct vers le manuscrit complet / Direct link to the full manuscript :
http://bit.do/Griffon_thesis

Institut de Mathématiques de Jussieu - Paris Rive Gauche
(CNRS – UMR 7586)
Université Paris Diderot (Paris 7)
Bâtiment Sophie Germain - Boîte courrier 7012
8 place Aurélie Nemours
75205 Paris Cedex 13
France

Ecole Doctorale de Sciences Mathématiques de Paris Centre
Boite courrier 290
4, Place Jussieu
75252 Paris Cedex 05
France

Résumé / Abstract

Résumé

Dans cette thèse, nous étudions le comportement asymptotique du ratio de Brauer-Siegel des familles de courbes elliptiques sur les corps de fonctions en caractéristique positive. Si E/K est une courbe elliptique sur un corps de fonctions K, on définit son ratio de Brauer-Siegel par

$$\mathfrak{Bs}(E/K) = \log(\#Ш(E/K) \cdot \mathrm{Reg}(E/K))/\log H(E/K),$$

où $\mathrm{Reg}(E/K)$ désigne le régulateur de Néron-Tate, $Ш(E/K)$ le groupe de Tate-Shafarevich et $H(E/K)$ la hauteur différentielle exponentielle de E/K. Cette quantité est définie en analogie avec le théorème éponyme pour les corps de nombres.

Nous démontrons que $\mathfrak{Bs}(E/K) \to 1$ (inconditionellement) lorsque E/K pacrourt l'une de cinq familles de courbes elliptiques, avec $H(E/K) \to \infty$. En d'autres termes, ces familles vérifient un analogue du théorème de Brauer-Siegel.

Pour prouver une telle relation asymptotique, nous commençons par exprimer les fonctions L des courbes elliptiques concernées en termes de sommes de caractères sur les corps finis. Puis, *via* la conjecture de Birch et Swinnerton-Dyer, nous relions le ratio $\mathfrak{Bs}(E/K)$ à la valeur spéciale $L^*(E/K, 1)$ de la fonction $L(E/K, s)$ en $s = 1$ (pour les cinq familles considérées, cette conjecture a été démontrée par d'autres auteurs). Reste alors à encadrer la taille de $L^*(E/K, 1)$ en termes de $H(E/K)$: la majoration est aisée, mais la minoration requiert des estimations plus délicates. Nous développons donc quelques outils adaptés : nous exprimons sous forme combinatoire la valuation q-adique d'un produit de nombres algébriques associés aux sommes de Jacobi et démontrons un résultat d'équidistribution en moyenne des sous-groupes de $(\mathbb{Z}/d\mathbb{Z})^\times$.

Nous obtenons au passage des résultats sur le rang, la torsion et le nombre de Tamagawa des courbes étudiées.

Mots-clefs

Courbes elliptiques sur les corps globaux, Corps de fonctions en caractéristique positive, Ratio de Brauer-Siegel, Régulateur de Néron-Tate, Groupe de Tate-Shafarevich, Théorème de Brauer-Siegel et analogues, onjecture de Birch et Swinnerton-Dyer, Sommes de caractères sur les corps finis, Fonctions L de courbes elliptiques, Valeurs spéciales de fonctions L, Minoration de valeurs spéciales.

Analogues of the Brauer-Siegel theorem for some families of elliptic curves

Abstract

In this thesis, we study the asymptotic behaviour of the Brauer-Siegel ratio in families of elliptic curves over function fields in positive characteristic. If E/K is an elliptic curve over a function field K, its Brauer-Siegel ratio is defined by

$$\mathfrak{Bs}(E/K) = \log(\#Ш(E/K) \cdot \mathrm{Reg}(E/K))/\log H(E/K),$$

where $\mathrm{Reg}(E/K)$ denotes the Néron-Tate regulator, $Ш(E/K)$ the Tate-Shafarevich group and $H(E/K)$ is the exponential differential height of E/K. This invariant is introduced by analogy with the Brauer-Siegel theorem for number fields.

We prove that $\mathfrak{Bs}(E/K) \to 1$ (unconditionally) when E/K runs through one of five families of elliptic curves, with $H(E/K) \to \infty$. In other words, these families satisfy an analogue of the Brauer-Siegel theorem.

To prove such an asymptotic relation, we first write the L-functions of the relevant elliptic curves in terms of character sums over finite fields. Then, *via* the Birch and Swinnerton-Dyer conjecture, we link $\mathfrak{Bs}(E/K)$ to the special value $L^*(E/K, 1)$ of the L function $L(E/K, s)$ at $s = 1$ (for the five families we sstudy, this conjecture has been proved by other authors). It then remains to bound the size of $L^*(E/K, 1)$: a good upper bound is easily proved, but the lower bound we require is more subtle. We thus develop tools to prove it: we find a combinatorial expression of the q-adic valuation of a product of algebrac numbers associated to Jacobi sums and we prove an average equidistribution result for subgroups of $(\mathbb{Z}/d\mathbb{Z})^\times$.

We also obtain auxiliary results about the Mordell-Weil rank, the torsion and the Tamagawa number of the elliptic curves under consideration.

Keywords

Elliptic curves over global fields, Function fields in positive characteristic, Brauer-Siegel ratio, Néron-Tate regulator, Shafarevich-Tate group, Brauer-Siegel theorem and analogues, Birch and Swinnerton-Dyer conjecture, Character sums over finite fields, L-functions of elliptic curves, Special values of L-functions, Lower bounds on special values.

« I don't know much about algebra, but I know
One plus one equals two
And it's me and you. »

Beyoncé Knowles – 1+1

« I think it's wonderful, just marvelous.
You really do love your work, dont you ?
Yeah, well, [...] I guess I do. It kind of grabs me sometimes, you know when theres a problem and you have to find an answer [...] or when you suddenly get an idea and you work on it and work on it and you twist it and yank it until it fits just right. »

Hubert Selby Jr. – The Demon

Remerciements

En premier lieu, je voudrais remercier mon directeur de thèse, Marc Hindry. Merci, déjà, de m'avoir proposé ce joli sujet et d'avoir eu confiance en moi. Je le remercie surtout pour son encadrement pendant ces années : pour sa patience à répondre à mes questions, pour sa porte toujours ouverte et sa disponibilité, pour ses grandes qualités pédagogiques, pour ses encouragements dans les moments de doute, pour les invitations à Moscou et pour la liberté qu'il m'a laissée dans mes recherches pas toujours fructueuses.

Je voudrais aussi remercier les rapporteurs Michael Tsfasman et Douglas Ulmer. Leurs travaux ont été d'une grande importance pour moi et je suis très honoré qu'ils aient accepté de rapporter ce manuscrit. Je les remercie pour leur lecture, leurs commentaires et leur rapport détaillés et encourageants.

Merci également aux membres du jury d'être présents le jour de la soutenance pour évaluer mon travail. Merci à Bruno Anglès, David Kohel et René Schoof d'avoir accepté de faire le déplacement. Je suis aussi très heureux de la présence de Loïc Merel, sous la direction duquel j'ai réalisé mon mémoire de M2.

Pendant ces années de thèse, j'ai eu l'occasion de recontrer de nombreux.ses mathématicien.ne.s : pour les discussions mathématiques (ou non), pour leurs questions, leurs suggestions et leurs encouragements, je voudrais remercier ici Amìlcar Pacheco, Huayi Chen, Pierre Parent, Marc Perret, Fabien Pazuki et Mathilde Herblot. Merci aussi à ceux qui m'ont invité à donner des exposés, en particulier : Bruno Kahn à Jussieu, Gaël Rémond et Éric Gaudron pour l'ANR GArDio à Grenoble, Philippe Lebacque et Alexey Zykin à Moscou, Nicolas Billerey à Clermont-Ferrand et David Kohel à Marseille. J'ai eu la chance d'assister à la conférence en l'honneur des 60 ans de Joseph Silverman et d'y présenter un poster. Je remercie Bjorn Poonen et Kenneth Ward pour l'intérêt qu'ils y ont porté et pour leurs suggestions.

Je voudrais aussi remercier les personnels administratifs, le support informatique, les secrétaires et les gestionnaires de l'IMJ, de l'UFR de maths, de l'ANR HaMoT et de l'ANR GArDio. Particulièrement Gaëlle Callouard, Christine Le Sueur, Pascal Chiettini (et son successeur Vincent Loiseau) pour leur efficacité et leur patience, qui ont largement compensé mon manque d'organisation. Merci aussi à la secrétaire de l'école doctorale, Élise Delos, de m'avoir guidé dans les procédures avant la soutenance.

Cette thèse est (aussi) l'aboutissement de quelques dix années d'études supérieures : celles-ci n'auraient probablement pas eu lieu sans l'appui de mes professeurs. Qu'ils trouvent ici l'expression de ma profonde gratitude. Autant que je me rappelle, c'est M. Méchinaud qui, en 5ème, m'a donné le goût des mathématiques. Merci à Mme. Montaigne qui m'a poussé à aller en prépa, Je tiens à remercier tout spécialement mes professeurs de prépa : Bernard Luron et surtout Denis Choimet, pour tout son soutien et pour les séminaires du soir qu'il organisait à Clemenceau. Plus tard, j'ai eu la chance de suivre les cours de Laurent Berger, de Claude Danthony, les TD de François Brunault, d'Agnès David et de Sandra Rozensztajn. Je souhaite aussi remercier Kevin Buzzard, qui m'a encadré pour mon stage de L3, pour le temps qu'il a passé à m'apprendre tant de belles choses.

Merci à celles et ceux qui ont partagé mon bureau à Chevaleret, puis à Sophie Germain : Lukas, Daniel, Mouchira, Alfredo, Tony et Eirini. Je voudrais aussi remercier les autres doctorant.e.s de

Sophie Germain pour la bonne ambiance qui y règne (de travail mais pas que) : Nicolas L., Assia N., Marco P., Baptiste M. pour sa bonne humeur constante, David D., Élie G., Kevin D., Antoine J. et Alexandre A..

Et bien sûr merci à Julie qui m'a supporté (dans son bureau, à Moscou et ailleurs) pendant trois ans et qui dépose sa thèse au moment où j'écris ces lignes (tout en me dictant « je remercie Julie ma petite soeur de thèse chérie que j'adore et que j'admire, la meilleure de l'univers »). Merci également à Benjamin et Victoria, mes autres frères et soeurs de thèse.

Je remercie aussi les membres de l'association Plaisir Maths : Alix, Alix, Anaïs pour toutes ces ateliers qu'on a animés ensemble et à Marielle pour ses conseils graphiques. Et merci surtout à son président Nicolas Pelay.

Dans le désordre le plus complet, espérant n'oublier personne, je voudrais remercier chaleureusement tou.te.s mes ami.e.s pour leur présence à mes côtés pendant tout ou partie de ces années. Il me faudrait bien plus que ces quelques lignes pour dire tout ce représente que votre amitié et tout ce que vous m'apportez.

Pour leur amitié depuis le collège, je remercie Jean Baptiste, Emmanuelle « ta rage n'est pas perdue », Noémie et surtout Jonathan. Merci à tous ceux que j'ai rencontrés à Lyon. Merci à Guillaume A. et Laura P. (revenez vite), Matthieu et Etienne pour ces moments Rue du Lac et après, Lucy M. pour l'ensemble de son oeuvre, Suzanne d'avoir supporté la colocation londonienne, Morgan L. camarade intarissable (et coucou à Andrea), Olivier D. sur sa plateforme, Julien B., Léa B. et Pierre François L., Julien V. notre modèle à tous, Antoine Wiki M. et Guillaume C. (D36 forever). Merci également aux matheux de Lyon : Roméo, Rrémi, Marielle, Bruno pour son coaching agreg, Sylvain et ses apparitions innatendues à Sophie Germain, François et Olivier. Et surtout Samuel Le Fourn (et Kevin Ro) pour toutes les discussions, questions et débats, mathématiques ou non. Merci aussi aux informaticiens de l'ENS Val de Marne : Pierre-Marie P., Jean Marie M. et Guillaume A..

Merci aussi aux Relous et aux Pompoms de m'avoir souvent accueilli le week-end à Lyon, et aussi pour leur humour et leur gentillesse : Léonie et Théodore M. et Mme Parfaits, Fanny et Clément pour les découvertes musicales décalées, Carole qui devrait revenir plus souvent de ses forêts, Augustin, et Camille. Un merci à part pour Simon, king of the bees.

Pour tous ces chouettes moments à Paris et ailleurs : visites, cafés, verres, soirées, etc., merci à Adrien D., Julien J., Bastien F., Alex P., Marguerite J., Antoine P., Félix A., Ariane L. pour les week-ends au vert, et Marc C. et Paul N. pour leurs soirées *Soucoupe Hippique*. Merci aux nantais exilés Clément M. et Guillaume T. Long. Merci aussi à Joris et Maxime le cosmonaute pour les vacances en Italie et pour le reste.

Un grand grand merci à Yann H. et Pauline B. pour les repas ensemble et la co-motivation à aller au sport, et bienvenue à Alexis (qui est né le jour où j'ai soumis ma thèse) ! Pour leur soutien quotidien, pour les vacances et les soirées et plus généralement pour tous les moments passés ensemble, un immense merci à Claire Abder. d'Auxerre, Sara(h) Loeuf ma moeuf, Dr. Alex LPLP Z., Germain L., Luc P., Yann L., les soeurs Odieuse de Beauregard et Maxime Igor.

Merci à tous, merci d'avoir été là et d'être encore là.

Je voudrais aussi remercier ma famille : sans leur soutien moral, je ne serais sûrement pas arrrivé au bout de ce périple. Un immense merci à mes parents de m'avoir toujours soutenu dans mes choix, pour leur aide et pour tout le reste. En particulier, merci pour le temps que vous avez passé à relire ce manuscrit (plusieurs fois) à la recherche des fautes de frappe, ... et désolé pour le retard que vous avez dû prendre dans vos mots croisés. Merci aussi à mes deux soeurs Sarah et Marjolaine, qui me supportent (et me supportent) depuis bien longtemps. Coucou à Markus. Merci également à Jeff et Evelyne, à mes cousines et à mes cousins. J'ai une pensée pour tonton François, qui nous a quittés pendant que je commençais à rédiger ma thèse. Et enfin, merci à ma grand-mère, que rien ni personne n'aurait pu empêcher d'assister à ma soutenance (avec quelques jours de retard : Joyeux anniversaire mamie !).

Table des matières

Introduction (in English)

The main concern of this thesis is the asymptotic study of an invariant associated to elliptic curves over global fields, namely the Brauer-Siegel ratio. This ratio combines three of the most important arithmetical invariants of an elliptic curve: its Néron-Tate regulator, the order of its Tate-Shafarevich group and its height. We prove analogues of the classical Brauer-Siegel theorem for several families of elliptic curves over $\mathbb{F}_q(t)$. We start by motivating the study of the Brauer-Siegel ratio and explaining the analogues we have in mind. We refer the reader to [Hin07] and [HP16, §1] for a thorough exposition of the problem in a more general setting.

Let $\mathbb{F}_q$ be a finite field of characteristic p and $K = \mathbb{F}_q(C)$ be the function field of a projective smooth and geometrically irreducible curve C over $\mathbb{F}_q$. For convenience, we suppose that $p \geqslant 5$. For concreteness, the reader may assume that K is the rational function field $\mathbb{F}_q(t)$ over $\mathbb{F}_q$.

Let E be an elliptic curve over K, given by a Weierstrass model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

with coefficients $a_i \in K$. There is a variety of invariants associated to E that encapsulate the "arithmetic complexity" of E: its minimal discriminant, its conductor, its height, ... We choose to order elliptic curves E/K with respect to their differential exponential height $H(E/K)$ defined by

$$H(E/K) = q^{\frac{1}{12}\deg \Delta_{\min}(E/K)},$$

where $\Delta_{\min}(E/K)$ is the minimal discriminant of E/K. The important point is that the height is readily computable from a Weierstrass model for E/K such as equation (1) (using Tate's algorithm for example, see [Tat75]). Note that $H(E/K)$ depends exponentially on (the degrees of) the coefficients $a_i \in K$.

For such an elliptic curve E/K, the Mordell-Weil theorem (proved by Lang and Néron in this context) says that the group $E(K)$ is finitely generated: we can thus write

$$E(K) = \mathbb{Z} \cdot P_1 \oplus \mathbb{Z} \cdot P_2 \oplus \cdots \oplus \mathbb{Z} \cdot P_r \oplus E(K)_{\text{tors}},$$

where the $P_i \in E(K)$ are non-torsion points and the torsion subgroup $E(K)_{\text{tors}}$ is finite. The integer r is called the *Mordell-Weil rank* of E/K (or simply the *rank*). The Mordell-Weil theorem is a qualitative one: it asserts the finiteness of r and $\#E(K)_{\text{tors}}$. But the main drawback of its proof is that it is, by nature, ineffective: it gives no recipe to compute r, the generators P_i or a set of generators for the torsion subgroup $E(K)_{\text{tors}}$; nor does it give bounds on their size (in terms of $H(E/K)$ for example). Nonetheless, finding quantitative versions of the Mordell-Weil theorem is of major diophantine interest: in order to "solve" the equation (1) with unknowns $x, y \in K$, one needs to compute the structure of $E(K)_{\text{tors}}$, the rank r and to find a basis $\{P_1, \ldots, P_r\}$ of the free part of $E(K)$.

The order of the torsion subgroup $E(K)_{\text{tors}}$ is the easiest to estimate. Indeed, there is a variety of methods to do so: reduction modulo a place of K, a suitable adaptation of the Lutz-Nagell theorem, modular methods, etc. In any case, we have good bounds on $\#E(K)_{\text{tors}}$ at our disposal. More precisely, Poonen showed the existence of a constant $b_K > 0$ (depending actually only on the genus of K) such that

$$\#E(K)_{\text{tors}} \leqslant b_K.$$

That is to say, when K is fixed, the torsion subgroups of elliptic curves over K are taken from a finite list, which is effectively computable (see [Poo07]; the analogous fact for elliptic curves over number fields is also known by theorems of Mazur, Momose and Merel). That being said, the rank r and the size of the non-torsion points P_i remain much more mysterious quantities.

We now specify what we mean by "the size of a point on E": recall that $E(K)$ is equipped with a non-degenerate quadratic form : the canonical Néron-Tate height $\hat{h}_{NT} : E(K) \to \mathbb{R}$. In this context, $\hat{h}_{NT}(P)$ differs from $(\deg x_P)/2$ by a bounded amount, where x_P is the x-coordinate of $P \in E(K)$ seen as a rational map $x_P : C \to \mathbb{P}^1$. We choose to normalize $\hat{h}_{NT} : E(K) \to \mathbb{R}$ in such a way that its values lie in $\mathbb{Q}$. From $\hat{h}_{NT}$, one deduces a non-degenerate $\mathbb{Z}$-bilinear pairing $\langle \cdot, \cdot \rangle_{NT} : E(K) \times E(K) \to \mathbb{R}$. This construction enables us to measure the "size" of non-torsion points: the bigger its height, the more complicated the point. As a measure of the "complexity" of computing $E(K)$, we can define the *Néron-Tate regulator of* E/K to be the covolume of the lattice $E(K)/E(K)_{\text{tors}}$ inside $E(K) \otimes \mathbb{R}$, with respect to the Euclidean structure induced by $\langle \cdot, \cdot \rangle_{NT}$:

$$\text{Reg}(E/K) := \left| \det \left[\langle P_i, P_j \rangle_{NT} \right]_{1 \leqslant i,j \leqslant r} \right|,$$

where, as above, $(P_1, \dots, P_r)$ denotes a $\mathbb{Z}$-basis of the free part of $E(K)$. A classical argument of geometry of numbers (namely, Hermite's theorem, see [Lan83a, Theorem 4.1]) implies that, to get upper bounds on $\hat{h}(P_i)$, it is sufficient to have an upper bound on $\text{Reg}(E/K)$ as well as a lower bound on the smallest height of a non-torsion point:

$$\Lambda_{E/K} = \min \left\{ \hat{h}(P), \ P \in E(K) \smallsetminus E(K)_{\text{tors}} \right\}.$$

About the latter, Lang conjectured in [Lan83a, Conjecture 2] that there should exist a constant $c_K > 0$ (depending only on K) such that

$$\hat{h}(P) \geqslant c_K \log H(E/K) \tag{2}$$

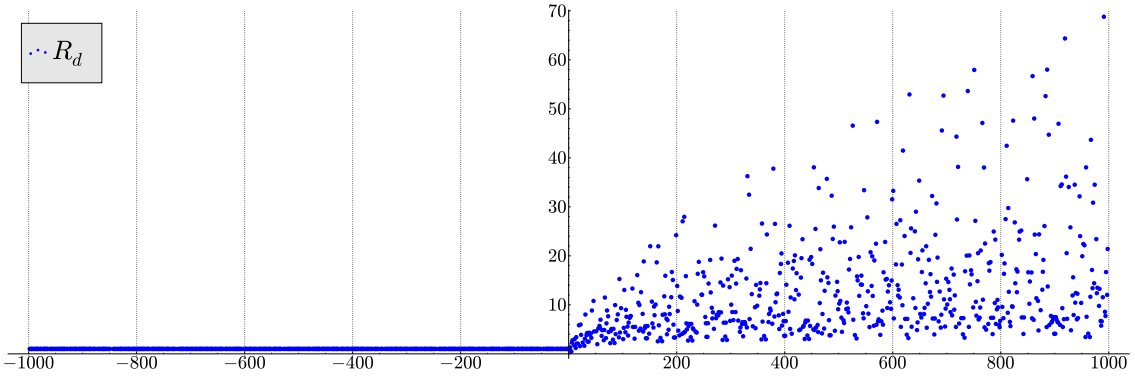
for all non-torsion $P \in E(K)$. So we turn to bounding the regulator $\text{Reg}(E/K)$ from above. In other words, we want to understand how complicated (in terms of $H(E/K)$) it is to compute generators for the Mordell-Weil group of E/K. We would also like to know how optimal the upper bound is, *i.e.* to compare it to a *lower* bound on $\text{Reg}(E/K)$.

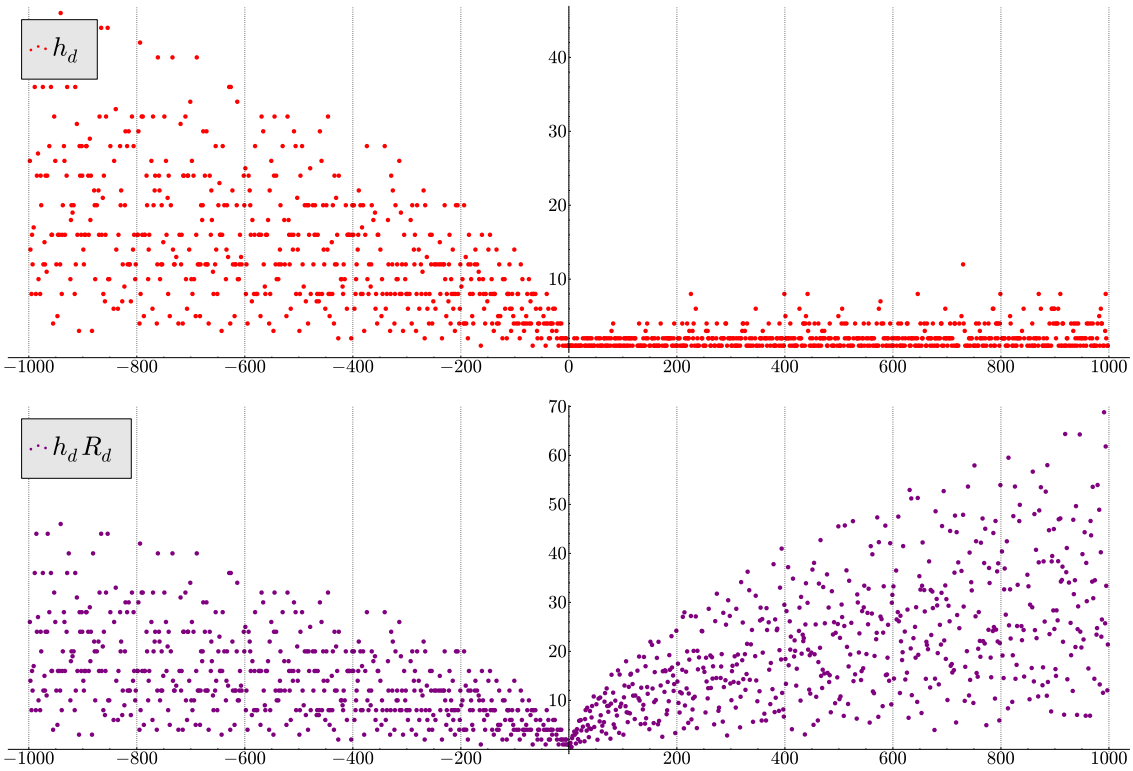
The situation at hand is reminiscent of the classical problem of giving upper bounds on the regulator of units $R_k = \text{Reg}(\mathcal{O}_k^\times)$ of a number field $k/\mathbb{Q}$ in terms of the absolute value Δ_k of its discriminant. In algorithmic terms, given a number field k, how difficult is it to find generators for its unit group $\mathcal{O}_k^\times$? Here, we are asking for bounds on the Weil height of generators of the free part of $\mathcal{O}_k^\times$, in terms of the discriminant Δ_k.

It turns out that computing a "basis" of the free part of the unit group $\mathcal{O}_k^\times$ alone is not much easier than computing both a basis for $\mathcal{O}_k^\times$ and a set of generators of the class-group $\mathcal{C}\ell(\mathcal{O}_k)$ (see [Len92, §5]). We denote by $h_k = \#\mathcal{C}\ell(\mathcal{O}_k)$ the class-number of k. In a vague way, this suggests that the quantity $h_k \cdot R_k$ has a smoother behaviour (with respect to Δ_k) than R_k alone. In any case, one has $h_k \geqslant 1$ so any upper bound on $h_k \cdot R_k$ can be easily translated into an upper bound on R_k. Better, if one knows *a priori* that the class-group is "big", an upper bound on $h_k \cdot R_k$ gives a sharper control on the regulator R_k! We will say more about these bounds later on.

We think the pictures below are illuminating: we restrict ourselves to quadratic number fields $k = \mathbb{Q}(\sqrt{d})$, ordered by their fundamental discriminant $d \in \mathbb{Z}$. For $|d| \leqslant 1000$, we plotted below:

(1) the regulator of units R_d of $\mathbb{Q}(\sqrt{d})$ (in blue),
(2) the class-number h_d of $\mathbb{Q}(\sqrt{d})$ (in red),
(3) and the product $h_d \cdot R_d$ (in purple).





As one clearly sees, the behaviour of $h_d \cdot R_d$ is more "regular" in terms of $|d|$ than each term taken separately. For example, when $d < 0$ the regulator $R_d = 1$ because the only units in $\mathbb{Q}(\sqrt{d})$ are roots of unity; but h_d looks like a growing function of $|d|$. On the contrary, when $d > 0$, the regulator seems to grow faster with d whereas the class number h_d grows very slowly, if at all (it is conjectured that infinitely many real quadratic number fields have class-number one). In both cases though, the product $h_d \cdot R_d$ seems to grow, albeit slowly, with $|d|$.

Remember that the class-group $\mathcal{C}\ell(\mathcal{O}_k)$ has an interpretation as a "local-to-global obstruction". Indeed, the class-group measures the defect of unique factorisation in the (global) ring of integers $\mathcal{O}_k$ of k; but all local rings $\mathcal{O}_v$ of k at its finite places are unique factorisation domains (since they are discrete valuation rings). In that sense, $\mathcal{C}\ell(\mathcal{O}_k)$ classifies equivalence classes of ideals that are everywhere locally principal, but not globally.

We now come back to the problem of bounding the Néron-Tate regulator $\mathrm{Reg}(E/K)$ of an elliptic curve E defined over a function field K. Inspired by the situation described in the last paragraph, we see that it might be easier to find bounds on $\mathrm{Reg}(E/K)$ if we coupled it with some measure of "local-to-global obstruction" on E. We recall that the *Tate-Shafarevich group of* E/K is defined in terms of Galois cohomology by

$$Ш(E/K) = \ker\left(\mathrm{H}^1(G_K, E(K^{\mathrm{sep}})) \to \prod_v \mathrm{H}^1(G_v, E(K_v^{\mathrm{sep}}))\right).$$

For our present purpose, it is enough to know that $Ш(E/K)$ classifies curves C/K with an action of E which become isomorphic to E over K^{sep} but are not isomorphic to E over K. In fancier terminology, $Ш(E/K)$ classifies principal homogeneous spaces over E that are everywhere locally trivial but not globally trivial (so $Ш(E/K)$ measures, in a certain sense, the failure of the "local-global principle"). It is conjectured that $Ш(E/K)$ is a finite group, but this has only been proved for a limited number of elliptic curves. In the context of elliptic curves over function fields, the finiteness of $Ш(E/K)$ is equivalent to the Birch and Swinnerton-Dyer conjecture (we will explain this further down).

We now have all the necessary ingredients to state a conjecture of Lang [Lan83a, Conjecture 1] to the effect that there should be an upper bound on $\#Ш(E/K) \cdot \mathrm{Reg}(E/K)$ in terms of the height $H(E/K)$. In analogy with the situation for number fields, Lang proposed:

Conjecture 1 (Lang)**.** *If E is an elliptic curve over a function field K, then (conditional to $Ш(E/K)$ being finite) one has*

$$\forall \varepsilon > 0, \exists c_\varepsilon > 0 \ \textit{s.t.} \quad \#Ш(E/K) \cdot \mathrm{Reg}(E/K) \leqslant c_\varepsilon \cdot H(E/K)^{1+\varepsilon}.$$

Note that the original conjecture deals with elliptic curves over $\mathbb{Q}$, but the translation to our context is straightforward. From this conjecture and the trivial lower bound $\#Ш(E/K) \geqslant 1$, one would deduce that

$$\mathrm{Reg}(E/K) \leqslant c_\varepsilon \cdot H(E/K)^{1+\varepsilon}. \tag{3}$$

This upper bound is not totally satisfactory: it gives an exponential bound on $\mathrm{Reg}(E/K)$ and hence on the Néron-Tate height of generators of the free part of $E(K)$, in terms of the data (the coefficients of a Weierstrass model of E, say). In vague terms, this upper bound means that computing the Mordell-Weil group of a given elliptic curve E/K is at most exponentially difficult in the data (granting Lang's conjecture and that the Tate-Shafarevich group is finite).

When the rank of $E(K)$ is positive, the upper bound (3) is in stark contrast to Lang's (conjectural) lower bound on the height (2), which would give

$$\log H(E/K) \ll \mathrm{Reg}(E/K) \leqslant \#Ш(E/K) \cdot \mathrm{Reg}(E/K) \tag{4}$$

if the rank is not too big. This leads us to wonder how optimal the upper bound of Lang's Conjecture 1 really is. In other words, is the computation of $E(K)$ really of exponential difficulty in the coefficients of E? Could one find a sharper upper bound on $\mathrm{Reg}(E/K)$?

The Brauer-Siegel ratio

Thus, we now investigate the optimality of the upper bound in Lang's Conjecture 1:

$$\#Ш(E/K) \cdot \mathrm{Reg}(E/K) \ll_\varepsilon H(E/K)^{1+\varepsilon}. \tag{5}$$

We would like to know what power $\alpha \in [0, 1+\varepsilon]$ of the height $H(E/K)$ appears (or should appear) in a corresponding lower bound of the form:

$$H(E/K)^\alpha \ll \#Ш(E/K) \cdot \mathrm{Reg}(E/K).$$

This led Hindry and Pacheco [HP16] to introduce the *Brauer-Siegel ratio*: for an elliptic curve E/K whose Tate-Shafarevich group is finite, set

$$\mathfrak{Bs}(E/K) := \frac{\log\big(\#Ш(E/K) \cdot \mathrm{Reg}(E/K)\big)}{\log H(E/K)}.$$

We note that this definition makes sense, more generally, for an abelian variety of arbitrary dimension over a function field (see [HP16, §1]) and even for an abelian variety over a number field (see [Hin07]). With this new invariant, Lang's Conjecture 1 can be rephrased as follows:

Conjecture 2 (Hindry)**.** *Let K be a function field. When E runs through the family of all elliptic curves over K, ordered by height, one has*

$$\mathfrak{Bs}(E/K) \leqslant 1 + o(1),$$

when $H(E/K) \to \infty$.

We turn to the problem of finding adequate lower bounds for the Brauer-Siegel ratio $\mathfrak{Bs}(E/K)$, *i.e.* of quantifying the optimality of the upper bound (5). A "trivial" lower bound shows the existence of a small constant $\gamma_K \geqslant 0$ (depending only on K) such that

$$-\gamma_K + o(1) \leqslant \mathfrak{Bs}(E/K) \qquad (\text{as } H(E/K) \to \infty)$$

for all elliptic curves E over K. A finer argument even yields $\gamma_K = 0$ (*cf.* [HP16, Proposition 7.6]).

Now, if indeed Mordell-Weil groups of elliptic curves are "exponentially hard to compute", there should exist an $\alpha_K > 0$ such that

$$0 < \alpha_K + o(1) \leqslant \mathfrak{Bs}(E/K) \qquad (\text{as } H(E/K) \to \infty)$$

for all elliptic curves (with finite $Ш(E/K)$) over a fixed function field K. Several heuristics, to which we come back later on, suggest otherwise that no such positive α_K can exist:

Conjecture 3 (Hindry)**.** *Let K be a function field. When E runs through the family of all elliptic curves over K, ordered by height, one has*

$$0 = \liminf \mathfrak{Bs}(E/K).$$

To this day, there are only 6 families of elliptic curves over $\mathbb{F}_q(t)$ for which one knows (unconditionally) that the Brauer-Siegel ratio has a limit when $H(E/K) \to \infty$: in all six cases, one has

$$\lim_{\substack{E\in\mathscr{E}\\ H(E/K)\to\infty}} \mathfrak{Bs}(E/K) = 1.$$

See [HP16, Theorem 7.12] and our Théorèmes 4.4.1, 5.4.1, 6.4.1, 7.4.4 et 8.4.2.

In order to give an idea of how the Brauer-Siegel ratio of elliptic curves can be bounded from above and/or from below, we turn back to the case of number fields. Indeed, the intuition behind Lang's Conjecture 1 is that $\#Ш(E/K)\cdot\mathrm{Reg}(E/K)$ for elliptic curves (ordered by height) should behave "like" $\#\mathcal{C}\ell(\mathcal{O}_k)\cdot\mathrm{Reg}(\mathcal{O}_k^\times)$ for number fields (ordered by discriminant). So it is natural to expect that one could prove bounds on $\#Ш(E/K)\cdot\mathrm{Reg}(E/K)$ "like" one would prove bounds on $\#\mathcal{C}\ell(\mathcal{O}_k)\cdot\mathrm{Reg}(\mathcal{O}_k^\times)$.

Let $k/\mathbb{Q}$ be a number field of degree $n = [k:\mathbb{Q}]$. Again, we denote by Δ_k the absolute value of its discriminant (over $\mathbb{Q}$). Let h_k be the class-number of k and R_k be the regulator of units in k. Here, we are looking for bounds on $h_k\cdot R_k$ in terms of Δ_k. For such a number field k, we define its *Brauer-Siegel ratio* to be

$$\mathfrak{Bs}(k/\mathbb{Q}) := \frac{\log\left(h_k\cdot R_k\right)}{\log\sqrt{\Delta_k}}.$$

With this notation set up, we quote the "classical" Brauer-Siegel theorem:

Theorem 4 (Brauer-Siegel)**.** *Let k run through an infinite family $\mathscr{K}$ of number fields with fixed degree n and growing discriminant. Then, as $\Delta_k\to\infty$,*

$$\lim_{\substack{k\in\mathscr{K}\\ \Delta_k\to+\infty}} \mathfrak{Bs}(k/\mathbb{Q}) = 1.$$

Usually, the conclusion of this theorem is written, with no reference to $\mathfrak{Bs}(k/\mathbb{Q})$, in the compact following form:

$$\log(h_k\cdot R_k)\sim\log\sqrt{\Delta_k}\qquad([k:\mathbb{Q}]\text{ fixed},\ \Delta_k\to+\infty).$$

Additionally, one can rephrase Theorem 4 as the combination of two bounds on $h_k\cdot R_k$ in terms of Δ_k:

$$\forall\varepsilon>0,\qquad \Delta_k^{1/2-\varepsilon}\ll_\varepsilon h_k\cdot R_k\ll_\varepsilon\Delta_k^{1/2+\varepsilon}.$$

The Brauer-Siegel theorem was first proven by Siegel for quadratic number fields (in [Sie35]) and by Brauer in the general case (in [Bra47]). Without going into too much detail, we recall how the proof of Theorem 4 works. It is of analytic nature and can be separated in three steps (in increasing order of difficulty):

Step 1. Classically, one attaches to k its Dedekind zeta function $\zeta_k(s)$: it is defined as a Dirichlet series, converging *a priori* on the half-plane $\mathrm{Re}(s)>1$, but has a meromorphic continuation to the whole complex plane $\mathbb{C}$. It has a simple pole at $s=1$ and the residue of $\zeta_k(s)$ at this pole can be written in terms of arithmetic invariants of k. More precisely, one has the Dirichlet class-number formula:

$$\rho_k := \lim_{s\to1}(s-1)\zeta_k(s) = \frac{h_k\cdot R_k}{\#\mu_k}\cdot 2^{r_1}(2\pi)^{r_2}\cdot\frac{1}{\sqrt{\Delta_k}},\tag{6}$$

where $\#\mu_k$ denotes the number of roots of unity in k and r_1 (resp. r_2) is the number of real (resp. complex) embeddings of k. When the degree n of k is fixed, the term $\frac{2^{r_1}(2\pi)^{r_2}}{\#\mu_k}$ in this formula is readily bounded in terms of n only, it is then apparent that

$$\mathfrak{Bs}(k/\mathbb{Q}) = 1+\frac{\log\rho_k}{\log\sqrt{\Delta_k}}+o(1)\qquad(\text{as }\Delta_k\to\infty).$$

Now, to prove Theorem 4, one has to bound ρ_k from above and from below. Specifically, we need to show that

$$\forall\varepsilon>0,\qquad \Delta_k^{-\varepsilon}\ll_\varepsilon\rho_k\ll_\varepsilon\Delta_k^{\varepsilon}.\tag{7}$$

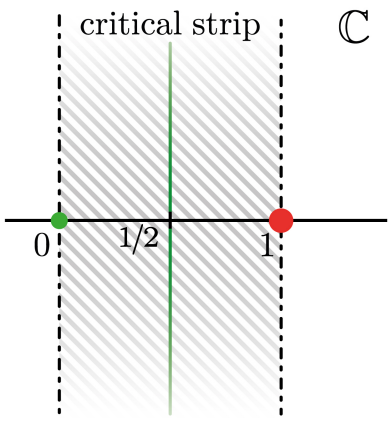
Step 2. Studying the size of ρ_k (in terms of Δ_k) is tantamount to studying the behaviour of $\zeta_k(s)$ in the neighborhood of its pole $s=1$ because

$$\zeta_k(s)\sim\frac{\rho_k}{s-1}\qquad(s\to1).$$

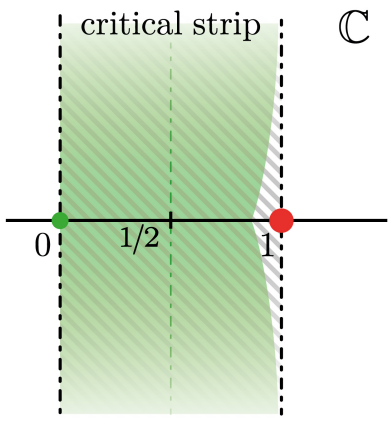
Actually, it suffices to study $x \mapsto \zeta_k(x)$ for real $x \neq 1$ near 1. The presence (or absence) of zeroes of $\zeta_k(x)$ close to $x = 1$ tends to influence the size of ρ_k. Since $\zeta_k(x)$ doesn't vanish on $]1, +\infty[$, the upper bound on ρ_k in (7) is easy to get. One can even prove an explicit and effective upper bound (see [Sie69]):

$$\rho_k \leqslant 4\left(\tfrac{e}{n-1}\right)^{n-1} \cdot (\log \Delta_k)^{n-1} \ll_{n,\varepsilon} \Delta_k^{\varepsilon}.$$

Step 3. The last step is the most difficult: in order to prove the lower bound in (7), we have to study the behaviour of $\zeta_k(x)$ when $x < 1$ (that is, when x is in the critical strip for ζ_k). As we mentioned, if $\zeta_k(s)$ has a zero close to 1, the residue is smaller. If one assumes the Generalized Riemann Hypothesis (GRH) for $\zeta_k(s)$, then $\zeta_k(s)$ has no zero in the interval $]1/2, 1[$ and we obtain a good lower bound on ρ_k. The following schematic pictures of the situation can be of some help to understand why this is so: let us first represent the critical strip for $\zeta_k(s)$ in the complex plane, together with the zone where the zeroes of $\zeta_k(s)$ can lie (in green). The red dot at $s = 1$ symbolizes the pole of $\zeta_k(s)$.

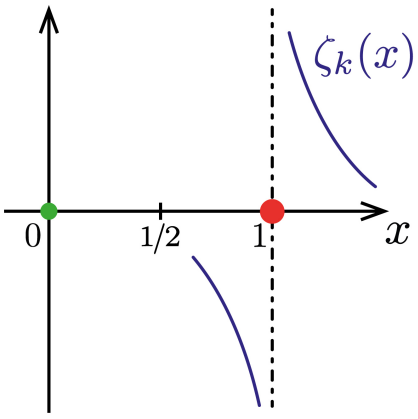


Zeroes of $\zeta_k(x)$ under GRH.

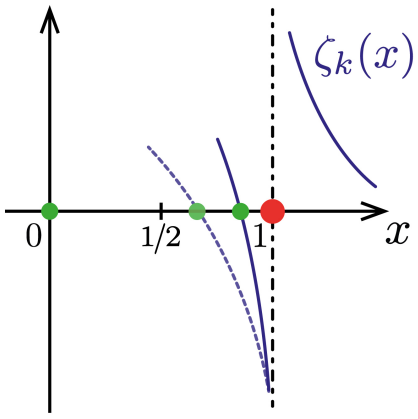


Zeroes of $\zeta_k(x)$ without GRH.

Next, we draw part of what the graph of $x \mapsto \zeta_k(x)$ looks like for a real x around $x = 1$.



Behaviour of $\zeta_k(x)$ under GRH.



Behaviour of $\zeta_k(x)$ without GRH.

- On the left figure, we assume GRH: all zeroes of ζ_k are on the critical line $\mathrm{Re}(s) = 1/2$ (the green line in the critical strip). As x grows to 1^-, $\zeta_k(x)$ tends gently to $-\infty$ so that its residue ρ_k can not be "too small".
- On the right picture now, we do not assume GRH. The green zone in the critical strip is where the potential zeroes of ζ_k can be (the complement of the green zone in the critical strip is a "zero-free region"). As one sees, if ζ_k does have a zero close to 1 (the green dots), the "slope" of the graph of ζ_k in $]1/2, 1[$ is much steeper (and the closer the zero to 1, the steeper the slope). This can be interpreted as ζ_k having a "small" residue.

The key part of the proof of Theorem 4 is then to bypass the assumption of GRH, by allowing *one* number field k in the family $\mathscr{K}$ to have a "small" residue ρ_k and checking that all others $k' \in \mathscr{K}$ have a big enough $\rho_{k'}$, *viz.* $\rho_{k'} \gg_{\varepsilon} \Delta_{k'}^{-\varepsilon}$. The main issue is that one has no control

on the alleged counterexample k: the lower bound on $\rho_{k'}$ is thus *ineffective*. Nevertheless, we point out that Stark analyzed cases where this bound can be made effective (see [Sta74]).

This is a very vague sketch of the proof: we refer the reader to [Lan94, Chapter XVI] and [Hin10, Lecture 5] for a more detailed argument. In relation with what follows, we want to make the following remark: by the functional equation for $\zeta_k(s)$, one sees that $\zeta_k(s)$ has a zero at $s = 0$ of multiplicity $r = r_1 + r_2 - 1 = \mathrm{rank}(\mathcal{O}_k^\times)$ and that the first non-zero coefficient of the Taylor expansion of $\zeta_k(s)$ around $s = 0$ is given by

$$\zeta^*(0) := \lim_{s\to 0} s^{-r} \cdot \zeta_k(s) = -\frac{h_k \cdot R_k}{\#\mu_k}.$$

Trying to bound $|\zeta^*(0)|$ in terms of Δ_k could thus be of interest to the study of $\mathfrak{Bs}(k/\mathbb{Q})$, but we know no proof of Theorem 4 using this fact (though the proof of the *upper* bound in that theorem is certainly feasible).

We mention that Theorem 4 has been generalized in various directions. Notably, Tsfasman and Vlăduţ [TV02] investigated in detail what happens when one lifts (or weakens) the condition that the degree is fixed. Under various sets of hypotheses on a family $\mathscr{K}$ of number fields k, they show that the limit

$$\lim_{\substack{k\in\mathscr{K}\\ \Delta_k\to\infty}} \mathfrak{Bs}(k/\mathbb{Q})$$

still exists, but can be different from 1! What's more, they give an expression of this limit in terms of arithmetic invariants of the family $\mathscr{K}$. Their article presents a thorough investigation of these questions (see also [Zyk05]). We also point out that one can prove analogues of the Brauer-Siegel theorem for families of function fields K over $\mathbb{F}_q$ (a fixed finite field), under various sets of hypotheses (see in particular [GL78], [War12] and [Zyk15]).

To close that paragraph, we note that Tsimerman proved an analogue of the Brauer-Siegel theorem for algebraic tori defined over $\mathbb{Q}$ of fixed dimension and growing "conductor" (see [Tsi12, Theorem 1.3]). The corresponding "class-number formula" was worked out earlier by Shyr [Shy77] and the analytic part of the proof is very similar to that of the classical case (see [Tsi12, Lemma 4.1]). This theorem is of importance in the study of special points on Shimura varieties, where it is used to obtain lower bounds for Galois orbits. See [UY15] for more details. Let us only retain that *some* algebraic groups of positive fixed dimension satisfy an analogue of the Brauer-Siegel theorem.

Having explained how the study of the Brauer-Siegel ratio of *number fields* goes, we turn back to the situation of elliptic curves over function fields. A natural starting point to find bounds on $\mathfrak{Bs}(E/K)$ is to try to mimic the proof of the Brauer-Siegel theorem in this setting. But before we do so, we need to introduce the analytic tool we use, namely the L-function. Let E be an elliptic curve over K. For each place v of K (of degree d_v, say), one can reduce an equation for E "modulo v": we obtain a cubic plane curve $\overline{E}_v$, defined over the residue field $\mathbb{F}_v$ of K at v (a finite extension of $\mathbb{F}_q$). Since $\mathbb{F}_v$ is finite, one can count the number of $\mathbb{F}_v$-rational points on it: we write

$$\#\overline{E}_v(\mathbb{F}_v) = \#\mathbb{F}_v + 1 - a_v(E) = q^{d_v} + 1 - a_v(E),$$

where $a_v(E)$ is an integer. If the curve $\overline{E}_v$ is non singular, then $|a_v(E)| \leqslant 2q^{d_v/2}$ by Hasse's theorem; if $\overline{E}_v$ is singular, then $a_v(E) \in \{0, -1, 1\}$. We combine those "local point counts" (for varying v) into a generating series defined by an Euler product: let

$$L(E/K, T) := \prod_{v\notin\mathcal{B}} \left(1 - a_v(E)\cdot T^{d_v} + q^{d_v}T^{2d_v}\right)^{-1} \cdot \prod_{v\in\mathcal{B}} \left(1 - a_v(E)\cdot T^{d_v}\right)^{-1}, \tag{8}$$

where $\mathcal{B}$ denotes the set of places where E has bad reduction (*i.e.* the places v for which the curve $\overline{E}_v$ is singular). From its definition, one sees that $L(E/K, T) \in \mathbb{Z}[[T]]$ is a formal power series with integer coefficients: it is called the *L-function of E/K*. It follows from difficult theorems of Grothendieck and Deligne that $L(E/K, T)$ is actually a rational function of T (and even a polynomial in T if E/K is not constant), whose degree is explicitly given in terms of the conductor of E, and which satisfies a functional equation with respect to $T \mapsto (q^2T)^{-1}$.

The function $s \mapsto \mathcal{L}(E/K, s)$ given by $\mathcal{L}(E/K, s) = L(E/K, q^{-s})$ is sometimes also called "the L-function of E/K". In terms of $\mathcal{L}(E/K, s)$, the facts just quoted mean that the Dirichlet series obtained by replacing T by q^{-s} in (8), *a priori* convergent on the half-plane $\mathrm{Re}(s) > 3/2$, can be meromorphically continued to the whole complex plane (and even holomorphically if E/K is not constant) and satisfies a functional equation with respect to $s \mapsto 2 - s$.

Another fact of major significance is that the analogue of the Riemann Hypothesis holds: it is a theorem of Deligne that the zeroes (in $\mathbb{C}$) of $s \mapsto L(E/K, q^{-s})$ have real part $\mathrm{Re}(s) = 1$. Coming back to the $T \mapsto L(E/K, T)$ version, it means that the inverse zeroes of $L(E/K, T)$ are algebraic integers of absolute value q (in any complex embedding). One advantage of working with elliptic curves over function fields is that those facts (analytic continuation, functional equation and Riemann hypothesis) are mostly conjectural for elliptic curves over number fields.

The first step in the proof of the classical Brauer-Siegel theorem is to link $\mathfrak{Bs}(k/\mathbb{Q})$ with the residue of $\zeta_k(s)$ at $s = 1$ *via* the class-number formula. In the context of elliptic curves over function fields, the link between $\mathfrak{Bs}(E/K)$ and the L-function is given by the Birch and Swinnerton-Dyer conjectures (henceforth abbreviated as BSD), which we now proceed to state. As we said, the L-function $\mathcal{L}(E/K, s)$ admits a meromorphic continuation to $\mathbb{C}$: we can thus study its behaviour around $s = 1$ (which is the center of symmetry of the functional equation) and define two more quantities. First, the *analytic rank* of E/K, denoted by $r_{an}(E/K)$, is the order of vanishing of $\mathcal{L}(E/K, s)$ at $s = 1$ or, correspondingly, the multiplicity of $T = q^{-1}$ as a root of the rational function $L(E/K, T)$, *i.e.*

$$r_{an}(E/K) := \mathrm{ord}_{s=1}\, \mathcal{L}(E/K, s) = \mathrm{ord}_{T=q^{-1}}\, L(E/K, T).$$

Secondly, one introduces the special value of the L-function at $s = 1$; it is usually defined as the first non-zero coefficient in the Taylor series of $\mathcal{L}(E/K, s)$ around $s = 1$:

$$\mathcal{L}(E/K, s) = \big(\text{special value}\big) \cdot (s-1)^{r_{an}(E/K)} + o\big((s-1)^{r_{an}(E/K)}\big) \qquad (\text{when } s \to 1).$$

But we actually prefer to work with a slightly different version of the special value: the rational function $L(E/K, T)$ has integer coefficients and has a zero of multiplicity $r_{an}(E/K)$ at $T = q^{-1}$, we put $L^*(E/K, T) = L(E/K, T)/(1 - qT)^{r_{an}(E/K)}$ and define the *special value* of $L(E/K, T)$ to be:

$$L^*(E/K, 1) := L^*(E/K, q^{-1}) = \left.\frac{L(E/K, T)}{(1-qT)^{r_{an}(E/K)}}\right|_{T=q^{-1}}.$$

Since $(1 - q^{1-s}) \sim \log q \cdot (s - 1)$ as $s \to 1$, it is readily seen that $L^*(E/K, 1)$ differs from the "usual" special value by a factor $(\log q)^{r_{an}(E/K)}$. The advantage of our normalization is that $L^*(E/K, 1)$ is a non-zero rational number.

Birch and Swinnerton-Dyer (and Tate, in this setting) conjectured that $r_{an}(E/K)$ and $L^*(E/K, 1)$ have the following arithmetic interpretation:

Conjecture 5 (Birch - Swinnerton-Dyer)**.** *Let E be an elliptic curve over a function field $K = \mathbb{F}_q(C)$, we denote by g_C the genus of C. Then the analytic rank $r_{an}(E/K)$ and the rank of the Mordell-Weil group $E(K)$ coincide:*

$$r_{an}(E/K) = \mathrm{ord}_{T=q^{-1}}\, L(E/K, T) = \mathrm{rank}\ E(K),$$

and the special value $L^*(E/K, 1)$ is given by

$$L^*(E/K, 1) = \frac{\#Ш(E/K) \cdot \mathrm{Reg}(E/K)}{\big(\#E(K)_{\mathrm{tors}}\big)^2} \cdot \mathcal{T}am(E/K) \cdot \frac{q^{1-g_C}}{H(E/K)}, \tag{9}$$

where $\mathcal{T}am(E/K)$ is the Tamagawa number of E/K.

The first part of the conjecture is sometimes called the "weak BSD conjecture" and the latter the "refined BSD conjecture". We note that finiteness of the Tate-Shafarevich is implicitly assumed in (9). Note also that the analytic continuation of the L-function is known here: for elliptic curves over number fields, this is still conjectural (except over $\mathbb{Q}$ where it follows from Wiles' modularity theorem). For elliptic curves over function fields (as opposed to elliptic curves over number fields), this conjecture is "almost a theorem". First of all, the work of Kato and Trihan [KT03] (building on previous work of Tate [Tat66], Milne [Mil75] and others) shows that the "full" Birch and Swinnerton-Dyer conjecture for E/K is equivalent to the "weak" conjecture, itself equivalent to the finiteness of the Tate-Shafarevich group $Ш(E/K)$ (or even of one its ℓ-primary parts $Ш(E/K)[\ell^\infty]$). Secondly, Conjecture 5 is completely proved in many cases. For example, Milne [Mil68] showed that isotrivial elliptic curves satisfy Conjecture 5. We note that the BSD conjecture in this context has a "geometric" counterpart: for an elliptic curve E over a function $K = \mathbb{F}_q(C)$, denote by $\pi : \mathcal{E} \to C$ the minimal regular model of E; the BSD conjecture for E is equivalent to the Tate conjecture [Tat94] for the surface $\mathcal{E}/\mathbb{F}_q$. This latter conjecture is known to hold for many surfaces (see [Gor79], [Mil75], [Shi86],

[SK79], ...) and can be used to produce many elliptic curves satisfying the BSD conjecture, including some non isotrivial ones.

The reader may now compare the class-number formula (6) for number fields and the conjectural BSD formula (9) for elliptic curves: they are both obtained as Taylor coefficients of a Dirichlet series at $s = 1$ and are, at least in their formal structure, very similar. One might set up the following "dictionary" to help with the translation between the two settings:

Number fields $k/\mathbb{Q}$		Elliptic curves E/K	
degree	$[k : \mathbb{Q}]$	$d = 1$	dimension
discriminant	Δ_k	$H(E/K)$	height
zeta function	$\zeta_k(s)$	$\mathcal{L}(E/K, s)$	L-function
class-number	$h_k = \#\mathcal{C}\ell(\mathcal{O}_k)$	$Ш(E/K)$	order of Tate-Shafarevich group
regulator of units	$R_k = \mathrm{Reg}(\mathcal{O}_k^\times)$	$\mathrm{Reg}(E/K)$	Néron-Tate regulator
# of roots of unity	$\#\mu_k = \#(\mathcal{O}_k^\times)_{\mathrm{tors}}$	$\#E(K)_{\mathrm{tors}}$	# of torsion points
"period"	$2^{r_1}(2\pi)^{r_2}$	$\mathcal{T}am(E/K)$	Tamagawa number.

We can now return to our idea of mimicking the proof in three steps of the classical Brauer-Siegel theorem (Theorem 4) to deduce information about the Brauer-Siegel ratio of elliptic curves. Let E be an elliptic curve over a function field K and suppose that E satisfies the BSD Conjecture (as we said above, assuming BSD is equivalent to assuming finiteness of $Ш(E/K)$). We will use the BSD formula (9) for the special value $L^*(E/K, 1)$ of its L-function to complete "**Step 1.**" of our program (see our sketch of the proof of Theorem 4): we link the size of $\mathfrak{Bs}(E/K)$ to that of $L^*(E/K, 1)$.

To do so, we need to ensure that the two "extra" terms $\#E(K)_{\mathrm{tors}}$ and $\mathcal{T}am(E/K)$ in (9) are not asymptotically significant and thus may be safely ignored; in the same way as one checks that $\#\mu_k$ and $2^{r_1}(2\pi)^{r_2}$ are negligible compared to Δ_k for a number field k. At the very beginning of this introduction, we have already pointed out that $\#E(K)_{\mathrm{tors}}$ is uniformly bounded once K is fixed:

$$1 \leqslant \#E(K)_{\mathrm{tors}} \leqslant b_K.$$

We note that a weaker upper bound of the form $\#E(K)_{\mathrm{tors}} \ll_\varepsilon H(E/K)^\varepsilon$ (for all $\varepsilon > 0$) would be sufficient for our purpose (and is easier to prove). The Tamagawa number term can also be bounded in terms of the height. More precisely, one can show that

$$\forall\, \varepsilon > 0, \qquad 1 \leqslant \mathcal{T}am(E/K) \ll_\varepsilon H(E/K)^\varepsilon,$$

where the implicit constant is effective. For elliptic curves over function fields, the proof is not so difficult (see our Théorème 1.5.4) but extending this bound to higher-dimensional abelian varieties is much more subtle (see [HP16, Theorem 6.5]). Once these two terms are discarded, we are left with the following inequality, valid for all elliptic curves E (over a fixed function field K) satisfying the BSD conjecture:

$$\mathfrak{Bs}(E/K) = 1 + \frac{\log|L^*(E/K, 1)|}{\log H(E/K)} + o(1) \qquad (H(E/K) \to \infty).$$

Thus, to study the size of $\mathfrak{Bs}(E/K)$, it remains to understand the size of the special value $L^*(E/K, 1)$ in terms of the height. Keeping the analogy with number fields in mind, we set out to investigate the behaviour of the L-function of E/K around $s = 1$: this would constitute the analogues of "**Step 2.**" and "**Step 3.**" of the proof of the classical Brauer-Siegel theorem.

First, we explain how to obtain upper bounds on the special value $L^*(E/K, 1)$ in terms of the height (thus completing "**Step 2.**"). Let E be an elliptic curve over a function field K, we assume for simplicity that E is not constant. Remember that its L-function $L(E/K, T)$ is a polynomial in T whose degree $\mathfrak{b}_{E/K}$ is bounded by $c_K \cdot \log H(E/K)$ (where c_K is a small explicit constant) and whose inverse zeroes have absolute value q. From this observation, one readily gets a "trivial" upper bound on the special value $L^*(E/K, 1)$:

$$\log|L^*(E/K, 1)| \ll \mathfrak{b}_{E/K} \leqslant c_K \cdot \log H(E/K), \tag{10}$$

where the implicit constants are effective and depend only on K. A more refined estimation, using complex analysis techniques on $\mathcal{L}(E/K, s)$ (see [HP16, Theorem 7.5]), actually leads to

$$\log|L^*(E/K, 1)| \ll \mathfrak{b}_{E/K} \cdot \frac{\log\log \mathfrak{b}_{E/K}}{\log \mathfrak{b}_{E/K}} = o\big(\mathfrak{b}_{E/K}\big) = o\big(\log H(E/K)\big). \tag{11}$$

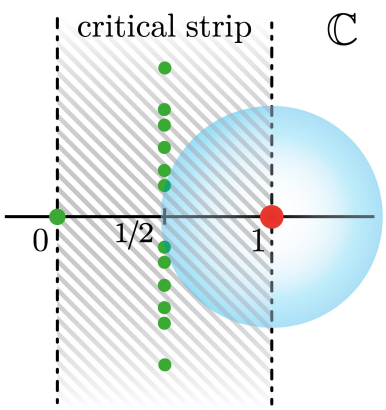
If our elliptic curve E/K satisfies the BSD conjecture, this improved upper bound on $L^*(E/K,1)$ immediately leads to

$$\mathfrak{Bs}(E/K) \leqslant 1 + o(1) \qquad (H(E/K) \to \infty).$$

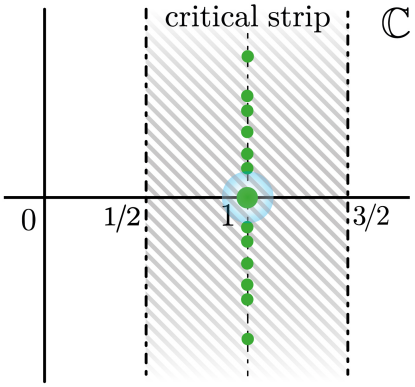
We now have completed "**Step 2.**" of the proof of an analogue of the Brauer-Siegel theorem.

There remains to find a lower bound on the special value $L^*(E/K,1)$. This problem is *significantly harder* and essentially still open in the general case. There are several reasons why adapting "**Step 3.**" for number fields to the situation at hand doesn't work quite as well as planned. One of these is the difference, from an analytic point of view, between the L-function $\mathcal{L}(E/K,s)$ and the zeta-function $\zeta_k(s)$ of a number field k. We study them both in the neighborhood of $s=1$, but:

- First, $\zeta_k(s)$ has a simple pole at $s=1$ whereas $\mathcal{L}(E/K,s)$ is expected to have a zero of high order at $s=1$. We mention that there are examples of elliptic curves over $\mathbb{F}_q(t)$ of arbitrarily large rank and which satisfy the Birch and Swinnerton-Dyer conjecture, see [TŠ67] and [Ulm02]. Now, it is classical that the behaviour of a meromorphic function around one of its poles gives strong information about the size of its residue there. But the behaviour of a meromorphic function around one of its zeroes, especially if it has high multiplicity, gives almost no lower bound on its Taylor coefficients.
- Then, in the number field case, we saw that assuming GRH for $\zeta_k(s)$ pushes the zeroes of $\zeta_k(s)$ "far" away from $s=1$ where its pole is so that we had a very good lower bound on the residue at $s=1$ (under GRH). When we turn to L-functions of elliptic curves over K, the critical strip is shifted to $1/2 < \mathrm{Re}(s) < 3/2$ and, as we said, the corresponding Riemann Hypothesis has been proved by Deligne: all the zeroes of $\mathcal{L}(E/K,s)$ have real part $\mathrm{Re}(s)=1$ (and they are symmetrically distributed with respect to the real axis). But we are studying $\mathcal{L}(E/K,s)$ around $s=1$, right in the middle of the critical strip! So there *are* zeroes of $\mathcal{L}(E/K,s)$ close to 1! The reader may compare the two pictures below: again, green dots symbolize hypothetical zeroes of $\zeta_k(s)$ or $\mathcal{L}(E/K,s)$ and the blue bubble around $s=1$ represents a "zero-free region".



Zeroes of $\zeta_k(s)$ (under GRH).



Zeroes of $\mathcal{L}(E/K,s)$ (under GRH).

The blue bubble for $\zeta_k(s)$ is almost independent of k, but when the height of E/K goes to infinity, the bubble for $\mathcal{L}(E/K,s)$ gets smaller and smaller. Not to mention the possibility that a "clump" of zeroes accumulates near the boundary of the blue bubble. This phenomenon is the major hindrance in finding non trivial lower bounds on $L^*(E/K,1)$.
The potential presence of "small zeroes" may be seen as a first vague evidence that the Brauer-Siegel ratio of elliptic curves can not always be "big" (*i.e.* it can be much smaller than 1).

Before passing to a review of known results concerning the Brauer-Siegel ratio, we allude to a closely related situation (some would say the "vertical case"). Namely, we fix an elliptic curve E over a function field K_0 and consider a tower of function fields $K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_i \subset \ldots$ (corresponding to a sequence of coverings of curves $C_0 \leftarrow C_1 \leftarrow C_2 \leftarrow \cdots \leftarrow C_i \leftarrow \ldots$). One might be interested in understanding the "growth" of the successive Mordell-Weil groups

$$E(K_0) \subset E(K_1) \subset E(K_2) \subset \cdots \subset E(K_i) \subset \ldots \qquad (i \to \infty).$$

When E is a constant elliptic curve over K_0, the BSD conjecture for E_i/K_i is a theorem of Milne [Mil68, Theorem 3] and Kunyavskiĭ and Tsfasman proved the following (see [KT08, Theorem 2.1]):

Theorem 6 (Kunyavskiĭ - Tsfasman)**.** *Let $\{K_i\}_{i\in\mathbb{N}}$ be a tower of function fields: $K_i = \mathbb{F}_p(C_i)$ is the function field of a curve C_i and the genus $g(C_i)$ tends to $+\infty$ (when $i \to \infty$). If E_0 is a constant*

elliptic curve $K_0 = \mathbb{F}_p(C_0)$, for all $i \in \mathbb{N}$, we denote by $E_i = E_0 \times_{K_0} K_i$ the base-change of E_0 to K_i. Then,

$$\lim_{i\to\infty} \frac{\log\left(\#Ш(E_i/K_i)\cdot \mathrm{Reg}(E_i/K_i)\right)}{\log p \cdot g(C_i)} = 1 - \sum_{m=1}^{\infty} \beta_m \cdot \log_p\left(\frac{\#E_0(\mathbb{F}_{p^m})}{p^m}\right),$$

where $\beta_m = \lim_{i\to\infty} \#C_i(\mathbb{F}_{p^m})/g(C_i)$ (up to extracting a sub-tower of $\{K_i\}_{i\in\mathbb{N}}$, one can assume that these limits do exist).

Unfortunately, the reader should be warned that there is a gap in their proof (see [KT10]). We note that the quantity $\log\left(\#Ш(E_i/K_i)\cdot \mathrm{Reg}(E_i/K_i)\right)/(\log p \cdot g(C_i))$ is closely related to $\mathfrak{Bs}(E_i/K_i)$: in the case where K_i has genus $g(C_i) \to \infty$, the main contribution to $\log H(E_i/K_i)$ is $\log p \cdot g(C_i)$. We won't say more about this setting except that the behaviour of $\mathfrak{Bs}(E_i/K_i)$ is expected to be radically different than in the previous situation (where K was fixed and E varied). We refer the reader to [Zyk15] for a presentation of a unified framework that could be used to treat the "horizontal" and the "vertical" conjectures on the same footing.

Previous results (and questions)

The introduction of the Brauer-Siegel ratio of elliptic curves over function fields is rather recent (see [HP16]), but there are already a few results about $\mathfrak{Bs}(E/K)$ which we now review. Note that the results of [HP16] hold, in greater generality, for abelian varieties of any dimension: we only state them for elliptic curves. Let $K = \mathbb{F}_q(C)$ be a function field over a finite field $\mathbb{F}_q$. We denote by $\mathscr{E}\ell\ell_{/K}$ the family of all elliptic curves over K (ordered by height). As was already pointed out, Hindry conjectured that

$$0 + o(1) \leqslant \mathfrak{Bs}(E/K) \leqslant 1 + o(1) \qquad (E \in \mathscr{E}\ell\ell_{/K},\ H(E/K) \to \infty)$$

for all elliptic curves whose Tate-Shafarevich group is finite (Conjecture 2). This conjecture is now proven (as a special case of [HP16, Corollary 1.13]):

Theorem 7 (Hindry-Pacheco)**.** *For a fixed function field $K = \mathbb{F}_q(C)$, let $\mathscr{E}\ell\ell_{/K}$ be the family of all elliptic curves over K. We assume that $Ш(E/K)$ is finite for all $E \in \mathscr{E}\ell\ell_{/K}$. Then*

$$0 \leqslant \liminf_{E\in\mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) \leqslant \limsup_{E\in\mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) \leqslant 1. \tag{12}$$

We note that the assumption of finiteness of $Ш(E/K)$ is equivalent to the assumption that E/K satisfies the Birch and Swinnerton-Dyer conjecture (see [KT03]). The upper bound in (12) is proven by analytic methods along the lines we sketched in the previous section : it follows from an upper bound on the special value $L^*(E/K, 1)$ of the L-function of E/K at $s = 1$ (see [HP16, Theorem 7.5]). The proof of the lower bound in (12) is more delicate:

- With analytic methods, one can prove a "weak" lower bound (thus completing a weak version of "**Step 3.**"). In the case of elliptic curves, Hindry and Pacheco obtain ([HP16, Lemma 7.1]) that
$$-5 \leqslant \liminf_{E\in\mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K),$$
again, under the assumption that the Tate-Shafarevich group is finite.
- But a subtle diophantine lower bound on the regulator $\mathrm{Reg}(E/K)$ (see [HP16, Proposition 7.6]) gives the desired
$$0 \leqslant \liminf_{E\in\mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K).$$
Written under this form, it is conditional to $Ш(E/K)$ being finite because the definition of $\mathfrak{Bs}(E/K)$ is. But it is actually an unconditional lower bound on $\mathrm{Reg}(E/K)$ in terms of the height $H(E/K)$.

In other words, Conjecture 2 above is true (conditional to the finiteness of Tate-Shafarevich groups). Furthermore, Hindry and Pacheco give an unconditional example where the upper bound in (12) is attained (see [HP16, Theorem 7.12]).

Theorem 8 (Hindry-Pacheco)**.** *Let $\mathbb{F}_q$ be a finite field of characteristic $p \geqslant 5$ and $K = \mathbb{F}_q(t)$. For any integer $d \geqslant 2$ prime to p, let E_d be the elliptic curve over K given in affine coordinates by*

$$E_d : \qquad Y^2 + XY = X^3 - t^d.$$

The Tate-Shafarevich group $Ш(E_d/K)$ *is finite (and thus,* E_d/K *satisfies the Birch and Swinnerton-Dyer conjecture). Moreover, as* $d \to \infty$*, the Brauer-Siegel ratio* $\mathfrak{Bs}(E_d/K)$ *has a limit and this limit is* 1*. That is to say,*

$$\log\big(\#Ш(E/K)\cdot \mathrm{Reg}(E_d/K)\big) \sim \log H(E_d/K) \sim \log q \cdot \frac{d}{6} \quad (d\to\infty).$$

The curves E_d/K had been previously considered by Ulmer (in [Ulm02]) who showed that they satisfy the Birch and Swinnerton-Dyer conjecture (see [Ulm02, Proposition 6.4]) and that the rank of $E_d(K)$ can be arbitrarily large when $d \to \infty$ ([Ulm02, Theorem 1.5]). With this example, one can rephrase Theorem 7 when $K = \mathbb{F}_q(t)$:

$$0 \leqslant \liminf_{E\in\mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) \leqslant \limsup_{E\in\mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) = 1,$$

where $\mathscr{E}\ell\ell_{/K}$ still denotes the family of all elliptic curves over K.

Note that Theorem 7 does not give a definitive answer to the question of knowing how small the Brauer-Siegel ratio can actually be (Conjecture 3). One could first be tempted to predict that a complete analogue of the classical Brauer-Siegel theorem (Theorem 4) holds for elliptic curves over function fields:

$$\lim_{\substack{E\in\mathscr{E}\ell\ell_{/K}\\ H(E/K)\to\infty}} \mathfrak{Bs}(E/K) = 1, \tag{?}$$

i.e. that the "lim inf" and "lim sup" in (12) coincide. At present, it is not clear if one should expect this to be true in general or, on the contrary, if Conjecture 3 holds.

Some strong heuristics recently came to light that suggest Conjecture 3 is closer to the truth (compare [Hin07, Conjecture 5.5] and [HP16, §7.5, §7.6]). In particular, Hindry and Pacheco predict that the behaviour of the Brauer-Siegel ratio in families of quadratic twists of a given elliptic curve is different from the "generic" one. We now sum these up in the case when $K = \mathbb{F}_q(t)$ is the rational function field. Let E/K be an elliptic curve.

1. As was mentioned earlier and as is discussed in detail in [HP16, §7.3], the presence of zeroes of the L-function $\mathcal{L}(E/K,s)$ of E near $s=1$ has an influence on the size of the special value $L^*(E/K,1)$ and thus on the size of $\mathfrak{Bs}(E/K)$. In vague terms, if $\mathcal{L}(E/K,s)$ has a zero very close to 1 (or if $\mathcal{L}(E/K,s)$ has a clump of zeroes close to 1) then $L^*(E/K,1)$ is expected to be very small. On the contrary, if the zeroes of $\mathcal{L}(E/K,s)$ are "well-spaced", one could reasonably expect that $L^*(E/K,1)$ is not too small.
   These expectations are made precise in [HP16, Lemma 7.7]: the authors isolate the contribution of "small zeroes" to the size of $L^*(E/K,1)$. One is thus led to study the distribution of the zeroes of $\mathcal{L}(E/K,s)$ on the line $\mathrm{Re}(s)=1$ on which they lie. This was carried out by Michel in [Mic99] who showed that for "most" elliptic curves E/K, the zeroes of $\mathcal{L}(E/K,s)$ are "well-distributed". So, for "most" elliptic curves, the Brauer-Siegel ratio should be bounded away from 0. Nonetheless, this does not remove the possibility that an infinite family of elliptic curves over K could have L-functions with "badly-distributed" zeroes and thus a smaller Brauer-Siegel ratio.
2. If E is non-constant, for any square-free $D \in \mathbb{F}_q[t]$, one can consider the quadratic twist $E^{(D)}/K$ of E by D. Assuming the Birch and Swinnerton-Dyer conjecture for $E^{(D)}$, an analogue of a theorem of Waldspurger links the value $\mathcal{L}(E/K,1)$ of $\mathcal{L}(E/K,s)$ at $s=1$ with the D-th Fourier coefficient $c_E(D)$ of a certain 3/2-weight modular form g_E.
   When $E^{(D)}$ has rank 0, one has $\mathcal{L}(E/K,1) = L^*(E/K,1)$ and the upper bound on $\mathfrak{Bs}(E^{(D)}/K)$ then follows from the (proven) Ramanujan conjecture for the Fourier coefficients of g_E: namely, $|c_E(D)| \ll_\varepsilon (q^{\deg D})^{1/4+\varepsilon}$. Now, a positive lower bound on $\mathfrak{Bs}(E^{(D)}/K)$ would mean that the non-zero coefficients $c_E(D)$ are *bounded away* from 0. This seems unlikely because it would mean that the Fourier coefficients of some 3/2-weight modular forms do not satisfy a "Sato-Tate distribution", *i.e.* they would be not equidistributed in the interval in which they lie.
3. If instead E/K is constant, there exists an elliptic curve E_0 over $\mathbb{F}_q$ such that $E = E_0 \times_{\mathbb{F}_q} K$. In this case, the BSD conjecture has been proved by Milne (see [Mil68, Theorem 3]) both for E and its quadratic twists $E^{(D)}$ by square-free polynomials $D \in \mathbb{F}_q[t]$. Let $a_E := q+1-\#E_0(\mathbb{F}_q)$, we denote by $F_D(T)$ the numerator of the zeta function of the hyperelliptic curve $C_D : y^2 = D(x)$ and by $g_D := g(C_D) = \lfloor (\deg D - 1)/2 \rfloor$ the genus of C_D. The special value $L^*(E^{(D)}/K,1)$ has been computed by Milne in terms of $F_D(T)$ and a_E. A little algebra yields the following expression for the Brauer-Siegel ratio $\mathfrak{Bs}(E^{(D)}/K)$ (see [HP16, Proposition 7.16]) :

$$\mathfrak{Bs}(E^{(D)}/K) = \frac{2\log|G_D^*(a_E)|}{g_D\cdot\log q} + o(1) \qquad (\deg D\to\infty),$$

where $G_D^*(T) \in \mathbb{Z}[T]$ can be explicitely computed from $F_D(T)$. Moreover, one has $G_D^*(a_E) \neq 0$, $\deg G_D^* = g_D - o\big(g_D\big)$; and all roots of $G_D^*(T)$ are real and lie in $[-2\sqrt{q}, 2\sqrt{q}]$. Now, when E_0 runs through all possible elliptic curves over $\mathbb{F}_q$, the integer a_E takes almost all integral values between $-2\sqrt{q}$ and $2\sqrt{q}$ (see [WM71]). As $\deg D$ gets bigger, $G_D^*(T)$ has more and more roots in the interval $[-2\sqrt{q}, 2\sqrt{q}]$ where a_E lies : it sounds plausible that $|G_D^*(a_E)| \in \mathbb{N}^*$ can indeed be "very small" compared to g_D.

Note the "reverse" construction : given an integer $a \in [-2\sqrt{q}, 2\sqrt{q}]$, it is easy to construct a sequence of polynomials $H_n(T) \in \mathbb{Z}[T]$ ($n \in \mathbb{N}^*$) of growing degree with the properties that the roots of $H_n(T)$ are all real and lie in the interval $[-2\sqrt{q}, 2\sqrt{q}]$, $H_n(T)$ does not vanish at a and $\log|H_n(a)|/\deg H_n$ is arbitrarily small. However, we do not know how to check that $H_n(T)$ actually corresponds to a "$G_D^*(T)$ polynomial" associated, as above, to the numerator of the zeta function of an hyperelliptic curve C_D.

Needless to say, exhibiting an explicit family of elliptic curves $E/\mathbb{F}_q(t)$ whose Brauer-Siegel ratio has a limit $\alpha < 1$, even conditional to the Birch and Swinnerton-Dyer, would be a breakthrough. As would a proof that the Brauer-Siegel ratio, on the contrary, always has limit 1 (thus disproving Conjecture 3). Maybe a study of the Brauer-Siegel ratio "on average" could give a hint as to which behaviour is typical; unless there are so few elliptic curves with small Brauer-Siegel ratio that their presence can not be detected by a too rough average upper bound.

As one sees, this question and its variants are far from settled and we intend to investigate further this circle of problems.

New results

We now present our contribution to the study of the Brauer-Siegel ratio. We break up this section in three parts. The first one states our main theorem, directly related to the Brauer-Siegel ratio. The second contains some results used in the proof of the main theorem but which might be of independent interest. In the last part, we mention two other results, which we didn't incorporate in this manuscript.

Main theorem

Let $\mathbb{F}_q$ be a finite field of characteristic $p \geqslant 5$. We denote by K the rational function field $K = \mathbb{F}_q(t)$ over $\mathbb{F}_q$. Consider one of the following families $\mathscr{E}_i$ of elliptic curves over K:

($\mathscr{E}_1$) for any integer $d \in \mathbb{N}^*$ prime to q, let E_d/K be given by the affine equation

$$E_d : \quad Y^2 = X(X+1)(X+t^d). \tag{13}$$

We call E_d a "Legendre elliptic curve" because its 2-torsion points are K-rational. It has been extensively studied by Ulmer, Conceição and Hall (see [Ulm14a], [CHU14] and [Ulm14b]).

($\mathscr{E}_2$) for any integer $d \in \mathbb{N}^*$ prime to q, let H_d/K be given by the affine equation

$$H_d : \quad Y^2 + 3t^d XY + Y = X^3. \tag{14}$$

H_d will be called a "Hessian elliptic curve" because it has a natural K-rational 3-torsion point.

($\mathscr{E}_3$) for any integer $d \in \mathbb{N}^*$ prime to q, let E_d/K be given by the affine equation

$$E_d : \quad Y^2 + XY + t^d Y = X^3 + t^d X^2. \tag{15}$$

The curve E_d has a natural K-rational 4-torsion point (and was studied by Ulmer in [Ulm13]).

($\mathscr{E}_4$) for any integer $d \in \mathbb{N}^*$ prime to q, let E_d/K be given by the affine equation

$$E_d : \quad Y^2 + XY - t^d Y = X^3. \tag{16}$$

These curves are studied by Davis and Occhipinti in [DO14], where the authors produce explicit rational points for certain values of d.

($\mathscr{E}_5$) for any *odd* integer $d \in \mathbb{N}^*$ prime to q, let $B_{1/2,d}/K$ be given in affine coordinates by

$$B_{1/2,d} : \quad Y^2 + 2t^d XY - 4t^{2d} Y = X^3 - 6t^d X^2 + 8t^{2d} X. \tag{17}$$

This elliptic curve is mentioned by Berger in [Ber08, §4.3, Example 6].

In this thesis, we show that the Brauer-Siegel ratio of elliptic curves E/K taken from one of the families above has a limit, and that the limit is actually 1. We record this in one theorem:

Theorem 9. *Let $\mathscr{E}_i$ (with $i \in \{1,2,3,4,5\}$) be one of the families above.*

- *For each elliptic curve $E \in \mathscr{E}_i$, the Birch and Swinnerton-Dyer conjecture is true for E/K. In particular, $Ш(E/K)$ is finite and $\mathfrak{Bs}(E/K)$ makes sense.*
- *When $H(E/K) \to +\infty$ with $E \in \mathscr{E}_i$, one has*

$$\mathfrak{Bs}(E/K) \xrightarrow[\substack{E\in\mathscr{E}_i \\ H(E/K)\to\infty}]{} 1.$$

In other words, for all $\varepsilon > 0$, there are constants such that

$$\forall E \in \mathscr{E}_i, \quad H(E/K)^{1-\varepsilon} \ll_\varepsilon \#Ш(E/K) \cdot \mathrm{Reg}(E/K) \ll_\varepsilon H(E/K)^{1+\varepsilon}.$$

To put it differently, when $E \in \mathscr{E}_i$,

$$\log\big(\#Ш(E/K) \cdot \mathrm{Reg}(E/K)\big) \sim \log H(E/K) \quad \text{as } H(E/K) \to \infty.$$

Actually, each family above is naturally indexed by integers $d \in \mathbb{N}^*$ (prime to p) and there exists a constant c_i (given below) such that for any curve E_d in the i-th family $\mathscr{E}_i$,

$$\log\big(\#Ш(E_d/K) \cdot \mathrm{Reg}(E_d/K)\big) \sim \log H(E_d/K) \sim \frac{\log q}{c_i} \cdot d \quad \text{as } d \to +\infty.$$

With

$$c_1 = 2, \quad c_2 = 1, \quad c_3 = 2, \quad c_4 = 3, \quad c_5 = 2.$$

This is an immediate consequence of Théorème 4.4.1, Théorème 5.4.1, Théorème 6.4.1, Théorème 7.4.4 and Théorème 8.4.2.

The 5 families of elliptic curves described above add to the example in [HP16, Theorem 7.12] to give a total of 6 families of elliptic curves (over $\mathbb{F}_q(t)$) for which one knows *unconditionally* that a complete analogue of the Brauer-Siegel theorem holds (that is, $\mathfrak{Bs}(E/K) \to 1$). We hope that, upon reading the proofs, the reader will be convinced that our method can be used to study the Brauer-Siegel ratio of other families.

This theorem could be seen as giving more evidence that, in Theorem 7, the "lim inf" and the "lim sup" are actually equal to 1. We prefer to think that the elliptic curves we study are part of the (conjectural) majority of those whose Brauer-Siegel ratio tends to 1. At least, this theorem tells us where *not to look* if one wants to find a family of elliptic curves with a smaller Brauer-Siegel ratio (conjecturally, a "thin" family among all elliptic curves).

As we explained above, for an elliptic curve E/K to have a "big" Brauer-Siegel ratio (that is to say, for $\mathfrak{Bs}(E/K)$ to be close to 1), it is necessary that the zeroes of the L-function $L(E/K,T)$ be sufficiently "well-behaved". In other words, the central part of the proof is to prove a *lower bound* on $\mathfrak{Bs}(E/K)$: to do so, we show that the special values $L^*(E/K,1)$ of the L-functions of elliptic curves $E \in \mathscr{E}_i$ never get too small. In general, the direct study of the distribution of the zeroes is delicate, so we took a "p-adic" approach, which we now roughly sketch. Suppose we have expressed the special value $L^*(E/K,1) = L_E^*$ of an elliptic curve E/K as a product

$$L_E^* = \prod_{m\in\mathcal{M}} \left(1 - \frac{\omega_m}{q^{u_m}}\right),$$

where ω_m are certain algebraic integers of absolute value q^{u_m}, $u_m \in \mathbb{N}^*$ and m runs through a set of indices $\mathcal{M}$ with $\#\mathcal{M} = o\big(\log H(E/K)\big)$. We give lower bounds for such products using the following idea. By construction, the product L_E^* is a non-zero element of $\mathbb{Z}[q^{-1}]$: as such, it can be written under the form

$$L_E^* = \frac{(\text{integer})}{q^{W_E}}, \tag{18}$$

for a certain exponent $W_E \in \mathbb{N}$. Hence, we can give a lower bound on $\log|L_E^*|$ (in terms of $H(E/K)$) by finding an upper bound on W_E in the denominator. Since the ω_m are an algebraic integers, multiplying the factor $(1 - \omega_m/q^{u_m})$ by q^{u_m} produces an algebraic integer whose norm is a rational integer. Hence, multiplying L_E^* by $q^{\sum u_m}$ leaves us with an integer and we see that $0 \leqslant W_E \leqslant \sum u_m$.

Now imagine that some of the ω_m are "very divisible" by q. Then there is no need to multiply the corresponding factors $(1-\omega_m/q^{u_m})$ by q^{u_m} to obtain an algebraic integer: a smaller power of q would do. So the exponent W_E in the denominator of L_E^* can be lowered. By keeping track of these "cancellations" in the factors of L_E^*, we manage to show that $W_E = o\big(\log H(E/K)\big)$ for the five families $\mathscr{E}_i$, which is enough to yield

$$\log|L_E^*| \geqslant -o\big(\log H(E/K)\big).$$

Auxiliary results

To prove Theorem 9 above, we require other results, whose interest surely lies beyond the only study of the Brauer-Siegel ratio. We sum up the most significant new theorems which are also proved in this thesis.

Let $\mathbb{F}_q$ be a finite field of odd characteristic. For any $b \in \mathbb{F}_q \smallsetminus \{1,-1\}$ and any non trivial character $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$, we define the associated *Legendre sum* by:

$$\boldsymbol{S}_q(\chi; b) := -\sum_{x\in\mathbb{F}_q} \chi(x)\cdot\mu\big(x^2+2b\cdot x+1\big),$$

where $\mu : \mathbb{F}_q^\times \to \{\pm 1\}$ is the unique non trivial character of order 2. These sums were defined by Evans in [Eva86] but there seems to be very few results about them in the literature. In order to compute some L-functions, we needed the Legendre sums to satisfy an analogue of the "Hasse-Davenport lifting relation for Gauss sums" and to satisfy a "Riemann hypothesis". To state our theorem, we recall the following construction: for any non trivial character $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ and any finite extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, define a character $\chi^{(n)}$ on $\mathbb{F}_{q^n}^\times$ by

$$\forall x \in \mathbb{F}_{q^n}^\times, \quad \chi^{(n)}(x) = \chi\circ\mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x),$$

where $\mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$ denotes the norm. We obtain:

Theorem 10. *Let $b \in \mathbb{F}_q \smallsetminus \{-1,1\}$ and $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ be a non trivial character. There exist two algebraic integers $\alpha_b(\chi)$ and $\beta_b(\chi)$ (depending only on b and χ) such that*

- *$\boldsymbol{S}_q(\chi, b) = \alpha_b(\chi) + \beta_b(\chi)$ and $\alpha_b(\chi)\cdot\beta_b(\chi) = q$,*
- *For any extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\boldsymbol{S}_{q^n}(\chi^{(n)}, b) = \alpha_b(\chi)^n + \beta_b(\chi)^n$ ("Hasse-Davenport relation"),*
- *In any complex embedding, $\alpha_b(\chi)$ and $\beta_b(\chi)$ have absolute value $\sqrt{q}$ ("Riemann hypothesis").*

See Théorème 2.2.21 and Corollaire 2.3.5. Note that, for a given $b \in \mathbb{F}_q \smallsetminus \{-1,1\}$, the Legendre sums naturally appear in the zeta function of the hyperelliptic curve D, defined over $\mathbb{F}_q$ by the affine equation:

$$D: \qquad y^2 = x^{2(q-1)} + 2b\cdot x^{q-1} + 1.$$

Indeed, the action of $(q-1)$-th roots of unity on D (given by $(x,y)\mapsto(\zeta\cdot x, y)$ for $\zeta \in \mu_{q-1}$) breaks up the cohomology of D into 2-dimensional subspaces on which the action of the Frobenius $x \mapsto x^q$ has trace $\boldsymbol{S}_q(\chi; b)$. More details can be found in Théorème 2.3.4.

As was mentioned before in this introduction, the Brauer-Siegel ratio is intimately linked with special values of L-functions. To say something about the limit of the Brauer-Siegel ratio of the families of Theorem 9, we had to compute explicitly the corresponding L-functions. Before giving the results of our computations, we set up some notations. Let $\mathbb{F}_q$ be a finite field of odd characteristic p and $d \geqslant 2$ an integer that is prime to q. There is a natural action of q on $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ by multiplication. Let $\mathcal{O}'_q(d) = (\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\})\big/\langle q \bmod d\rangle$ be the set of orbits.

Fix a prime ideal $\overline{\mathfrak{P}}$ of $\overline{\mathbb{Z}}$ above p: reduction modulo $\overline{\mathfrak{P}}$ induces an isomorphism between the group $\mu'_p \subset \overline{\mathbb{Q}}^\times$ of roots of unity whose orders are prime to p and the multiplicative group $\overline{\mathbb{F}_q}^\times$. Let $\mathbf{t} : \overline{\mathbb{F}_q}^\times \simeq (\overline{\mathbb{Z}}/\overline{\mathfrak{P}})^\times \to \mu'_p \subset \overline{\mathbb{Q}}^\times$ be the inverse of this isomorphism (we call $\mathbf{t}$ the Teichmüller character). We also denote by the same letter $\mathbf{t}$ the restriction of the Teichmüller character to any subfield of $\overline{\mathbb{F}_q}$. To any integer $d \geqslant 2$ prime to q, we attach a set (indexed by $a \in [\![1, d-1]\!]$ or $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$) of characters $\mathbf{t}_a : \mathbb{F}_{q^{u(a)}}^\times \to \overline{\mathbb{Q}}^\times$ defined over various extensions $\mathbb{F}_{q^{u(a)}}/\mathbb{F}_q$ and whose orders divide d. More precisely, for any $a \in [\![1, d-1]\!]$, let $u(a) = \min\big\{n\in\mathbb{N}^* \;\big|\; q^n a \equiv a \bmod d\big\} = \mathrm{ord}^\times\big(q \bmod (d/\gcd(d,a))\big)$ and

$$\mathbf{t}_a : x \in \mathbb{F}_{q^{u(a)}}^\times \mapsto \mathbf{t}(x)^{(q^{u(a)}-1)a/d} \in \overline{\mathbb{Q}}^\times.$$

In the results below, the reader interested in the case when $d \mid q-1$ can replace "$m \in \mathcal{O}'_q(d)$" by "$a = m \in [\![1, d-1]\!]$", $u(a)$ by 1 for all $a \in [\![1, d-1]\!]$ and $\mathbf{t}_a$ by the powers χ^a of a fixed character $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ of exact order d.

With these characters, we computed the L-functions of the elliptic curves in the families $\mathscr{E}_i$. For the next five theorems, we let $\mathbb{F}_q$ be a finite field of characteristic $p \geqslant 5$ and $K = \mathbb{F}_q(t)$.

First of all, we obtain the L-functions of the "Hessian curves" in family $\mathscr{E}_2$ (see Théorème 5.2.1).

Theorem 11. *For any integer $d \geqslant 2$ prime to q, let H_d be the "Hessian elliptic curve" over K, given by* (14)*. The L-function $L(H_d/K, T)$ of H_d can be written in the form:*

$$L\big(H_d/K, T\big) = \prod_{m \in \mathcal{O}_q^{(3)}(3d)} \Big(1 - \mathbf{J}_m \cdot T^{u(m)}\Big)$$

where $\mathcal{O}_q^{(3)}(3d)$ is the set of orbits of $\mathbb{Z}/3d\mathbb{Z} \smallsetminus \{0, d, 2d\}$ under the action of q by multiplication and, for any $m \in \mathcal{O}_q^{(3)}(3d)$, $\mathbf{J}_m$ denotes the following sum:

$$\mathbf{J}_m = \mathbf{t}_a(27) \cdot \mathbf{j}_{q^{u(a)}}(\mathbf{t}_a, \mathbf{t}_a, \mathbf{t}_a) = \mathbf{t}_a(27) \cdot \sum_{\substack{x,y,z \in \mathbb{F}_{q^{u(a)}} \\ x+y+z=1}} \mathbf{t}_a(x)\mathbf{t}_a(y)\mathbf{t}_a(z),$$

for any choice of representative $a \in \mathbb{Z}/d\mathbb{Z}$ of the orbit m (up to a root of unity, $\mathbf{J}_m$ is a Jacobi sum). Please note that the characters $\mathbf{t}_a$ here are those attached to $3d$, not to d.

With techniques very similar to [CHU14, §3], we compute the L-functions of elliptic curves in family $\mathscr{E}_3$, having a rational point of 4-torsion (see Théorème 6.2.1).

Theorem 12. *For any integer $d \geqslant 2$ prime to q, let E_d be the elliptic curve over K, given by* (15)*. The L-function $L(E_d/K, T)$ of E_d can be written in the form:*

$$L(E_d/K, T) = \prod_{m \in \mathcal{O}_q^{(2)}(d)} (1 - {\mathbf{J}'_m}^2 \cdot T^{u(m)})$$

where $\mathcal{O}_q^{(2)}(d)$ is the set of orbits of $\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, (d/2)\}$ under the action of q by multiplication (with the orbit $\{d/2\}$ removed if d is even) and, for any orbit $m \in \mathcal{O}_q^{(2)}(d)$, $\mathbf{J}'_m$ denotes the following Jacobi sum:

$$\mathbf{J}'_m = \mathbf{j}_{q^{u(a)}}(\mathbf{t}_a, \mathbf{t}_a) = -\sum_{\substack{x,y,z \in \mathbb{F}_{q^{u(a)}} \\ x+y=1}} \mathbf{t}_a(x)\mathbf{t}_a(y),$$

for any choice of representative $a \in \mathbb{Z}/d\mathbb{Z}$ of m.

Next, for the family $\mathscr{E}_4$ of elliptic curves studied in Chapter 7, we get the following result (see Théorème 7.2.1).

Theorem 13. *For any integer $d \geqslant 2$ prime to q, let E_d be the elliptic curve over K, given by* (16)*. The L-function $L(E_d/K, T)$ of E_d can be written in the form:*

$$L\big(E_d/K, T\big) = \prod_{m \in \mathcal{O}_q^{(3)}(d)} \Big(1 - \mathbf{J}_m \cdot T^{u(m)}\Big).$$

where $\mathcal{O}_q^{(3)}(d)$ is the set of orbits of $\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, (d/3, 2d/3)\}$ under multiplication by q (with orbits $\{d/3\}$ and $\{2d/3\}$ removed if $3 \mid d$) and for all $m \in \mathcal{O}_q^{(3)}(d)$, $\mathbf{J}_m$ is a "2-dimensional" Jacobi sum:

$$\mathbf{J}_m = \mathbf{j}_{q^{u(a)}}(\mathbf{t}_a, \mathbf{t}_a, \mathbf{t}_a) = \sum_{\substack{x,y,z \in \mathbb{F}_{q^{u(a)}} \\ x+y+z=1}} \mathbf{t}_a(x)\mathbf{t}_a(y)\mathbf{t}_a(z),$$

for any choice of representative $a \in \mathbb{Z}/d\mathbb{Z}$ of m.

Finally, for the family of elliptic curves $\mathscr{E}_5$ taken from [Ber08, §4.3, Example 6], we first obtain a general expression of the L-function (see Théorème 8.2.1):

Theorem 14. *Let $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ and $d \geqslant 2$ be an integer prime to q. We denote by $B_{a,d}$ the elliptic curve over $K = \mathbb{F}_q(t)$ defined in affine coordinates by*

$$B_{a,d}: \quad Y^2 + t^d XY - at^{2d}Y = X^3 - (a+1)t^d X^2 + at^{2d}X.$$

The L-function $L(B_{a,d}/K,T)$ of $B_{a,d}$ can be written in the form

$$L\big(B_{a,d}/K,T\big) = (1-qT)\cdot \prod_{m\in\mathcal{O}_q^{(2)}(d)} \Big(1 - \mathbf{J}'_m\cdot \boldsymbol{S}_m \cdot T^{u(m)} + {\mathbf{J}'_m}^2 \cdot q^{u(m)}\cdot T^{2u(m)}\Big),$$

where, as above, $\mathcal{O}_q^{(2)}(d)$ is the set of orbits of $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0,(d/2)\}$ under the action of q by multiplication (with the orbit $\{d/2\}$ removed in case d is even) and for any orbit $m \in \mathcal{O}_q^{(2)}(d)$ and any choice of a representative $i \in \mathbb{Z}/d\mathbb{Z}$ of m, $\mathbf{J}'_m$ is a Jacobi sum (up to a root of unity):

$$\mathbf{J}'_m = \mathbf{t}_i(-1)\cdot \mathbf{j}_{q^{u(i)}}(\mathbf{t}_i,\mathbf{t}_i) = -\mathbf{t}_i(-1)\cdot \sum_{\substack{x,y\in\mathbb{F}_{q^{u(i)}}\\ x+y=1}} \mathbf{t}_i(x)\mathbf{t}_i(y),$$

and $\boldsymbol{S}_m$ is a Legendre sum

$$\boldsymbol{S}_m := \boldsymbol{S}_{q^{u(i)}}(\mathbf{t}_i; 1-2a) = -\sum_{x\in\mathbb{F}_{q^{u(i)}}} \mathbf{t}_i(x)\cdot\mu\left(x^2+2(1-2a)\cdot x+1\right).$$

In the case where $a = 1/2 \in \mathbb{F}_q$ and d is odd, the expression of the L-function of $L(B_{1/2,d}/K,T)$ in the above theorem "simplifies" to give the following result about the L-functions of elliptic curves in family $\mathscr{E}_5$ (see Théorème 8.3.2).

Theorem 15. *Let $d \geqslant 2$ be an* odd *integer prime to q. Let $B_{1/2,d}$ be the elliptic curve over $K = \mathbb{F}_q(t)$ defined by* (17)*:*

$$B_{1/2,d}: \quad Y^2 + 2t^d XY - 4t^{2d}Y = X^3 - 6t^d X^2 + 8t^{2d}X.$$

Then the L-function $L(B_{1/2,d}/K,T)$ of $B_{1/2,d}$ can be written in the form

$$L\big(B_{1/2,d}/K,T\big) = (1-qT)\cdot \prod_{n\in\mathcal{O}_q^{(2)}(2d)} \Big(1 - \mathbf{J}'_n\cdot T^{u(n)}\Big),$$

where $\mathcal{O}_q^{(2)}(2d)$ is the set of orbits of $\mathbb{Z}/2d\mathbb{Z}\smallsetminus\{0,d\}$ under the action of q by multiplication and for any orbit $n \in \mathcal{O}_q^{(2)}(2d)$ and any choice of a representative $i \in \mathbb{Z}/2d\mathbb{Z}$ of n, $\mathbf{J}'_n$ is a "2-dimensional" Jacobi sum (up to a root of unity):

$$\mathbf{J}'_n := \mathbf{t}_i(-4)\cdot \mathbf{j}_{q^{u(i)}}(\mathbf{t}_i,\mathbf{t}_i,\mathbf{t}_i^2) = \mathbf{t}_i(-4)\cdot \sum_{\substack{x,y,z\in\mathbb{F}_{q^{u(i)}}\\ x+y+z=1}} \mathbf{t}_i(x)\mathbf{t}_i(y)\mathbf{t}_i(z)^2.$$

Please note that the characters $\mathbf{t}_i$ here ($i \in [\![1, 2d-1]\!]$) are those associated to $2d$ (and not to d).

We hope that these computations prove useful for some other purposes. That is why we tried to keep the hypotheses in the last five theorems very light: we only assume that d is prime to the characteristic of $\mathbb{F}_q(t)$. We also mention here that we prove a result of "unbounded rank in towers" for the $B_{a,d}$ curves (see Corollaire 8.3.13):

Theorem 16. *In the family of elliptic curves $B_{a,d}/K$ (with $d \geqslant 2$ ranging through all integers prime to q and $a \in \mathbb{F}_q \smallsetminus \{0,1\}$), the rank $r_{a,d} = \operatorname{rang} B_{a,d}(K)$ is not bounded:*

$$\limsup_{\substack{\gcd(d,q)=1\\ a\in\mathbb{F}_q\smallsetminus\{0,1\}}} \operatorname{rank}\, B_{a,d}(K) = \limsup_{\gcd(d,q)=1} \operatorname{rank}\, B_{1/2,d}(K) = +\infty.$$

As noted in [Ber08, §4.3, Example 6], the unboundedness of the rank for $B_{a,d}$ is not a consequence of the general theorem of Ulmer [Ulm07b, Theorem 4.7].

The central part of the proof of Theorem 4 and our main technical result is a lower bound for special values of L-functions satisfying certain hypotheses (see Théorème 3.2.2). We do not go into details here but we give a flavour of how that theorem works. Fix $\mathbb{F}_q$ a finite field of odd characteristic and $K = \mathbb{F}_q(t)$. Let $d \geqslant 2$ be an integer prime to q. Most of the L-functions displayed above are written under the schematic following form:

$$L_d(T) = \prod_{m \in \mathcal{O}'_q(d)} \left(1 - \omega_m \cdot T^{u(m)}\right) \in \mathbb{Z}[T],$$

where $\mathcal{O}'_q(d)$ denotes the set of orbits of $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ under the action of q by multiplication and the ω_m are certain algebraic integers. By definition, the special value consists of the value of $L_d(T)$ at $T = q^{-1}$ once we have removed all the factors $1 - \omega_m \cdot T^{u(m)}$ that vanish at $T = q^{-1}$ (up to a manageable integral term, whose logarithm is positive). The main term that needs to be bounded from below can be written under the form of a product

$$L_d^* := \prod_{m \in \mathcal{M}} \left(1 - \frac{\omega_m}{q^{u(m)}}\right),$$

where m runs through a certain set of orbits $\mathcal{M} \subset \mathcal{O}'_q(d)$. We now add the hypotheses that the ω_m lie in the cyclotomic field $\mathbb{Q}(\zeta_{d_m})$ (where $d_m := d/\gcd(d,m)$) and that the numbering of $\{\omega_m\}_m$ is "compatible" with the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \simeq (\mathbb{Z}/d\mathbb{Z})^\times$ (*i.e.* we assume that $\sigma_t(\omega_m) = \omega_{t\cdot m}$ if σ_t is the Galois automorphism corresponding to $t \in (\mathbb{Z}/d\mathbb{Z})^\times$). Note that both hypotheses are satisfied by the L-functions of elliptic curves in the five families $\mathscr{E}_i$. We fix, once and for all, a prime ideal $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$ above p and put $\mathfrak{p}_m = \mathbb{Q}(\zeta_{d_m}) \cap \overline{\mathfrak{P}}$ for all $m \in \mathcal{M}$.

Theorem 17. *Under these hypotheses, one has*

$$\log|L_d^*| \gg_q -\sum_{m \in \mathcal{M}} \max\left\{0, u(m) - \frac{\mathrm{ord}_{\mathfrak{p}_m}\omega_m}{[\mathbb{F}_q : \mathbb{F}_p]}\right\} := -W_d. \tag{19}$$

For a detailed account of our hypotheses and a precise statement, we refer the reader to Section 3.2. Note that Shioda proved a somewhat related result (see [Shi87, Proposition 2.1]) when ω_m is a Jacobi sum of "even dimension". We adapt his proof to work with more general ω_m.

The inequality (19) is true as soon as the L-function satisfies our hypotheses. What's more, one always has a "naïve" upper bound on the sum W_d on the right-hand side of (19), namely

$$W_d = \sum_{m \in \mathcal{M}} \max\left\{0, u(m) - \frac{\mathrm{ord}_{\mathfrak{p}_m}\omega_m}{[\mathbb{F}_q : \mathbb{F}_p]}\right\} \leqslant d.$$

The corresponding lower bound on $\log|L_d^*|$ gives nothing more than the "Liouville bound":

$$\log|L^*(E_d/K, 1)| \gg_q -\log H(E_d/K).$$

Now, to prove that the Brauer-Siegel ratio of the elliptic curves E_d in one of the families $\mathscr{E}_i$ has limit 1, we need to show a much stronger lower bound on $\log|L_d^*|$: we require that W_d be $o(d)$ when $d \to \infty$. Such an asymptotic relation would follow if "on average" the terms "$u(m) - \mathrm{ord}_{\mathfrak{p}_m}\omega_m/[\mathbb{F}_q : \mathbb{F}_p]$" in W_d were "not too big". For a general data $\{\omega_m\}$, there is no reason why this should hold.

However, in the case where the ω_m are Jacobi sums (or products of Jacobi sums), making use of a variant of Stickelberger's theorem (Théorème 3.3.9) allows to compute the terms $\mathrm{ord}_{\mathfrak{p}_m}\omega_m$. We then obtain a more or less explicit expression of W_d and there remains to prove that W_d is negligible when $d \to \infty$. To do so, we need a special case of the following equidistribution theorem. We denote the fractional part of a real number x by $\{x\} \in [0,1[$.

Theorem 18. *Let $I \subset [0,1]$ be an interval of length b and $\mathscr{D} \subset \mathbb{N}^*$ be an infinite set of integers. Suppose we are given, for any $d \in \mathscr{D}$, a subgroup H_d of $G_d = (\mathbb{Z}/d\mathbb{Z})^\times$ such that $\frac{\#H_d}{\log\log d} \xrightarrow[d\to\infty]{} +\infty$. Then, when $d \to \infty$ (and $d \in \mathscr{D}$), one has*

$$\frac{1}{\#G_d}\sum_{g \in G_d}\left| b - \frac{1}{\#H_d}\cdot\#\left\{t \in H_d \;\middle|\; \left\{\tfrac{gt}{d}\right\} \in I\right\}\right| \ll \left(\frac{\log\log d}{\#H_d}\right)^{1/6} = o(1).$$

For more details, we invite the reader to see Théorème 3.4.1 and its corollaries.

Other results

We also obtained two other results which are not included in this manuscript. First, we computed the L-function of another (infinite) family of elliptic curves over $\mathbb{F}_q(t)$. More precisely, fix a finite field $\mathbb{F}_q$ of characteristic $p \geqslant 5$ and a parameter $a \in \{0, 1, 1/2\}$, for all integers d prime to p, let $F_{a,d}$ be the elliptic curve over K given in affine coordinates by

$$F_{a,d}: \quad Y^2 + (1-t^d)XY + a^2(t^d - t^{2d})Y = X^3 + (a^2+2a)t^dX^2 + (2a^3+a^2)t^{2d}X + a^4t^{3d}.$$

The rank of this curve is studied in [Occ12]: Occhipinti computes "semi-explicitly" the L-function of $F_{a,d}/K$ when d divides $q-1 = \#\mathbb{F}_q^\times$. He also uses the theorem of [Ber08] to prove that $F_{a,d}$ satisfies the Birch and Swinnerton-Dyer conjecture. By a different method and weakening the hypothesis that d divides $q-1$, we were able to prove:

Theorem 19. *With notations as above, for any integer d prime to p, the L-function $L(F_{a,d}/K, T)$ is given by*

$$L(F_{a,d}/K,T) = (1-qT)\cdot \prod_{m\in\mathcal{O}'_q(d)} \left(1 - q^{u(m)}T^{u(m)}\right)\left(1 - (\boldsymbol{S}_m^2 - 2q^{u(m)})T^{u(m)} + q^{2u(m)}T^{2u(m)}\right), \quad (20)$$

where $\mathcal{O}'_q(d)$ denotes the set of orbits of $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ under the action of q by multiplication, $u(m)$ denotes the cardinality of m and, for any $m \in \mathcal{O}'_q(d)$ and any choice of representative $i \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ of m, $\boldsymbol{S}(m)$ denotes the Legendre sum

$$\boldsymbol{S}_m = -\boldsymbol{S}_{q^{u(i)}}(\mathbf{t}_i; 1-2a) = -\sum_{x\in\mathbb{F}_{q^{u(i)}}} \mathbf{t}_i(x)\cdot\mu\left(x^2 + 2(1-2a)x + 1\right).$$

The Hasse-Davenport relation and the Riemann hypothesis for Legendre sums ensure the existence of algebraic integers α_m and β_m ($m \in \mathcal{O}'_q(d)$) such that

$$\forall m \in \mathcal{O}'_q(d), \qquad \boldsymbol{S}_m = \alpha_m + \beta_m,\ \alpha_m\cdot\beta_m = q^{u(m)} \text{ and } |\alpha_m| = |\beta_m| = q^{u(m)/2}.$$

With this notation, one can rewrite the L-function in a factorized form:

$$L(F_{a,d}/K,T) = (1-qT)\cdot \prod_{m\in\mathcal{O}'_q(d)} \left(1 - q^{u(m)}\cdot T^{u(m)}\right)\left(1 - \alpha_m^2\cdot T^{u(m)}\right)\left(1 - \beta_m^2\cdot T^{u(m)}\right).$$

The proof uses computations of character sums and hinges on the fact that $F_{a,d}$ is birational to the curve $X_d \subset \mathbb{P}^1\times\mathbb{P}^1$ defined over K and given in affine coordinates by

$$X_{a,d}: \quad \frac{x(x-1)}{x-a} = t^d\cdot\frac{y(y-1)}{y-a}.$$

It is clear on the expression (20) that the L-function vanishes at order at least $d = 1 + \#\mathcal{O}'_q(d)$ at $T = q^{-1}$. Hence, since $F_{a,d}$ satisfies the Birch and Swinnerton-Dyer conjecture, $F_{a,d}(\mathbb{F}_q(t))$ has rank at least d. Unfortunately, we are currently unable to give bounds on the size of the special value of $L(F_{a,d}/K,T)$ at $T = q^{-1}$ other than the "trivial" ones:

$$-6 + o(1) \leqslant \frac{\log L^*(F_{a,d}/K, 1)}{\log H(F_{a,d}/K)} \leqslant 0 + o(1) \quad (d\to\infty).$$

Indeed, we have close to no information about how the numbers $\boldsymbol{S}_m/q^{u(m)/2}$ are distributed in the interval $[-2,2]$ in which they lie (equivalently, we don't know how the $\alpha_m/q^{u(m)/2}$ and $\beta_m/q^{u(m)/2}$ are distributed angularwise on the unit circle).

Following a suggestion of Hindry, we also started the study of the Brauer-Siegel ratio of a family of quadratic twists of a constant curve. The setting is as follows: let $\mathbb{F}_q$ be a finite field of characteristic $p \geqslant 5$ and let E_0 be an elliptic curve over $\mathbb{F}_q$ with affine equation $E_0: y^2 = x^3 + Ax + B$ ($A, B \in \mathbb{F}_q$). Then $E := E_0 \times_{\mathbb{F}_q} \mathbb{F}_q(t)$ is a constant elliptic curve over $K = \mathbb{F}_q(t)$. For any integer d prime to p, consider the quadratic twist $E^{(d)}$ of E by the polynomial $t^d + 1 \in \mathbb{F}_q[t] \subset K$, whose affine equation is

$$E^{(d)}: \quad (t^d+1)\cdot y^2 = x^3 + Ax + B.$$

Then $E^{(d)}/K$ satisfies the Birch and Swinnerton-Dyer conjecture (because it is isotrivial, see [Mil68, Theorem 3]). Thus, by [HP16, Corollary 1.13], when $d\to\infty$, one has

$$0 + o(1) \leqslant \text{Ш}(E^{(d)}/K) \leqslant 1 + o(1).$$

We proved a refined bound on $\text{Ш}(E^{(d)}/K)$ for special values of d:

Theorem 20. *Let $\mathscr{D}_{ss} \subset \mathbb{N}^*$ be the (infinite) set of integers $d \geqslant 2$ such that d divides q^n+1 (for some $n \in \mathbb{N}$). Such an integer $d \in \mathscr{D}_{ss}$ is often called* supersingular *for q (see [SK79]). Then, as $d \to \infty$,*

$$\lim_{\substack{d \in \mathscr{D}_{ss} \\ d \to \infty}} \mathfrak{BS}(E^{(d)}/K) = 1.$$

At the moment, we are unable to remove the condition that d be supersingular (nor are we sure that the conclusion still holds if one removes the assumption). The proof is essentially based on three ingredients. First, the L-function of $E^{(d)}/K$ is easily expressed in terms of the zeta function of the hyperelliptic curve $C_d : y^2 = x^d + 1$. A computation of Weil (see [Wei49]) asserts that the zeroes β_j of this zeta function are n-th roots of Jacobi sums. Under our hypothesis that $d \in \mathscr{D}_{ss}$, note that the Jacobi sums in question are real numbers. The conclusion follows by an application of the Baker-Wüstholz theorem (see [BW93]) to $\log|1 - \beta_j/q|$ in the spirit of [BK10, Theorem 4.1].

Detailed contents

To close this chapter, we review how this manuscript is organized.

The first chapter is a general introduction to selected topics in the arithmetic of elliptic curves over function fields, with an emphasis on their L-functions, the Birch and Swinnerton-Dyer conjecture and diophantine inequalities between their invariants. It contains almost no proofs but we give numerous references. In the last section of this chapter, we define the Brauer-Siegel ratio $\mathfrak{BS}(E/K)$ of an elliptic curve E/K and recall conjectures and known facts about it.

The next two chapters introduce the tools we use to carry out the analytic study of the families $\mathscr{E}_i$: the second chapter will enable us to compute the L-functions of elliptic curves $E \in \mathscr{E}_i$ and we will use the results of the third chapter to bound their special values.

More precisely, the second chapter centers around character sums. First, we recall classical facts about characters of finite fields, Gauss sums and Jacobi sums. Then, we explain in detail the construction of the characters "$\mathbf{t}_a$" which appear in the L-functions displayed above: these form a natural family of characters whose orders divide d. We use this framework to prove a "transformation formula" for generating series built-up from character sums: this result is of constant use in the following computations of L-functions. Furthermore, we introduce Legendre sums and prove analogues of the Hasse-Davenport lifting relation and of the Riemann hypothesis for those. The proof requires the computation of the zeta function of certain hyperelliptic curves.

In the third chapter, we take the computation of L-functions for granted and focus on bounding their special values. The first section quickly recounts how upper bounds on the rank and on special values are obtained. In the second section, we give a lower bound on products π^* of algebraic numbers which typically appear in the special values of the L-functions we study. Our hypotheses are gathered in Section 3.2.1. This lower bound, however, can only be used if one has a good knowledge of the "p-adic valuations" of the algebraic numbers in the product π^*. Thus, we recall how these "p-adic valuations" are computed in the case of Jacobi sums. Finally, we prove an equidistribution statement to the effect that "big" subgroups of $(\mathbb{Z}/d\mathbb{Z})^\times$ become equidistributed on average when $d \to \infty$.

In Chapters 4 to 8, we study individually the families of elliptic curves introduced earlier (the family $\mathscr{E}_i$ is studied in Chapter $i+3$). The structure of these chapters is very similar. We start by computing the basic invariants attached to the elliptic curves $E \in \mathcal{E}_i$. Secondly, we find an explicit expression for the L-functions of those: we use the tools set up in Chapter 2. We briefly recall why all elliptic curves in the five families satisfy the BSD conjecture. For some families, we are further able to find a quick proof that the rank is unbounded. In the last section of each chapter, we employ the bounds on special values obtained at Chapter 3 and we finish the proof of the analogue of the Brauer-Siegel theorem for the family $\mathscr{E}_i$.

Table summarizing the studied families

Let $\mathbb{F}_q$ be a finite field of characteristic $p \geqslant 5$ and $K := \mathbb{F}_q(t)$. In the table below, we record the families of elliptic curves that are studied in this thesis (as well as that of [HP16, Theorem 7.12]). The first column gives a Weierstrass equation of E/K and the parameter(s) on which it depends. We then give an expression for the j-invariant $j = j(E/K) \in \mathbb{F}_q(t)$ of E and for the differential (exponential) height $H = H(E/K)$ as functions of the parameter(s). The reader can thus convince himself that these curves are mutually non-isomorphic over $\mathbb{F}_q(t)$. The last column summarizes the result we obtain as regards the Brauer-Siegel ratio.

	Weierstrass model and parameter(s)	j-invariant	Height	Brauer-Siegel ratio
[HP16]	$E_d : y^2 + xy = x^3 - t^d$ $d \in \mathbb{N}^*$, $\gcd(d,p) = 1$	$j = \dfrac{1}{t^d(1 - 2^4 3^3 t^d)}$	$H = q^{\lfloor \frac{d+5}{6} \rfloor}$	$\lim\limits_{d\to\infty} \mathfrak{Bs}(E_d/K) = 1$
Chap. 4	$E_d : y^2 = x(x+1)(x+t^d)$ $d \in \mathbb{N}^*$, $\gcd(d,p) = 1$	$j = \dfrac{2^8(t^{2d} - t^d + 1)^3}{t^{2d}(t^d - 1)^2}$	$H = q^{\lfloor \frac{d-1}{2} \rfloor}$	$\lim\limits_{d\to\infty} \mathfrak{Bs}(E_d/K) = 1$
Chap. 5	$H_d : y^2 + 3t^d xy + y = x^3$ $d \in \mathbb{N}^*$, $\gcd(d,p) = 1$	$j = \dfrac{3^3 t^{3d}(9t^{3d} - 8)^3}{t^{3d} - 1}$	$H = q^d$	$\lim\limits_{d\to\infty} \mathfrak{Bs}(H_d/K) = 1$
Chap. 6	$E_d : y^2 + xy + t^d y = x^3 + t^d x^2$ $d \in \mathbb{N}^*$, $\gcd(d,p) = 1$	$j = \dfrac{(16t^{2d} - 16t^d + 1)^3}{-t^{4d}(16t^d - 1)}$	$H = q^{\lfloor \frac{d-1}{2} \rfloor + 1}$	$\lim\limits_{d\to\infty} \mathfrak{Bs}(E_d/K) = 1$
Chap. 7	$E_d : y^2 + xy - t^d y = x^3$ $d \in \mathbb{N}^*$, $\gcd(d,p) = 1$	$j = \dfrac{24t^d + 1}{-t^{3d}(27t^d - 1)}$	$H = q^{\lfloor \frac{d+2}{3} \rfloor}$	$\lim\limits_{d\to\infty} \mathfrak{Bs}(E_d/K) = 1$
Chap. 8	$B_{a,d} : y^2 + t^d xy - at^{2d} y = x^3 - (a+1)t^d x^2 + at^{2d} x$ $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ and $d \in \mathbb{N}^*$, $\gcd(d,p) = 1$	$j = \dfrac{(t^{2d} + 8(2a-1)t^d + 16(a^2 - a + 1))^3}{a^2(a-1)^2(t^{2d} + 8(2a-1)t^d + 16)}$	$H = q^{\lfloor \frac{d+1}{2} \rfloor}$	$\lim\limits_{\substack{d\to\infty \\ d \text{ odd}}} \mathfrak{Bs}(B_{1/2,d}/K) = 1$ if $a = 1/2$

Introduction (en français)

Le sujet de cette thèse est l'étude asymptotique d'un invariant associé aux courbes elliptiques sur les corps globaux : le ratio de Brauer-Siegel. Celui-ci combine trois des plus importants invariants arithmétiques d'une courbe elliptique : le régulateur de Néron-Tate, l'ordre de son groupe de Tate-Shafarevich et sa hauteur. Nous démontrons des analogues du théorème de Brauer-Siegel classique pour plusieurs familles de courbes elliptiques sur $\mathbb{F}_q(t)$. Nous commençons par motiver l'étude du ratio de Brauer-Siegel et par expliquer quel genre d'analogues sont visés. Le lecteur peut consulter [HP16, §1] et [Hin07] pour un exposé détaillé de ce problème dans un cadre plus général.

Motivations

Soit $\mathbb{F}_q$ un corps fini de caractéristique p et $K = \mathbb{F}_q(C)$ le corps des fonctions rationnelles sur une courbe projective lisse et géométriquement irréductible C définie sur $\mathbb{F}_q$. Par commodité, on fait l'hypothèse que $p \geqslant 5$. Le lecteur peut supposer sans problème que K est le corps des fractions rationnelles $\mathbb{F}_q(t)$ à coefficients dans $\mathbb{F}_q$.

Soit E une courbe elliptique définie sur K et donnée par un modèle de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

de coefficients $a_i \in K$. On peut associer à E un certain nombre d'invariants censés quantifier la « complexité arithmétique » de E : son discriminant minimal, son conducteur, sa hauteur, ... Nous choisissons ici d'ordonner la famille des courbes elliptiques E/K en fonction de leur hauteur différentielle (exponentielle) $H(E/K)$: celle-ci est définie par

$$H(E/K) = q^{\frac{1}{12}\deg \Delta_{\min}(E/K)},$$

où $\Delta_{\min}(E/K)$ est le diviseur discriminant minimal de E/K. Retenons que la hauteur se calcule facilement à partir d'un modèle de Weierstrass (1) de E/K (par l'algorithme de Tate par exemple, voir [Tat75]). Notons aussi que $H(E/K)$ dépend exponentiellement des (degrés des) coefficients $a_i \in K$.

Pour une telle courbe elliptique E/K, le théorème de Mordell-Weil (démontré par Lang et Néron dans ce contexte) assure que le groupe $E(K)$ des points K-rationnels sur E est de type fini : on peut donc l'écrire

$$E(K) = \mathbb{Z} \cdot P_1 \oplus \mathbb{Z} \cdot P_2 \oplus \cdots \oplus \mathbb{Z} \cdot P_r \oplus E(K)_{\text{tors}},$$

où les $P_i \in E(K)$ sont des points d'ordre infini et le sous-groupe de torsion $E(K)_{\text{tors}}$ est fini. L'entier r est appelé *rang de Mordell-Weil* de E/K (ou simplement *rang*). Le théorème de Mordell-Weil est purement qualitatif : il affirme la finitude de r et $\#E(K)_{\text{tors}}$. Mais le principal inconvénient de sa preuve est qu'elle est de nature ineffective : on ne peut pas en déduire une recette pour calculer r, des générateurs P_i de la partie libre ou des générateurs de $E(K)_{\text{tors}}$, ni non plus une borne sur la taille de ces objets (en termes de $H(E/K)$ par exemple). Cela dit, disposer d'une version quantitative du théorème de Mordell-Weil présente un intérêt majeur pour répondre à des questions diophantiennes : pour « résoudre » complètement l'équation (1) d'inconnues $x, y \in K$, il s'agit d'élucider la structure de $E(K)_{\text{tors}}$, de calculer le rang r et de trouver une base $\{P_1, \ldots, P_r\}$ de la partie libre de $E(K)$.

L'ordre du sous-groupe de torsion $E(K)_{\text{tors}}$ est le plus simple à évaluer. En effet, il y a une grande variété de méthodes pour le faire : réduction modulo une place de K, une adaptation du théorème de Lutz-Nagell, des méthodes modulaires, etc. Dans tous les cas, on dispose de bonnes bornes sur $\#E(K)_{\text{tors}}$. Plus précisément, Poonen a démontré l'existence d'une constante b_K (qui ne dépend que du genre de K) telle que

$$\#E(K)_{\text{tors}} \leqslant b_K.$$

C'est-à-dire que, lorsque K est fixé, les sous-groupes de torsion des courbes elliptiques définies sur K forment une liste finie, qui est de plus effectivement calculable (voir [Poo07] ; le fait analogue pour les courbes elliptiques sur les corps de nombres est également connu grâce aux travaux de Mazur, Momose et Merel). Cependant, le rang r et la taille des points d'ordre infini P_i restent encore bien mystérieux.

Il devient nécessaire de spécifier ce que l'on entend par « taille d'un point sur E ». Rappelons à cet effet que $E(K)$ est munie d'une forme quadratique non dégénérée : la hauteur canonique de Néron-Tate $\hat{h}_{NT} : E(K) \to \mathbb{R}$. Dans notre contexte, $\hat{h}_{NT}$ diffère de $(\deg x_P)/2$ par une quantité bornée, où x_P est la coordonnée en x d'un point P (vue comme une application rationnelle $x_P : C \to \mathbb{P}^1$). Nous choisissons de normaliser $\hat{h}_{NT} : E(K) \to \mathbb{R}$ de sorte qu'elle soit à valeurs dans $\mathbb{Q}$. Cette construction nous permet de mesurer la « taille » d'un point : plus sa hauteur est grande, plus le point est compliqué. De la hauteur $\hat{h}_{NT}$, on déduit une application $\mathbb{Z}$-bilinéaire $\langle \cdot, \cdot \rangle_{NT} : E(K) \times E(K) \to \mathbb{R}$, qui est également non dégénérée et munit $E(K)$ d'une structure euclidienne. En outre, on peut à présent définir le *régulateur de Néron-Tate de E/K* comme étant le covolume du réseau $E(K)/E(K)_{\text{tors}}$ dans $E(K) \otimes \mathbb{R}$ par rapport à la structure euclidienne induite par $\langle \cdot, \cdot \rangle_{NT}$:

$$\operatorname{Reg}(E/K) := \left| \det \left[\langle P_i, P_j \rangle_{NT} \right]_{1 \leqslant i,j \leqslant r} \right|,$$

où, comme ci-dessus, $(P_1, \ldots, P_r)$ désigne une $\mathbb{Z}$-base de la partie libre de $E(K)$. Ce dernier modélise la « complexité » de calculer $E(K)$. Un argument classique de géométrie des nombres (le théorème d'Hermite, voir [Lan83a, Theorem 4.1]) implique que, pour obtenir des majorations sur $\hat{h}(P_i)$, il suffit de connaître une majoration de $\operatorname{Reg}(E/K)$ ainsi qu'une minoration de la plus petite hauteur d'un point d'ordre infini :

$$\Lambda_{E/K} = \min \left\{ \hat{h}(P),\ P \in E(K) \smallsetminus E(K)_{\text{tors}} \right\}.$$

À propos de cette dernière quantité, Lang a conjecturé (*cf.* [Lan83a, Conjecture 2]) l'existence d'une constante $c_K > 0$ (ne dépendant que de K) telle que

$$\hat{h}(P) \geqslant c_K \log H(E/K) \tag{2}$$

pour tout point $P \in E(K)$ d'ordre infini. Ainsi, on cherche à présent à majorer le régulateur $\operatorname{Reg}(E/K)$. En des termes vagues, on veut quantifier (en fonction de $H(E/K)$) la complexité de calculer des générateurs du groupe de Mordell-Weil de E/K. En outre, on aimerait savoir à quel point la borne obtenue est optimale, *i.e.* on souhaite trouver également une *minoration* de $\operatorname{Reg}(E/K)$.

Ce problème rappelle une question classique : étant donné un corps de nombres $k/\mathbb{Q}$, peut-on donner une majoration du régulateur des unités $\operatorname{Reg}(\mathcal{O}_k^\times) = R_k$ en termes de son discriminant Δ_k ? Ou, d'un point de vue plus « algorithmique », quelle est la complexité du calcul de générateurs du groupe des unités $\mathcal{O}_k^\times$ d'un corps de nombres k ? La question diophantienne sous-jacente est de majorer la hauteur de Weil d'unités fondamentales (*i.e.* qui engendrent la partie libre de $\mathcal{O}_k^\times$) en fonction du discriminant Δ_k.

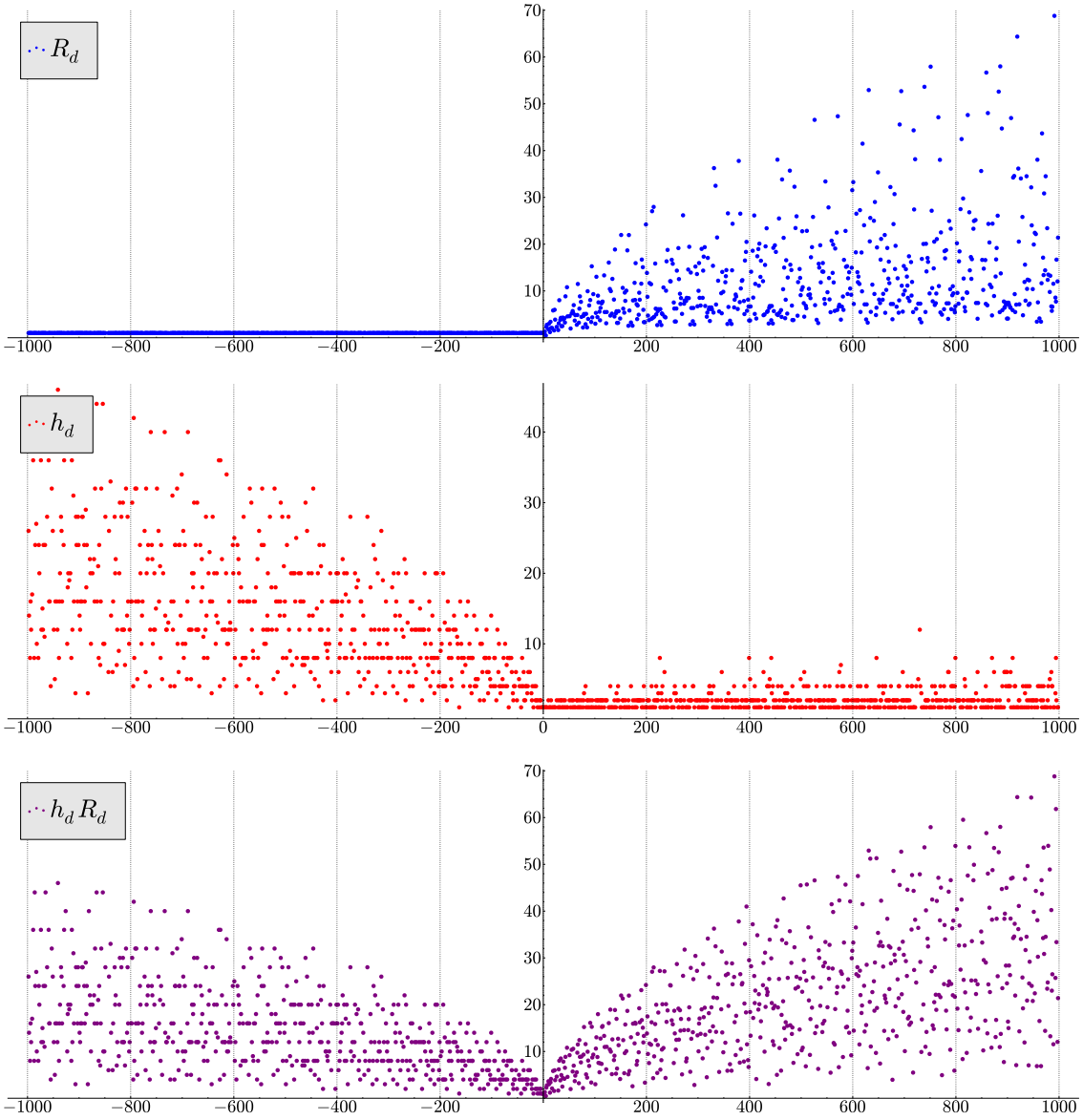
Il s'avère que calculer seulement une « base » de la partie libre du groupe des unités $\mathcal{O}_k^\times$ n'est pas beaucoup plus simple que d'expliciter à la fois une telle base *et* un ensemble de générateurs du groupe des classes $\mathcal{C}\ell(\mathcal{O}_k)$ de k (voir [Len92, §5]). On note $h_k = \#\mathcal{C}\ell(\mathcal{O}_k)$ le nombre de classes de k. En un certain sens, ceci suggère que la quantité $h_k \cdot R_k$ a un comportement plus « lisse » (vis-à-vis de Δ_k) que la quantité R_k seule. De toute façon, on a $h_k \geqslant 1$ donc toute majoration de $h_k \cdot R_k$ se traduit immédiatement en une majoration de R_k. Mieux encore, si l'on sait *a priori* que le groupe des classes est « gros », une majoration de $h_k \cdot R_k$ donne un meilleur contrôle de R_k ! Nous reviendrons sur ces bornes plus loin.

Les trois graphes ci-dessous illustrent ce phénomène : on se restreint au cas des corps quadratiques $k = \mathbb{Q}(\sqrt{d})$, ordonnés par leur discriminant fondamental $d \in \mathbb{Z}$. En fonction de $|d| \leqslant 1000$, nous avons tracé ci-dessous :

(1) le régulateur des unités R_d de $\mathbb{Q}(\sqrt{d})$ (en bleu),

(2) le nombre de classes h_d de $\mathbb{Q}(\sqrt{d})$ (en rouge),

(3) et leur produit $h_d \cdot R_d$ (en violet).



Comme on le voit, le comportement de $h_d \cdot R_d$ en fonction de $|d|$ est plus « régulier ». Par exemple, lorsque $d < 0$ le régulateur est trivial ($R_d = 1$) car les seules unités de $\mathbb{Q}(\sqrt{d})$ sont des racines de l'unité ; mais h_d a l'air de « croître lentement » avec $|d|$. Au contraire, lorsque $d > 0$, le régulateur semble croître assez vite, mais le nombre de classes h_d reste petit (on conjecture qu'il y a une infinité de corps quadratiques réels dont le nombre de classes est 1). Dans les deux cas cependant, le produit $h_d R_d$ a l'air grand lorsque $|d|$ est grand.

Rappelons que le groupe des classes $\mathcal{C}\ell(\mathcal{O}_k)$ peut être interprété comme une « obstruction local-global ». En effet, celui-ci mesure le défaut de factorisation unique dans l'anneau (global) $\mathcal{O}_k$ des entiers de k ; mais tous les anneaux locaux $\mathcal{O}_v$ de k en ses places finies sont des anneaux factoriels (puisque ce sont des anneaux de valuation discrète). En ce sens, $\#\mathcal{C}\ell(\mathcal{O}_k)$ recense les classes d'équivalence d'idéaux qui sont partout localement triviaux, mais non globalement.

Revenons à présent au problème de borner le régulateur de Néron-Tate $\mathrm{Reg}(E/K)$ d'une courbe elliptique E définie sur un corps de fonctions K. Inspirés par la situation décrite au paragraphe précédent, on peut penser qu'il serait plus aisé de trouver un encadrement de $\mathrm{Reg}(E/K)$ si on le « couplait » à une mesure de l'« obstruction local-global » sur E. Rappelons que le *groupe de Tate-Shafarevich de* E/K est défini à l'aide de la cohomologie galoisienne par

$$Ш(E/K) = \ker\left(\mathrm{H}^1(G_K, E(K^{\mathrm{sep}})) \to \prod_v \mathrm{H}^1(G_v, E(K_v^{\mathrm{sep}}))\right).$$

À propos de ce groupe, il nous suffira de savoir que $Ш(E/K)$ classifie les courbes C/K munies d'une action de E, qui deviennent isomorphes à E sur K^{sep} mais qui ne le sont pas sur K. Ou encore, $Ш(E/K)$ classifie les espaces principaux homogènes sur E qui sont partout localement triviaux, mais pas globalement triviaux. Ce groupe donne bien une mesure du défaut du « principe local-global » pour E. On conjecture que $Ш(E/K)$ est un groupe fini, mais ceci n'a été démontré que pour un nombre limité de courbes elliptiques. Dans le contexte présent, la finitude du groupe de Tate-Shafarevich est équivalente à ce que E vérifie la conjecture de Birch et Swinnerton-Dyer (sur laquelle nous revenons plus bas).

Nous pouvons maintenant citer une conjecture de Lang [Lan83a, Conjecture 1] selon laquelle il devrait exister une majoration du produit $\#Ш(E/K)\cdot \mathrm{Reg}(E/K)$ en termes de la hauteur $H(E/K)$. Par analogie avec la situation d'un corps de nombres, Lang propose :

Conjecture 1 (Lang). *Si E est une courbe elliptique sur un corps de fonctions K dont le groupe de Tate-Shafarevich $Ш(E/K)$ est fini, alors*

$$\forall \varepsilon > 0, \exists c_\varepsilon > 0 \ t.q. \quad \#Ш(E/K)\cdot \mathrm{Reg}(E/K) \leqslant c_\varepsilon \cdot H(E/K)^{1+\varepsilon}.$$

La conjecture originale ne concerne que les courbes elliptiques définies sur $\mathbb{Q}$, mais sa traduction à notre contexte est directe. De cette conjecture et de la minoration triviale $\#Ш(E/K) \geqslant 1$, on déduirait que

$$\mathrm{Reg}(E/K) \leqslant c_\varepsilon \cdot H(E/K)^{1+\varepsilon}. \tag{3}$$

Toutefois, cette dernière majoration n'est pas totalement satisfaisante : elle donne une borne exponentielle sur $\mathrm{Reg}(E/K)$ (et, par conséquent, sur la taille des générateurs de la partie libre de $E(K)$) en les coefficients d'un modèle de Weierstrass de E (*i.e.* les « données »). En un sens, la majoration (3) signifie que le calcul du groupe de Mordell-Weil d'une courbe elliptique donnée est un problème de complexité *au plus* exponentielle en les données (conditionnellement à la conjecture de Lang et la finitude du groupe de Tate-Shafarevich).

Mais, lorsque le rang de $E(K)$ est strictement positif, la majoration (3) est d'ordre tout à fait différent de la minoration conjecturale (2) de la hauteur, qui impliquerait que

$$\log H(E/K) \ll \mathrm{Reg}(E/K) \tag{4}$$

si le rang n'est pas trop grand, suggérant ainsi que trouver des générateurs de $E(K)$ est un problème de complexité *polynômiale* en les données. On peut donc s'interroger sur l'optimalité de la majoration dans la Conjecture 1 de Lang. Laquelle de la majoration (3) ou de la minoration (4) est la plus proche de la réalité ? Autrement dit, calculer $E(K)$ est-il réellement un problème exponentiellement difficile en les coefficients de E ?

Le ratio de Brauer-Siegel

Nous nous intéressons donc au problème de savoir à quel point la majoration

$$\#Ш(E/K)\cdot \mathrm{Reg}(E/K) \ll_\varepsilon H(E/K)^{1+\varepsilon} \tag{5}$$

est optimale : on aimerait savoir quelle puissance $\alpha \in [0, 1+\varepsilon]$ de la hauteur $H(E/K)$ devrait apparaître dans une minoration de la forme

$$H(E/K)^\alpha \ll \#Ш(E/K)\cdot \mathrm{Reg}(E/K).$$

Ceci a conduit Hindry et Pacheco [HP16] à introduire le *ratio de Brauer-Siegel* : pour toute courbe elliptique E/K dont le groupe de Tate-Shafarevich est fini, celui-ci est défini par

$$\mathfrak{Bs}(E/K) := \frac{\log\big(\#Ш(E/K)\cdot \mathrm{Reg}(E/K)\big)}{\log H(E/K)}.$$

Il convient de remarquer que cette définition a un sens, plus généralement, pour une variété abélienne de dimension quelconque sur un corps de fonctions (voir [HP16, §1]), voire même pour une variété abélienne sur un corps de nombres (voir [Hin07]). À l'aide de ce nouvel invariant, la Conjecture 1 se reformule comme suit :

Conjecture 2 (Hindry). *Soit K un corps de fonctions. Lorsque E parcourt la famille de toutes les courbes elliptiques définies sur K, ordonnée par hauteur, alors*

$$\mathfrak{Bs}(E/K) \leqslant 1 + o(1),$$

lorsque $H(E/K) \to \infty$.

Tâchons à présent de trouver des minorations convenables du ratio de Brauer-Siegel $\mathfrak{Bs}(E/K)$, *i.e.* de quantifier l'optimalité de la majoration (5). Une minoration « triviale » de celui-ci implique déjà l'existence d'une petite constante $\gamma_K \geqslant 0$ (ne dépendant que de K) telle que

$$-\gamma_K + o(1) \leqslant \mathfrak{Bs}(E/K) \qquad (\text{lorsque } H(E/K) \to \infty)$$

pour toutes les courbes elliptiques E sur K (pour lesquelles $Ш(E/K)$ est fini). Un argument plus fin permet même de montrer que $\gamma_K = 0$ convient (voir [HP16, Proposition 7.6]).

Si réellement les groupes de Mordell-Weil des courbes elliptiques sont « exponentiellement difficiles à calculer », il devrait y avoir une constante $\alpha_K > 0$ minimale telle que

$$0 < \alpha_K + o(1) \leqslant \mathfrak{Bs}(E/K) \qquad (\text{lorsque } H(E/K) \to \infty)$$

pour toute courbe elliptique E définie sur un corps de fonctions K fixé. Plusieurs heuristiques, sur lesquelles nous reviendrons, suggèrent au contraire qu'un tel α_K ne saurait être strictement positif :

Conjecture 3 (Hindry)**.** *Soit K un corps de fonctions. Lorsque E parcourt la famille de toutes les courbes elliptiques définies sur K, ordonnée par hauteur, alors*

$$0 = \liminf \mathfrak{Bs}(E/K).$$

À l'heure actuelle, il n'y a que 6 familles $\mathscr{E}$ de courbes elliptiques E définies sur $K = \mathbb{F}_q(t)$ pour lesquelles on sait (inconditionnellement) démontrer que le ratio de Brauer-Siegel a une limite lorsque $H(E/K) \to \infty$: dans chacun de ces cas, on a

$$\lim_{\substack{E \in \mathscr{E} \\ H(E/K) \to \infty}} \mathfrak{Bs}(E/K) = 1.$$

Voir [HP16, Theorem 7.12] et nos Théorèmes 4.4.1, 5.4.1, 6.4.1, 7.4.4 et 8.4.2.

Afin d'expliquer les méthodes qui permettent d'encadrer le ratio de Brauer-Siegel des courbes elliptiques, il nous semble pertinent de revenir sur le cas des corps de nombres. En effet, la Conjecture 1 de Lang est motivée par le fait que le produit $\#Ш(E/K) \cdot \mathrm{Reg}(E/K)$ pour les courbes elliptiques (ordonnées par leur hauteur) devrait se comporter « comme » le produit $\#\mathcal{C}\ell(\mathcal{O}_k) \cdot \mathrm{Reg}(\mathcal{O}_k^\times)$ pour les corps de nombres (ordonnés par leur discriminant), voir [Lan83a, §1]. Il est donc naturel de penser pouvoir encadrer $\#Ш(E/K) \cdot \mathrm{Reg}(E/K)$ « comme » on encadrerait $\#\mathcal{C}\ell(\mathcal{O}_k) \cdot \mathrm{Reg}(\mathcal{O}_k^\times)$.

Soit $k/\mathbb{Q}$ un corps de nombres de degré $n = [k : \mathbb{Q}]$. À nouveau, nous notons Δ_k la valeur absolue de son discriminant (sur $\mathbb{Q}$). Soit h_k le nombre de classes de k et R_k le régulateur des unités de k. Nous cherchons ici un encadrement de $h_k \cdot R_k$ en termes de Δ_k. Pour un tel corps de nombres k, définissons son *ratio de Brauer-Siegel* par

$$\mathfrak{Bs}(k/\mathbb{Q}) := \frac{\log\left(h_k \cdot R_k\right)}{\log \sqrt{\Delta_k}}.$$

Avec cette notation, nous citons le théorème de Brauer-Siegel « classique » :

Théorème 4 (Brauer-Siegel)**.** *Lorsque k parcourt une famille infinie $\mathscr{K}$ de corps de nombres dont le degré n est fixé et avec $\Delta_k \to \infty$, on a*

$$\lim_{\substack{k \in \mathscr{K} \\ \Delta_k \to +\infty}} \mathfrak{Bs}(k/\mathbb{Q}) = 1.$$

La forme compacte ci-dessous (sans référence à $\mathfrak{Bs}(k/\mathbb{Q})$) est peut-être plus usuelle :

$$\log(h_k \cdot R_k) \sim \log \sqrt{\Delta_k} \qquad (\text{à } [k : \mathbb{Q}] \text{ fixé}, \ \Delta_k \to +\infty).$$

En outre, on peut reformuler le Théorème 4 sous la forme d'une combinaison de deux inégalités sur $h_k \cdot R_k$ en fonction de Δ_k :

$$\forall \varepsilon > 0, \qquad \Delta_k^{1/2-\varepsilon} \ll_\varepsilon h_k \cdot R_k \ll_\varepsilon \Delta_k^{1/2+\varepsilon}.$$

Le théorème de Brauer-Siegel a été démontré par Siegel pour les corps quadratiques (voir [Sie35]) et par Brauer dans le cas général (voir [Bra47]). Sans rentrer dans trop de détails, rappelons comment la preuve du Théorème 4 s'articule. Celle-ci est de nature analytique et est généralement séparée en trois étapes (par ordre croissant de difficulté) :

Étape 1. On associe à k sa fonction zeta de Dedekind $\zeta_k(s)$: c'est une série de Dirichlet, *a priori* convergente sur le demi-plan $\mathrm{Re}(s) > 1$, qui admet un prolongement méromorphe au plan complexe $\mathbb{C}$. La fonction ainsi prolongée a un pôle simple en $s = 1$ et le résidu de $\zeta_k(s)$ en celui-ci s'écrit en termes d'invariants arithmétiques de k. Plus précisément, on a la formule des classes de Dirichlet :

$$\rho_k := \lim_{s\to 1}(s-1)\zeta_k(s) = \frac{h_k \cdot R_k}{\#\mu_k} \cdot 2^{r_1}(2\pi)^{r_2} \cdot \frac{1}{\sqrt{\Delta_k}}, \tag{6}$$

où $\#\mu_k$ désigne le nombre de racines de l'unité dans k et r_1 (resp. r_2) est le nombre de plongements réels (resp. complexes) de k. Lorsque le degré n de k est fixé, il est facile de montrer que le terme $\frac{2^{r_1}(2\pi)^{r_2}}{\#\mu_k}$ apparaissant dans cette formule est borné. On peut alors écrire :

$$\mathfrak{Bs}(k/\mathbb{Q}) = 1 + \frac{\log \rho_k}{\log \sqrt{\Delta_k}} + o(1) \qquad (\text{lorsque } \Delta_k \to \infty).$$

Pour démontrer le Théorème 4, il s'agit à présent d'encadrer le résidu ρ_k en fonction de Δ_k. Plus spécifiquement, il faut voir que

$$\forall \varepsilon > 0, \qquad \Delta_k^{-\varepsilon} \ll_\varepsilon \rho_k \ll_\varepsilon \Delta_k^{\varepsilon}. \tag{7}$$

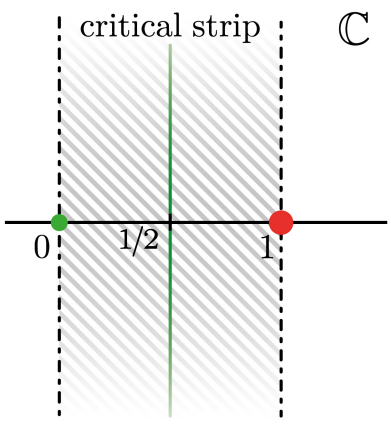
Étape 2. Étudier la taille de ρ_k (en fonction de Δ_k) est équivalent à étudier le comportement de $\zeta_k(s)$ au voisinage de son pôle $s = 1$ car

$$\zeta_k(s) \sim \frac{\rho_k}{s-1} \qquad (s \to 1).$$

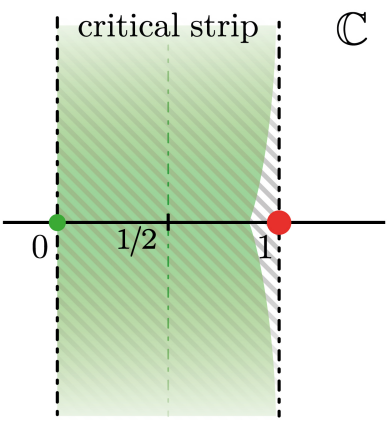
En fait, il suffit même d'étudier $x \mapsto \zeta_k(x)$ lorsque $x \neq 1$ est un réel proche de 1. La présence (ou l'absence) de zéros de $\zeta_k(x)$ voisins de $x = 1$ a une grande influence sur la taille de ρ_k. Comme $x \mapsto \zeta_k(x)$ ne s'annule pas sur $]1, +\infty[$, la majoration de ρ_k dans (7) s'obtient facilement. On peut même montrer une version explicite et effective de celle-ci (voir [Sie69]) :

$$\rho_k \leqslant 4\left(\tfrac{e}{n-1}\right)^{n-1} \cdot (\log \Delta_k)^{n-1} \ll_{n,\varepsilon} \Delta_k^{\varepsilon}.$$

Étape 3. La dernière étape est la plus délicate : pour prouver la minoration de ρ_k dans (7), il faut étudier le comportement de $\zeta_k(x)$ lorsque $x < 1$ (c'est-à-dire lorsque x est dans la bande critique de $\zeta_k(s)$). Comme on l'a mentionné, si $\zeta_k(s)$ a un zéro proche de 1, le résidu tend à être plus petit. Si l'on suppose l'Hypothèse de Riemann Généralisée (ci-après abrégée en GRH) pour $\zeta_k(s)$, alors $\zeta_k(s)$ n'a aucun zéro dans l'intervalle $]1/2, 1[$ et l'on obtient une bonne minoration de son résidu ρ_k. Ci-dessous, nous avons schématisé la situation : dans un premier temps, représentons la bande critique de $\zeta_k(s)$ dans le plan complexe (la bande hachurée) ainsi que la zone où les zéros de $\zeta_k(s)$ sont répartis (en vert). Le point rouge en $s = 1$ symbolise le pôle de $\zeta_k(s)$.

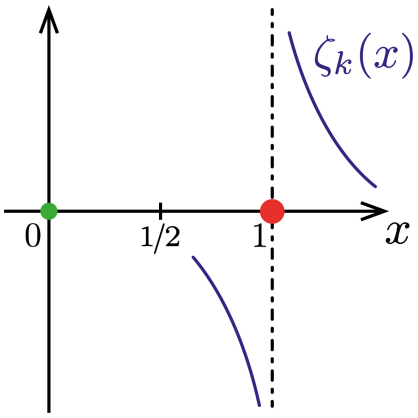


Zéros de $\zeta_k(x)$ en supposant GRH.

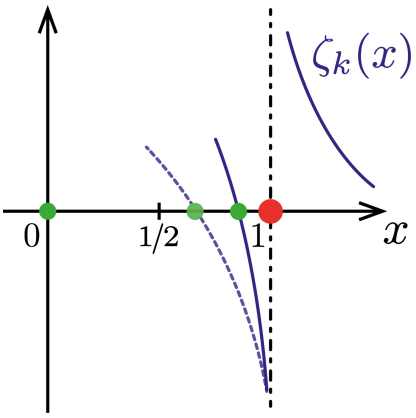


Zéros de $\zeta_k(x)$ sans supposer GRH.

Traçons maintenant l'allure d'une partie du graphe de $x \mapsto \zeta_k(x)$ pour $x \in \mathbb{R}$ au voisinage de $x = 1$.



Comportement de $\zeta_k(x)$ sous GRH.



Comportement de $\zeta_k(x)$ sans GRH.

– Sur la figure de gauche, on suppose GRH : tous les zéros de ζ_k sont sur la droite critique $\mathrm{Re}(s) = 1/2$ (la droite verte au centre de la bande critique). Lorsque x tend vers 1^-, $\zeta_k(x)$ tend « doucement » vers $-\infty$ de sorte que son résidu ρ_k ne peut pas être « trop petit ».
– Sur la figure de droite maintenant, on ne suppose plus GRH. La zone verte représente les endroits où peuvent se trouver les zéros de ζ_k (le complémentaire de la zone verte dans la bande critique est une « zone sans zéros »). Comme on le voit, si ζ_k a effectivement un zéro proche de 1 (les points verts), le graphe de ζ_k sur $]1/2, 1[$ est bien plus « pentu » (et plus le zéro est proche de 1, plus la pente est importante). Ceci peut s'interpréter comme un signe que ζ_k a un « petit » résidu.

Le point-clé de la preuve du Théorème 4 est alors de contourner l'usage de GRH en autorisant *un* des corps de nombres k dans la famille $\mathscr{K}$ à avoir un « petit » résidu ρ_k et en vérifiant que tous les autres $k' \in \mathscr{K}$ ont un résidu $\rho_{k'}$ aussi « gros » que nécessaire, c'est-à-dire $\rho_{k'} \gg_\varepsilon \Delta_{k'}^{-\varepsilon}$. Le principal inconvénient de cette approche est l'absence de contrôle sur l'éventuel « contre-exemple » k : la minoration de ρ_k dans (7) est donc *ineffective*. Cependant, mentionnons que Stark a décrit les cas dans lesquels la minoration peut être rendue effective (*cf.* [Sta74]).

Cette equisse de preuve est assez sommaire : le lecteur pourra consulter [Lan94, Chapter XVI] et [Hin10, Lecture 5] pour un argument plus détaillé. Remarquons, en lien avec le problème qui nous intéresse, le fait suivant : à l'aide de l'équation fonctionnelle de $\zeta_k(s)$, il est possible de voir que $\zeta_k(s)$ s'annule en $s = 0$ avec multiplicité $r = r_1 + r_2 - 1 = \mathrm{rang}(\mathcal{O}_k^\times)$ et que le premier coefficient non nul dans le développement de Taylor de $\zeta_k(s)$ en $s = 0$ est donné par

$$\zeta^*(0) := \lim_{s \to 0} s^{-r} \cdot \zeta_k(s) = -\frac{h_k \cdot R_k}{\#\mu_k}.$$

Tenter de borner $|\zeta^*(0)|$ en fonction de Δ_k pourrait donc être intéressant pour l'étude de $\text{Ш}(k/\mathbb{Q})$, mais nous ne connaissons aucune preuve du Théorème 4 qui utilise ce fait (bien que la preuve de la majoration du théorème de Brauer-Siegel semble faisable).

Signalons que le Théorème 4 a été généralisé dans de multiples directions. Notamment par Tsfasman et Vlăduţ [TV02] qui ont analysé en détail ce qui arrive lorsque l'on enlève (ou que l'on affaiblit) la condition que le degré des corps $k \in \mathscr{K}$ est fixé. En imposant divers ensembles d'hypothèses sur une famille $\mathscr{K}$ de corps de nombres k, ils ont montré que la limite

$$\lim_{\substack{k \in \mathscr{K} \\ \Delta_k \to \infty}} \text{Ш}(k/\mathbb{Q})$$

existe encore, mais qu'elle peut être différente de 1 ! De plus, ils donnent une expression explicite de cette limite en termes d'invariants arithmétiques de la famille $\mathscr{K}$. Nous renvoyons à leur article pour l'étude détaillée de ces questions (voir également [Zyk05]). Notons aussi que des analogues du théorème de Brauer-Siegel existent pour des familles de corps de fonctions K sur $\mathbb{F}_q$ (un corps fini fixé), sous des hypothèses diverses (voir en particulier [GL78], [War12] et [Zyk15]).

Pour clore ce paragraphe, mentionnons que Tsimerman a démontré un analogue du Théorème 4 pour les tores algébriques définis sur $\mathbb{Q}$ dont la dimension est fixée et dont le conducteur croît (voir [Tsi12, Theorem 1.3]). La « formule des classes » correspondante avait précédemment été exprimée

par Shyr [Shy77] et la partie analytique de la preuve est très proche de celle du cas classique (voir [Tsi12, Lemma 4.1]). Le théorème de Tsimerman est important pour l'étude des points spéciaux sur les variétés de Shimura, où il est utilisé pour produire des minorations d'orbites galoisiennes (à ce sujet, voir [UY15]). Retenons seulement que *certains* groupes algébriques de dimension fixée vérifient un analogue (correctement formulé) du théorème de Brauer-Siegel.

Maintenant que l'on a détaillé comment se déroule l'étude du ratio de Brauer-Siegel des *corps de nombres*, nous revenons à la situation des courbes elliptiques sur les corps de fonctions. Une idée de départ naturelle est d'essayer d'imiter la preuve du théorème de Brauer-Siegel pour l'adapter à notre problème. Avant de s'y lancer, nous introduisons l'outil analytique nécessaire, à savoir la fonction L. Fixons une courbe elliptique E définie sur un corps de fonctions K. Pour toute place v de K (dont on note d_v le degré), on peut réduire « modulo v » une équation de E : on obtient alors une courbe cubique plane $\overline{E}_v$, définie sur le corps résiduel $\mathbb{F}_v$ de K en v. Comme $\mathbb{F}_v$ est fini (c'est une extension finie de $\mathbb{F}_q$), on peut compter le nombre de points $\mathbb{F}_v$-rationnels sur $\overline{E}_v$: écrivons le résultat sous la forme

$$\#\overline{E}_v(\mathbb{F}_v) = \#\mathbb{F}_v + 1 - a_v(E) = q^{d_v} + 1 - a_v(E),$$

où $a_v(E)$ est un entier. Si la courbe $\overline{E}_v$ est lisse, alors $|a_v(E)| \leqslant 2q^{d_v/2}$ par le théorème de Hasse ; si $\overline{E}_v$ est singulière, alors $a_v(E) \in \{0, -1, 1\}$. On combine alors ces « comptages locaux de points » (pour toute place v) en une série génératrice définie par un produit eulérien : soit

$$L(E/K, T) := \prod_{v \notin \mathcal{B}} \left(1 - a_v(E) \cdot T^{d_v} + q^{d_v} T^{2d_v}\right)^{-1} \cdot \prod_{v \in \mathcal{B}} \left(1 - a_v(E) \cdot T^{d_v}\right)^{-1}, \tag{8}$$

où $\mathcal{B}$ désigne l'ensemble des places de K où E a mauvaise réduction (*i.e.* les places v pour lesquelles la courbe $\overline{E}_v$ est singulière). D'après sa définition, on voit que $L(E/K, T) \in \mathbb{Z}[[T]]$ est une série formelle à coefficients entiers : on l'appelle la *fonction L de E/K*. Des théorèmes profonds de Grothendieck et Deligne montrent qu'en fait, $L(E/K, T)$ est une fraction rationnelle en T (et même un polynôme en T si E/K n'est pas constante), dont le degré est donné explicitement en termes du conducteur de E et qui satisfait à une équation fonctionnelle pour $T \mapsto (q^2 T)^{-1}$.

La fonction $s \mapsto \mathcal{L}(E/K, s)$ donnée par $\mathcal{L}(E/K, s) = L(E/K, q^{-s})$ est parfois aussi appelée « fonction L de E ». Les résultats sus-cités se réécrivent comme suit pour $\mathcal{L}(E/K, s)$: la série de Dirichlet obtenue en remplaçant T par q^{-s} dans (8), *a priori* convergente sur le demi-plan $\mathrm{Re}(s) > 3/2$, peut être prolongée en une fonction méromorphe sur le plan complexe (voire même holomorphe si E/K n'est pas constante) et satisfait à une équation fonctionnelle pour $s \mapsto 2 - s$.

Un autre théorème de Deligne, d'importance majeure, assure que l'analogue de l'hypothèse de Riemann est vraie pour $\mathcal{L}(E/K, s)$: les zéros (dans $\mathbb{C}$) de $s \mapsto \mathcal{L}(E/K, s)$ sont de partie réelle $\mathrm{Re}(s) = 1$. Revenant à la version $T \mapsto L(E/K, T)$ de la fonction L, ceci se traduit par le fait que les inverses des zéros de $L(E/K, T)$ sont des entiers algébriques de module q dans tout plongement complexe. Un des avantages de travailler avec les courbes elliptiques sur les corps de fonctions est que la plupart de ces faits (prolongement analytique, équation fonctionnelle et hypothèse de Riemann) sont encore largement conjecturaux pour les courbes elliptiques sur les corps de nombres.

La première étape de la preuve du théorème de Brauer-Siegel classique est de relier $\mathfrak{Bs}(k/\mathbb{Q})$ au résidu de la fonction $\zeta_k(s)$ en $s = 1$ *via* la formule du nombre de classes. Dans le contexte des courbes elliptiques sur les corps de fonctions, le lien analogue entre $\mathfrak{Bs}(E/K)$ et la fonction L est donné par la conjecture de Birch et Swinnerton-Dyer (dorénavant abrégée en BSD), que nous présentons maintenant. Comme on l'a dit, la fonction $\mathcal{L}(E/K, s)$ admet un prolongement méromorphe à $\mathbb{C}$: on peut donc étudier son comportement au voisinage de $s = 1$ (qui est le centre de symétrie pour l'équation fonctionnelle) et définir deux quantités supplémentaires. Premièrement, le *rang analytique* de E/K, noté $r_{an}(E/K)$, est l'ordre d'annulation de $\mathcal{L}(E/K, s)$ en $s = 1$ ou, de façon équivalente, la multiplicité de $T = q^{-1}$ comme racine de la fraction rationnelle $L(E/K, T)$, *i.e.*

$$r_{an}(E/K) := \mathrm{ord}_{s=1} \mathcal{L}(E/K, s) = \mathrm{ord}_{T=q^{-1}} L(E/K, T).$$

Deuxièmement, on introduit la valeur spéciale de la fonction L en $s = 1$: celle-ci est couramment définie comme étant le premier coefficient non nul dans le développement de Taylor de $\mathcal{L}(E/K, s)$ en $s = 1$:

$$\mathcal{L}(E/K, s) = \big(\text{valeur spéciale}\big) \cdot (s-1)^{r_{an}(E/K)} + o\big((s-1)^{r_{an}(E/K)}\big) \qquad (\text{lorsque } s \to 1).$$

Nous préférons travailler avec une version légèrement différente de la valeur spéciale, définie comme suit : la fraction rationnelle $L(E/K, T)$ est à coefficients entiers et s'annule en $T = q^{-1}$ avec multiplicité

$r_{an}(E/K)$, on pose alors $L^*(E/K,T) = L(E/K,T)/(1-qT)^{r_{an}(E/K)}$ et l'on définit la *valeur spéciale* de $L(E/K,T)$ par :

$$L^*(E/K,1) := L^*(E/K,q^{-1}) = \left.\frac{L(E/K,T)}{(1-qT)^{r_{an}(E/K)}}\right|_{T=q^{-1}}.$$

Comme $(1-q^{1-s}) \sim \log q \cdot (s-1)$ quand $s \to 1$, il est facile de constater que $L^*(E/K,1)$ diffère de la valeur spéciale « usuelle » par un facteur $(\log q)^{r_{an}(E/K)}$. Avec notre normalisation, la valeur spéciale $L^*(E/K,1)$ a l'avantage d'être un nombre rationnel non nul.

Birch et Swinnerton-Dyer (et Tate, dans ce contexte) ont conjecturé que $r_{an}(E/K)$ et $L^*(E/K,1)$ ont une interprétation arithmétique frappante :

Conjecture 5 (Birch - Swinnerton-Dyer)**.** *Soit E une courbe elliptique définie sur un corps de fonctions $K = \mathbb{F}_q(C)$, on notera g_C le genre de C. Alors, le rang analytique $r_{an}(E/K)$ et le rang du groupe de Mordell-Weil $E(K)$ coïncident :*

$$r_{an}(E/K) = \mathrm{ord}_{T=q^{-1}} L(E/K,T) = \mathrm{rank}\ E(K),$$

et la valeur spéciale $L^*(E/K,1)$ s'écrit :

$$L^*(E/K,1) = \frac{\#Ш(E/K)\cdot \mathrm{Reg}(E/K)}{\left(\#E(K)_{\mathrm{tors}}\right)^2} \cdot \mathcal{T}am(E/K) \cdot \frac{q^{1-g_C}}{H(E/K)}, \tag{9}$$

où $\mathcal{T}am(E/K)$ est le nombre de Tamagawa de E/K.

La première assertion est parfois appelée « conjecture de BSD faible » et la seconde « conjecture de BSD forte ». Notons que, dans (9), on suppose implicitement la finitude du groupe de Tate-Shafarevich. Pour les courbes elliptiques sur les corps de fonctions (contrairement au cas des courbes elliptiques sur les corps de nombres par exemple), cette conjecture est « presque un théorème ». Tout d'abord, les travaux de Kato et Trihan [KT03] (complétant des résultats antérieurs de Tate [Tat66], Milne [Mil75] et d'autres) montrent que la conjecture « complète » de BSD pour une courbe E/K est équivalente à la conjecture « faible », elle-même équivalente à la finitude du groupe de Tate-Shafarevich $Ш(E/K)$ (ou même à la finitude d'une des composantes ℓ-primaires $Ш(E/K)[\ell^\infty]$). En outre, la Conjecture 5 est complètement démontrée dans beaucoup de cas. Par exemple, Milne [Mil68] a prouvé que les courbes elliptiques isotriviales vérifient la Conjecture 5. Notons également que la conjecture de BSD a, dans le présent contexte, un pendant « géométrique » : pour une courbe elliptique E définie sur $K = \mathbb{F}_q(C)$, on note $\pi : \mathcal{E} \to C$ son modèle régulier minimal ; la conjecture de BSD pour E/K est équivalente à la conjecture de Tate pour la surface $\mathcal{E}/\mathbb{F}_q$. Cette dernière conjecture est connue pour beaucoup de surfaces (voir entre autres [Gor79], [Mil75], [Shi86], [SK79], ...) et peut être utilisée pour produire de nombreuses courbes elliptiques satisfaisant la conjecture de BSD. Certaines d'entre elles sont non isotriviales.

Le lecteur peut à présent comparer la formule du nombre de classes de Dirichlet (6) pour un corps de nombres et la formule conjecturale de BSD (9) pour les courbes elliptiques : toutes deux expriment un coefficient de Taylor en $s = 1$ d'une série de Dirichlet en termes d'invariants arithmétiques et elles sont, au moins dans leur structure formelle, très similaires. Mettons en place un « dictionnaire » partiel pour clarifier l'analogie entre les deux situations :

Corps de nombres $k/\mathbb{Q}$		Courbes elliptiques E/K	
degré	$[k:\mathbb{Q}]$	$d=1$	dimension
discriminant	Δ_k	$H(E/K)$	hauteur
fonction zeta	$\zeta_k(s)$	$\mathcal{L}(E/K,s)$	fonction L
nombre de classes	$h_k = \#\mathcal{C}\ell(\mathcal{O}_k)$	$Ш(E/K)$	ordre du groupe de Tate-Shafarevich
régulateur des unités	$R_k = \mathrm{Reg}(\mathcal{O}_k^\times)$	$\mathrm{Reg}(E/K)$	régulateur de Néron-Tate
# de racines de l'unité	$\#\mu_k = \#(\mathcal{O}_k^\times)_{\mathrm{tors}}$	$\#E(K)_{\mathrm{tors}}$	# de points de torsion
« période »	$2^{r_1}(2\pi)^{r_2}$	$\mathcal{T}am(E/K)$	nombre de Tamagawa.

Revenons à présent à l'idée émise plus haut d'imiter la preuve en trois étapes du théorème de Brauer-Siegel classique (Théorème 4) pour obtenir un encadrement du ratio de Brauer-Siegel d'une courbe elliptique. Soit E une courbe elliptique définie sur un corps de fonctions K, supposons que E vérifie la conjecture de BSD (comme on l'a remarqué, supposer que BSD est vraie est équivalent

à supposer la finitude du groupe de Tate-Shafarevich). Utilisons la formule (9) de BSD exprimant la valeur spéciale $L^*(E/K,1)$ de la fonction L de E pour mener à bien l'« **Étape 1.** » de notre programme (la numérotation fait référence à notre esquisse de la preuve du Théorème 4) : il s'agit de relier la taille de $\text{Ш}(E/K)$ à celle de $L^*(E/K,1)$.

Pour ce faire, nous devons nous assurer que les deux termes « parasites » $\#E(K)_{\text{tors}}$ et $\mathcal{T}am(E/K)$ dans (9) ne sont pas significatifs asymptotiquement et que l'on peut sans encombres les négliger ; de la même façon que dans le cas d'un corps de nombres k, il a fallu vérifier que $\#\mu_k$ et $2^{r_1}(2\pi)^{r_2}$ sont négligeables devant Δ_k. Au tout début de cette introduction, on a déjà relevé l'existence d'une borne uniforme pour $\#E(K)_{\text{tors}}$ (lorsque K est fixé) :

$$1 \leqslant \#E(K)_{\text{tors}} \leqslant b_K.$$

Notons qu'une majoration plus faible (de la forme $\#E(K)_{\text{tors}} \ll_\varepsilon H(E/K)^\varepsilon$, pour tout $\varepsilon > 0$) nous serait suffisante. Le nombre de Tamagawa $\mathcal{T}am(E/K)$ peut également être majoré en termes de la hauteur : précisément, on peut démontrer que

$$\forall\, \varepsilon > 0, \qquad 1 \leqslant \mathcal{T}am(E/K) \ll_\varepsilon H(E/K)^\varepsilon,$$

où la constante implicite est effective. Pour les courbes elliptiques sur les corps de fonctions, la preuve n'est pas très difficile (voir notre Théorème 1.5.4) mais l'extension de celle-ci à des variétés abéliennes de dimension plus grande est nettement plus subtile (voir [HP16, Theorem 6.5]). Une fois que ces deux termes sont contrôlés, on a l'inégalité ci-dessous, valide pour toutes les courbes elliptiques E vérifiant la conjecture de BSD définies sur un corps de fonctions fixé K :

$$\text{Ш}(E/K) = 1 + \frac{\log|L^*(E/K,1)|}{\log H(E/K)} + o(1) \qquad (H(E/K) \to \infty).$$

Par conséquent, pour encadrer $\text{Ш}(E/K)$, il s'agit d'estimer la taille de la valeur spéciale en fonction de la hauteur. Gardant à l'esprit l'analogie avec les corps de nombres, nous entreprenons d'étudier le comportement de la fonction L de E/K au voisinage de $s = 1$: ceci constituera les analogues des « **Étape 2.** » et « **Étape 3.** » de la preuve du théorème de Brauer-Siegel classique.

En premier lieu, nous expliquons comment obtenir des majorations de la valeur spéciale $L^*(E/K,1)$ en termes de la hauteur (achevant ainsi l'« **Étape 2.** »). Soit E une courbe elliptique sur un corps de fonctions K ; on suppose, pour simplifier, que E n'est pas constante. Souvenons-nous qu'alors $L(E/K,T)$, la fonction L de E, est un polynôme à coefficients entiers en T dont le degré $\mathfrak{b}_{E/K}$ est borné par $c_K \cdot \log H(E/K)$ (où c_K est une petite constante explicite) et dont les inverses des zéros sont de valeur absolue q. Il suit de cette observation une première majoration de la valeur spéciale (dite « triviale ») :

$$\log|L^*(E/K,1)| \ll \mathfrak{b}_{E/K} \ll \log H(E/K), \tag{10}$$

où les constantes implicites sont effectives et dépendent seulement de K. Une estimation plus fine de $\mathcal{L}(E/K,s)$, utilisant des techniques standards d'analyse complexe (voir [HP16, Theorem 7.5]), conduit à

$$\log|L^*(E/K,1)| \ll \mathfrak{b}_{E/K} \cdot \frac{\log\log \mathfrak{b}_{E/K}}{\log \mathfrak{b}_{E/K}} = o\big(\mathfrak{b}_{E/K}\big) = o\big(\log H(E/K)\big). \tag{11}$$

Si notre courbe elliptique E/K satisfait à la conjecture de BSD, cette majoration améliorée donne que

$$\text{Ш}(E/K) \leqslant 1 + o(1) \qquad (H(E/K) \to \infty).$$

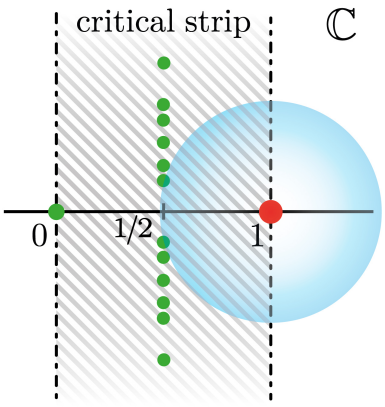
Ce qui termine l'« **Étape 2.** » de la preuve d'un analogue du théorème de Brauer-Siegel.

Il ne nous reste à présent qu'à trouver une minoration de la valeur spéciale $L^*(E/K,1)$. Ce problème est *nettement plus compliqué* que ce qui précède et essentiellement, encore largement ouvert. Il y a plusieurs raisons pour lesquelles l'adaptation de l'« **Étape 3.** » des corps de nombres aux courbes elliptiques ne se déroule pas aussi bien que l'on pourrait le prévoir. Une de ces raisons est la différence, d'un point de vue analytique, entre la fonction $\mathcal{L}(E/K,s)$ associée à une courbe elliptique et la fonction $\zeta_k(s)$ d'un corps de nombres k. Toutes deux sont étudiées au voisinage de $s = 1$ mais :

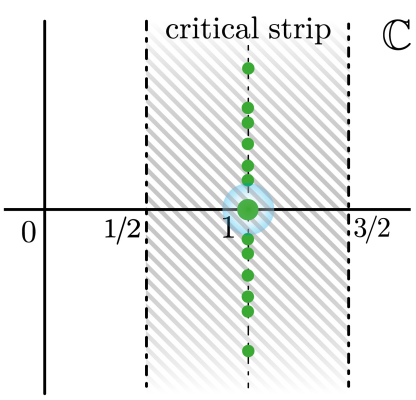
– D'abord, $\zeta_k(s)$ a un pôle simple en $s = 1$, alors que $\mathcal{L}(E/K,s)$ a vraisemblablement un zéro de grande multiplicité en $s = 1$. Nous mentionnons ici, qu'il y a des exemples explicites de courbes elliptiques sur $\mathbb{F}_q(t)$ de rang arbitrairement grand et qui satisfont à la conjecture de BSD, voir [TŠ67] et [Ulm02]. Il est classique, en analyse complexe, que le comportement d'une fonction méromorphe autour de l'un de ses pôles donne des informations fortes sur la taille de

son résidu en ce pôle. Au contraire, le comportement d'une fonction méromorphe autour de l'un de ses zéros, surtout si celui-ci est d'ordre élevé, ne donne quasiment aucune minoration de ses coefficients de Taylor en ce point.

– Ensuite, dans le cas des corps de nombres, on a vu que supposer l'hypothèse de Riemann pour $\zeta_k(s)$ repousse les zéros de $\zeta_k(s)$ « loin » de son pôle en $s = 1$; on en tire une très bonne minoration du résidu de $\zeta_k(s)$ en $s = 1$ (sous GRH). Lorsque l'on revient aux fonctions L des courbes elliptiques sur les corps de fonctions, la bande critique est cette fois $1/2 < \mathrm{Re}(s) < 3/2$ et l'hypothèse de Riemann a été démontrée par Deligne : tous les zéros de $\mathcal{L}(E/K, s)$ sont de partie réelle $\mathrm{Re}(s) = 1$ (et sont distribués symétriquement par rapport à l'axe réel). Or, nous souhaitons précisément étudier $\mathcal{L}(E/K, s)$ autour de $s = 1$, en plein milieu de la bande critique ! Il *y a* donc des zéros de $\mathcal{L}(E/K, s)$ qui sont proches de 1 ! Le lecteur peut comparer les deux figures ci-dessous : à nouveau, les points verts symbolisent les positions possibles de zéros de $\zeta_k(s)$ ou $\mathcal{L}(E/K, s)$ dans la bande critique et la bulle bleue centrée en $s = 1$ représente une « région sans zéros ».



Zéros de $\zeta_k(s)$ (sous GRH).



Zéros de $\mathcal{L}(E/K, s)$ (sous GRH).

La bulle bleue de $\zeta_k(s)$ est presque indépendante de k ; mais lorsque la hauteur de E/K croît, la bulle de $\mathcal{L}(E/K, s)$ devient de plus en plus petite. Sans compter la possibilité qu'un « paquet » de zéros « s'accumule » en bordure de la bulle bleue. Ce phénomène est l'obstacle majeur à trouver des minorations non triviales de $L^*(E/K, 1)$. La présence potentielle de *petits zéros* peut être considérée comme un premier indice vague que le ratio de Brauer-Siegel des courbes elliptiques ne peut pas toujours être « gros » (*i.e.* il pourrait être beaucoup plus petit que 1).

Avant de passer en revue les résultats connus concernant le ratio de Brauer-Siegel, nous mentionnons une situation étroitement liée à la précédente (on pourrait parler du « cas vertical »). Spécifiquement, on fixe une courbe elliptique E définie sur un corps de fonctions K_0 et on considère une tour de corps de fonctions $K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_i \subset \ldots$ (correspondant à une suite de revêtements de courbes $C_0 \leftarrow C_1 \leftarrow C_2 \leftarrow \cdots \leftarrow C_i \leftarrow \ldots$). On pourrait s'intéresser à encadrer la « croissance » des groupes de Mordell-Weil successifs :

$$E(K_0) \subset E(K_1) \subset E(K_2) \subset \cdots \subset E(K_i) \subset \ldots \qquad (i \to \infty).$$

Dans cette optique, lorsque E est une courbe elliptique constante sur K_0, Kunyavskiĭ et Tsfasman ont démontré (voir [KT08, Theorem 2.1]) :

Théorème 6 (Kunyavskiĭ - Tsfasman). *Soit $\{K_i\}_{i\in\mathbb{N}}$ une tour de corps de fonctions : $K_i = \mathbb{F}_p(C_i)$ est le corps des fonctions d'une courbe C_i et le genre $g(C_i)$ tend vers $+\infty$ (lorsque $i \to \infty$). Soit E_0 une courbe elliptique constante définie sur $K_0 = \mathbb{F}_p(C_0)$. Pour tout $i \in \mathbb{N}$, on désigne par $E_i = E_0 \times_{K_0} K_i$ le changement de base de E_0 à K_i. Alors*

$$\lim_{i\to\infty} \frac{\log\left(\#Ш(E_i/K_i)\cdot \mathrm{Reg}(E_i/K_i)\right)}{\log p \cdot g(C_i)} = 1 - \sum_{m=1}^{\infty} \beta_m \cdot \log_p\left(\frac{\#E_0(\mathbb{F}_{p^m})}{p^m}\right),$$

où $\beta_m = \lim_{i\to\infty} \#C_i(\mathbb{F}_{p^m})/g(C_i)$ (quitte à extraire une sous-tour de $\{K_i\}_{i\in\mathbb{N}}$, on peut toujours supposer que ces limites existent).

Malheureusement, il semble y avoir un problème dans leur preuve (voir [KT10]). Noter que la quantité $\log\left(\#Ш(E_i/K_i)\cdot \mathrm{Reg}(E_i/K_i)\right)/(\log p \cdot g(C_i))$ dont il s'agit de trouver la limite est très liée

au ratio de Brauer-Siegel $\mathfrak{Bs}(E_i/K_i)$: dans le cas où le corps de fonctions K_i a un genre $g(C_i) \to \infty$, la principale contribution à $\log H(E_i/K_i)$ est $\log p \cdot g(C_i)$. Nous n'irons pas plus loin dans cette direction, mais mentionnons que l'on s'attend à ce que le comportement de $\mathfrak{Bs}(E_i/K_i)$ soit radicalement différent du comportement de $\mathfrak{Bs}(E/K)$ lorsque K est fixé et que E varie. La lectrice peut consulter l'article de Zykin [Zyk15] présentant un cadre unifié, qui pourrait être utilisé pour étudier les conjectures « horizontales » et « verticales » sur un pied d'égalité.

Résultats et questions antérieurs

L'introduction du ratio de Brauer-Siegel pour les courbes elliptiques est relativement récente (voir [HP16]). Cependant, il y a déjà quelques résultats importants à son propos, que nous allons maintenant expliquer. Noter que les résultats de [HP16] sont énoncés, dans une plus grande généralité, pour les variétés abéliennes de dimension quelconque : nous ne les énoncerons que pour les courbes elliptiques. Soit $K = \mathbb{F}_q(C)$ un corps de fonctions sur un corps fini $\mathbb{F}_q$. Nous noterons $\mathscr{E}\ell\ell_{/K}$ la famille de toutes les courbes elliptiques définies sur K (ordonnée par la hauteur). Comme on l'a expliqué ci-avant, Hindry a conjecturé que

$$0 + o(1) \leqslant \mathfrak{Bs}(E/K) \leqslant 1 + o(1) \qquad (E \in \mathscr{E}\ell\ell_{/K},\ H(E/K) \to \infty)$$

pour toutes les courbes elliptiques dont le groupe de Tate-Shafarevich est fini (Conjecture 2). Cette conjecture est à présent démontrée (comme un cas particulier de [HP16, Corollary 1.13]) :

Théorème 7 (Hindry-Pacheco)**.** *Fixons un corps de fonctions $K = \mathbb{F}_q(C)$. Soit $\mathscr{E}\ell\ell_{/K}$ la famille de toutes les courbes elliptiques sur K. On suppose que $Ш(E/K)$ est fini pour toute $E \in \mathscr{E}\ell\ell_{/K}$. Alors*

$$0 \leqslant \liminf_{E \in \mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) \leqslant \limsup_{E \in \mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) \leqslant 1. \tag{12}$$

Nous remarquons à nouveau que l'hypothèse de finitude du groupe de Tate-Shafarevich $Ш(E/K)$ équivaut à supposer que E/K satisfait à la conjecture de Birch et Swinnerton-Dyer (voir [KT03]). La majoration dans (12) est démontrée par des méthodes analytiques selon les grandes lignes que l'on a esquissées dans la section précédente : elle suit d'une majoration de la valeur spéciale $L^*(E/K, 1)$ de la fonction L associée à E/K (voir [HP16, Theorem 7.5]). La preuve de la minoration dans (12) est plus délicate :

– En employant les méthodes analytiques, on n'obtient qu'une minoration « faible ». Dans le cas des courbes elliptiques, Hindry et Pacheco (voir [HP16, Lemma 7.1]) montrent que, si le groupe de Tate-Shafarevich est fini, on a

$$-5 \leqslant \liminf_{\substack{E \in \mathscr{E}\ell\ell_{/K} \\ H(E/K) \to \infty}} \mathfrak{Bs}(E/K).$$

– Un habile argument diophantien permet en fait de démontrer une minoration de $\mathrm{Reg}(E/K)$ (voir [HP16, Proposition 7.6]) qui implique que

$$0 \leqslant \liminf_{\substack{E \in \mathscr{E}\ell\ell_{/K} \\ H(E/K) \to \infty}} \mathfrak{Bs}(E/K).$$

Sous cette dernière forme, la minoration est conditionnelle à la finitude de $Ш(E/K)$ (car la définition de $\mathfrak{Bs}(E/K)$ l'est), mais il s'agit bien d'une minoration inconditionnelle de $\mathrm{Reg}(E/K)$ en termes de la hauteur $H(E/K)$.

En d'autres termes, le Théorème 7 démontre la Conjecture 2 (conditionnellement à la finitude des groupes de Tate-Shafarevich). En outre, Hindry et Pacheco explicitent un exemple inconditionnel pour lequel la majoration dans (12) est atteinte (voir [HP16, Theorem 7.12]).

Théorème 8 (Hindry-Pacheco)**.** *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \geqslant 2$ premier à p, soit E_d la courbe elliptique définie sur K donnée en coordonnées affines par*

$$E_d : \qquad Y^2 + XY = X^3 - t^d.$$

Le groupe de Tate-Shafarevich $Ш(E_d/K)$ est fini (donc E_d/K satisfait la conjecture de Birch et Swinnerton-Dyer). De plus, lorsque $d \to \infty$, le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ a une limite et

$$\lim_{\substack{\mathrm{pgcd}(d,q)=1 \\ d \to \infty}} \mathfrak{Bs}(E_d/K) = 1.$$

C'est-à-dire que l'on a

$$\log\big(\#Ш(E/K)\cdot \mathrm{Reg}(E_d/K)\big) \sim \log H(E_d/K) \sim \log q\cdot \frac{d}{6} \quad (d\to\infty).$$

Les courbes E_d/K ont été amplement étudiées par Ulmer (dans [Ulm02]) qui a démontré qu'elles satisfont à la conjecture de BSD (voir [Ulm02, Proposition 6.4]) et que le rang de $E_d(K)$ peut être arbitrairement grand lorsque $d\to\infty$ ([Ulm02, Theorem 1.5]). Avec cet exemple, on peut reformuler le Théorème 7 lorsque $K=\mathbb{F}_q(t)$ sous la forme :

$$0 \leqslant \liminf_{E\in\mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) \leqslant \limsup_{E\in\mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) = 1,$$

où $\mathscr{E}\ell\ell_{/K}$ désigne encore la famille de toutes les courbes elliptiques sur K.

Constatons que le Théorème 7 ne donne pas pour autant une réponse définitive quant à la Conjecture 3 : on ne déduit pas de (12) que le ratio de Brauer-Siegel peut *effectivement* être petit (*i.e.* proche de 0). On pourrait être tenté de prédire que les courbes elliptiques sur un corps de fonctions vérifient un analogue complet du théorème de Brauer-Siegel classique (Théorème 4) ; ce que l'on pourrait écrire

$$\lim_{\substack{E\in\mathscr{E}\ell\ell_{/K}\\ H(E/K)\to\infty}} \mathfrak{Bs}(E/K) = 1, \qquad (?)$$

i.e. la « lim inf » et la « lim sup » dans (12) coïncident. À l'heure actuelle, il est loin d'être clair que l'on peut s'attendre à ce que cette égalité soit vraie en général ou si, au contraire, la Conjecture 3 est vraie. Toutefois, plusieurs heuristiques ont été récemment avancées qui suggèrent que la Conjecture 3 est plus proche de la vérité (comparer [Hin07, Conjecture 5.5] et [HP16, §7.5, §7.6]). En particulier, Hindry et Pacheco prédisent que le comportement du ratio de Brauer-Siegel dans les familles de tordues quadratiques d'une courbe elliptique donnée est différent du comportement « générique ». Résumons celles-ci dans le cas plus concret où $K=\mathbb{F}_q(t)$. Soit E/K une courbe elliptique.

1. Comme on l'a déjà mentionné, la présence de zéros de la fonction $\mathcal{L}(E/K,s)$ proches de $s=1$ a une influence sur la taille de la valeur spéciale $L^*(E/K,1)$ et donc sur la taille de $\mathfrak{Bs}(E/K)$ (ce point est discuté en détail dans [HP16, §7.3]). En des termes vagues, si $\mathcal{L}(E/K,s)$ a un zéro très proche de 1 (ou si $\mathcal{L}(E/K,s)$ a un paquet de zéros proches de 1) alors on peut s'attendre à ce que $L^*(E/K,1)$ soit très petite. Au contraire, si les zéros de $\mathcal{L}(E/K,s)$ sont suffisamment « bien espacés », il semble raisonnable de penser que $L^*(E/K,1)$ n'est pas trop petite.

   Ces attentes vagues sont quantifiées dans [HP16, Lemma 7.7] : les auteurs isolent la contribution des « petits zéros » à la taille de $L^*(E/K,1)$. Ceci suggère d'étudier la distribution des zéros de $\mathcal{L}(E/K,s)$ sur la droite $\mathrm{Re}(s)=1$. À ce propos, Michel a démontré (voir [Mic99]) que les zéros de $\mathcal{L}(E/K,s)$ sont « bien distribués » pour « la plupart » des courbes elliptiques E/K. Par suite, pour « la plupart » des courbes elliptiques, le ratio de Brauer-Siegel devrait être relativement gros (*i.e.* assez loin de 0). Pour autant, ceci n'exclut pas la possibilité qu'il existe une famille infinie de courbes elliptiques sur K dont les fonctions L ont des zéros « mal distribués » et donc un ratio de Brauer-Siegel plus petit.

2. Si E/K n'est pas constante, pour tout polynôme $D\in\mathbb{F}_q[t]$ sans facteurs carrés, on peut considérer la tordue quadratique $E^{(D)}/K$ de E par D. En supposant la conjecture de Birch et Swinnerton-Dyer, un analogue du théorème de Waldspurger relie la valeur $\mathcal{L}(E/K,1)$ de $\mathcal{L}(E/K,s)$ en $s=1$ avec le D-ième coefficient de Fourier $c_E(D)$ d'une certaine forme modulaire de poids 3/2 (notons la g_E).

   Lorsque le rang de $E^{(D)}$ est nul, on a $\mathcal{L}(E/K,1)=L^*(E/K,1)$ et la majoration de $\mathfrak{Bs}(E^{(D)}/K)$ suit de la conjecture de Ramanujan pour les coefficients de Fourier de g_E (cette conjecture est démontrée dans ce cas) : on a $|c_E(D)| \ll_\varepsilon (q^{\deg D})^{1/4+\varepsilon}$. Mais, si il existe une minoration $\mathfrak{Bs}(E^{(D)}/K)$ par une quantité strictement positive, celle-ci impliquerait que les coefficients de Fourier $c_E(D)$ non nuls sont « repoussés loin de 0 ». Ce qui semble improbable car l'on s'attend plutôt à ce que les coefficients de Fourier d'une forme modulaire soient équirépartis dans l'intervalle dans lequel ils se trouvent (*i.e.* à ce qu'ils satisfassent une sorte de « loi de Sato-Tate »).

3. Si maintenant E/K est constante, on peut fixer une courbe elliptique E_0 sur $\mathbb{F}_q$ telle que $E=E_0\times_{\mathbb{F}_q} K$. La conjecture de Birch et Swinnerton-Dyer a été, dans ce cas, démontrée par Milne (voir [Mil68, Theorem 3]) à la fois pour E et pour ses tordues quadratiques $E^{(D)}$ par des polynômes $D\in\mathbb{F}_q[t]$ sans facteurs carrés. Écrivons $a_E := q+1-\#E_0(\mathbb{F}_q)\in\mathbb{Z}$, on désigne par $F_D(T)$ le numérateur de la fonction zeta de la courbe hyperelliptique $C_D : y^2=D(x)$ et par $g_D := g(C_D) = \lfloor(\deg D-1)/2\rfloor$ le

genre de C_D. Milne a donné une expression de la valeur spéciale $L^*(E^{(D)}/K,1)$ en fonction de $F_D(T)$ et a_E. Un calcul rapide conduit à l'expression ci-dessous du ratio de Brauer-Siegel $\mathfrak{Bs}(E^{(D)}/K)$ (*cf.*[HP16, Proposition 7.16]) :

$$\mathfrak{Bs}(E^{(D)}/K) = \frac{2\log|G_D^*(a_E)|}{g_D\cdot\log q} + o(1) \qquad (\deg D\to\infty),$$

où $G_D^*(T)\in\mathbb{Z}[T]$ peut être explicitement calculé à partir de $F_D(T)$. En outre, on a $G_D^*(a_E)\neq 0$, $\deg G_D^* = g_D - o\big(g_D\big)$ et toutes les racines de $G_D^*(T)$ sont réelles et se trouvent dans l'intervalle $[-2\sqrt{q},2\sqrt{q}]$. Si E_0 parcourt l'ensemble de toutes les courbes elliptiques définies sur $\mathbb{F}_q$, l'entier a_E prend presque toutes les valeurs entières entre $-2\sqrt{q}$ et $2\sqrt{q}$ (voir [WM71]). Lorsque $\deg D$ devient grand, $G_D^*(T)$ a de plus en plus de racines dans l'intervalle $[-2\sqrt{q},2\sqrt{q}]$ où se trouve a_E : il semble alors raisonnable que $|G_D^*(a_E)|\in\mathbb{N}^*$ peut être « très petit » devant g_D.

Il convient de noter la construction « inverse » : étant donné un entier $a\in[-2\sqrt{q},2\sqrt{q}]$, il est facile de construire une suite de polynômes $H_n(T)\in\mathbb{Z}[T]$ ($n\in\mathbb{N}^*$) de degrés croissants avec les propriétés suivantes : toutes les racines de $H_n(T)$ sont réelles et se trouvent dans l'intervalle $[-2\sqrt{q},2\sqrt{q}]$, $H_n(T)$ ne s'annule pas en a et $\log|H_n(a)|/\deg H_n$ est arbitrairement petit. Cependant, nous ne savons pas démontrer que de tels polynômes $H_n(T)$ sont effectivement des « polynômes $G_D^*(T)$ » associés, comme ci-dessus, aux numérateurs des fonctions zeta des courbes hyperelliptiques C_D.

Il va sans dire que la découverte d'une famille explicite de courbes elliptiques $E/\mathbb{F}_q(t)$ dont le ratio de Brauer-Siegel a une limite $\alpha<1$ (même conditionnellement à la conjecture de BSD) constituerait une avancée majeure. De même qu'une preuve que le ratio de Brauer-Siegel, au contraire, tend toujours vers 1 (ce qui mettrait en défaut la Conjecture 3). Peut-être qu'une étude du ratio de Brauer-Siegel « en moyenne » permettrait de donner une idée du comportement typique de $\mathfrak{Bs}(E/K)$; sauf s'il y a tellement peu de courbes elliptiques dont le ratio de Brauer-Siegel est petit, que leur présence ne peut être détectée par une majoration en moyenne trop grossière.

Comme on le constate, cette question et ses variantes sont loin d'être résolues et nous entendons continuer à explorer ce cercle de problèmes.

Résultats nouveaux

Nous présentons maintenant notre contribution à l'étude du ratio de Brauer-Siegel. Nous avons séparé cette section en trois parties. La première contient notre théorème principal, lié au ratio de Brauer-Siegel. La seconde partie expose des résultats auxiliaires importants, utilisés dans la preuve mais dont l'intérêt dépasse sûrement la présente étude. Dans la troisième partie, nous passons en revue deux autres résultats, que l'on n'a pas inclus dans ce manuscrit.

Théorème principal

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p\geqslant 5$. On note $K=\mathbb{F}_q(t)$ le corps des fractions rationnelles sur $\mathbb{F}_q$. Considérons l'une des cinq familles de courbes elliptiques sur K ci-dessous :

($\mathscr{E}_1$) pour tout entier $d\in\mathbb{N}^*$ premier à q, soit E_d/K la courbe elliptique donnée par l'équation affine

$$E_d : \quad Y^2 = X(X+1)(X+t^d). \tag{13}$$

On appellera E_d une « courbe de Legendre » car tous ses points de 2-torsion sont K-rationnels. Elle a déjà été amplement étudiée par Ulmer, Conceição et Hall (voir [Ulm14a], [CHU14] et[Ulm14b]).

($\mathscr{E}_2$) pour tout entier $d\in\mathbb{N}^*$ premier à q, soit H_d/K la courbe elliptique d'équation affine

$$H_d : \quad Y^2 + 3t^dXY + Y = X^3. \tag{14}$$

H_d sera appelée « courbe Hessienne » car elle est munie d'un point K-rationnel de 3-torsion.

($\mathscr{E}_3$) pour tout entier $d\in\mathbb{N}^*$ premier à q, soit E_d/K la courbe donnée en coordonnées affines par

$$E_d : \quad Y^2 + XY + t^dY = X^3 + t^dX^2. \tag{15}$$

Cette courbe E_d dispose d'un point K-rationnel de 4-torsion (et a également été étudiée par Ulmer dans [Ulm13]).

($\mathscr{E}_4$) pour tout entier $d \in \mathbb{N}^*$ premier à q, soit E_d/K la courbe elliptique dont un modèle affine est

$$E_d : \quad Y^2 + XY - t^d Y = X^3. \tag{16}$$

Mentionnons à propos de E_d les travaux de Davis et Occhipinti (voir [DO14]), les auteurs y produisent des points rationnels explicites sur E_d pour certaines valeurs de d.

($\mathscr{E}_5$) pour tout entier $d \in \mathbb{N}^*$ premier à q, soit $B_{1/2,d}/K$ la courbe donnée en coordonnées affines par

$$B_{1/2,d} : \quad Y^2 + 2t^d XY - 4t^{2d} Y = X^3 - 6t^d X^2 + 8t^{2d} X. \tag{17}$$

Cette courbe elliptique est mentionnée par Berger dans [Ber08, §4.3, Example 6].

Dans cette thèse, nous montrons que le ratio de Brauer-Siegel des courbes elliptiques E/K prises dans l'une des familles ci-dessus admet une limite et que celle-ci vaut 1 (inconditionnellement). Nous consignons ces résultats en un théorème :

Théorème 9. *Soit $\mathscr{E}_i$ ($i \in \{1,2,3,4,5\}$) l'une des familles de courbes elliptiques ci-dessus.*

- *Pour toute courbe elliptique $E \in \mathscr{E}_i$, la conjecture de Birch et Swinnerton-Dyer est vraie pour E/K. En particulier, $Ш(E/K)$ est fini et le ratio de Brauer-Siegel $\mathfrak{Bs}(E/K)$ a un sens.*
- *Lorsque $H(E/K) \to +\infty$ avec $E \in \mathscr{E}_i$, on a*

$$\mathfrak{Bs}(E/K) \xrightarrow[\substack{E\in\mathscr{E}_i \\ H(E/K)\to\infty}]{} 1.$$

En d'autres termes, pour tout $\varepsilon > 0$, il existe des constantes telles que

$$\forall E \in \mathscr{E}_i, \quad H(E/K)^{1-\varepsilon} \ll_\varepsilon \#Ш(E/K) \cdot \mathrm{Reg}(E/K) \ll_\varepsilon H(E/K)^{1+\varepsilon}.$$

Ou encore, lorsque $E \in \mathscr{E}_i$, on a

$$\log\big(\#Ш(E/K) \cdot \mathrm{Reg}(E/K)\big) \sim \log H(E/K) \quad \textit{quand } H(E/K) \to \infty.$$

Comme on peut le constater, chaque famille $\mathscr{E}_i$ ci-dessus est naturellement indexée par les entiers $d \in \mathbb{N}^*$ (premiers à q) et on montre qu'il existe une constante c_i (donnée ci-dessous) telle que, pour toute courbe E_d dans la i-ième famille $\mathscr{E}_i$, on a

$$\log\big(\#Ш(E_d/K) \cdot \mathrm{Reg}(E_d/K)\big) \sim \log H(E_d/K) \sim \frac{\log q}{c_i} \cdot d \quad \text{quand } d \to +\infty.$$

Avec

$$c_1 = 2, \quad c_2 = 1, \quad c_3 = 2, \quad c_4 = 3, \quad c_5 = 2.$$

Ce théorème est une combinaison des Théorème 4.4.1, Théorème 5.4.1, Théorème 6.4.1, Théorème 7.4.4 et Théorème 8.4.2.

Les 5 familles de courbes elliptiques définies ci-dessus s'ajoutent donc à l'exemple de [HP16, Theorem 7.12] pour former un total de six familles de courbes elliptiques (définies sur $\mathbb{F}_q(t)$) pour lesquelles on sait inconditionnellement montrer que le ratio de Brauer-Siegel a une limite. Dans les six cas, cette limite vaut 1 (on dira que ces familles vérifient un analogue complet du théorème de Brauer-Siegel). Nous espérons qu'à la lecture des preuves, le lecteur sera convaincu que notre méthode permettrait d'étudier le ratio de Brauer-Siegel de plusieurs autres familles.

Le Théorème 9 pourrait être vu comme autant d'indices suggérant que, dans le Théorème 7, la « lim inf » et la « lim sup » coïncident et sont toujours égales à 1. Nous préférons cependant penser que les courbes elliptiques que l'on étudie font partie de la majorité (conjecturale) pour lesquelles un analogue complet du théorème de Brauer-Siegel est vrai. Peut-être donne-t-il plus d'indications quant aux familles à *ne pas étudier* si l'on cherche des courbes elliptiques avec un ratio de Brauer-Siegel « petit » (conjecturalement, une famille « fine » parmi toutes les courbes elliptiques).

Comme on l'a expliqué ci-avant, pour qu'une courbe elliptique E/K ait un « gros » ratio de Brauer-Siegel (c'est-à-dire un ratio de Brauer-Siegel proche de 1), il est nécessaire que les zéros de sa fonction L soient suffisamment « bien distribués ». En d'autres termes, la partie centrale de la preuve est l'obtention d'une *minoration* de $\mathfrak{Bs}(E/K)$: nous montrons à cet effet que les valeurs spéciales $L^*(E/K,1)$ des courbes elliptiques $E \in \mathscr{E}_i$ ne deviennent jamais trop petites. L'étude directe de la distribution des zéros de $L(E/K,T)$ est, en général, très délicate. Nous avons donc préféré suivre une

approche « p-adique », que nous esquissons rapidement. Supposons avoir exprimé la valeur spéciale $L^*(E/K,1) = L_E^*$ d'une courbe elliptique E/K sous la forme d'un produit

$$L_E^* = \prod_{m\in\mathcal{M}} \left(1 - \frac{\omega_m}{q^{u_m}}\right),$$

où les ω_m sont certains entiers algébriques de valeur absolue q, $u_m \in \mathbb{N}^*$ et m parcourt un ensemble d'indices $\mathcal{M}$ vérifiant $\#\mathcal{M} = o\big(\log H(E/K)\big)$. Nous démontrons une minoration de tels produits L_E^* en formalisant l'idée suivante. Par construction, le produit L_E^* est un élément non nul de $\mathbb{Z}[q^{-1}]$: en tant que tel, il peut s'écrire

$$L_E^* = \frac{(\text{entier})}{q^{W_E}}, \tag{18}$$

pour un certain exposant $W_E \in \mathbb{N}$. Pour donner une minoration de $\log|L_E^*|$ en termes de $H(E/K)$, il s'agit de majorer le plus finement possible l'exposant W_E du dénominateur. Comme les ω_m sont des entiers algébriques, multiplier le facteur $(1-\omega_m/q^{u_m})$ par q^{u_m} produit un entier algébrique dont la norme est un entier. Par suite, le produit $q^{\sum u_m}\cdot L_E^*$ est un entier : on voit donc que $0 \leqslant W_E \leqslant \sum u_m$.

À présent, imaginons que certains ω_m soient « très divisibles » par q. Nul besoin alors de multiplier $(1-\omega_m/q^{u_m})$ par q^{u_m} pour obtenir un entier algébrique : une plus petite puissance de q y suffit. L'exposant W_E du dénominateur de L_E^* peut ainsi être diminué d'autant. En prenant en compte ces « simplifications » dans les facteurs de L_E^*, nous parvenons à démontrer que $W_E = o\big(\log H(E/K)\big)$ pour les cinq familles $\mathscr{E}_i$. Ce qui est suffisant pour déduire que

$$\log|L_E^*| \geqslant -o\big(\log H(E/K)\big).$$

Résultats auxiliaires

Afin de démontrer le Théorème 9 ci-dessus, nous aurons besoin d'un certain nombre de résultats intermédiaires. L'intérêt de ceux-ci dépasse sûrement la simple étude du ratio de Brauer-Siegel. Résumons les théorèmes nouveaux les plus significatifs démontrés dans cette thèse.

Soit $\mathbb{F}_q$ un corps fini de caractéristique impaire. Pour tout $b \in \mathbb{F}_q \smallsetminus \{1,-1\}$ et tout caractère non trivial $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$, définissons une *somme de Legendre* par

$$\boldsymbol{S}_q(\chi;b) := -\sum_{x\in\mathbb{F}_q} \chi(x)\cdot\mu\big(x^2+2b\cdot x+1\big),$$

où $\mu : \mathbb{F}_q^\times \to \{\pm 1\}$ est l'unique caractère non trivial d'ordre 2 sur $\mathbb{F}_q^\times$. Ces sommes ont été introduites par Evans dans [Eva86] mais il semble y avoir très peu de résultats à leur propos dans la littérature. Pour calculer les fonctions L de certaines courbes elliptiques, nous avions besoin de savoir que les sommes de Legendre vérifient une « relation de Hasse-Davenport » et l'« hypothèse de Riemann ». Ce que nous avons démontré. Pour énoncer le théorème obtenu, rappelons la construction suivante : pour tout caractère non trivial $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ et toute extension finie $\mathbb{F}_{q^n}/\mathbb{F}_q$, on définit un caractère $\chi^{(n)}$ sur $\mathbb{F}_{q^n}^\times$ par

$$\forall x \in \mathbb{F}_{q^n}^\times, \quad \chi^{(n)}(x) = \chi\circ\mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x),$$

où $\mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$ désigne la norme.

Théorème 10. *Soit $b \in \mathbb{F}_q \smallsetminus \{-1,1\}$ et un caractère non trivial $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$. Il existe deux entiers algébriques $\alpha_b(\chi)$ et $\beta_b(\chi)$ (qui ne dépendent que de b et de χ) tels que*

- $\boldsymbol{S}_q(\chi,b) = \alpha_b(\chi)+\beta_b(\chi)$ *et* $\alpha_b(\chi)\cdot\beta_b(\chi) = q$,
- *Pour toute extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\boldsymbol{S}_{q^n}(\chi^{(n)},b) = \alpha_b(\chi)^n+\beta_b(\chi)^n$ (« relation de Hasse-Davenport »),*
- *Dans tout plongement complexe, $\alpha_b(\chi)$ et $\beta_b(\chi)$ sont de module $\sqrt{q}$ (« hypothèse de Riemann »).*

Voir le Théorème 2.2.21 et le Corollaire 2.3.5. Notons que, pour $b \in \mathbb{F}_q \smallsetminus \{-1,1\}$ donné, les sommes de Legendre apparaissent naturellement dans la fonction zeta de la courbe hyperelliptique D, définie sur $\mathbb{F}_q$ par l'équation affine :

$$D: \qquad y^2 = x^{2(q-1)} + 2b\cdot x^{q-1} + 1.$$

En effet, l'action des racines $(q-1)$-ièmes de l'unité sur D (donnée par $(x,y)\mapsto(\zeta\cdot x,y)$ pour $\zeta\in\mu_{q-1}$) « découpe » la cohomologie de D en sous-espaces de dimension 2 sur lesquel le Frobenius $x\mapsto x^q$ agit avec trace $\boldsymbol{S}_q(\chi;b)$. La lectrice trouvera plus de détails sur ce point au Théorème 2.3.4.

Comme on l'a mentionné à plusieurs reprises dans cette introduction, le ratio de Brauer-Siegel est intimement lié aux valeurs spéciales des fonctions L. Pour expliciter la limite du ratio de Brauer-Siegel des familles énumérées dans le Théorème 9, nous avons calculé explicitement les fonctions L correspondantes. Avant d'énoncer les résultats de ces calculs, mettons en place quelques notations. Soit $\mathbb{F}_q$ un corps fini de caractéristique impaire p et $d \geqslant 2$ un entier premier à q. Il y a une action naturelle de q sur $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ par multiplication : on note $\mathcal{O}'_q(d) = (\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\})/\langle q \bmod d\rangle$ l'ensemble des orbites.

Une fois pour toutes, fixons un idéal premier $\overline{\mathfrak{P}}$ de $\overline{\mathbb{Z}}$ au-dessus de p : la réduction modulo $\overline{\mathfrak{P}}$ induit un isomorphisme entre le groupe $\mu'_p \subset \overline{\mathbb{Q}}^\times$ des racines de l'unité d'ordre premier à p et le groupe multiplicatif $\overline{\mathbb{F}_q}^\times$. Soit alors $\mathbf{t} : \overline{\mathbb{F}_q}^\times \simeq (\overline{\mathbb{Z}}/\overline{\mathfrak{P}})^\times \to \mu'_p \subset \overline{\mathbb{Q}}^\times$ l'inverse de cet isomorphisme ($\mathbf{t}$ est appelé le caractère de Teichmüller). On notera également $\mathbf{t}$ la restriction du caractère de Teichmüller à tout sous-corps de $\overline{\mathbb{F}_q}$. À chaque entier $d \geqslant 2$ premier à q, on associe un ensemble (indexé par $a \in [\![1, d-1]\!]$ ou $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$) de caractères $\mathbf{t}_a : \mathbb{F}_{q^{u(a)}}^\times \to \overline{\mathbb{Q}}^\times$ définis sur diverses extensions finies $\mathbb{F}_{q^{u(a)}}$ de $\mathbb{F}_q$, et dont l'ordre divise d. Plus précisément, pour tout $a \in [\![1, d-1]\!]$, soit $u(a) = \min\left\{n \in \mathbb{N}^* \;\middle|\; q^n a \equiv a \bmod d\right\} = \mathrm{ord}^\times\left(q \bmod (d/\operatorname{pgcd}(d,a))\right)$ et

$$\mathbf{t}_a : x \in \mathbb{F}_{q^{u(a)}}^\times \mapsto \mathbf{t}(x)^{(q^{u(a)}-1)a/d} \in \overline{\mathbb{Q}}^\times.$$

Dans les résultats ci-dessous, le lecteur intéressé uniquement par le cas où $d \mid q-1$ peut remplacer « $m \in \mathcal{O}'_q(d)$ » par « $a = m \in [\![1, d-1]\!]$ », $u(a)$ par 1 pour tout $a \in [\![1, d-1]\!]$, et $\mathbf{t}_a$ par les puissances χ^a d'un caractère fixé $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ d'ordre exactement d.

À l'aide de ces caractères, nous avons calculé explicitement les fonctions L des courbes elliptiques des familles $\mathscr{E}_i$ définies ci-dessus. Pour les cinq prochains théorèmes, on fixe un corps fini $\mathbb{F}_q$ de caractéristique $p \geqslant 5$ et on note $K = \mathbb{F}_q(t)$.

Premièrement, nous obtenons les fonctions L des « courbes Hessiennes » de la famille $\mathscr{E}_2$ (voir Théorème 5.2.1).

Théorème 11. *Pour tout entier $d \geqslant 2$ premier à q, soit H_d la « courbe elliptique Hessienne » définie sur K par l'équation* (14)*. La fonction L de H_d/K s'écrit sous la forme :*

$$L\big(H_d/K, T\big) = \prod_{m \in \mathcal{O}_q^{(3)}(3d)} \Big(1 - \mathbf{J}_m \cdot T^{u(m)}\Big)$$

où $\mathcal{O}_q^{(3)}(3d)$ désigne l'ensemble d'orbites de $\mathbb{Z}/3d\mathbb{Z}\smallsetminus\{0, d, 2d\}$ sous l'action de q par multiplication et, pour toute orbite $m \in \mathcal{O}_q^{(3)}(3d)$, $\mathbf{J}_m$ désigne la somme

$$\mathbf{J}_m = \mathbf{t}_a(27) \cdot \mathbf{j}_{q^{u(a)}}(\mathbf{t}_a, \mathbf{t}_a, \mathbf{t}_a) = \mathbf{t}_a(27) \cdot \sum_{\substack{x,y,z \in \mathbb{F}_{q^{u(a)}} \\ x+y+z=1}} \mathbf{t}_a(x)\mathbf{t}_a(y)\mathbf{t}_a(z),$$

pour tout choix de représentant $a \in \mathbb{Z}/d\mathbb{Z}$ de l'orbite m (à une racine de l'unité près, $\mathbf{J}_m$ est une somme de Jacobi). Noter que les caractères $\mathbf{t}_a$ utilisés ici sont ceux que l'on associe à $3d$ et non à d.

Avec des techniques très similaires à celles de [CHU14, §3], nous calculons également les fonctions L des courbes de la famille $\mathscr{E}_3$, qui ont un point de 4-torsion (voir Théorème 6.2.1).

Théorème 12. *Pour tout entier $d \geqslant 2$ premier à q, soit E_d la courbe elliptique définie sur K par l'équation* (15)*. La fonction L de E_d/K s'écrit sous la forme :*

$$L(E_d/K, T) = \prod_{m \in \mathcal{O}_q^{(2)}(d)} (1 - {\mathbf{J}'_m}^2 \cdot T^{u(m)})$$

où $\mathcal{O}_q^{(2)}(d)$ désigne l'ensemble des orbites de $\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, (d/2)\}$ sous l'action de q par multiplication (on retire l'orbite $\{d/2\}$ si d est pair) et, pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$, $\mathbf{J}'_m$ est la somme de Jacobi

$$\mathbf{J}'_m = \mathbf{j}_{q^{u(a)}}(\mathbf{t}_a, \mathbf{t}_a) = -\sum_{\substack{x,y,z \in \mathbb{F}_{q^{u(a)}} \\ x+y=1}} \mathbf{t}_a(x)\mathbf{t}_a(y),$$

pour tout choix de représentant $a \in \mathbb{Z}/d\mathbb{Z}$ de m.

Ensuite, pour la famille $\mathscr{E}_4$ de courbes elliptiques étudiée au Chapitre 7, nous obtenons le théorème ci-dessous (voir Théorème 7.2.1).

Théorème 13. *Pour tout entier $d \geqslant 2$ premier à q, soit E_d la courbe elliptique définie sur K par l'équation* (16)*. La fonction L de E_d/K*

$$L\big(E_d/K, T\big) = \prod_{m \in \mathcal{O}_q^{(3)}(d)} \Big(1 - \mathbf{J}_m \cdot T^{u(m)}\Big).$$

où $\mathcal{O}_q^{(3)}(d)$ désigne l'ensemble des orbites de $\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, (d/3, 2d/3)\}$ sous l'action de q par multiplication (on retire les orbites $\{d/3\}$ et $\{2d/3\}$ si $3 \mid d$) et, pour toute orbite $m \in \mathcal{O}_q^{(3)}(d)$, $\mathbf{J}_m$ est une somme de Jacobi « de dimension 2 » :

$$\mathbf{J}_m = \mathbf{j}_{q^{u(a)}}(\mathbf{t}_a, \mathbf{t}_a, \mathbf{t}_a) = \sum_{\substack{x,y,z \in \mathbb{F}_{q^{u(a)}} \\ x+y+z=1}} \mathbf{t}_a(x)\mathbf{t}_a(y)\mathbf{t}_a(z),$$

pour tout choix de représentant $a \in \mathbb{Z}/d\mathbb{Z}$ de m.

Enfin, en ce qui concerne la famille $\mathscr{E}_5$ (empruntée à [Ber08, §4.3, Example 6]), nous obtenons dans un premier temps une expression un peu plus générale que nécessaire pour la fonction L (voir Théorème 8.2.1) :

Théorème 14. *Soit $a \in \mathbb{F}_q \smallsetminus \{0, 1\}$ et $d \geqslant 2$ un entier premier à q. On considère $B_{a,d}$ la courbe elliptique définie sur $K = \mathbb{F}_q(t)$ en coordonnées affines par*

$$B_{a,d} : \quad Y^2 + t^d XY - at^{2d}Y = X^3 - (a+1)t^d X^2 + at^{2d}X. \tag{19}$$

La fonction L de $B_{a,d}/K$ s'écrit :

$$L\big(B_{a,d}/K, T\big) = (1 - qT) \cdot \prod_{m \in \mathcal{O}_q^{(2)}(d)} \Big(1 - \mathbf{J}'_m \cdot \boldsymbol{S}_m \cdot T^{u(m)} + {\mathbf{J}'_m}^2 \cdot q^{u(m)} \cdot T^{2u(m)}\Big),$$

où, comme ci-avant, $\mathcal{O}_q^{(2)}(d)$ est l'ensemble des orbites de $\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, (d/2)\}$ sous l'action de q par multiplication (on retire l'orbite $\{d/2\}$ si d est pair) et, pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$ et tout choix de représentant $i \in \mathbb{Z}/d\mathbb{Z}$ de m, $\mathbf{J}'_m$ est (à une racine de l'unité près) une somme de Jacobi :

$$\mathbf{J}'_m = \mathbf{t}_i(-1) \cdot \mathbf{j}_{q^{u(i)}}(\mathbf{t}_i, \mathbf{t}_i) = -\mathbf{t}_i(-1) \cdot \sum_{\substack{x,y \in \mathbb{F}_{q^{u(i)}} \\ x+y=1}} \mathbf{t}_i(x)\mathbf{t}_i(y),$$

et $\boldsymbol{S}_m$ est une somme de Legendre :

$$\boldsymbol{S}_m := \boldsymbol{S}_{q^{u(i)}}(\mathbf{t}_i; 1-2a) = -\sum_{x \in \mathbb{F}_{q^{u(i)}}} \mathbf{t}_i(x) \cdot \mu\left(x^2 + 2(1-2a) \cdot x + 1\right).$$

Dans un second temps, on spécialise le théorème ci-dessus au cas où $a = 1/2 \in \mathbb{F}_q$ et d est impair : l'expression de la fonction $L(B_{1/2,d}/K, T)$ dans le théorème ci-dessus se simplifie quelque peu et donne (voir Théorème 8.3.2) :

Théorème 15. *Soit $d \geqslant 2$ un entier* impair *et premier à q. Soit $B_{1/2,d}$ la courbe elliptique définie sur $K = \mathbb{F}_q(t)$ par l'équation* (17) *:*

$$B_{1/2,d} : \quad Y^2 + 2t^d XY - 4t^{2d}Y = X^3 - 6t^d X^2 + 8t^{2d}X.$$

Alors la fonction L de $B_{1/2,d}/K$ s'écrit sous la forme :

$$L\big(B_{1/2,d}/K, T\big) = (1 - qT) \cdot \prod_{n \in \mathcal{O}_q^{(2)}(2d)} \Big(1 - \mathbf{J}'_n \cdot T^{u(n)}\Big),$$

où $\mathcal{O}_q^{(2)}(2d)$ est l'ensemble des orbites de $\mathbb{Z}/2d\mathbb{Z} \smallsetminus \{0, d\}$ sous l'action de q par multiplication et, pour toute orbite $n \in \mathcal{O}_q^{(2)}(2d)$ et tout choix de représentant $i \in \mathbb{Z}/2d\mathbb{Z}$ de n, $\mathbf{J}'_n$ est (à une racine de l'unité près) une somme de Jacobi « de dimension 2 » :

$$\mathbf{J}'_n := \mathbf{t}_i(-4) \cdot \mathbf{j}_{q^{u(i)}}(\mathbf{t}_i, \mathbf{t}_i, \mathbf{t}_i^2) = \mathbf{t}_i(-4) \cdot \sum_{\substack{x,y,z \in \mathbb{F}_{q^{u(i)}} \\ x+y+z=1}} \mathbf{t}_i(x)\mathbf{t}_i(y)\mathbf{t}_i(z)^2.$$

Noter qu'ici les caractères $\mathbf{t}_i$ ($i \in [\![1, 2d-1]\!]$) sont ceux que l'on associe à $2d$ (et non à d).

Nous espérons que ces calculs peuvent être utiles à d'autres fins. C'est pourquoi nous avons essayé de garder les hypothèses aussi faibles que possible : nous supposons uniquement que d est premier à q, là où beaucoup d'auteurs se placent dans le cas où $d \mid q-1$. Nous mentionnons ici que nous avons également prouvé un résultat de « rang non borné » concernant les courbes $B_{a,d}$ de la famille $\mathscr{E}_5$ (voir Corollaire 8.3.13) :

Théorème 16. *Dans la famille des courbes elliptiques $B_{a,d}/K$ définies par* (17) *(avec $d \geqslant 2$ parcourant les entiers premiers à q et $a \in \mathbb{F}_q \smallsetminus \{0,1\}$), le rang $r_{a,d} = \operatorname{rang} B_{a,d}(K)$ n'est pas borné :*

$$\limsup_{\substack{\gcd(d,q)=1 \\ a\in\mathbb{F}_q\smallsetminus\{0,1\}}} \operatorname{rang}\, B_{a,d}(K) = \limsup_{\gcd(d,q)=1} \operatorname{rang}\, B_{1/2,d}(K) = +\infty.$$

Comme il est noté dans [Ber08, §4.3, Example 6], ce résultat sur le rang de $B_{a,d}(K)$ n'est pas une conséquence du théorème général de Ulmer [Ulm07b, Theorem 4.7].

Le résultat central qui sous-tend le Théorème 9 et notre principal théorème technique est une minoration des valeurs spéciales de fonctions L satisfaisant certaines hypothèses (voir Théorème 3.2.2). Nous ne rentrons pas dans les détails ici mais donnons un aperçu du fonctionnement de ce théorème. Fixons $\mathbb{F}_q$ un corps fini de caractéristique p impaire et $K = \mathbb{F}_q(t)$. Soit $d \geqslant 2$ un entier premier à q. La plupart des fonctions L explicitées ci-dessus peuvent s'écrire sous la forme schématique suivante :

$$L_d(T) = \prod_{m\in\mathcal{O}'_q(d)} \left(1 - \omega_m \cdot T^{u(m)}\right) \in \mathbb{Z}[T],$$

où $\mathcal{O}'_q(d)$ désigne l'ensemble des orbites de $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ sous l'action de q par multiplication et les ω_m sont certains entiers algébriques. Par définition, calculer la valeur spéciale de $L_d(T)$ consiste à l'évaluer en $T = q^{-1}$ une fois qu'on lui a retiré tous ses facteurs qui s'annulent en $T = q^{-1}$ (à un terme entier près, dont le logarithme est positif). Le terme principal qu'il faut minorer peut s'écrire sous la forme d'un produit

$$L_d^* := \prod_{m\in\mathcal{M}} \left(1 - \frac{\omega_m}{q^{u(m)}}\right),$$

où m parcourt un certain ensemble d'orbites $\mathcal{M} \subset \mathcal{O}'_q(d)$. On ajoute maintenant deux hypothèses : on suppose d'abord que ω_m est un entier du corps cyclotomique $\mathbb{Q}(\zeta_{d_m})$ (où $d_m := d/\gcd(d,m)$) et ensuite que la numérotation de $\{\omega_m\}_m$ est « compatible » à l'action du groupe de Galois $\operatorname{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \simeq (\mathbb{Z}/d\mathbb{Z})^\times$ (*i.e.* on suppose que $\sigma_t(\omega_m) = \omega_{t\cdot m}$ si σ_t est l'automorphisme correspondant à $t \in (\mathbb{Z}/d\mathbb{Z})^\times$). Noter que ces deux hypothèses sont satisfaites par les fonctions L des courbes elliptiques des 5 familles $\mathscr{E}_i$. On fixe une fois pour toutes un idéal premier $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$ au-dessus de p et on pose $\mathfrak{p}_m = \mathbb{Q}(\zeta_{d_m}) \cap \overline{\mathfrak{P}}$ pour tout $m \in \mathcal{M}$.

Théorème 17. *Sous ces hypothèses, on a*

$$\log|L_d^*| \gg_q -\sum_{m\in\mathcal{M}} \max\left\{0, u(m) - \frac{\operatorname{ord}_{\mathfrak{p}_m}\omega_m}{[\mathbb{F}_q:\mathbb{F}_p]}\right\} := -W_d. \tag{20}$$

Pour un exposé détaillé de nos hypothèses et un énoncé précis de ce théorème, nous renvoyons à la Section 3.2. Signalons que Shioda a démontré un résultat assez similaire (voir [Shi87, Proposition 2.1]) lorsque ω_m est une somme de Jacobi de « dimension paire ». Nous avons adapté sa preuve pour qu'elle fonctionne avec des ω_m plus généraux.

L'inégalité (20) est vraie dès que la fonction L sous-jacente vérifie nos hypothèses. Qui plus est, on a toujours une minoration « naïve » sur la somme W_d dans le membre de droite de (20) : précisément

$$W_d = \sum_{m\in\mathcal{M}} \max\left\{0, u(m) - \frac{\operatorname{ord}_{\mathfrak{p}_m}\omega_m}{[\mathbb{F}_q:\mathbb{F}_p]}\right\} \leqslant d.$$

La minoration correspondante de $\log|L_d^*|$ ne donne rien d'autre que « la borne de Liouville ». À présent, pour démontrer que le ratio de Brauer-Siegel des courbes elliptiques de l'une des familles $\mathscr{E}_i$ a pour limite 1, nous devons prouver une minoration bien plus fine de $\log|L_d^*|$. Il faut de fait montrer que $W_d = o(d)$ lorsque $d \to \infty$. Une telle relation asymptotique suivrait d'une preuve que, « en moyenne », les termes « $u(m) - \operatorname{ord}_{\mathfrak{p}_m}\omega_m/[\mathbb{F}_q:\mathbb{F}_p]$ » ne sont « pas trop gros ». Pour une donnée générale $\{\omega_m\}_m$, il n'y a pas de raison que ceci soit vrai.

Toutefois, dans le cas où les ω_m sont des sommes de Jacobi (ou des produits de sommes de Jacobi), en utilisant une variante du théorème de Stickelberger pour calculer $\operatorname{ord}_q \omega_m$, nous obtiendrons

une expression assez explicite de W_d. Il s'agira alors d'estimer W_d et de montrer que W_d est négligeable devant d lorsque $d \to \infty$. Pour ce faire, nous aurons besoin d'un cas particulier du résultat d'équidistribution ci-dessous. On note $\{x\} \in [0,1[$ la partie fractionnaire d'un nombre réel x.

Théorème 18. *Soit $I \subset [0,1]$ un intervalle de longueur b et $\mathscr{D} \subset \mathbb{N}^*$ un ensemble infini d'entiers. Supposons donné, pour tout $d \in \mathscr{D}$, un sous-groupe H_d de $G_d = (\mathbb{Z}/d\mathbb{Z})^\times$ tel que $\frac{\#H_d}{\log\log d} \xrightarrow[d\to\infty]{} +\infty$. Alors, lorsque $d \to \infty$ (avec $d \in \mathscr{D}$), on a*

$$\frac{1}{\#G_d}\sum_{g\in G_d}\left| b - \frac{1}{\#H_d}\cdot \#\left\{t \in H_d \;\middle|\; \left\{\tfrac{gt}{d}\right\} \in I\right\}\right| \ll \left(\frac{\log\log d}{\#H_d}\right)^{1/6} = o(1).$$

Pour plus de détails, nous invitons le lecteur à consulter le Théorème 3.4.1 et ses corollaires.

Autres résultats

Nous avons également démontré deux résultats (encore partiels), dont les preuves ne sont pas incluses dans ce manuscrit. Tout d'abord, nous avons calculé les fonctions L des courbes elliptiques d'une autre famille (infinie). On fixe un corps fini $\mathbb{F}_q$ de caractéristique $p \geqslant 5$ et un paramètre $a \in \mathbb{F}_q \smallsetminus \{0,1\}$, pour tout entier d premier à q, soit $F_{a,d}$ la courbe elliptique définie sur $K = \mathbb{F}_q(t)$ par l'équation affine :

$$F_{a,d}: \quad Y^2 + (1-t^d)XY + a^2(t^d - t^{2d})Y = X^3 + (a^2+2a)t^dX^2 + (2a^3+a^2)t^{2d}X + a^4t^{3d}.$$

Le rang de cette courbe est étudié dans [Occ12] : Occhipinti y calcule « semi-explicitement » la fonction L de $F_{a,d}/K$ lorsque d divise $q-1 = \#\mathbb{F}_q^\times$. Il utilise également le théorème de Berger (voir [Ber08]) pour démontrer que $F_{a,d}$ vérifie la conjecture de Birch et Swinnerton-Dyer. Par une méthode différente, et en allégeant l'hypothèse que d divise $q-1$, nous avons pu prouver :

Théorème 19. *Avec les notations introduites ci-avant, pour tout entier d premier à q, la fonction $L(F_{a,d}/K,T)$ est donnée par*

$$L(F_{a,d}/K,T) = (1-qT)\cdot \prod_{m\in\mathcal{O}'_q(d)} \left(1-q^{u(m)}T^{u(m)}\right)\left(1-(\boldsymbol{S}_m^2 - 2q^{u(m)})T^{u(m)} + q^{2u(m)}T^{2u(m)}\right), \quad (21)$$

où $\mathcal{O}'_q(d)$ désigne l'ensemble des orbites de $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ sous l'action de q par multiplication, $u(m)$ est le cardinal de l'orbite m et, pour tout $m \in \mathcal{O}'_q(d)$ et tout choix d'un représentant $i \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ de m, $\boldsymbol{S}_m$ est une somme de Legendre :

$$\boldsymbol{S}_m = -\boldsymbol{S}_{q^{u(i)}}(\mathbf{t}_i; 1-2a) = -\sum_{x\in\mathbb{F}_{q^{u(i)}}} \mathbf{t}_i(x)\cdot\mu\left(x^2 + 2(1-2a)x + 1\right).$$

La relation de Hasse-Davenport et l'hypothèse de Riemann pour les sommes de Legendre assurent l'existence d'entiers algébriques α_m et β_m (pour $m \in \mathcal{O}'_q(d)$) tels que

$$\forall m \in \mathcal{O}'_q(d), \qquad \boldsymbol{S}_m = \alpha_m + \beta_m,\ \alpha_m\cdot\beta_m = q^{u(m)} \text{ et } |\alpha_m| = |\beta_m| = q^{u(m)/2}.$$

Avec ceux-ci, on peut réécrire la fonction L sous une forme plus factorisée :

$$L(F_{a,d}/K,T) = (1-qT)\cdot \prod_{m\in\mathcal{O}'_q(d)} \left(1-q^{u(m)}\cdot T^{u(m)}\right)\left(1-\alpha_m^2\cdot T^{u(m)}\right)\left(1-\beta_m^2\cdot T^{u(m)}\right).$$

La preuve utilise des évaluations de sommes de caractères et repose sur le fait que la courbe $F_{a,d}$ est birationnelle à la courbe $X_d \subset \mathbb{P}^1\times\mathbb{P}^1$ définie sur K et donnée en coordonnées affines par

$$X_{a,d}: \quad \frac{x(x-1)}{x-a} = t^d\cdot\frac{y(y-1)}{y-a}.$$

Il est assez clair sur l'expression (21) que la fonction L s'annule au moins à l'ordre $d = 1 + \#\mathcal{O}'_q(d)$ en $T = q^{-1}$. Par suite, comme $F_{a,d}$ vérifie la conjecture de Birch et Swinnerton-Dyer, le groupe de Mordell-Weil $F_{a,d}(\mathbb{F}_q(t))$ est de rang au moins d. Malheureusement, nous sommes pour l'heure incapables de donner un meilleur encadrement de la valeur spéciale de $L(F_{a,d}/K,T)$ en $T = q^{-1}$ que l'encadrement « trivial » :

$$-6 + o(1) \leqslant \frac{\log L^*(F_{a,d}/K,1)}{\log H(F_{a,d}/K)} \leqslant 0 + o(1) \quad (d\to\infty).$$

En effet, nous n'avons quasiment aucune information sur la distribution des nombres $\boldsymbol{S}_m/q^{u(m)/2}$ dans l'intervalle $[-2,2]$ dans lequel ils sont répartis (de façon équivalente, on ne sait pas comment sont répartis angulairement les nombres $\alpha_m/q^{u(m)/2}$ et $\beta_m/q^{u(m)/2}$ sur le cercle unité).

Suivant une suggestion de Hindry, nous avons aussi entamé l'étude du ratio de Brauer-Siegel pour une famille de tordues quadratiques d'une courbe elliptique constante sur $\mathbb{F}_q(t)$. Plus précisément, le cadre est le suivant : on fixe un corps fini $\mathbb{F}_q$ de caractéristique $p \geqslant 5$ et une courbe elliptique E_0 définie sur $\mathbb{F}_q$, d'équation affine $E_0 :\ y^2 = x^3 + Ax + B$ (avec $A, B \in \mathbb{F}_q$). Dans ce cas, $E := E_0 \times_{\mathbb{F}_q} \mathbb{F}_q(t)$ est une courbe elliptique constante sur $K = \mathbb{F}_q(t)$. Pour tout entier d premier à p, on considère la tordue quadratique $E^{(d)}$ de E par le polynôme $t^d + 1 \in \mathbb{F}_q[t] \subset K$, une équation affine de $E^{(d)}$ est :

$$E^{(d)} :\quad (t^d + 1) \cdot y^2 = x^3 + Ax + B.$$

Alors $E^{(d)}/K$ vérifie la conjecture de Birch et Swinnerton-Dyer (car elle est isotriviale, voir [Mil68, Theorem 3]). Ainsi, d'après [HP16, Corollary 1.13], lorsque $d \to \infty$, on a

$$0 + o(1) \leqslant \mathfrak{Bs}(E^{(d)}/K) \leqslant 1 + o(1).$$

Nous avons prouvé une minoration plus forte de $\mathfrak{Bs}(E^{(d)}/K)$ pour certaines valeurs de d :

Théorème 20. *Soit $\mathscr{D}_{ss} \subset \mathbb{N}^*$ l'ensemble (infini) des entiers $d \geqslant 2$ tels que d divise $q^n + 1$ (pour un certain $n \in \mathbb{N}$). Un tel entier $d \in \mathscr{D}_{ss}$ est parfois appelé* supersingulier pour q *(cf. [SK79]). Avec cette notation, on a :*

$$\lim_{\substack{d \in \mathscr{D}_{ss} \\ d \to \infty}} \mathfrak{Bs}(E^{(d)}/K) = 1.$$

Pour le moment, nous n'avons pas réussi à nous passer de la condition que d est supersingulier pour démontrer ce théorème (nous ne sommes d'ailleurs pas complètement sûrs que la conclusion soit encore vraie si on l'enlève). La preuve repose essentiellement sur trois ingrédients. D'abord, la fonction L de $E^{(d)}/K$ s'exprime aisément en fonction de la fonction zeta, notée $Z_d(T)$, de la courbe hyperelliptique $C_d : y^2 = x^d + 1$. Un calcul de Weil (voir [Wei49]) affirme que les zéros β_j de $Z_d(T)$ sont des racines n-ièmes de sommes de Jacobi. Sous notre hypothèse que $d \in \mathscr{D}_{ss}$, noter que les sommes de Jacobi en question sont réelles. On conclut la preuve par une application du théorème de Baker-Wüstholz (voir [BW93]) aux nombres $\log|1 - \beta_j/q|$, dans l'esprit de [BK10, Theorem 4.1].

Présentation du contenu

Pour conclure ce chapitre, nous présentons la façon dont sont répartis les résultats de ce manuscrit.

Le premier chapitre constitue une introduction générale à l'arithmétique des courbes elliptiques sur les corps de fonctions, avec un accent sur leur fonction L, la conjecture de Birch et Swinnerton-Dyer et les inégalités diophantiennes entre leurs invariants. Nous ne donnons presque aucune preuve mais renvoyons à de nombreuses références. Dans la dernière section de ce chapitre, nous définissons le ratio de Brauer-Siegel $\mathfrak{Bs}(E/K)$ d'une courbe elliptique E/K et rappelons les conjectures et les faits connus le concernant. Les deux chapitres suivants développent les outils nécessaires à l'étude analytique des familles $\mathscr{E}_i$ de courbes elliptiques : le second chapitre nous permettra de calculer leurs fonctions L et le troisième de borner leurs valeurs spéciales.

Plus précisément, le deuxième chapitre est axé sur les sommes de caractères. Dans un premier temps, nous rappelons des faits classiques sur les caractères des corps finis, sur les sommes de Gauss et sur les sommes de Jacobi. Ensuite, nous expliquons en détail la construction des caractères « $\mathbf{t}_a$ » qui apparaissent dans les expressions des fonctions L données ci-dessus : ceux-ci forment une famille naturelle de caractères dont l'ordre divise d. Nous utilisons ce cadre pour démontrer une « formule de réindexation » pour des séries génératrices dont les coefficients sont des sommes de caractères : ce résultat est d'usage constant dans les calculs de fonctions L qui suivent. Nous introduisons également les sommes de Legendre et prouvons les analogues de la relation de Hasse-Davenport et de l'hypothèse de Riemann. Pour mener à bien la preuve, nous calculons la fonction zeta de certaines courbes hyperelliptiques.

Au troisième chapitre, nous supposons disposer d'expressions explicites de fonctions L et nous nous concentrons sur l'encadrement de leur valeur spéciale. La première section montre comment on peut retrouver rapidement des majorations du rang et de la valeur spéciale dans le(s) cas particulier(s) qui nous concernent. À la seconde section, nous donnons une minoration de produits π^* de nombres algébriques qui apparaissent typiquement dans les valeurs spéciales des fonctions L des familles $\mathscr{E}_i$. Nos hypothèses sont rassemblées à la Section 3.2.1. Cependant, la minoration obtenue ne peut être utilisée que si l'on a une bonne connaissance des « valuations p-adiques » des nombres algébriques dans le produit π^*. Nous rappelons donc comment expliciter ces « valuations p-adiques » dans le cas des sommes de Jacobi. Finalement, nous démontrons un résultat d'équidistribution selon lequel les « gros » sous-groupes de $(\mathbb{Z}/d\mathbb{Z})^\times$ deviennent équidistribués en moyenne lorsque $d \to \infty$.

Dans les Chapitres 4 à 8, nous étudions individuellement les familles $\mathscr{E}_i$ précédemment introduites (la famille $\mathscr{E}_i$ est étudiée au Chapitre $i+3$). Les structures de ces chapitres sont relativement similaires. Nous commençons par calculer les invariants basiques des courbes elliptiques $E \in \mathcal{E}_i$. Dans un second temps, nous trouvons une expression explicite de leur fonction L en utilisant les outils mis en place au Chapitre 2. Nous rappelons alors brièvement la démonstration de la conjecture de Birch et Swinnerton-Dyer pour les courbes elliptiques $E \in \mathscr{E}_i$. Pour certaines familles, nous donnons également une preuve rapide que les rangs de Mordell-Weil ne sont pas bornés. Dans la dernière section de chacun de ces chapitres, nous utilisons les bornes sur les valeurs spéciales obtenues au Chapitre 3 et nous terminons la preuve que la famille $\mathscr{E}_i$ vérifie un analogue complet du théorème de Brauer-Siegel.

Tableau récapitulatif des familles étudiées

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Dans le tableau ci-dessous, nous récapitulons les familles de courbes elliptiques étudiées dans cette thèse (ainsi que celle de [HP16, Theorem 7.12]). La première colonne donne une équation de Weierstrass de E/K et le(s) paramètre(s) dont elle dépend. Nous donnons ensuite l'expression du j-invariant $j = j(E/K) \in \mathbb{F}_q(t)$ de E et sa hauteur différentielle $H = H(E/K)$ (exponentielle) en fonction de(s) paramètre(s). Le lecteur peut ainsi se convaincre que ces courbes sont deux-à-deux non isomorphes sur $\mathbb{F}_q(t)$. La dernière colonne rappelle les résultats obtenus quant au ratio de Brauer-Siegel.

	Modèle de Weierstrass et paramètre(s)	Invariant j	Hauteur	Ratio de Brauer-Siegel
[HP16]	$E_d : y^2 + xy = x^3 - t^d$ $d \in \mathbb{N}^*$, $\mathrm{pgcd}(d,p) = 1$	$j = \dfrac{1}{t^d(1 - 2^4 3^3 t^d)}$	$H = q^{\lfloor \frac{d+5}{6} \rfloor}$	$\lim\limits_{d\to\infty} \mathfrak{Bs}(E_d/K) = 1$
Chap. 4	$E_d : y^2 = x(x+1)(x+t^d)$ $d \in \mathbb{N}^*$, $\mathrm{pgcd}(d,p) = 1$	$j = \dfrac{2^8(t^{2d} - t^d + 1)^3}{t^{2d}(t^d - 1)^2}$	$H = q^{\lfloor \frac{d-1}{2} \rfloor}$	$\lim\limits_{d\to\infty} \mathfrak{Bs}(E_d/K) = 1$
Chap. 5	$H_d : y^2 + 3t^d xy + y = x^3$ $d \in \mathbb{N}^*$, $\mathrm{pgcd}(d,p) = 1$	$j = \dfrac{3^3 t^{3d}(9t^{3d} - 8)^3}{t^{3d} - 1}$	$H = q^d$	$\lim\limits_{d\to\infty} \mathfrak{Bs}(H_d/K) = 1$
Chap. 6	$E_d : y^2 + xy + t^d y = x^3 + t^d x^2$ $d \in \mathbb{N}^*$, $\mathrm{pgcd}(d,p) = 1$	$j = \dfrac{(16t^{2d} - 16t^d + 1)^3}{-t^{4d}(16t^d - 1)}$	$H = q^{\lfloor \frac{d-1}{2} \rfloor + 1}$	$\lim\limits_{d\to\infty} \mathfrak{Bs}(E_d/K) = 1$
Chap. 7	$E_d : y^2 + xy - t^d y = x^3$ $d \in \mathbb{N}^*$, $\mathrm{pgcd}(d,p) = 1$	$j = \dfrac{24t^d + 1}{-t^{3d}(27t^d - 1)}$	$H = q^{\lfloor \frac{d+2}{3} \rfloor}$	$\lim\limits_{d\to\infty} \mathfrak{Bs}(E_d/K) = 1$
Chap. 8	$B_{a,d} : y^2 + t^d xy - at^{2d} y = x^3 - (a+1)t^d x^2 + at^{2d} x$ $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et $d \in \mathbb{N}^*$, $\mathrm{pgcd}(d,p) = 1$	$j = \dfrac{(t^{2d} + 8(2a-1)t^d + 16(a^2 - a + 1))^3}{a^2(a-1)^2(t^{2d} + 8(2a-1)t^d + 16)}$	$H = q^{\lfloor \frac{d+1}{2} \rfloor}$	$\lim\limits_{\substack{d\to\infty \\ d \text{ impair}}} \mathfrak{Bs}(B_{1/2,d}/K) = 1$ si $a = 1/2$

1 Préliminaires

Dans ce chapitre, nous rappelons quelques faits classiques sur l'arithmétique des courbes elliptiques sur les corps de fonctions en caractéristique positive et sur leurs invariants. Ceci nous permet de fixer les notations utilisées et les conventions suivies. Nous ne rentrons pas dans les détails des preuves, préférant renvoyer le lecteur à des références précises. La dernière section est dédiée au ratio de Brauer-Siegel.

Dans toute la suite, une variété sur un corps k est un schéma séparé, irréductible et réduit de type fini sur k. Une courbe est une variété de dimension (pure) 1 et une surface est une variété de dimension (pure) 2.

1.1 Courbes elliptiques sur les corps de fonctions

Les rappels de cette section et de la suivante sont en partie inspirés des notes de cours [Ulm11]. On pourra aussi consulter les premiers chapitres de [Sil09] pour les notions de base de l'arithmétique des courbes elliptiques, [Sil94] pour plus de détails sur les courbes elliptiques sur les corps de fonctions (en caractéristique 0). Notons également l'article de survol [SS10] contenant plus spécifiquement des résultats sur les courbes elliptiques sur les corps de fonctions, avec un point de vue plus géométrique. Citons également le survol [Gro11], axé sur les conjectures de Birch et Swinnerton-Dyer. Mentionnons aussi [Oes90, §3], qui détaille particulièrement le cas où la courbe E/K est constante.

1.1.1 Corps de fonctions en caractéristique positive

Soit $\mathbb{F}_q$ un corps fini, dont on note p la caractéristique.

On appellera *corps de fonctions sur* $\mathbb{F}_q$ tout corps finiment engendré K, de degré de transcendance 1 sur $\mathbb{F}_q$ et dans lequel $\mathbb{F}_q$ est algébriquement clos ([Har77, Chapter I, §6]). Autrement dit, un corps de fonctions sur $\mathbb{F}_q$ est une extension algébrique finie de $\mathbb{F}_q(x)$, le corps des fractions rationnelles sur $\mathbb{F}_q$. Ainsi défini, un corps de fonctions s'écrit comme le corps des fonctions rationnelles sur une courbe définie sur $\mathbb{F}_q$, qu'on peut supposer projective lisse et géométriquement irréductible ([Har77, Chapter I, Theorem 6.9 & Corollary 6.11]). Plus précisément, il y a une équivalence de catégories entre corps de fonctions sur $\mathbb{F}_q$ et courbes projectives lisses sur $\mathbb{F}_q$ (voir [Sil09, Chapter 2], [Har77, Chapter I, Corollary 6.12]).

Si C est une courbe projective lisse et géométriquement irréductible définie sur $\mathbb{F}_q$ et que $K = \mathbb{F}_q(C)$ est son corps des fonctions rationnelles, il y a une bijection entre l'ensemble des *points fermés* de C (*i.e.* les $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbites de points $\overline{\mathbb{F}_q}$-rationnels sur C) et l'ensemble des *places* de K (*i.e.* les classes d'équivalence de valuations discrètes sur $K^\times$). Nous identifierons librement une place de K au point fermé de C qui lui correspond, voire à un élément de $C(\overline{\mathbb{F}_q})$ si aucune confusion n'en résulte.

Dans toute la suite, nous abrègerons « corps de fonctions en caractéristique positive » en « corps de fonctions ». Pour de plus amples détails sur les corps de fonctions et leur arithmétique, on pourra se référer à [Ros02, Chapter V], à [Ulm11, Lecture 0, §2] et aux références qui s'y trouvent, ou encore à [vF14, Chapter 1].

Pour toute place v d'un corps de fonctions $K = \mathbb{F}_q(C)$, on notera souvent $\mathrm{ord}_v : K^\times \to \mathbb{Z}$ la valuation discrète associée, $\mathcal{O}_{C,v}$ l'anneau local de C en v, $\mathfrak{M}_{C,v}$ son idéal maximal et $\mathbb{F}_v = \mathcal{O}_{C,v}/\mathfrak{M}_{C,v}$ son corps résiduel. Le degré d'une place v est le degré de l'extension $\mathbb{F}_v/\mathbb{F}_q$, il sera noté $\deg v$ ou d_v.

Pour tout diviseur D sur une courbe C, nous noterons $\deg D$ son degré : si $D = \sum n_v \cdot v$, on a

$$\deg D = \sum n_v \cdot \deg v.$$

Exemple 1.1.1. L'exemple fondamental de corps de fonctions est le corps $K = \mathbb{F}_q(t)$, corps des fonctions rationnelles sur $C = \mathbb{P}^1$. On peut diviser les places de K en deux types :
- la place « à l'infini » ∞, correspondant à la valuation $K^\times \to \mathbb{Z}$ donnée par $\mathrm{ord}_\infty : f \mapsto -\deg(f)$
- les places « finies », qui sont en bijection avec l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_q[t]$; à un polynôme irréductible unitaire $P \in \mathbb{F}_q[t]$ correspond la valuation $\mathrm{ord}_P : K^\times \to \mathbb{Z}$ donnée, pour tout polynôme $f \in \mathbb{F}_q[t]$, par $\mathrm{ord}_P(f) = n$ où n est l'exposant de P dans la décomposition en produits d'irréductibles de f.

Les corps de fonctions sont, au même titre que les corps de nombres, des corps globaux. C'est la raison pour laquelle la plupart de l'« arithmétique » se transpose bien à notre contexte. On pourra consulter [Lan83b, Chapter II, §2-3], [HS00, Chapter A, §9.2] ou [RV99, Chapter 4, §4]. Pour plus de détails sur les valeurs absolues et les places, voir [Lan83b, Chapter I], [HS00, Chapter B, §1] ou [Ser97, §2.1].

1.1.2 Courbes elliptiques sur les corps de fonctions

Définition 1.1.2. Soit $K = \mathbb{F}_q(C)$ un corps de fonctions. Une courbe elliptique sur K est une courbe projective lisse et géométriquement irréductible de genre 1, définie sur K et munie d'un point K-rationnel $\mathcal{O}$.

On munit une telle courbe elliptique E d'une structure de groupe algébrique commutatif de neutre $\mathcal{O}$ par « processus de cordes et tangentes » (voir [Hin08, Chapitre 5, §1], [Sil09, Chapter III, §2]).

De plus, E peut être représentée comme une cubique plane et définie par une équation de Weierstrass (*cf.* [Cas91, §8], [Har77, Chapter IV, §4] ou [SS10, §2.3]). Plus précisément, $E \subset \mathbb{P}^2$ est donnée par une équation de la forme

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6, \tag{1.1}$$

où $a_1, \ldots, a_6$ sont des éléments de K. On peut aussi donner l'équation sous forme affine :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

avec $x = X/Z$ et $y = Y/Z$. Le seul point sur E qui n'est pas dans cette carte affine est le point à l'infini $\mathcal{O} = [0 : 1 : 0]$. On peut alors définir les quantités usuelles associées à un modèle de E.

Définition 1.1.3. Soit E une courbe elliptique sur K, de modèle de Weierstrass (1.1). On définit les quantités suivantes :

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 & b_6 &= a_3^2 + 4a_6 \\ b_4 &= 2a_4 + a_1a_3 & b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 & c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

On appelle *discriminant du modèle* (1.1) la quantité

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = \frac{c_4^3 - c_6^2}{1728} \in K.$$

L'*invariant* j du modèle (1.1) est donné par

$$j = \frac{c_4^3}{\Delta} = \frac{\left(b_2^2 - 24b_4\right)^3}{\Delta} \in K.$$

On montre alors, comme dans le cas général d'une courbe elliptique sur un corps quelconque, que l'invariant j est indépendant du modèle de Weierstrass choisi pour E : c'est un invariant de la classe de $\overline{K}$-isomorphisme de E. Noter aussi que l'invariant j est indépendant du corps de base choisi sur lequel E est définie. En tant qu'éléments de $K = \mathbb{F}_q(c)$, les quantités j et Δ peuvent être vues comme des fonctions rationnelles sur la courbe C, *i.e.* des morphismes $j : C \to \mathbb{P}^1$ et $\Delta : C \to \mathbb{P}^1$. En particulier, on peut poser les deux définitions ci-dessous, qui n'ont pas d'analogues pour les courbes elliptiques sur les corps de nombres.

Définition 1.1.4. Soit E une courbe elliptique sur K. On dit que E est constante si il existe une courbe elliptique E_0 définie sur $\mathbb{F}_q$ telle que E est isomorphe (sur K) à $E_0 \times_{\mathbb{F}_q} K$.

De façon équivalente, E est constante si et seulement si elle admet un modèle de Weierstrass (1.1) où les coefficients a_i sont « constants », *i.e.* des éléments de $\mathbb{F}_q \subset K$.

Définition 1.1.5. Soit E une courbe elliptique sur K. On dit que E est isotriviale si il existe une extension finie K'/K telle que $E_{K'} = E \times_K K'$ est une courbe elliptique constante sur K'.

De façon équivalente (voir [Ulm11, Lecture 1, §1]), E est isotriviale si et seulement si son invariant j est un élément de $\mathbb{F}_q \subset K$. Autrement dit, l'application rationnelle $j : C \to \mathbb{P}^1$ correspondante à $j \in K = \mathbb{F}_q(C)$ est constante.

La théorie des courbes elliptiques sur un corps de fonctions est expliquée dans [SS10, §2], [Sil94, Chapter III, §1 - §3] en caractéristique 0 et [Ulm11, Lecture 1, §1] en caractéristique p comme ici. Les courbes elliptiques sont des variétés abéliennes de dimension 1 : la lectrice peut, à leur propos, consulter [HS00, Chapter A, §7] ou [Mil86].

1.1.3 Réduction en une place

Soit E une courbe elliptique sur $K = \mathbb{F}_q(C)$ et v une place de K (on identifie v au point fermé de C qui lui correspond) et $\mathrm{ord}_v : K^\times \to \mathbb{Z}$ la valuation associée.

Définition 1.1.6. Un modèle de Weierstrass

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6$$

de E est dit *entier en v* si et seulement si $\mathrm{ord}_v(a_i) \geqslant 0$ pour tout $i \in \{1, 2, 3, 4, 6\}$ (*i.e.* si les coefficients a_i sont des éléments de l'anneau local $\mathcal{O}_{C,v}$ de C en v). La valuation $\mathrm{ord}_v(\Delta)$ du discriminant d'un tel modèle est donc un entier positif. Par suite, il existe un modèle de E, entier en v et tel que cette valuation $\mathrm{ord}_v(\Delta)$ est minimale. Un tel modèle est appelé *modèle entier minimal de E en v.*

Une fois choisi un tel modèle minimal et entier de E en v :

$$Y^2Z + a_{1,v}XYZ + a_{3,v}YZ^2 = X^3 + a_{2,v}X^2Z + a_{4,v}XZ^2 + a_{6,v} \tag{1.3}$$

avec $a_{i,v} \in \mathcal{O}_{C,v}$, on peut le réduire modulo l'idéal maximal $\mathfrak{M}_{C,v}$ de l'anneau local $\mathcal{O}_{C,v}$: on obtient des coefficients $\overline{a_i} \in \mathbb{F}_v$ et une courbe cubique plane dans $\mathbb{P}^2$ définie sur $\mathbb{F}_v$, notée $\overline{E}_v$, d'équation

$$Y^2Z + \overline{a_{1,v}}XYZ + \overline{a_{3,v}}YZ^2 = X^3 + \overline{a_{2,v}}X^2Z + \overline{a_{4,v}}XZ^2 + \overline{a_{6,v}}. \tag{1.4}$$

La classe d'isomorphisme de cette cubique réduite ne dépend pas du choix de modèle entier minimal (1.3). Si le discriminant $\Delta = \Delta(a_{1,v}, \ldots, a_{6,v}) \in K$ d'un modèle entier minimal de E en v vérifie $\mathrm{ord}_v(\Delta) \neq 0$, *i.e.* si Δ est une unité de $\mathcal{O}_{C,v}$, alors l'équation réduite (1.4) définit une courbe cubique lisse sur $\mathbb{F}_v$, c'est-à-dire une courbe elliptique sur $\mathbb{F}_v$. Si, au contraire, $\mathrm{ord}_v(\Delta) > 0$, la courbe cubique définie par (1.4) sur $\mathbb{F}_v$ est singulière.

Définition 1.1.7. Soit E une courbe elliptique sur K et soit v une place de K.

- Si $\overline{E}_v$ est une cubique lisse, on dit que E *a bonne réduction en v.*
- Si $\overline{E}_v$ a un point singulier avec deux tangentes, on dit que E *a réduction multiplicative en v* : on distingue alors deux cas selon que
  - les tangentes sont définies sur $\mathbb{F}_v$ (réduction multiplicative *déployée*)
  - ou sur une extension quadratique de $\mathbb{F}_v$ (réduction multiplicative *non déployée*).
- Enfin, si $\overline{E}_v$ est une cubique avec une seule tangente en son point singulier, on parle de *réduction additive en v* pour E.

Voir [Sil09, Chapter III, §1] ou [Gro11, Appendix A] pour des détails sur les points singuliers des courbes planes de genre 1. On note $\mathcal{B}(E/K)$ l'ensemble des places de K en lesquelles E a mauvaise réduction, il correspond à l'ensemble des points fermés v sur C en lesquels la fonction $\Delta : C \to \mathbb{P}^1$ s'annule (on dit que la place v divise Δ), *i.e.* les places en lesquelles $\mathrm{ord}_v\ \Delta > 0$ pour le choix d'un modèle entier de E. En particulier, on a :

Proposition 1.1.8. *Une courbe elliptique E/K a un nombre fini de places de mauvaise réduction.*

1.1.4 Discriminant minimal et conducteur

Dans cette section, on fixe une courbe elliptique E définie sur un corps de fonctions $K = \mathbb{F}_q(C)$. Nous lui associons trois invariants importants.

Définition 1.1.9. Pour chaque place v de K, on choisit un modèle entier minimal (1.3) de E en v : on note $\Delta_v \in \mathcal{O}_{C,v}$ le discriminant de ce modèle. On définit alors le *discriminant minimal* de E par

$$\Delta_{\min}(E/K) := \sum_v \mathrm{ord}_v(\Delta_v) \cdot [v],$$

la somme portant sur toutes les places de v, identifiées à l'ensemble des points fermés de C.

Ainsi défini, le discriminant minimal $\Delta_{\min}(E/K)$ peut être considéré comme un diviseur effectif sur C. Notons que le degré $\deg \Delta_{\min}(E/K) \in \mathbb{N}$ de ce diviseur est toujours un multiple de 12 (*cf.* par exemple [Sil86a, §1]).

Définition 1.1.10. Pour toute place v de K, on définit l'*exposant local du conducteur en v* par

$$n_v(E/K) := \begin{cases} 0 & \text{si } E \text{ a bonne réduction en } v \\ 1 & \text{si } E \text{ a réduction multiplicative en } v \\ 2 + \delta_v & \text{si } E \text{ a réduction additive en } v, \end{cases}$$

où $\delta_v \in \mathbb{N}$ vaut $\delta_v = 0$ si $p \geqslant 5$. Nous renvoyons le lecteur à [Sil94, Chapter IV, §10] pour les détails de la définition de δ_v dans le cas où $p = 2, 3$. Disons simplement que δ_v encode la présence éventuelle de ramification sauvage dans l'action du groupe de Galois local $\mathrm{Gal}(K_v^{\mathrm{sep}}/K_v)$ sur le module de Tate de E.

Définition 1.1.11. Le *conducteur* de la courbe elliptique E est le diviseur effectif sur C défini par

$$\mathcal{N}(E/K) := \sum_v n_v(E/K) \cdot [v] \in \mathrm{Div}(C),$$

la somme portant sur toutes les places de K, identifiées encore à l'ensemble des points fermés de C.

Les définitions ci-dessus sont détaillées et commentées plus avant dans [Ulm11, Lecture 1, §8], [Gro11, Lecture 2, §2] et [SS10, §5.9]. On peut également définir le conducteur d'une courbe elliptique comme le conducteur d'Artin du module de Tate de E/K (voir [Sil94, Chapter IV, §10]). Rappelons également que le discriminant minimal et le conducteur d'une courbe elliptique E/K sont reliés par la formule de Ogg ([Sil94, Chapter IV, §11]) : pour toute place v de K, on a

$$n_v(E/K) = \mathrm{ord}_v(\Delta_v) + 1 - m_v, \tag{1.5}$$

où m_v est le nombre de composantes irréductibles du modèle régulier minimal de E en v (voir Section 1.1.5).

Définition 1.1.12. Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$. On définit sa hauteur différentielle $H(E/K)$ par

$$H(E/K) = q^{\frac{1}{12}\deg \Delta_{\min}(E/K)},$$

une puissance entière de q.

Soit $\mathcal{B}(E/K)$ l'ensemble des places de K où E a mauvaise réduction. D'après leur définition, les diviseurs $\mathcal{N}(E/K)$ et $\Delta_{\min}(E/K)$ ont même support $\mathcal{B}(E/K)$ et l'on a $\deg \mathcal{N}(E/K) \leqslant \deg \Delta_{\min}(E/K)$. Leurs degrés sont de plus reliés « dans l'autre sens » par l'inégalité suivante :

Théorème 1.1.13 (Pesenti – Szpiro)**.** *Soit E une courbe elliptique* non isotriviale *sur un corps de fonctions $K = \mathbb{F}_q(C)$. On note g_C le genre de C et $\mathfrak{f}_{E/K}$ le degré du conducteur $\mathcal{N}(E/K)$. Alors :*

$$\deg \Delta_{\min}(E/K) \leqslant 6p^e \cdot \big(2g_C - 2 + \mathfrak{f}_{E/K}\big),$$

où p^e est le degré d'inséparabilité de $j(E/K) : C \to \mathbb{P}^1$.

Voir [Szp90] pour la preuve de cette inégalité dans le cas où E/K est semi-stable et [PS00, Theorem 0.1] pour le cas général. Citons également [GS95, Theorem 3] et [HS88, Theorem 5.1]. Pour les courbes elliptiques sur les corps de nombres, l'inégalité correspondante est l'objet de la Conjecture de Szpiro [HS00, Conjecture F.3.2], équivalente à la Conjecture *abc* (voir [Hin08, Chapitre 6, §5]).

Remarque 1.1.14. Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$. On suppose, pour simplifier, que l'invariant j de E/K est séparable. La formule de Ogg (1.5) et le Théorème 1.1.13 permettent d'écrire :

$$\frac{\log q}{12} \cdot \deg \mathcal{N}(E/K) \leqslant \log H(E/K) \leqslant \log q \cdot \left(g_C - 1 + \frac{\deg \mathcal{N}(E/K)}{2} \right).$$

En particulier, il existe des constantes (dépendant de K) telles que

$$\deg \mathcal{N}(E/K) \ll_q \log H(E/K) \ll_{q,g_C} \deg \mathcal{N}(E/K).$$

1.1.5 Modèle régulier minimal

Considérons une courbe elliptique E définie sur un corps de fonctions $K = \mathbb{F}_q(C)$. Parmi les surfaces $\mathcal{E}$ définies sur $\mathbb{F}_q$ et munies d'un morphisme $\pi : \mathcal{E} \to C$ dont la fibre générique est E/K, il y en a une privilégiée, appelée modèle régulier minimal de E/K. Commençons par rappeler la définition suivante.

Définition 1.1.15. Soit $\mathcal{E}$ une surface projective lisse et géométriquement irréductible, C une courbe projective lisse et géométriquement irréductible, toutes deux définies sur $\mathbb{F}_q$. On dit qu'un morphisme $\pi : \mathcal{E} \to C$ est *relativement minimal* si, pour toute surface $\mathcal{E}'$ projective lisse et géométriquement irréductible définie sur $\mathbb{F}_q$ et munie d'un morphisme $\pi' : \mathcal{E}' \to C$, tout morphisme birationnel $\phi : \mathcal{E} \to \mathcal{E}'$ qui commute à π et π' est un isomorphisme.

La relative minimalité d'un morphisme $\pi : \mathcal{E} \to C$ est équivalente à la condition suivante (« critère de Castelnuovo ») : il n'y a aucune courbe rationnelle d'auto-intersection -1 dans les fibres de π (*i.e.* il n'y a pas de courbes qui peuvent être contractées dans les fibres de π). On peut alors énoncer le théorème ci-dessous.

Théorème 1.1.16. *Soit E une courbe elliptique définie sur un corps de fonctions $K = \mathbb{F}_q(C)$. À isomorphisme près, il existe une unique surface $\mathcal{E}$ définie sur $\mathbb{F}_q$ et munie d'un morphisme $\pi : \mathcal{E} \to C$ avec les propriétés suivantes :*

1. *$\mathcal{E}$ est projective lisse et géométriquement irréductible sur $\mathbb{F}_q$,*
2. *π est surjectif et relativement minimal,*
3. *la fibre générique de π est isomorphe à E.*

La donnée de $\mathcal{E}$ et du morphisme structurel $\pi : \mathcal{E} \to C$ est appelée modèle régulier minimal de E/K.

Remarquons que le morphisme structural $\pi : \mathcal{E} \to C$ admet une section $\varepsilon : C \to \mathcal{E}$ (appelée *section neutre*) et que presque toutes ses fibres sont des courbes lisses de genre 1. En outre, il y a une bijection entre l'ensemble des points K-rationnels sur E et l'ensemble des sections globales $s : C \to \mathcal{E}$ de $\pi : \mathcal{E} \to C$ (voir [SS10, §3.4]).

La construction d'une telle surface étant assez délicate, contentons-nous de rappeler les grandes lignes de la preuve. Le lecteur peut consulter [Sil94, Chapter IV, §7], [Liu02, Chapter 9, §9.3] ou [Con15, §3] pour plus de détails. Citons également [HS00, Chapter A, §9.3] et [Shi90, §1].

Grossièrement, le modèle minimal est obtenu par désingularisation (éclatements) des points singuliers des fibres du modèle de Weierstrass. On écrit une équation de E à coefficients dans $K = \mathbb{F}_q(C)$ (sous forme de Weierstrass). Après avoir retiré de C les points fermés en lesquels le discriminant $\Delta : C \to \mathbb{P}^1$ de ce modèle s'annule, on obtient un ouvert non-vide C' de C et une surface $\mathcal{W}$ lisse, quasi-projective et munie d'une fibration $\pi' : \mathcal{W} \to C$ dont la fibre générique est E/K. Le morphisme π' est lisse au-dessus de C'. De plus, π' admet une section $\varepsilon' : C \to \mathcal{W}$. Au-dessus de chacun des points $x \in C' \smallsetminus C$ (il y en a un nombre fini), on « remplace » la fibre $\pi^{-1}(x)$ par une fibre F_x convenable obtenue par éclatement des points singuliers sur $\pi^{-1}(x)$. En recollant le tout, on dispose alors d'une surface projective lisse $\pi : \mathcal{E} \to C$ avec les propriétés requises. L'unicité d'une telle surface suit de résultats généraux sur les modèles minimaux.

Notons enfin que la suite d'éclatements à effectuer sur une fibre singulière $\pi^{-1}(x)$ est donnée (implicitement) par l'*algorithme de Tate* (*cf.* [Tat75], [SS10, §4.1- §4.6]). Les fibres F_x obtenues sont classées par *types de Kodaira*. On pourra se référer à [Ulm11, Lecture 3, §1] ou [SS10, §3.5] pour une construction explicite du modèle régulier minimal.

Soit $\pi : \mathcal{E} \to C$ le modèle régulier minimal d'une courbe elliptique E/K. On note S l'ensemble (fini) des points $s \in \mathcal{E}$ qui sont singuliers dans les fibres de π. Alors $\mathcal{E}_N := \mathcal{E} \smallsetminus S$ (munie du morphisme $\pi_N : \mathcal{E}_N \to C$ induit par π) est le *modèle de Néron* de E/K : tout point K-rationnel sur E se prolonge en une section $C \to \mathcal{E}_N$ et la loi de groupe sur E s'étend en un morphisme $\mathcal{E}_N \times_C \mathcal{E}_N \to \mathcal{E}_N$ munissant $\mathcal{E}_N$ d'une structure de schéma en groupes sur C ([Art86], [HS00, Chapter A, §9.4], [Sil94, Chapter IV]).

Remarque 1.1.17. On peut maintenant donner une autre interprétation de la hauteur différentielle d'une courbe elliptique. Si E est une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$, on note $\pi : \mathcal{E} \to C$ son modèle régulier minimal et $\varepsilon : C \to \mathcal{E}$ la section neutre de celui-ci. On note $\Omega^1_{\mathcal{E}/C}$ le faisceau des 1-formes différentielles relatives de $\mathcal{E}/C$ et $\omega_{E/K} = \varepsilon^*\Omega^1_{\mathcal{E}/C}$ son tiré en arrière à C. Alors $\omega_{E/K}$ est un faisceau inversible sur C et l'on peut définir

$$H(E/K) = q^{\deg \omega_{E/C}}.$$

C'est la « vraie » définition de la hauteur (*cf.* [HP16, Definition 2.1], [GS95, §4] ou [Szp90, §1]). Celle-ci se généralise aux variétés abéliennes de dimension plus grande lorsque l'on remplace « modèle régulier minimal » par « modèle de Néron ». L'équivalence de ces deux définitions suit d'une adaptation de [Sil86a, Proposition 1.1].

1.1.6 Nombre de Tamagawa

Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$. Pour toute place v de K, on note K_v la complétion de K en v et $\mathbb{F}_v$ le corps résiduel en v. On choisit un modèle entier minimal de E en v comme à la Section 1.1.3 et on note $\overline{E}_v$ la réduction de ce modèle modulo v : c'est une courbe cubique plane définie sur $\mathbb{F}_v$ (singulière si E a mauvaise réduction en v). Il y a une application naturelle de « réduction modulo v » sur les points $r_v : E(K_v) \to \overline{E}_v(\mathbb{F}_v)$ (c'est même un morphisme de groupes). On peut alors considérer $\overline{E}_v^{ns}(\mathbb{F}_v) \subset \overline{E}_v(\mathbb{F}_v)$, le sous-ensemble des points non singuliers de $\overline{E}_v(\mathbb{F}_v)$. On note également

$$E_0(K_v) = \left\{ P \in E(K_v) \;\middle|\; r_v(P) \in \overline{E}_v^{ns}(\mathbb{F}_v) \right\} \subset E(K_v).$$

Alors $E_0(K_v)$ est un sous-groupe d'indice fini de $E(K_v)$ (*cf.* [Sil09, Chapter VII, Theorem 6.1], [Sil09, Appendix C, Theorem 15.2] ou [Sil94, Chapter IV, Corollary 9.2]). On appelle *nombre de Tamagawa local* de E en v, l'indice

$$c_v(E/K) = [E(K_v) : E_0(K_v)] = \#\big(E_0(K_v)/E(K_v)\big).$$

Pour presque toute place v de K, on a $c_v(E/K) = 1$. En effet, si E a bonne réduction en v, tous les points de $\overline{E}_v$ sont réguliers et $\overline{E}_v^{ns}(\mathbb{F}_v) = \overline{E}_v(\mathbb{F}_v)$: il suit immédiatement que $c_v(E/K) = 1$. On peut donc définir :

Définition 1.1.18. Le *nombre de Tamagawa* (global) de E/K est l'entier

$$\mathcal{T}am(E/K) = \prod_v c_v(E/K),$$

le produit portant sur toutes les places v de K.

Remarque 1.1.19. Le nombre de Tamagawa local $c_v(E/K)$ peut aussi être défini de la façon suivante. Soit à nouveau v une place de K et $\mathcal{E}_v \to \operatorname{Spec} \mathcal{O}_v$ le modèle de Néron de E_v/K_v (où $\mathcal{O}_v$ est l'anneau local de K en v) et $\widetilde{\mathcal{E}}_v \to \operatorname{Spec} \mathbb{F}_v$ sa fibre spéciale. On note alors $\widetilde{\mathcal{E}}_v^0$ la composante neutre de $\widetilde{\mathcal{E}}_v$ et $\Phi_{E,v} = \widetilde{\mathcal{E}}_v/\widetilde{\mathcal{E}}_v^0$ le groupe des composantes du modèle de Néron en v. Alors $c_v(E/K)$ vaut

$$\#\Phi_{E,v}(\mathbb{F}_v) = \#\widetilde{\mathcal{E}}_v(\mathbb{F}_v)/\widetilde{\mathcal{E}}_v^0(\mathbb{F}_v).$$

C'est-à-dire que $c_v(E/K)$ est le nombre de composantes de la fibre spéciale $\widetilde{\mathcal{E}}_v$ qui sont $\mathbb{F}_v$-rationnelles. Voir [Sil94, Chapter IV, Corollary 9.2], [Hin07, §3] ou [HP16, Definition 1.20] pour plus de détails. Remarquons également qu'il y a une interprétation « volumétrique » de $c_v(E/K)$ ([Tat75, Theorem 5.2] ou [Gro11, Lemma A.4]).

À propos du nombre de Tamagawa local, mentionnons encore le résultat suivant :

Théorème 1.1.20 (Kodaira-Néron)**.** *Soit E une courbe elliptique sur un corps de fonctions K. Pour toute place v de K, on note Δ_v le discriminant d'un modèle minimal entier de E en v. Alors*

- $c_v(E/K) = \operatorname{ord}_v \Delta_v = -\operatorname{ord}_v j(E/K)$ *si E a réduction multiplicative déployée en v,*
- $c_v(E/K) \in \{1, 2, 3, 4\}$ *dans tous les autres cas.*

Ce Théorème est démontré en détail dans [Sil09, Chapter VII, Theorem 6.1] ou [Sil94, Chapter IV, Corollary 9.2 (d)].

1.2 Groupe de Mordell-Weil

1.2.1 Hauteur de Néron-Tate

Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$. On suppose que E est donnée par un modèle de Weierstrass (1.1). En d'autres termes, on choisit un plongement $E \hookrightarrow \mathbb{P}^2$ et des coordonnées sur $\mathbb{P}^2$. On peut alors définir la *hauteur naïve* d'un point $P \in E(K) \smallsetminus \{\mathcal{O}\}$, de coordonnées $(x_P, y_P) \in K^2$, par

$$h(P) := \frac{\deg(x_P)}{2},$$

où $\deg x_P$ est le degré de l'application rationnelle $x_P : C \to \mathbb{P}^1$. On pose également $h(\mathcal{O}) = 0$. En termes de « Weil's Height Machine », h est une hauteur de Weil associée au diviseur ample $(\mathcal{O})$ (rappelons que $2(\mathcal{O}) = x^*\infty$). Un fait classique est que h est « presque quadratique », au sens où l'application

$$(P, Q) \in E(K) \times E(K) \mapsto h(P + Q) - h(P) - h(Q)$$

est bornée ([Sil94, Chapter III, Theorem 4.2]). Posons alors

$$\forall P \in E(K), \quad \hat{h}_{NT}(P) := \lim_{n\to\infty} \frac{1}{4^n} h\left(2^n \cdot P\right).$$

La « presque quadraticité » de h garantit la convergence de cette suite et l'on obtient une application quadratique définie positive $\hat{h}_{NT} : E(K) \to \mathbb{Q}$ (voir [Lan83b, Chapter 5, §3], [Ser97, §3.3, §3.8], [SS10, Theorem 11.5]) qui ne dépend pas des choix effectués et telle que la différence $\hat{h}_{NT} - h$ est bornée sur $E(K)$ (voir [Sil94, Chapter III, Theorem 4.3]).

Définition 1.2.1. L'application $\hat{h}_{NT} : E(K) \to \mathbb{Q}$ est appelée *hauteur de Néron-Tate* sur E.

Remarquons que $E(K)_{\text{tors}} \subset E(K)$ est exactement le sous-groupe formé des points P tels que $\hat{h}_{NT}(P) = 0$.

Définition 1.2.2. Pour tous points $P, Q \in E(K)$, on pose

$$\langle P, Q\rangle_{NT} := \frac{1}{2}\left(\hat{h}_{NT}(P + Q) - \hat{h}_{NT}(P) - \hat{h}_{NT}(Q)\right).$$

L'application $\mathbb{Z}$-bilinéaire $\langle\cdot,\cdot\rangle_{NT} : E(K) \times E(K) \to \mathbb{Q}$ ainsi définie est appelée *accouplement de Néron-Tate*.

Remarque 1.2.3. Il est aussi possible de définir l'accouplement $\langle\cdot,\cdot\rangle_{NT}$ en termes de théorie de l'intersection sur la surface minimale $\pi : \mathcal{E} \to C$ associée à E. Voir [Shi90, Part T, §2], [SS10, §11.6] ou [Sil94, Chapter III, §9] (en particulier [Sil94, Chapter III, Theorem 9.3]). On peut alors également décomposer $\hat{h}_{NT}$ en sommes de contributions locales ([Lan83b, Chapter XI, §4]). Entre autres, cette définition rend tout à fait évident que $\langle P, Q\rangle_{NT} \in \mathbb{Q}$ pour tous points $P, Q \in E(K)$.

Remarque 1.2.4. Notre normalisation de la hauteur de Néron-Tate diffère de celle utilisée par certains auteurs (notamment [Tat66], [Gro11], ...). Suivant [Sil94, Chapter III, §4], [Shi90], [Mil68], ... nous avons préféré avoir une hauteur à valeurs dans $\mathbb{Q}$ plutôt que dans $(\log q) \cdot \mathbb{Q}$.

Les détails de la construction de $\hat{h}_{NT}$ peuvent être trouvés dans [Sil86b, §4], [Sil09, Chapter VIII, §9], [HS00, Chapter B, §5], [Ser97, §3.1, §3.5], [Sil94, Chapter III, §4] ou [Gro11, Lecture 1, §4].

1.2.2 Théorème de Mordell-Weil

S. Lang et A. Néron [LN59] ont généralisé le théorème de Mordell-Weil classique au contexte des courbes elliptiques sur les corps de fonctions.

Théorème 1.2.5 (Mordell-Weil-Lang-Néron)**.** *Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$. Alors le groupe des points K-rationnels $E(K)$ est un groupe abélien de type fini.*

Ce théorème s'applique plus généralement à des variétés abéliennes de dimension quelconque sur un corps finiment engendré sur son corps premier, il faut alors prendre en compte la partie constante de A/K (la K/k-trace) : *cf.* l'article original [LN59]. Donnons simplement quelques idées de la démonstration de ce théorème : deux approches sont possibles. On peut adapter la preuve classique du théorème de Mordell-Weil (pour les courbes elliptiques sur les corps de nombres) : l'argument se décompose alors en deux parties. Tout d'abord, on montre que $E(K)/mE(K)$ est fini (pour un certain

entier $m \in \mathbb{N}^*$, usuellement $m = 2$) à l'aide d'un groupe de Selmer (« Mordell-Weil faible »). Ensuite, on conclut par des arguments de descente infinie à l'aide de la hauteur de Néron-Tate.

Une autre approche, plus géométrique (et spécifique au cadre des courbes elliptiques sur les corps de fonctions) est la suivante : on peut relier $E(K)$ avec le groupe de Néron-Severi $\mathrm{NS}(\mathcal{E})$ du modèle régulier minimal $\pi : \mathcal{E} \to C$ de E (voir [SS10, §6.3]). Or, le groupe de Néron-Severi d'une surface est de type fini (c'est le théorème de la base, voir [Lan83b, Chapter 6], [Mil80, Chapter V, Theorem 3.25] ou [Con06]). Des considérations géométriques montrent que cet énoncé est équivalent au théorème de Mordell-Weil pour E (voir [SS10, Theorem 6.3]). On pourra consulter [Shi90] ou [SS10, §6, §11].

Ces deux preuves sont résumées dans [Ulm11, Lecture 1, §5]. On pourra compulser [Lan83b, Chapter 6], [Sil94, Chapter III, §2, §6] (en caractéristique 0) ou [SS10, §6.2] pour des détails.

Remarque 1.2.6. Tout comme le théorème de Mordell-Weil pour les courbes elliptiques sur les corps de nombres, le Théorème 1.2.5 est *ineffectif*. Précisément, la preuve ne donne pas de moyen de calculer des générateurs de $E(K)$.

Le Théorème 1.2.5 permet d'écrire le groupe de points K-rationnels de E sous la forme

$$E(K) \simeq \mathbb{Z}^r \oplus E(K)_{\mathrm{tors}},$$

où $E(K)_{\mathrm{tors}}$ est un groupe fini et $r \in \mathbb{N}$ est un entier, appelé le *rang de Mordell-Weil de E sur K* (ou simplement *rang*), noté dorénavant $r = \operatorname{rang} E(K)$. En outre, maintenant que l'on sait que $E(K)$ admet une « base » finie de générateurs, on peut définir la quantité suivante :

Définition 1.2.7. Soit E une courbe elliptique sur $K = \mathbb{F}_q(C)$. On fixe $P_1, \dots, P_r$ une $\mathbb{Z}$-base de $E(K)/E(K)_{\mathrm{tors}}$. Le *régulateur de Néron-Tate* de E est le déterminant

$$\mathrm{Reg}(E/K) := \left| \det \left(\langle P_i, P_j \rangle_{NT} \right)_{1 \leqslant i,j \leqslant r} \right|.$$

Le régulateur est donc le carré du volume du réseau $E(K)/E(K)_{\mathrm{tors}}$ dans $E(K) \otimes \mathbb{R}$. On remarque aussi que sa valeur ne dépend pas de la $\mathbb{Z}$-base choisie pour le définir (un autre choix de base donne lieu à une matrice de $\mathrm{GL}_2(\mathbb{Z})$ de « changement de base », qui est de déterminant ± 1).

Remarque 1.2.8. Vu notre choix de normalisation de la hauteur de Néron-Tate, le régulateur est un nombre rationnel strictement positif. En particulier, il n'y a pas de « $(\log q)^{\operatorname{rang} E(K)}$ » dans la définition de $\mathrm{Reg}(E/K)$.

1.2.3 Groupe de Tate-Shafarevich

La définition du groupe de Tate-Shafarevich est tout à fait similaire à sa forme usuelle pour les courbes elliptiques sur un corps de nombres. La différence principale est que l'on utilise la cohomologie galoisienne relative à une clôture séparable K^{sep} du corps de base (et non plus une clôture algébrique).

Soit $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ le groupe de Galois absolu de K. Ce groupe agit sur le groupe $E(K^{\mathrm{sep}})$ par des automorphismes continus. De même, pour toute place v de K, notant K_v la complétion de K en v, il y a une action continue du groupe de Galois local $G_v = \mathrm{Gal}(K_v^{\mathrm{sep}}/K_v)$ sur $E(K_v)$. Il y a donc des groupes de cohomologie galoisienne $\mathrm{H}^1(G_K, E(K^{\mathrm{sep}}))$ et $\mathrm{H}^1(G_v, E(K_v^{\mathrm{sep}}))$ correspondant à ces actions. Pour toute place v de K, il y a de plus une flèche « de restriction » des classes de cohomologie $\mathrm{res}_v : \mathrm{H}^1(G_K, E(K^{\mathrm{sep}})) \to \mathrm{H}^1(G_v, E(K_v^{\mathrm{sep}}))$ (voir [Cas91, §21, §23]). On définit alors :

Définition 1.2.9. Le groupe de Shafarevich-Tate de E/K est le groupe

$$Ш(E/K) := \ker \left(\mathrm{H}^1(G_K, E(K^{\mathrm{sep}})) \xrightarrow{\prod_v \mathrm{res}_v} \prod_v \mathrm{H}^1(G_v, E(K_v^{\mathrm{sep}})) \right).$$

Ce groupe $Ш(E/K)$ mesure en un certain sens une obstruction au « principe local-global ». On peut en effet en donner une définition équivalente sous la forme : le groupe $Ш(E/K)$ est formé des classes d'équivalence d'espaces principaux homogènes H pour E qui sont localement triviaux (*i.e.* H a un point K_v-rationnel pour toute place v de K). Ceci est détaillé dans [HS00, Chapter C, §4-5] ou ou [Cas91, §22].

Comme $\mathrm{H}^1(G_K, E(K^{\mathrm{sep}}))$ est un groupe de torsion, le groupe de Tate-Shafarevich $Ш(E/K)$ est également de torsion. Cependant, il reste assez mystérieux :

Conjecture 1.2.10 (Shafarevich-Tate)**.** *Le groupe $Ш(E/K)$ est fini.*

Notons que cette conjecture n'est connue que dans un nombre très limité de cas, dont nous reparlerons à la section 1.4.3. Remarquons également que dans tous les cas où cette conjecture a été démontrée, elle l'a été *via* une preuve de la Conjecture de Birch et Swinnerton-Dyer (Conjecture 1.4.1 ci-dessous).

Remarque 1.2.11. Si le groupe de Tate-Shafarevich d'une courbe elliptique E/K est fini, Goldfeld et Szpiro ont démontré (*cf.* [GS95, Theorem 15]) que

$$\forall \varepsilon > 0, \qquad \#Ш(E/K) \ll_{q,g_C} H(E/K)^{1+\varepsilon},$$

pour peu que l'invariant j de E soit séparable.

1.3 Fonctions zeta et fonctions L des courbes elliptiques

1.3.1 Fonctions zeta des variétés sur un corps fini

Soit X une variété projective et lisse, de dimension d définie sur un corps fini $\mathbb{F}_q$. On notera $|X|$ l'ensemble des points fermés de X, c'est-à-dire les classes de conjugaison sous l'action de $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ des points de $X(\overline{\mathbb{F}_q})$. Pour un point fermé $x \in |X|$, le corps résiduel $\mathbb{F}_x$ de X en x est une extension finie de $\mathbb{F}_q$: on note $\deg x = [\mathbb{F}_x : \mathbb{F}_q]$.

Définition 1.3.1. Soit X une variété projective et lisse définie sur un corps fini $\mathbb{F}_q$. On définit la *fonction zeta* $Z(X/\mathbb{F}_q, T)$ de $X/\mathbb{F}_q$ comme le produit eulérien suivant :

$$Z(X/\mathbb{F}_q, T) = \prod_{x \in |X|} \left(1 - T^{\deg x}\right)^{-1} \in \mathbb{Z}[[T]].$$

Un calcul classique et essentiellement formel montre que la fonction zeta s'écrit aussi sous la forme :

$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})}{n} T^n\right).$$

Le point-clé est qu'un point fermé $x \in X$ de degré exactement d donne lieu à exactement d points $\mathbb{F}_{q^d}$-rationnels sur X (*cf.* [Hin10, §2.3], [Ser65]). Notons alors l'identité formelle :

$$\frac{Z'(X/\mathbb{F}_q, T)}{Z(X/\mathbb{F}_q, T)} = \frac{\mathrm{d} \log Z(X/\mathbb{F}_q, T)}{\mathrm{d}T} = \sum_{n \geqslant 1} \#X(\mathbb{F}_{q^n}) T^{n-1}.$$

Pour $s \in \mathbb{C}$ convenable, on pose $\zeta(X/\mathbb{F}_q, s) := Z(X/\mathbb{F}_q, q^{-s})$. La série $\zeta(X/\mathbb{F}_q, s)$ s'écrit comme une série de Dirichlet en q^{-s}, qui est convergente dans le demi-plan $\mathrm{Re}(s) > \dim X$. Ce dernier point suit d'une majoration du nombre de points $\mathbb{F}_{q^n}$-rationnels sur X ($\#X(\mathbb{F}_{q^n}) \ll q^{n \dim X}$ suffit).

La fonction zeta $Z(X/\mathbb{F}_q, T)$ est l'objet des *conjectures de Weil* (voir [Wei49]) démontrées par A. Grothendieck et P. Deligne ([Del74], [Del80]). Fixons une variété projective et lisse X définie sur $\mathbb{F}_q$ et de dimension d. La série formelle $Z(X/\mathbb{F}_q, T)$ est en fait une fraction rationnelle en T : on peut l'écrire sous la forme

$$Z(X/\mathbb{F}_q, T) = \frac{P_1(T) \cdot P_3(T) \cdot \cdots \cdot P_{2d-1}(T)}{P_0(T) \cdot \cdots \cdot P_{2d}(T)},$$

où les polynômes $P_i(T)$ sont à coefficients entiers de coefficient constant $P_i(0) = 1$. De plus, $P_0(T) = 1 - T$ et $P_{2d}(T) = 1 - q^d T$. Pour $i \in [\![1, d-1]\!]$, il existe des entiers algébriques $\alpha_{i,j}$ tels que

$$P_i(T) = \prod_{j=1}^{\deg P_i} (1 - \alpha_{i,j} T).$$

Les inverses $\alpha_{i,j}$ des racines de P_i sont des entiers algébriques de module $q^{i/2}$ dans tout plongement complexe (des *q-nombres de Weil de poids i*). En outre, la fonction zeta $Z(X/\mathbb{F}_q, T)$ vérifie une équation fonctionnelle :

$$Z\left(X/\mathbb{F}_q, \frac{1}{q^d T}\right) = \pm (q^d T^2)^{\chi(X)/2} \cdot Z(X/\mathbb{F}_q, T), \tag{1.6}$$

où $\chi(X) = \sum_{i=0}^{2g} (-1)^i \deg P_i$ est un entier, qu'on peut calculer de façon « purement topologique ». Mieux, les polynômes $P_i(T)$ sont reliés par : $P_{d-i}(T) = P_i(q^{d-i} T)$.

Pour la fonction $\zeta(X/\mathbb{F}_q, s) = Z(X/\mathbb{F}_q, q^{-s})$, ces résultats se réécrivent comme suit. La fonction $\zeta(X/\mathbb{F}_q, s)$ (définie *a priori* sur le demi-plan $\mathrm{Re}(s) > d$) admet un prolongement méromorphe à $\mathbb{C}$. De plus, elle satisfait à une équation fonctionnelle pour $s \mapsto d - s$. Les pôles de $\zeta(X/\mathbb{F}_q, s)$ sont situés sur les droites $\mathrm{Re}(s) \in \{0, 1, \ldots, d\}$ et ses zéros sont situés sur les droites $\mathrm{Re}(s) \in \{1/2, 3/2, \ldots, d - 1/2\}$. Ce dernier point est l'analogue de l'hypothèse de Riemann pour $\zeta(X/\mathbb{F}_q, s)$.

La preuve des conjectures de Weil est basée sur une interprétation cohomologique de $Z(X/\mathbb{F}_q, T)$. Si l'on note $\overline{X} = X \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$, le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ agit sur $\overline{X}$. Pour un nombre premier $\ell \neq p$, il y a des espaces de cohomologie étale $\mathrm{H}^i_{\text{ét}}(\overline{X}, \mathbb{Q}_\ell)$ associés fonctoriellement à $X/\mathbb{F}_q$: nous les noterons $\mathrm{H}^i(X)$. Ce sont des $\mathbb{Q}_\ell$-espaces vectoriels de dimension finie et ils sont munis d'une action continue induite par l'action sur $\overline{X}$ du Frobenius $\mathrm{Fr}_q : x \mapsto x^q$, le générateur topologique de $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Dans le cas où X est projective et lisse, cette action est semi-simple. De plus, $\mathrm{H}^i(X) = 0$ lorsque $i < 0$ ou $i > 2d$. Avec les notations ci-dessus, on a

$$P_i(T) = \det\left(1 - \mathrm{Fr}_q^* \cdot T \,\middle|\, \mathrm{H}^i(X)\right)$$

et les racines inverses $\alpha_{i,j} \in \overline{\mathbb{Z}}$ de $P_i(T)$ sont les valeurs propres de Fr_q^* agissant sur $\mathrm{H}^i(X)$. Voir [Mil80, Chapter VI] pour les preuves de ces théorèmes. Nous renvoyons le lecteur à [Hin10, §2.3], [Kat81, §I-§II], [Ulm11, Lecture 0, §3- §4].

1.3.2 Cas particuliers des courbes

Les résultats de la section précédente s'écrivent de la façon plus simple dans le cas où $X = C$ est une courbe.

Théorème 1.3.2 (Weil, Grothendieck, Deligne)**.** *Soit C une courbe algébrique lisse et projective, définie sur un corps fini $\mathbb{F}_q$. Soit g le genre de C. Alors,*

(1) La fonction zeta $Z(C/\mathbb{F}_q, T)$ est une fraction rationnelle en T :

$$Z(C/\mathbb{F}_q, T) = \frac{L(C/\mathbb{F}_q, T)}{(1-T)(1-qT)},$$

où $L(C/\mathbb{F}_q, T)$ est un polynôme à coefficients entiers, de degré $2g$ et de coefficient constant 1.

(2) La fonction zeta $Z(C/\mathbb{F}_q, T)$ vérifie une équation fonctionnelle :

$$Z(C/\mathbb{F}_q, T) = (qT^2)^{g-1} \cdot Z\left(C/\mathbb{F}_q, (qT)^{-1}\right). \tag{1.7}$$

(3) Il existe des entiers algébriques $\alpha_1, \ldots, \alpha_{2g}$ tels que

$$L(C/\mathbb{F}_q, T) = \prod_{j=1}^{2g} (1 - \alpha_j T),$$

et α_i est de module $\sqrt{q}$ dans tout plongement complexe. L'ensemble des $\{\alpha_1, \ldots, \alpha_{2g}\}$ (avec multiplicités) est stable par $\alpha \mapsto q/\alpha$.

La preuve des conjectures de Weil dans le cas des courbes est bien antérieure au résultat de Deligne. Elle est due à F.K. Schmidt, H. Hasse (pour $g = 1$) et A. Weil. En termes de $\zeta(C/\mathbb{F}_q, s) = Z(C/\mathbb{F}_q, q^{-s})$, ces résultats impliquent que $s \mapsto \zeta(C/\mathbb{F}_q, s)$ admet un prolongement méromorphe à $\mathbb{C}$, qui satisfait une équation fonctionnelle pour $s \leftrightarrow 1 - s$; la fonction $\zeta(C/\mathbb{F}_q, s)$ ainsi prolongée a des pôles simples en $s = 0$ et $s = 1$ et ses zéros sont situés sur la droite $\mathrm{Re}\, s = 1/2$. Le théorème ci-dessus permet de déduire :

Corollaire 1.3.3 (Weil)**.** *Soit C une courbe algébrique lisse et projective de genre g, définie sur un corps fini $\mathbb{F}_q$. Il existe des entiers algébriques $\alpha_1, \ldots, \alpha_{2g}$ de module $|\alpha_i| = \sqrt{q}$ dans tout plongement complexe tels que,*

$$\forall n \geqslant 1, \quad \#C(\mathbb{F}_{q^n}) = q^n + 1 - \left(\alpha_1^n + \alpha_2^n + \cdots + \alpha_{2g}^n\right).$$

En particulier, on a

$$|\#C(\mathbb{F}_{q^n}) - q^n - 1| \leqslant 2g\sqrt{q}^n.$$

La fonction $\zeta(C/\mathbb{F}_q, s)$ a donc des pôles simples en $s \in \frac{2i\pi}{\log q} \cdot \mathbb{Z}$ et ses zéros sont sur la droite $\mathrm{Re}\, s = 1/2$. En particulier,

Remarque 1.3.4. Il y a un lien entre la fonction zeta (de Weil) de la courbe C et la fonction zeta (de Dedekind) de son corps de fonctions $K = \mathbb{F}_q(C)$ (voir [Ros02, Theorem 5.9]).

Remarque 1.3.5. La fonction zeta $\zeta(C/\mathbb{F}_q, s)$ a un pôle simple en $s = 1$, de résidu

$$\lim_{s\to 1}(s-1)\zeta(C/\mathbb{F}_q, s) = \frac{h_K}{q^g(1-1/q)\log q},$$

où $h_k = \prod_{j=1}^{2g}(1-\alpha_i)$ s'interprète comme un « nombre de classes » : h_k est le nombre de points $\mathbb{F}_q$-rationnels sur la jacobienne $\mathrm{Jac}(C)$ de C.

Exemple 1.3.6. Détaillons un cas particulier important. Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Comme E est de genre 1 la fonction zeta $Z(E/\mathbb{F}_q, T)$ de E est de la forme :

$$Z(E/\mathbb{F}_q, T) = \frac{(1-\alpha T)(1-\overline{\alpha}T)}{(1-T)(1-qT)},$$

où α est un entier algébrique de module $|\alpha| = \sqrt{q}$ dans tout plongement complexe. En particulier,

$$\forall n \in \mathbb{N}^*, \quad \#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \overline{\alpha}^n) = q^n + 1 - a_E(n),$$

où $a_E(n)$ est un entier. Ce dernier vérifie donc l'inégalité $|a_E(n)| = |\alpha^n + \overline{\alpha}^n| \leqslant 2q^{n/2}$. Sous cette forme, l'hypothèse de Riemann pour les courbes elliptiques est équivalente au Théorème de Hasse (*cf.* Théorème 1.3.9 ci-dessous). À chaque (classe d'isomorphisme de) courbe elliptique $E/\mathbb{F}_q$ est ainsi attaché un entier $a_E = \alpha + \overline{\alpha}$ tel que $a_E \in \mathbb{Z} \cap [-2\sqrt{q}, 2\sqrt{q}]$. Réciproquement, si $\mathbb{F}_q = \mathbb{F}_p$, la théorie de Honda-Tate (voir [WM71]) donne des conditions sur un entier a dans l'intervalle $[-2\sqrt{p}, 2\sqrt{p}]$ pour qu'il existe une courbe elliptique $E/\mathbb{F}_p$ telle que $a = a_E$ (et donc $\#E(\mathbb{F}_p) = p + 1 - a$).

Terminons ce paragraphe en rappelant l'identité ci-dessous (« de changement de base »).

Proposition 1.3.7. *Soit C une courbe projective lisse de genre g définie sur $\mathbb{F}_q$. Soit*

$$L(C/\mathbb{F}_q, T) = \prod_{i=1}^{2g}(1-\alpha_i \cdot T)$$

le numérateur de la fonction zeta $Z(C/\mathbb{F}_q, T)$. Pour toute extension finie $F_{q^n}/\mathbb{F}_q$, on a

$$L\left((C \times_{\mathbb{F}_q} \mathbb{F}_{q^n})/\mathbb{F}_{q^n}, T\right) = \prod_{i=1}^{2g}(1-\alpha_i^n \cdot T).$$

1.3.3 Fonction L d'une courbe elliptique

Soit E une courbe elliptique définie sur un corps de fonctions $K = \mathbb{F}_q(C)$. On note $\mathcal{B}(E/K)$ l'ensemble fini des places de K en lesquelles E a mauvaise réduction. Comme ci-avant, pour toute place v de K, on note d_v le degré de v et $\mathbb{F}_v$ le corps résiduel de K en v (de cardinal $q_v = q^{d_v}$). Pour toute place v, on désigne par $\overline{E}_v$ la courbe définie sur $\mathbb{F}_v$ dont un modèle est la réduction en v d'un modèle entier et minimal en v de E/K ($\overline{E}_v$ est une cubique plane, non nécessairement lisse). La fonction L de E/K est définie de façon analogue à la fonction L d'une courbe elliptique sur un corps de nombres, par des « décomptes locaux de points » : pour toute place v de K, on définit un entier a_v comme suit :

$$a_v := \begin{cases} q_v + 1 - \#\overline{E}_v(\mathbb{F}_v) & \text{si } E \text{ a bonne réduction en } v \\ 1 & \text{si } E \text{ a réduction multiplicative déployée en } v \\ -1 & \text{si } E \text{ a réduction multiplicative non déployée en } v \\ 0 & \text{si } E \text{ a réduction additive en } v. \end{cases}$$

Quelque soit le type de réduction de E en v, l'entier a_v satisfait $a_v = q_v + 1 - \#\overline{E}_v(\mathbb{F}_v)$ (voir [Ulm11, Lecture I, §8], [Sil09, Appendix C, §16]).

Ces entiers a_v sont l'ingrédient principal de la définition des facteurs locaux de la fonction L :

Définition 1.3.8. Soit E une courbe elliptique sur $K = \mathbb{F}_q(C)$. Pour toute place v de K, dont on note d_v le degré, on pose

$$L_v(E/K, T) := \begin{cases} 1 - a_v T^{d_v} + q^{d_v} \cdot T^{2d_v} & \text{si } E \text{ a bonne réduction en } v, \\ 1 - a_v T^{d_v} & \text{sinon.} \end{cases}$$

La *fonction L de E/K*, notée $L(E/K,T)$, est alors définie comme le produit eulérien de ces facteurs locaux :

$$L(E/K,T) := \prod_v L_v(E/K,T)^{-1} \in \mathbb{Z}[[T]],$$

le produit portant sur toutes les places v de K. De façon équivalente, on a

$$L(E/K,T) = \prod_{v\notin\mathcal{B}(E/K)} (1 - a_v T^{\deg v} + q_v T^{2\deg v})^{-1} \cdot \prod_{v\in\mathcal{B}(E/K)} (1 - a_v T^{\deg v})^{-1}.$$

Rappelons alors le Théorème (voir [Sil09, Chap. V, Thm 1.1] ou [Gro11, Lecture 2, §1-§2]) :

Théorème 1.3.9 (Hasse)**.** *Soit $v \notin \mathcal{B}(E/K)$ une place de bonne réduction, alors l'entier a_v satisfait*

$$|a_v| \leqslant 2\sqrt{q_v}.$$

Ainsi, les racines α_v et $\overline{\alpha_v}$ du polynôme $P(T) = 1 - a_v T + q_v T^2$ sont dans un corps quadratique imaginaire. De plus, si $\mathbb{F}_{v^n}/\mathbb{F}_v$ est l'unique extension de degré n de $\mathbb{F}_v$, on a

$$\#\overline{E}(\mathbb{F}_{v^n}) = q_v^n + 1 - (\alpha_v^n + \overline{\alpha_v}^n).$$

Pour $s \in \mathbb{C}$ convenable, on pose $\mathcal{L}(E/K,s) := L(E/K,q^{-s})$: c'est une série de Dirichlet à coefficients entiers en q^{-s}. Ce Théorème permet de montrer que $\mathcal{L}(E/K,s)$ est convergente dans le demi-plan $\mathrm{Re}(s) > 3/2$.

Noter que la fonction L de E détermine E à isogénie près (c'est une conséquence du théorème de Tate sur les endomorphismes des courbes elliptiques sur les corps finis). Renvoyons le lecteur à [Gro11, Appendix C] pour plus de détails.

Remarque 1.3.10. On peut aussi définir $L(E/K,T)$ comme fonction L d'Artin d'une représentation galoisienne. On procède comme suit (voir [HS00, Chapter F, §4.1], [Ulm11, Lecture 0, §5.2]). On fixe un nombre premier $\ell \neq p$ et on définit le module de Tate ℓ-adique de E par $T_\ell(E) := \varprojlim_{n\to\infty} E(K^{\mathrm{sep}})[\ell^n]$, ainsi que $V_\ell(E) := T_\ell(E)\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$. Ce dernier est muni d'une action $\mathbb{Q}_\ell$-linéaire continue de $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ et celle-ci induit une représentation

$$\rho_{E,\ell} : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to GL(V_\ell(E)) \simeq GL_2(\mathbb{Q}_\ell).$$

On définit alors ([Ulm11, Lecture 4, §1.3, §2.2])

$$L(E/K,T) := \prod_v \det\left(1 - \rho_{E,\ell}(\mathrm{Fr}_v)\cdot T^{d_v} \;\middle|\; (V_\ell(E)^\vee)^{I_v}\right)^{-1},$$

le produit portant sur toutes les places de K. On a noté Fr_v le Frobenius en v et I_v le groupe d'inertie de $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ en v. Cette définition se généralise aux variétés abéliennes de dimension supérieure.

Dans le cadre des courbes elliptiques sur les corps de fonctions, résumons les propriétés majeures de $L(E/K,T)$ en un théorème, dû à Grothendieck, Deligne, Raynaud, ...

Théorème 1.3.11 (Grothendieck, Deligne, Raynaud, ...)**.** *Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$. On notera g_C le genre de C.*

- *La fonction $L(E/K,T)$ est une fraction rationnelle à coefficients entiers en T,*
- *Son degré vaut*
$$\mathfrak{b}_{E/K} := \deg L(E/K,T) = \deg \mathcal{N}(E/K) + 4g_C - 4, \tag{1.8}$$
- *Elle satisfait à l'équation fonctionnelle suivante :*
$$L(E/K,T) = \pm(qT)^{\mathfrak{b}_{E/K}} \cdot L\left(E/K, \frac{1}{q^2T}\right),$$
- *De plus, si E n'est pas une courbe constante, $L(E/K,T)$ est un polynôme en T.*
- *Les racines inverses β_j de $L(E/K,T)$ sont de module $|\beta_j| = q$ dans tout plongement complexe.*

Une partie de ce théorème a été démontrée par Grothendieck (voir [Gro95]) au moyen de la cohomologie étale. La rationalité de $L(E/K,T)$ résulte alors de l'existence d'une formule de points fixes de Lefschetz, l'équation fonctionnelle se déduit de la dualité de Poincaré. Un bon résumé de la preuve se trouve dans [Ulm11, Lecture 1, §9], pour plus de détails, on peut consulter [Gro11, Appendix D] ou [Mil80, Chapter VI, §13]. L'« hypothèse de Riemann », *i.e.* l'assertion sur le module des racines

de $L(E/K,T)$, a été démontrée par Deligne. Enfin, la formule donnant le degré de $L(E/K,T)$ comme fraction rationnelle en T est due à Raynaud [Ray95] : c'est un calcul de caractéristique d'Euler-Poincaré pour un faisceau en cohomologie étale. Noter que le calcul du degré peut se faire de façon élémentaire, voir [Hal06, Corollary 5].

En termes de la fonction $s \mapsto \mathcal{L}(E/K,s) = L(E/K,q^{-s})$, ce théorème donne les résultats suivants : $\mathcal{L}(E/K,s)$ admet un prolongement méromorphe à $\mathbb{C}$ (et même holomorphe si E/K n'est pas constante), elle satisfait à une équation fonctionelle pour $s \mapsto 2-s$ et ses zéros sont situés sur la droite $\mathrm{Re}(s)=1$. En particulier, $\mathcal{L}(E/K,s)$ est méromorphe dans un voisinage de $s=1$.

Ceci permet de définir un nouvel invariant de E/K : son *rang analytique* $\mathrm{rang}_{an}\, E(K)$ donné par

$$\mathrm{rang}_{an}\, E(K) = \mathrm{ord}_{s=1}\, \mathcal{L}(E/K,s) = \mathrm{ord}_{T=q^{-1}}\, L(E/K,T).$$

On peut de plus définir la quantité suivante :

Définition 1.3.12. Soit E une courbe elliptique définie sur $K=\mathbb{F}_q(C)$. On appelle *valeur spéciale* de $L(E/K,T)$ (ou simplement de E/K) en $T=q^{-1}$, le réel $L^*(E/K,1)$ défini par l'évaluation en $T=q^{-1}$ de

$$L^*(E/K,T) := \frac{L(E/K,T)}{(1-qT)^r},$$

où $r = \mathrm{ord}_{T=q^{-1}}\, L(E/K,T)$. Ainsi défini, $L^*(E/K,1)$ est un nombre rationnel non nul.

Remarque 1.3.13. La définition de la valeur spéciale ci-dessus n'est peut-être pas la plus standard. En effet, on a plutôt l'habitude de définir la valeur spéciale comme : le premier coefficient non nul dans le développement de Taylor de $\mathcal{L}(E/K,s)$ en $s=1$:

$$\mathcal{L}(E/K,s) = L^* \cdot (s-1)^r + o((s-1)^r) \qquad (s \to 1).$$

Comme $(1-q^{1-s}) \sim (s-1)\cdot \log q$ (lorsque $s \to 1$), notre définition est équivalente à la version usuelle, à un facteur $(\log q)^r$ près. Nous préférons éviter l'apparition de facteurs irrationnels. Ce choix est cohérent avec la normalisation choisie de la hauteur de Néron-Tate. Entre autres, la conjecture « forte » de Birch et Swinnerton-Dyer ((BSD 3) dans la Conjecture 1.4.1 ci-dessous) s'écrit alors comme une égalité entre deux nombres rationnels.

Remarquons également que, si E/K n'est pas constante, la fonction $L(E/K,T)$ est un polynôme à coefficients entiers, divisible par $(1-qT)^r$ (où $r = \mathrm{ord}_{T=q^{-1}}\, L(E/K,T)$). Par suite, le polynôme $L^*(E/K,T)$ défini ci-dessus est lui-même à coefficients entiers et la valeur spéciale $L^*(E/K,1)$ est un élément de $\mathbb{Z}[q^{-1}]$.

Par ailleurs, l'hypothèse de Riemann pour $L(E/K,T)$ implique que la valeur spéciale $L^*(E/K,1)$ est strictement *positive* . En effet, comme les zéros de $s \mapsto \mathcal{L}(E/K,s)$ sont tous de partie réelle $\mathrm{Re}(s)=1$, la fonction $x \in \mathbb{R} \mapsto \mathcal{L}(E/K,x)$ ne s'annule pas sur $]1,+\infty]$ et est donc positive sur cet intervalle (puisque, par définition, $\mathcal{L}(E/K,x)$ est positif pour tout $x \in]3/2,+\infty]$). De même, $x \mapsto \mathcal{L}(E/K,x)/(x-1)^r$ est positive sur $x \in]1,+\infty]$: à la limite lorsque $x \to 1^+$, on voit donc que $L^*(E/K,1)$ est positive (elle est non nulle par construction).

1.3.4 Calcul pratique

Soit E une courbe elliptique non isotriviale sur un corps de fonctions $K=\mathbb{F}_q(C)$. En général, on sait dire peu de choses sur $L(E/K,T)$ sans la calculer explicitement comme un polynôme en T. Nous proposons deux approches pour calculer la fonction L d'une courbe elliptique E définie sur $K=\mathbb{F}_q(C)$.

Première approche Notons $\pi : \mathcal{E} \to C$ le modèle régulier minimal de E/K. On notera $\mathcal{B}$ l'ensemble des points fermés $v \in C$ pour lesquels la fibre $\pi^{-1}(v)$ est singulière.

Un calcul essentiellement formel relie alors les fonctions zeta de $\mathcal{E}$ et C à la fonction $L(E/K,T)$:

$$L(E/K,T) = \frac{Z(C/\mathbb{F}_q,T)\cdot Z(C/\mathbb{F}_q,qT)}{Z(\mathcal{E}/F_q,T)} \cdot \prod_{v\in\mathcal{B}} f_v(T),$$

où $f_v(T)$ est une fraction rationnelle à coefficients entiers, dépendant du type de Kodaira de la fibre de $\pi : \mathcal{E} \to C$ au-dessus de v. On trouvera les expressions explicites des différentes $f_v(T)$ possibles dans le formulaire de [Ulm11, Lecture 3, §6]. Un calcul différent, plus axé sur la géométrie de la surface elliptique $\mathcal{E} \to C$, est effectué dans [Shi92].

Le problème de calculer $L(E/K,T)$ se ramène donc, si $Z(C/\mathbb{F}_q,T)$ est connue, à expliciter $Z(\mathcal{E}/\mathbb{F}_q,T)$. Or, la fonction zeta de la surface $\mathcal{E}/\mathbb{F}_q$ s'écrit sous la forme :

$$Z(\mathcal{E}/\mathbb{F}_q,T)=\frac{P_1(T)\cdot P_1(qT)}{(1-T)\cdot P_2(T)\cdot(1-q^2T)},$$

où $P_1(T)\in\mathbb{Z}[T]$ est un polynôme dont les racines réciproques sont de module $\sqrt{q}$ et $P_2(T)\in\mathbb{Z}[T]$ est un polynôme dont les racines réciproques sont de module q (voir [Tat66], ou [Shi92, §2]). D'après l'interprétation cohomologique de la fonction zeta $Z(\mathcal{E}/\mathbb{F}_q,T)$, on a

$$P_1(T)=\det\left(1-\mathrm{Fr}_q^*\cdot T\,\middle|\,\mathrm{H}^1(\mathcal{E})\right)\quad\text{et}\quad P_2(T)=\det\left(1-\mathrm{Fr}_q^*\cdot T\,\middle|\,\mathrm{H}^2(\mathcal{E})\right),$$

où l'on a noté $\mathrm{H}^i(\mathcal{E})$ le i-ième groupe de cohomologie étale $\mathrm{H}^i_{\acute{e}t}(\overline{\mathcal{E}},\mathbb{Q}_\ell)$ et Fr_q^* l'endomorphisme de $\mathrm{H}^i(\mathcal{E})$ induit par l'action du Frobenius sur $\overline{\mathcal{E}}$. Pour préciser plus avant les polynômes $P_1(T)$ et $P_2(T)$, on a besoin d'une description explicite de la surface $\mathcal{E}/\mathbb{F}_q$. Citons trois situations favorables :

- Si $\mathcal{S}=X_1\times X_2$ est un produit de courbes projectives et lisses X_1,X_2 définies sur $\mathbb{F}_q$, alors la formule de Künneth [Mil80, Chapter VI, Theorem 8.5] permet de « décomposer » l'action de Fr_q^* sur $\mathrm{H}^i(\mathcal{S})$ en termes de son action sur les espaces $\mathrm{H}^a(X_1)$ et $\mathrm{H}^b(X_2)$ $(a,b\in\{0,1,2\})$. On peut alors exprimer $Z(\mathcal{S}/\mathbb{F}_q,T)$ en fonction de $Z(X_1/\mathbb{F}_q,T)$ et $Z(X_2/\mathbb{F}_q,T)$.
- Si $\mathcal{S}$ est une surface donnée comme un quotient $\mathcal{S}'/G$ d'une surface sous l'action d'un groupe fini abélien G agissant par $\mathbb{F}_q$-automorphismes (*i.e.* l'action de G commute à celle de Fr_q sur $\overline{\mathcal{S}'}$), alors G agit sur $\mathrm{H}^i(\mathcal{S}')$ par des automorphismes $\mathbb{Q}_\ell$-linéaires et on a (voir [Mil80, Chapter III, Theorem 2.20])
$$\mathrm{H}^i(\mathcal{S})=\mathrm{H}^i(\mathcal{S}'/G)\simeq\mathrm{H}^i(\mathcal{S}')^G.$$
Ce qui permet en théorie d'exprimer $Z(\mathcal{S}/\mathbb{F}_q,T)$ en fonction de $Z(\mathcal{S}'/\mathbb{F}_q,T)$.
- Si $\mathcal{S}'$ est obtenue par n éclatements en des points $\mathbb{F}_q$-rationnels à partir d'une surface $\mathcal{S}/\mathbb{F}_q$, alors
$$\begin{aligned}\det\left(1-\mathrm{Fr}_q^*\cdot T\,\middle|\,\mathrm{H}^1(\mathcal{S}')\right)&=\det\left(1-\mathrm{Fr}_q^*\cdot T\,\middle|\,\mathrm{H}^1(\mathcal{S})\right)\\ \text{et }\det\left(1-\mathrm{Fr}_q^*\cdot T\,\middle|\,\mathrm{H}^2(\mathcal{S}')\right)&=(1-qT)^n\cdot\det\left(1-\mathrm{Fr}_q^*\cdot T\,\middle|\,\mathrm{H}^2(\mathcal{S})\right).\end{aligned}$$
Voir [Mil80, Chapter V, Proposition 3.11]. Il s'ensuit que $Z(\mathcal{S}'/\mathbb{F}_q,T)=(1-qT)^{-n}\cdot Z(\mathcal{S}/\mathbb{F}_q,T)$.

Par suite, si le modèle régulier minimal d'une courbe elliptique E/K est donné comme désingularisation du quotient d'un produit de courbes sous l'action d'un groupe fini, la combinaison des trois techniques ci-dessus permet de donner explicitement $Z(\mathcal{E}/\mathbb{F}_q,T)$. Un tel calcul est mené à bien dans [Occ12, §2 -§3] ou dans [Ulm02, §3, §7]. L'inconvénient majeur de cette approche est la nécessité de construire le modèle régulier minimal, ce qui peut s'avérer délicat.

Seconde approche On peut également revenir à la définition de $L(E/K,T)$ comme une série génératrice. Rappelons que

$$L(E/K,T)=\prod_{v\notin\mathcal{B}}(1-a_vT^{\deg v}+q_vT^{2\deg v})^{-1}\cdot\prod_{v\in\mathcal{B}}(1-a_vT^{\deg v})^{-1}.$$

On peut alors démontrer les deux lemmes suivants :

Lemme 1.3.14. *Soit E une courbe elliptique définie sur un corps de fonctions $K=\mathbb{F}_q(C)$. Pour toute place v de K, de degré d_v, on note $\overline{E}_v$ la réduction modulo v d'un modèle entier et minimal de E en v (cf. Section 1.1.3). On pose alors*

$$a_v=q_v+1-\#\overline{E}_v(\mathbb{F}_v)=\begin{cases}\alpha_v+\overline{\alpha_v} & \text{si } E \text{ a bonne réduction en } v \text{ (voir Théorème 1.3.9),}\\ 0,\pm1 & \text{sinon (voir Définition 1.3.8).}\end{cases}$$

Alors, pour tout $n\in\mathbb{N}^*$, notant $\mathbb{F}_{v^n}$ l'extension de $\mathbb{F}_v$ de degré n, on a

$$\#\overline{E}_v(\mathbb{F}_{v^n})=\begin{cases}q_v^n+1-(\alpha_v^n+\overline{\alpha_v}^n) & \text{si } E \text{ a bonne réduction en } v,\\ q_v^n+1-a_v^n & \text{si } E \text{ a mauvaise réduction en } v.\end{cases}$$

Démonstration. Si E a bonne réduction en v, l'identité à démontrer est une conséquence directe du Théorème de Hasse (Théorème 1.3.9). Si E a mauvaise réduction, une analyse des trois cas possibles (réduction additive, réduction multiplicative déployée, réduction multiplicative non déployée) permet de conclure. □

Lemme 1.3.15. *Soit E une courbe elliptique définie sur $K = \mathbb{F}_q(t) = \mathbb{F}_q(\mathbb{P}^1)$. Pour tout point fermé $\tau \in \mathbb{P}^1$, auquel correspond une place v_τ de K, on note $\overline{E}_\tau$ la réduction d'un modèle entier minimal de E en v_τ. Pour tout $n \in \mathbb{N}^*$ et tout $\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})$, on pose*

$$A(\tau, q^n) := q^n + 1 - \#\overline{E}_\tau(\mathbb{F}_{q^n}).$$

Alors la fonction L de E vérifie l'identité formelle suivante :

$$\log L(E/K, T) = \sum_{n=1}^{\infty} \left(\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau, q^n) \right) \frac{T^n}{n}.$$

Démonstration. On pourra également consulter la première partie de la preuve de [CHU14, Theorem 3.2.1]. On note $\mathcal{B} \subset \mathbb{P}^1$ l'ensemble fini des places de K où E a mauvaise réduction. Par définition,

$$L(E/K, T) = \prod_{v \notin \mathcal{B}} (1 - a_v T^{\deg v} + q^{\deg v} T^{2 \deg v})^{-1} \cdot \prod_{v \in \mathcal{B}} (1 - a_v T^{\deg v})^{-1}.$$

Pour toute place v de K, on note d_v le degré de v, $\mathbb{F}_v$ son corps résiduel et $q_v = q^{d_v} = \#\mathbb{F}_v$. D'après le Lemme précédent, pour toute place v de K et toute extension $\mathbb{F}_{q_v^n}/\mathbb{F}_{q_v}$, on a

$$\#\overline{E}_v(\mathbb{F}_{q_v^n}) = \begin{cases} q_v^n + 1 - (\alpha_v^n + \overline{\alpha_v}^n) & \text{si } E \text{ a bonne réduction en } v, \\ q_v^n + 1 - a_v^n & \text{si } E \text{ a mauvaise réduction en } v. \end{cases}$$

On développe alors formellement le produit eulérien définissant $L(E/K, T)$ et on réarrange les termes. Sauf mention du contraire, les sommes $\sum_v$ portent sur l'ensemble des places de K.

$$\begin{aligned}
\log L(E_d/K, T) &= \sum_{v \notin \mathcal{B}} -\log\left((1 - \alpha_v T^{\deg v})(1 - \overline{\alpha_v} T^{\deg v})\right) + \sum_{v \in \mathcal{B}} -\log(1 - a_v T^{\deg v}) \\
&= \sum_{v \notin \mathcal{B}} \sum_{n=1}^{\infty} \frac{(\alpha_v^n + \overline{\alpha_v}^n)}{n} T^{n \deg v} + \sum_{v \in \mathcal{B}} \sum_{n=1}^{\infty} \frac{a_v^n}{n} T^{n \deg v} \\
&= \sum_{v \notin \mathcal{B}} \sum_{n=1}^{\infty} \frac{(\alpha_v^n + \overline{\alpha_v}^n)}{n} T^{n} + \sum_{v \in \mathcal{B}} \sum_{n=1}^{\infty} \frac{a_v^n}{n} T^{n \deg v} \\
&= \sum_{v} \sum_{n=1}^{\infty} \frac{q_v^n + 1 - \#\overline{E}_v(\mathbb{F}_{q_v^n})}{n} T^{n \deg v} = \sum_{n=1}^{\infty} \sum_{v} \frac{q_v^n + 1 - \#\overline{E}_v(\mathbb{F}_{q_v^n})}{n} T^{n \deg v} \\
&= \sum_{n=1}^{\infty} \sum_{v} \frac{q^{n \deg v} + 1 - \#\overline{E}_v(\mathbb{F}_{q^{n \deg v}})}{n} T^{n \deg v} \\
&= \sum_{m=1}^{\infty} \sum_{\substack{v \\ \text{tq. } \deg v | m}} \frac{q^m + 1 - \#\overline{E}_v(\mathbb{F}_{q^m})}{m / \deg v} T^m \\
&= \sum_{m=1}^{\infty} \frac{T^m}{m} \left(\sum_{\substack{v \text{ tq.} \\ \deg v | m}} \deg v \cdot \left(q^m + 1 - \#\overline{E}_v(\mathbb{F}_{q^m})\right) \right).
\end{aligned}$$

Soit $m \in \mathbb{N}^*$, à une place v de K de degré $d = \deg v$ divisant m correspond une $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbite de points $\tau \in \mathbb{P}^1(\mathbb{F}_{q^m})$ et cette orbite est de cardinal $\deg v$. Ainsi, à m fixé, on a

$$\sum_{\substack{v \text{ tq.} \\ \deg v | m}} \deg v \cdot \left(q^m + 1 - \#\overline{E}_v(\mathbb{F}_{q^m})\right) = \sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^m})} \left(q^m + 1 - \#\overline{E}_\tau(\mathbb{F}_{q^m})\right) = \sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^m})} A(\tau, q^m).$$

Ce qui conclut la preuve du Lemme. □

Nous privilégions dans nos calculs cette seconde approche, plus élémentaire.

1.4 Conjectures de Birch et Swinnerton-Dyer

La conjecture de Birch et Swinnerton-Dyer est une des conjectures majeures dans l'arithmétique des courbes elliptiques (et plus généralement, des variétés abéliennes) sur les corps globaux. Sur les corps de nombres, seuls quelques cas sont connus (voir par exemple [Sil09, Appendix C, §16.5], [HS00, Conjecture F.4.1.6]). C'est la raison pour laquelle ce travail se concentre sur les courbes elliptiques sur les corps de fonctions en caractéristique positive, où il est « facile » de dégager des familles infinies de courbes elliptiques vérifiant la conjecture de Birch et Swinnerton-Dyer. Nous parlons de quelques-unes de ces familles dans la Section 1.4.4.

1.4.1 Énoncé des conjectures de Birch et Swinnerton-Dyer

Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$. Dans ce contexte, l'énoncé des conjectures de Birch et Swinnerton-Dyer est dû à J. Tate [Tat66, Conjecture (C)]. La conjecture « faible » de Birch et Swinnerton-Dyer relie le comportement analytique de la fonction $L(E/K,T)$ (construite à partir d'invariants locaux de E) au groupe de Mordell-Weil (un invariant global) :

$$\operatorname{ord}_{T=q^{-1}} L(E/K,T) = \operatorname{rang} E(K).$$

La conjecture « forte » relie alors la valeur spéciale de $L(E/K,T)$ en $T = q^{-1}$ à des invariants arithmétiques de E/K.

Conjecture 1.4.1 (Birch et Swinnerton-Dyer)**.** *Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$. On désigne par g_C le genre de C. Alors*

(BSD 1) *La fonction $L(E/K,T)$, vue comme une fraction rationnelle en T, a un zéro en $T = q^{-1}$ de multiplicité égale au rang de $E(K)$. Autrement dit, on a*

$$\operatorname{rang} E(K) = \operatorname{rang}_{an} E(K) = \operatorname{ord}_{T=q^{-1}} L(E/K,T).$$

(BSD 2) *Le groupe de Tate-Shafarevich $Ш(E/K)$ est fini (Conjecture 1.2.10).*

(BSD 3) *La valeur spéciale $L^*(E/K,1)$ s'exprime de la façon suivante :*

$$L^*(E/K,1) = \frac{\#Ш(E/K)\cdot \operatorname{Reg}(E/K)}{\left(\#E(K)_{\mathrm{tors}}\right)^2}\cdot \mathcal{T}am(E/K)\cdot \frac{q^{1-g_C}}{H(E/K)}.$$

Les quantités du membre de droite ont été définies plus haut.

Remarque 1.4.2. Ces conjectures sont parfois appelées « la conjecture de Birch et Swinnerton-Dyer ». Pour plus de détails sur l'énoncé de celle(s)-ci dans ce contexte ou celui des variétés abéliennes sur les corps de fonctions, nous renvoyons la lectrice à [Tat66], [Ulm11, Lecture 1, §10 - §11], [Gro11, Lecture 2, §4], [Oes90, §3], [Gor79, §1.1] [Hin10, Conjecture 4.5] ou [HP16, §2]. Remarquons que [Tat66, Conjecture (C)] est énoncée en termes géométriques, c'est-à-dire à l'aide du modèle régulier minimal $\mathcal{E} \to C$ de la courbe E/K.

Noter également que nos normalisations de la hauteur de Néron-Tate (Définition 1.2.1) et de la valeur spéciale (Définition 1.3.12) permettent d'écrire (BSD 3) comme une égalité entre nombres *rationnels* (voir [HP16, Remark 2.5]).

Remarque 1.4.3. Observons la forte analogie de (BSD 3) avec la « formule des classes de Dirichlet » donnant le résidu de la fonction zeta d'un corps de nombres $k/\mathbb{Q}$ (*cf.* [Lan94, Chapter VIII, §2, Theorem 5], [RV99, Chapter 7, Theorem 7.2.1], [Hin10, Theorem 4.3] par exemple). Plus précisément, soit $k/\mathbb{Q}$ un corps de nombres de degré n et d'anneau des entiers $\mathcal{O}_k$: on note r_1 (resp. r_2) le nombre de plongements réels (resp. complexes) de k, $h_k = \#\mathcal{C}\ell(\mathcal{O}_k)$ son nombre de classes, $R_k = \operatorname{Reg}(\mathcal{O}_k^\times)$ son régulateur des unités, $\mu_k = \mathbb{G}_m(\mathcal{O}_k)_{\mathrm{tors}}$ le groupe des racines de l'unité de k et Δ_k la valeur absolue du discriminant (absolu) de k. Soit également $\zeta_k(s)$ la fonction zeta de Dedekind de k, prolongée grâce à son équation fonctionnelle en une fonction méromorphe sur $\mathbb{C}$. Alors $\zeta_k(s)$ a un pôle simple en $s = 1$, de résidu

$$\operatorname{res}_{s=1}\zeta_k(s) = \lim_{s\to 1}(s-1)\cdot\zeta_k(s) = \frac{h_k\cdot R_k}{\#\mu_k}\cdot 2^{r_1}(2\pi)^{r_2}\cdot\frac{1}{\sqrt{\Delta_k}}. \tag{1.9}$$

D'après son équation fonctionnelle, la fonction $\zeta_k(s)$ a un zéro d'ordre $r = r_1 + r_2 - 1 = \operatorname{rang}(\mathcal{O}_k^\times)$ en $s = 0$ et la formule des classes (1.9) peut se réécrire sous la forme :

$$\lim_{s\to 0}\frac{\zeta_k(s)}{s^r} = -\frac{h_k\cdot R_k}{\#\mu_k}.$$

Le lecteur peut consulter [HS00, Remark F.4.1.7], [Hin10, §5.2] pour plus de détails sur cette analogie et ses limites.

Remarque 1.4.4. La fonction L d'une courbe elliptique E/K est un invariant de la classe de K-isogénie de E, c'est donc aussi le cas de la valeur spéciale $L^*(E/K, 1)$. Cependant, les termes $\mathrm{Reg}(E/K)$, $\#Ш(E/K)$, $H(E/K)$, ... qui apparaissent dans la conjecture (BSD 3) sont (individuellement) seulement des invariants de la classe de K-isomorphisme de E : ils peuvent varier au sein d'une classe d'isogénie. Néanmoins, le produit du membre de droite de (BSD 3) est bien un invariant de la classe de K-isogénie de E (voir [Cas65], [Tat66, Theorem 2.1]).

1.4.2 Conjecture de Tate

Les conjectures de Birch et Swinnerton-Dyer pour les courbes elliptiques sur les corps de fonctions en caractéristique positive ont un pendant géométrique, que nous énonçons ici. J. Tate a en effet également proposé une conjecture plus générale et plus géométrique (voir [Tat65] et [Tat94]) concernant les surfaces sur les corps finis.

Soit S une surface projective et lisse définie sur $\mathbb{F}_q$. On note $\mathrm{NS}(S)$ son groupe de Néron-Séveri, le groupe des diviseurs sur S modulo la relation d'équivalence numérique (*cf.* [Ulm11, Lecture 2, §3.3], [Gor79, §4]). Le théorème de la base ([LN59], [Gor79, Corollary §4.3] [Lan83b, Chapter 6], [Con06]) affirme que $\mathrm{NS}(S)$ est un groupe de type fini : on note $r = \operatorname{rang} \mathrm{NS}(S)$ son rang. Soit par ailleurs $Z(S/\mathbb{F}_q, T)$ la fonction zeta de la surface $S/\mathbb{F}_q$ (voir Section 1.3.1). Vue comme une fraction rationnelle en T, $Z(S/\mathbb{F}_q, T)$ a un pôle en $T = q^{-1}$ et l'on a :

$$\operatorname{rang} \mathrm{NS}(S) \leqslant -\operatorname{ord}_{T=q^{-1}} Z(S/\mathbb{F}_q, T). \tag{1.10}$$

Voir les discussions de [Ulm11, Lecture 2, §9] et [SS10, §14.6]. On peut maintenant énoncer (une partie de) la conjecture de Tate (parfois appelée « conjecture T2 ») :

Conjecture 1.4.5 (Tate)**.** *Soit S une surface projective et lisse, définie sur $\mathbb{F}_q$. On a*

$$\operatorname{rang} \mathrm{NS}(S) = -\operatorname{ord}_{T=q^{-1}} Z(S/\mathbb{F}_q, T).$$

Nous renvoyons le lecteur à [Tat94], [Gor79, §1.1], [Ulm11, Lecture 2, Conjecture 9.2] pour de plus amples commentaires. La plupart des progrès en direction de la conjecture de Birch et Swinnerton-Dyer sont liés à la conjecture de Tate. Dans la suite du présent travail, nous aurons besoin de disposer de situations où les conjectures de Birch et Swinnerton-Dyer sont vraies inconditionnellement, il nous semble donc opportun de rappeler quelques faits à propos de la conjecture de Tate.

Théorème 1.4.6. *Soit C_1, C_2 deux courbes projectives et lisses définies sur $\mathbb{F}_q$. Alors la conjecture de Tate est vraie pour la surface $S = C_1 \times C_2$.*

Voir [Ulm11, Lecture 2, Theorem 12.1], le point important de la preuve est le théorème de Tate sur l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ sur les modules de Tate des jacobiennes de C_1 et C_2.

Théorème 1.4.7. *Soit S et S' deux surfaces projectives et lisses définies sur $\mathbb{F}_q$. On suppose qu'il existe un morphisme dominant $f : S \twoheadrightarrow S'$. Si la conjecture de Tate est vraie pour S, alors elle est vraie pour S'.*

Voir [Ulm11, Lecture 2, Proposition 11.1]. Il s'ensuit que :

Corollaire 1.4.8. *Soit S et S' deux surfaces projectives et lisses définies sur $\mathbb{F}_q$. On suppose que S et S' sont birationnelles. Alors la conjecture de Tate est vraie pour S si et seulement si elle l'est pour S'.*

La conjecture de Tate est en outre vérifiée par certaines surfaces explicites :

Théorème 1.4.9 (Shioda)**.** *Soit $\delta \in \mathbb{N}^*$ un entier premier à q et $c_0, \ldots, c_3 \in \mathbb{F}_q^\times$. La conjecture de Tate est vraie pour la surface de Fermat $\mathcal{F}'_d \subset \mathbb{P}^3$ définie sur $\mathbb{F}_q$ par*

$$\mathcal{F}'_d : \quad c_0 \cdot x_0^\delta + c_1 \cdot x_1^\delta + c_2 \cdot x_2^\delta + c_3 \cdot x_3^\delta = 0.$$

Le lecteur peut se reporter à [SK79, Theorem I] ou [Ulm11, Lecture 3, §10]. La démonstration est basée sur la structure « inductive » des variétés de Fermat : plus précisément, on peut montrer ([SK79, Lemma 1.1]) qu'il existe une application rationnelle dominante $F_1 \times F_2 \dashrightarrow \mathcal{F}'_\delta$, où F_1 et F_2 sont deux courbes de Fermat définies sur $\mathbb{F}_q$. Les Théorèmes 1.4.6 et 1.4.7 permettent alors de conclure.

1.4.3 Faits généraux sur les conjectures de Birch et Swinnerton-Dyer

Un certain nombre de résultats positifs sont connus à propos de la conjecture de Birch et Swinnerton-Dyer pour les courbes elliptiques sur les corps de fonctions. Premièrement, contrairement à la plupart des courbes elliptiques sur les corps de nombres, le prolongement analytique de la fonction L est connu (c'est le Théorème 1.3.11) et l'inégalité ci-dessous est toujours vraie (voir [Tat66], [Mil75]) :

$$\operatorname{rang} E(K) \leqslant \operatorname{rang}_{an} E(K) = \operatorname{ord}_{T=q^1} L(E/K, T). \tag{1.11}$$

Le résultat général le plus récent en direction de la Conjecture 1.4.1 s'écrit :

Théorème 1.4.10. *Soit E une courbe elliptique définie sur un corps de fonctions $K = \mathbb{F}_q(C)$. Alors les assertions suivantes sont équivalentes :*

(i) $\operatorname{rang}_{an} E(K) = \operatorname{rang} E(K)$ *(i.e.* (1.11) *est une égalité),*

(ii) $Ш(E/K)$ *est fini,*

(iii) Il existe un nombre premier ℓ ($\ell = p$ est autorisé) tel que $Ш(E/K)[\ell^\infty]$ de $Ш(E/K)$ est fini.

De plus, si l'une de ces conditions est satisfaite, les conjectures (BSD 1), (BSD 2) et (BSD 3) sont vraies.

Ce théorème est la combinaison de travaux de J. Tate [Tat66], J. Milne [Mil75] et K. Kato, F. Trihan [KT03] (pour un historique plus détaillé, voir [HP16, Remark 2.4]). Entre autres, ce résultat implique qu'il suffit de vérifier la conjecture « faible » de Birch et Swinnerton-Dyer (l'égalité entre rangs analytique et algébrique) pour démontrer la conjecture « forte ». Voir [Ulm11, Lecture 3, Theorem 8.1], [HP16, §2] et les références qui s'y trouvent. Citons à présent deux corollaires utiles de ces travaux, dont on trouvera les preuves dans [Tat66], [Mil75], [Gor79, Theorem §6.1] ou [Ulm11, Lecture 3, Theorem 8.1].

Théorème 1.4.11. *Soit E une courbe elliptique sur un corps de fonctions K. Si L/K est une extension finie et si la conjecture de Birch et Swinnerton-Dyer est vraie pour E_L/L, alors elle est vraie pour E/K.*

Théorème 1.4.12 (Gordon)**.** *Soit E une courbe elliptique sur un corps de fonctions K, on note $\pi : \mathcal{E} \to \mathbb{P}^1$ son modèle régulier minimal. La conjecture de Birch et Swinnerton-Dyer est vraie pour E/K si et seulement si la Conjecture de Tate est vraie pour $\mathcal{E}/\mathbb{F}_q$.*

Nous utiliserons en fait uniquement l'implication « Conjecture de Tate pour $\mathcal{E}$ $\Rightarrow$ Conjecture de Birch et Swinnerton-Dyer pour E ». Par ailleurs, la véracité de la Conjecture 1.4.1 pour une courbe elliptique E/K ne dépend que de la classe de K-isogénie de E (que cette isogénie soit de degré premier à p ou non, *cf.* [Tat66, Theorem 2.1]).

En combinant les résultats connus sur la conjecture de Tate et le Théorème 1.4.12, on obtient :

Théorème 1.4.13 (« Domination by a Product of Curves »)**.** *Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$, dont on note $\pi : \mathcal{E} \to C$ le modèle régulier minimal. On suppose qu'il existe une application rationnelle dominante*

$$C_1 \times C_2 \dashrightarrow \mathcal{E},$$

où C_1 et C_2 sont deux courbes projectives et lisses définies sur $\mathbb{F}_q$. Alors les conjectures de Birch et Swinnerton-Dyer sont vraies pour la courbe E/K.

Consulter [Ulm11, Lecture 3, Theorem 9.1] pour plus de détails. À l'aide de ce Théorème, nous pouvons énoncer plusieurs cas dans lesquels la conjecture de Birch et Swinnerton-Dyer est connue.

1.4.4 Cas connus des conjectures de Birch et Swinnerton-Dyer

Il existe plusieurs situations dans lesquelles la conjecture de Birch et Swinnerton-Dyer est vraie pour une courbe elliptique E/K. Citons-en trois, qui nous seront utiles dans la suite de ce travail. Dans tous ces cas, le point-clé est de démontrer que le modèle régulier minimal $\pi : \mathcal{E} \to C$ de E/K vérifie la conjecture de Tate (Théorème 1.4.12).

Courbes isotriviales

Théorème 1.4.14 (Milne). *Soit E une courbe elliptique* isotriviale *sur un corps de fonctions K. Alors la conjecture de Birch et Swinnerton-Dyer est vraie pour E/K.*

Démonstration. D'après le Théorème 1.4.11, il suffit de démontrer que la conjecture de Birch et Swinnerton-Dyer est vraie pour les courbes elliptiques constantes (puisqu'une extension finie de K rend constante une courbe elliptique isotriviale). Or si E est constante, il existe une courbe elliptique E_0 définie sur $\mathbb{F}_q$ telle que $E = E_0 \times_{\mathbb{F}_q} \mathbb{F}_q(C)$. Le modèle régulier minimal $\pi : \mathcal{E} \to C$ est alors un produit de courbes, nommément $\mathcal{E} = E_0 \times C$, et la conjecture de Tate est connue pour ces surfaces. On pourra consulter [Mil68] pour une preuve détaillée (ou [Gro11, Lecture 3, §2] pour un résumé). □

En particulier, la conjecture de Birch et Swinnerton-Dyer complète est vraie si E/K est une courbe elliptique constante. Passons maintenant en revue deux constructions de courbes elliptiques *non isotriviales* vérifiant les conjectures de Birch et Swinnerton-Dyer (*cf.* [Ulm11, Lecture 1, §12] [Gro11, Lecture 3, §3]).

Construction de Shioda Soit $\mathbb{F}_q$ un corps fini de caractéristique p. Considérons un polynôme en trois variables $f \in \mathbb{F}_q[X_1, X_2, X_3]$ qui est la somme d'exactement 4 monômes non nuls :

$$f = c_1 \cdot X_1^{a_{1,1}} X_2^{a_{1,2}} X_3^{a_{1,3}} + c_2 \cdot X_1^{a_{2,1}} X_2^{a_{2,2}} X_3^{a_{2,3}} + c_3 \cdot X_1^{a_{3,1}} X_2^{a_{3,2}} X_3^{a_{3,3}} + c_4 \cdot X_1^{a_{4,1}} X_2^{a_{4,2}} X_3^{a_{4,3}},$$

où les coefficients $c_i \in \mathbb{F}_q$ sont non nuls et $a_{i,j} \in \mathbb{N}$. Pour tout $i \in \{1,2,3,4\}$, on pose $a_{i,4} = 1 - a_{i,1} - a_{i,2} - a_{i,3}$ et A_f la matrice carrée formée avec les $a_{i,j}$:

$$A_f := [a_{i,j}]_{1 \leqslant i,j \leqslant 4} \in \mathcal{M}_4(\mathbb{Z}).$$

Soit alors $d(f) := |\det A_f| \in \mathbb{N}$: noter que $d(f)$ ne dépend ni de l'ordre des variables X_i, ni des coefficients $c_i \in \mathbb{F}_q^\times$. On dit que f satisfait la *condition de Shioda* si $d(f) \not\equiv 0 \bmod p$. L'intérêt de cette construction réside dans le Théorème ci-dessous [Ulm11, Lecture 1, Theorem 12.4] :

Théorème 1.4.15 (Ulmer, Shioda). *Soit E une courbe elliptique définie sur $K = \mathbb{F}_q(t)$. On suppose que E est birationnelle à une courbe affine plane $C_f \subset \mathbb{A}^2$ définie sur K par*

$$C_f : \quad f(t, X, Y) = 0,$$

où $f \in \mathbb{F}_q[t, X, Y] \subset K[X, Y]$ est la somme d'exactement 4 monômes non nuls et satisfait la condition de Shioda. Alors la conjecture de Birch et Swinnerton-Dyer est vraie pour $E/\mathbb{F}_q(t)$.

Démonstration. On pourra consulter [Ulm11, Lecture 3, §10] pour une preuve détaillée : celle-ci consiste essentiellement à utiliser le Théorème 1.4.13 avec le Théorème 1.4.9 de Shioda. □

Remarque 1.4.16. Soit $f_1 \in \mathbb{F}_q[t, X, Y]$ un polynôme satisfaisant la condition de Shioda. Pour tout entier d premier à q, on pose $f_d(t, X, Y) := f_1(t^d, X, Y)$. Alors f_d est la somme de 4 monômes non nuls et satisfait la condition de Shioda (voir [Ulm11, Lecture 3, Exercise 10.1]). On obtient un exemple de « Domination by a Product of Curves in a Tower ».

Noter que cette construction est relativement « rigide », au sens où varier les coefficients du 4-nôme f ne change pas la classe de $\overline{\mathbb{F}_q}(t)$-isomorphisme de la courbe E_f correspondante.

Construction de Berger Plus récemment, L. Berger [Ber08] a dégagé une nouvelle classe de courbes elliptiques sur $K = \mathbb{F}_q(t)$ pour lesquelles la conjecture de Birch et Swinnerton-Dyer est vraie :

Théorème 1.4.17 (Berger). *Soit E une courbe elliptique définie sur $K = \mathbb{F}_q(t)$. On suppose que E est birationnelle à une courbe projective $X \subset \mathbb{P}^1 \times \mathbb{P}^1$ définie sur K, dont une équation affine est*

$$X : \quad f(x) = t^d \cdot g(y),$$

où f et g sont deux fonctions rationnelles sur $\mathbb{P}^1$ et $d \in \mathbb{N}^*$ est premier à p. Alors la conjecture de Birch et Swinnerton-Dyer est vraie pour $E/\mathbb{F}_q(t)$.

La lectrice est invitée à consulter [Ber08, Theorem 2.3] ou [Ulm13] pour la preuve de ceci (dans un cadre plus général). Une esquisse de démonstration se trouve dans [Ulm11, Lecture 3, §11], [Ulm11, Lecture 5, §1]. La forme spécifique de la courbe $X/\mathbb{F}_q(t)$ assure une « Domination by a Product of Curves in a Tower » pour E.

Plus récemment encore, R. Pries et D. Ulmer [PU14, Corollary 3.1.4] ont démontré :

Théorème 1.4.18 (Pries-Ulmer). *Soit E une courbe elliptique définie sur $K = \mathbb{F}_q(t)$. On suppose que E est birationnelle à une courbe projective $Y \subset \mathbb{P}^1 \times \mathbb{P}^1$ définie sur K, dont une équation affine est*

$$Y : \quad f(x) - A(t) = g(y),$$

où f, g sont deux fonctions rationnelles sur $\mathbb{P}^1$ et $A \in \mathbb{F}_q[t]$ est un polynôme additif séparable. Alors la conjecture de Birch et Swinnerton-Dyer est vraie pour $E/\mathbb{F}_q(t)$.

1.5 Estimations diophantiennes

Avant d'entamer la description précise du ratio de Brauer-Siegel, présentons une série de résultats de nature « diophantienne » donnant des encadrements d'invariants associés à des courbes elliptiques.

1.5.1 Majoration de la torsion

Soit E une courbe elliptique définie sur un corps de fonctions $K = \mathbb{F}_q(C)$. Une conséquence immédiate du théorème de Mordell-Weil (Section 1.2.2) est que le sous-groupe de torsion $E(K)_{\text{tors}}$ est un groupe fini. Se pose alors naturellement la question d'en élucider la structure, ou plus simplement d'en majorer l'ordre en fonction d'invariants de E/K. Dans cette direction, D. Goldfeld et L. Szpiro [GS95, Theorem 13] ont obtenu :

Théorème 1.5.1 (Goldfeld-Szpiro). *Soit E une courbe elliptique* non constante *sur un corps de fonctions $K = \mathbb{F}_q(C)$. On note g_C le genre de C, p^e le degré d'inséparabilité de $j(E/K) : C \to \mathbb{P}^1$ et $\mathfrak{f}_{E/K}$ le degré du conducteur $\mathcal{N}(E/K)$. Alors :*

$$\#E(K)_{\text{tors}} \leqslant \max\left\{16(q-1)^2, \left(6p^e \cdot \frac{2g_C - 2 + \mathfrak{f}_{E/K}}{\mathfrak{f}_{E/K}}\right)^2\right\}.$$

En fait, on peut même donner une borne « uniforme » pour $\#E(K)_{\text{tors}}$:

Théorème 1.5.2. *Soit $K = \mathbb{F}_q(C)$ le corps des fonctions d'une courbe C de genre g_C. Il existe une constante $T_{g_C,q} > 0$ ne dépendant que de g_C et de q telle que, pour toute courbe elliptique E définie sur K, on a*

$$1 \leqslant \#E(K)_{\text{tors}} \leqslant T_{g_C,p}.$$

Ceci se démontre facilement dans le cas où E est isotriviale puisqu'alors un point de torsion correspond à une section constante de $\pi : \mathcal{E} \to C$:

$$\#E(K)_{\text{tors}} = \#E(\mathbb{F}_q) \leqslant (\sqrt{q}+1)^2.$$

Dans le cas général, on pourra consulter [Poo07] pour argument basé sur la gonalité des courbes modulaires (ou [Ulm11, Lecture 1, §7]).

Remarque 1.5.3. Pour le problème qui nous intéresse (*cf.* Section 1.6), nous pourrions nous contenter d'une majoration de la forme :

$$\forall \varepsilon > 0, \quad 1 \leqslant \#E(K)_{\text{tors}} \ll_\varepsilon H(E/K)^\varepsilon.$$

1.5.2 Majoration du nombre de Tamagawa

Soit E une courbe elliptique sur un corps de fonctions K. Nous aurons besoin (*cf.* Section 1.6) d'une majoration du nombre de Tamagawa $\mathcal{T}am(E/K)$ en termes de la hauteur $H(E/K)$.

Théorème 1.5.4. *Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$. On note g_C le genre de C. Le nombre de Tamagawa global de E est majoré de la façon suivante :*

$$\forall \varepsilon > 0, \qquad \mathcal{T}am(E/K) \ll_{K,\varepsilon} H(E/K)^\varepsilon,$$

où la constante implicite est effective et ne dépend que de ε, q et g_C.

C'est un cas particulier de [HP16, Theorem 6.5] si l'on suppose que la caractéristique de K est $\geqslant 5$ ou que E a réduction semi-stable en toute place de K. Le Théorème [HP16, Theorem 6.5] concerne de façon bien plus générale les variétés abéliennes A sur un corps de fonctions K (sous l'hypothèse que $p > 2d+1$ ou que A/K a partout réduction semi-stable). La preuve en est assez délicate, même dans le cas où A est une jacobienne. Nous donnons ci-dessous une preuve élémentaire dans le cas des courbes elliptiques (sans hypothèse spécifique sur la semi-stabilité ou la caractéristique). Celle-ci ne se généralise pas à des variétés abéliennes de plus grande dimension.

Démonstration. Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$ fixé. Nous noterons $g = g_C$ le genre de C. Pour démontrer le Théorème, il suffit de prouver que, lorsque $H(E/K) \to +\infty$,

$$\log \mathcal{T}am(E/K) = o\big(\log H(E/K)\big).$$

Par définition de la hauteur, on a $\log H(E/K) = \frac{\log q}{12} \cdot \deg \Delta_{\min}(E/K)$, il suffit donc de démontrer que, lorsque $\deg \Delta_{\min}(E/K) \to +\infty$,

$$\log \mathcal{T}am(E/K) = o\big(\deg \Delta_{\min}(E/K)\big).$$

C'est donc vers la preuve de cette dernière inégalité que nous nous tournons. Notons que nous utilisons ici le fait que la hauteur différentielle de E s'exprime en fonction de $\deg \Delta_{\min}(E/K)$, un invariant qui n'a pas d'analogue pour les variétés abéliennes de dimension plus grande. Soit v une place de K de degré $\deg v$: pour alléger les écritures, posons $c_v = c_v(E/K)$ le nombre de Tamagawa local de E en v et $\theta_v = \operatorname{ord}_v \Delta_v$ la valuation v-adique d'un discriminant minimal de E en v (voir Section 1.1.3). Enfin, nous désignons par $\mathcal{B}$ l'ensemble des places de K en lesquelles E a mauvaise réduction et $D = \deg \Delta_{\min}(E/K) = \sum_v \theta_v \deg v$. On peut supposer que $\mathcal{B}$ est non vide, *i.e.* que $D > 0$ (sinon, il n'y a rien à démontrer). D'après l'inégalité arithmético-géométrique, on a

$$0 \leqslant \log \mathcal{T}am(E/K) = \sum_{v \in \mathcal{B}} \log c_v \leqslant \#\mathcal{B} \cdot \log\left(\frac{1}{\#\mathcal{B}} \cdot \sum_{v \in \mathcal{B}} c_v\right). \tag{1.12}$$

Commençons par remarquer que

$$\sum_{v \in \mathcal{B}} c_v \leqslant 5 \cdot \deg \Delta_{\min} = 5 \cdot D. \tag{1.13}$$

En effet, pour toute place $v \in \mathcal{B}$ de mauvaise réduction, le théorème de Kodaira-Néron (Théorème 1.1.20) montre que

$$c_v \leqslant \max\{4, \operatorname{ord}_v \Delta_v\} \leqslant 4 + \operatorname{ord}_v \Delta_v \leqslant 5 \cdot \operatorname{ord}_v \Delta_v = 5\theta_v \leqslant 5\theta_v \cdot \deg v$$

et il ne reste qu'à sommer sur $v \in \mathcal{B}$ pour obtenir (1.13). Remarquons que, si la caractéristique de K est $\geqslant 5$ ou si E/K est semi-stable, on a même $c_v \leqslant \operatorname{ord}_v \Delta_v = \theta_v$. De (1.12), nous tirons que :

$$\log \mathcal{T}am(E/K) \leqslant \#\mathcal{B} \cdot \log\left(\frac{5D}{\#\mathcal{B}}\right). \tag{1.14}$$

Il s'agit maintenant de comparer $\#\mathcal{B}$ à D. Pour ce faire, introduisons un paramètre $Y > 0$ à fixer ultérieurement et séparons $\#\mathcal{B} = \sum_{v \in \mathcal{B}} 1$ en deux parties :

$$\#\mathcal{B} \leqslant \#\left\{v \in \mathcal{B} \;\middle|\; \theta_v \deg v \leqslant Y\right\} + \#\left\{v \in \mathcal{B} \;\middle|\; \theta_v \deg v \geqslant Y\right\}.$$

Le deuxième terme se majore facilement car $\theta_v \deg v \geqslant Y$ si et seulement si $1 \leqslant \frac{\theta_v \deg v}{Y}$:

$$\sum_{\substack{v \in \mathcal{B} \text{ tq.} \\ \theta_v \deg v \geqslant Y}} 1 \leqslant \sum_{\substack{v \in \mathcal{B} \text{ tq.} \\ \theta_v \deg v \geqslant Y}} \frac{\theta_v \cdot \deg v}{Y} \leqslant \frac{1}{Y} \sum_{v \in \mathcal{B}} \theta_v \deg v = \frac{\deg \Delta_{\min}}{Y} = \frac{D}{Y}.$$

Passons donc à la majoration du premier terme. On a

$$\sum_{\substack{v \in \mathcal{B} \text{ tq.} \\ \theta_v \deg v \leqslant Y}} 1 \leqslant \#\left\{v \in \mathcal{B} \;\middle|\; \theta_v \deg v \leqslant Y\right\} \leqslant \#\left\{v \in \mathcal{B} \;\middle|\; \deg v \leqslant Y\right\} \leqslant \#\left\{v \;\middle|\; \deg v \leqslant Y\right\}.$$

Or, l'analogue du Théorème des Nombres Premiers pour les corps de fonctions (voir [Bru92, Proposition 6.3] ou [Ros02]) implique l'existence d'une constante $\beta_K > 0$ (ne dépendant que de g_C et de q) telle que

$$\forall n \in \mathbb{N}^*, \quad \left|\#\left\{v \;\middle|\; \deg v = n\right\} - \frac{q^n}{n}\right| \leqslant \beta_K \cdot q^{n/2}.$$

De plus, on peut choisir $\beta_K = (2g_c + 1)/(1 - q^{-1})$. On en déduit (assez grossièrement) que

$$\#\left\{v \;\middle|\; \deg v \leqslant Y\right\} \leqslant 4(g_C + 1) \cdot q^Y.$$

Par conséquent, on a

$$\#\mathcal{B} \leqslant 4(g_C+1)\cdot q^Y + \frac{D}{Y}.$$

Choisissons à présent $Y>0$ tel que $q^Y = \frac{D}{\log D}$. La majoration ci-dessus s'écrit alors :

$$\#\mathcal{B} \leqslant 4(g_C+1)\cdot\frac{D}{\log D} + \frac{\log q\cdot D}{\log D+\log\log D} \leqslant 12(g_C+1)\log q\cdot\frac{D}{\log D} = \gamma_K\cdot\frac{D}{\log D}, \tag{1.15}$$

où l'on a posé $\gamma_K = 12(g_C+1)\log q$. À l'aide de (1.14), on peut à présent conclure la preuve du Théorème. Soit $\varepsilon>0$, distinguons deux cas :

– Ou bien $\#\mathcal{B} \leqslant \frac{\varepsilon}{2}\cdot\frac{D}{\log D}$, auquel cas la minoration triviale $\#\mathcal{B}\geqslant 1$ conduit à

$$\log \mathcal{T}am(E/K) \leqslant \#\mathcal{B}\cdot\log\left(\frac{5D}{\#\mathcal{B}}\right) \leqslant \#\mathcal{B}\cdot\log(5D) \leqslant \frac{\varepsilon}{2}\cdot D\cdot\left(1+\frac{\log 5}{\log D}\right).$$

Pour $D\geqslant 5$, nous avons donc $\log\mathcal{T}am(E/K)\leqslant\varepsilon\cdot D$.

– Ou bien $\#\mathcal{B} > \frac{\varepsilon}{2}\cdot\frac{D}{\log D}$ et l'on utilise la majoration (1.15). Ce qui entraîne que

$$\log \mathcal{T}am(E/K) \leqslant \#\mathcal{B}\cdot\log\left(\frac{5D}{\#\mathcal{B}}\right) \leqslant \gamma_K\cdot D\cdot\left(\frac{\log(10/\varepsilon)}{\log D}+\frac{\log\log D}{\log D}\right).$$

Pour D suffisamment grand (disons $D\geqslant d_0$), on a également $\log\mathcal{T}am(E/K)\leqslant\varepsilon\cdot D$.

Ainsi, pour tout $\varepsilon>0$, il existe $\delta=\max\{5,d_0\}\in\mathbb{N}^*$ (ne dépendant que de ε, q et g_C) tel que

$$\log\mathcal{T}am(E/K)\leqslant\varepsilon\cdot\deg\Delta_{\min}(E/K)$$

pour toute courbe elliptique E/K avec $\deg\Delta_{\min}(E/K)>\delta$. Ce qu'il fallait démontrer. □

1.5.3 Majoration du rang

Soit $K=\mathbb{F}_q(C)$ un corps de fonctions sur $\mathbb{F}_q$, on note g_C le genre de la courbe C. Si E est une courbe elliptique sur K, on peut s'attacher à majorer le rang de $E(K)$ en termes du conducteur $\mathcal{N}(E/K)$ ou de la hauteur $H(E/K)$ de E. Il existe deux telles bornes : celles-ci sont démontrées de façon « analytique » à partir de l'inégalité

$$\operatorname{rang}E(K)\leqslant\operatorname{ord}_{T=q^{-1}}L(E/K,T).$$

La première borne est basée sur le fait que $\operatorname{ord}_{T=q^{-1}}L(E/K,T)\leqslant\deg L(E/K,T)$: on a

$$\operatorname{rang}E(K)\leqslant\begin{cases}4g_C & \text{si } E/K \text{ est constante}\\ 4g_C-4+\deg\mathcal{N}(E/K) & \text{sinon.}\end{cases} \tag{1.16}$$

Cette majoration est « géométrique » : la quantité majorante n'est pas affectée par une extension finie $k/\mathbb{F}_q$ du corps des constantes. Mais, pour différentes extensions $k/\mathbb{F}_q$, à la fois $E(k(C))$ et la fonction $L(E/k(C),T)$ peuvent varier beaucoup. Ceci suggère de chercher une borne « arithmétique » qui serait sensible aux extensions $k(C)/\mathbb{F}_q(C)$.

Théorème 1.5.5 (Brumer). *Soit E une courbe elliptique sur le corps des fonctions $K=\mathbb{F}_q(C)$ d'une courbe C de genre g_C. On note $\mathfrak{f}_{E/K}$ le degré de son conducteur $\mathcal{N}(E/K)$. Alors le rang du groupe de Mordell-Weil $E(K)$ est majoré par*

$$\operatorname{rang}E(K)\leqslant\frac{(4g_C-4+\mathfrak{f}_{E/K})}{2\log\mathfrak{f}_{E/K}}\cdot\log q+\mathcal{O}\left(\frac{\mathfrak{f}_{E/K}\cdot(\log q)^2}{\sqrt{q}\cdot(\log\mathfrak{f}_{E/K})^2}\right), \tag{1.17}$$

la constante implicite ne dépendant que de q et de g_C.

Nous renvoyons la lectrice à [Bru92, Proposition 6.9] pour la preuve de ce Théorème, basée sur l'utilisation des formules explicites de Weil. Ce théorème est un analogue (inconditionnel) de la majoration (conditionnelle) de J.-F. Mestre [Mes86, Proposition II.1] du rang des courbes elliptiques sur $\mathbb{Q}$. La borne (1.17) est bien meilleure que la majoration « géométrique » (1.16) lorsque $\mathfrak{f}_{E/K}=\deg\mathcal{N}(E/K)$ est « grand » devant q.

Remarque 1.5.6. Contrairement au cas des courbes elliptiques sur les corps de nombres, on connaît des courbes elliptiques E définies sur $K = \mathbb{F}_q(t)$ dont le rang est arbitrairement grand. Autrement dit, il existe des familles infinies $\mathscr{E}$ de courbes elliptiques $E/\mathbb{F}_q(t)$ telles que

$$\limsup_{\substack{E\in\mathscr{E}\\ H(E/K)\to\infty}} \operatorname{rang} E(\mathbb{F}_q(t)) = +\infty.$$

Le premier tel exemple est dû à I. Shafarevich et J. Tate : il s'agit d'une famille de courbes elliptiques isotriviales (voir [TŠ67]). Le premier exemple de courbe elliptique non isotriviale dont le rang est arbitrairement grand est dû à D. Ulmer [Ulm02]. On pourra également consulter [Ulm14a] pour un autre exemple (dont nous reparlerons). Ces exemples montrent de fait que la majoration (1.17) est optimale lorsque $\deg \mathcal{N}(E/K) \to \infty$.

Signalons de plus que [Ulm07b, Theorem 4.7] permet, sous des hypothèses faibles, de démontrer que de nombreuses familles de courbes elliptiques sur $\mathbb{F}_q(t)$ sont de rang non borné. Ce phénomène de « rang non borné » semble même relativement « courant » sur les corps de fonctions (*cf.* [Ulm11, Lecture 4, Theorem 3.1.1]).

1.6 Ratio de Brauer-Siegel des courbes elliptiques

Pour conclure ce chapitre préliminaire, nous introduisons le principal objet d'étude de cette thèse et décrivons les problématiques liées. Nous renvoyons le lecteur à l'Introduction (ainsi qu'à [Hin07] et [HP16]) pour un exposé plus détaillé des motivations à considérer le ratio de Brauer-Siegel des courbes elliptiques.

1.6.1 Rappels sur le théorème de Brauer-Siegel

Soit $k/\mathbb{Q}$ un corps de nombres de degré $n = [k : \mathbb{Q}]$. On note Δ_k la valeur absolue de son discriminant. Alors les deux grands théorèmes de finitude de la théorie algébrique des nombres permettent de définir deux invariants arithmétiques importants :

- le groupe $\mathcal{C}\ell(\mathcal{O}_k)$ des classes d'idéaux de k est fini. On note $h_k = \#\mathcal{C}\ell(\mathcal{O}_k)$ son ordre, le *nombre de classes de* k.
- le groupe des unités de k, noté $\mathcal{O}_k^\times$, est un groupe de type fini. On peut définir $R_k = \operatorname{Reg}(\mathcal{O}_k^\times)$, le *régulateur des unités de* k.

Se pose naturellement la question d'encadrer ces deux quantités h_k et R_k en termes de Δ_k (le degré n de k étant un invariant trop grossier). De tels encadrements sont en général difficiles à obtenir : pour contourner en partie cette difficulté, on forme le *produit* $h_k \cdot R_k$: il s'avère que celui-ci est plus contrôlable (en termes de Δ_k) que les quantités h_k ou R_k prises individuellement. En effet :

Théorème 1.6.1 (Brauer-Siegel)**.** *Lorsque k parcourt une famille de corps de nombres, dont le degré $n = [k : \mathbb{Q}]$ est fixé et avec $\Delta_k \to \infty$, on a*

$$\forall \varepsilon > 0, \quad \Delta_k^{1/2-\varepsilon} \ll_\varepsilon h_k \cdot R_k \ll_\varepsilon \Delta_k^{1/2+\varepsilon}.$$

Ce théorème a été démontré par Siegel pour la famille des corps quadratiques (voir [Sie35]) et par Brauer dans le cas général (voir [Bra47]). On pourra consulter [Lan94, Chapter XVI] pour une preuve complète, ou [Hin10, Lecture 5] pour une esquisse détaillée. La preuve du Théorème 1.6.1 est généralement découpée en trois parties (par ordre de complexité croissante). Tout d'abord, au moyen de la formule des classes (Remarque 1.4.3), on relie $h_k \cdot R_k$ au résidu de la fonction zeta $\zeta_k(s)$ en $s = 1$, noté res_k. Encadrer $h_k \cdot R_k$ comme ci-dessus revient alors à obtenir, par des méthodes analytiques, un encadrement de la forme

$$\forall \varepsilon > 0, \quad \Delta_k^{-\varepsilon} \ll_\varepsilon \operatorname{res}_k \ll_\varepsilon \Delta_k^{\varepsilon}. \tag{1.18}$$

On commence par prouver la majoration dans (1.18), ce qui est relativement aisé. Il est même possible (*cf.* [Sie69]) d'écrire une majoration effective et explicite :

$$\operatorname{res}_k \leqslant 4\left(\tfrac{e}{n-1}\right)^{n-1} \cdot (\log \Delta_k)^{n-1} \ll_{n,\varepsilon} \Delta_k^{\varepsilon}.$$

La minoration de (1.18), elle, est nettement plus difficile à démontrer : il faut « contourner » (par l'absurde) la présence éventuelle de zéros de $\zeta_k(s)$ dans l'intervalle $[1 - c/\log \Delta_k, 1[$, qui sont à même de faire diminuer la taille du résidu res_k. La minoration du Théorème 1.6.1 est par conséquent *ineffective*.

1.6.2 Définition de $\mathfrak{Bs}(E/K)$

Suivant [HP16, Definition 1.2], posons la définition suivante.

Définition 1.6.2. Soit E une courbe elliptique définie sur un corps de fonctions $K = \mathbb{F}_q(C)$, on suppose que son groupe de Tate-Shafarevich $Ш(E/K)$ est fini. On définit alors son *ratio de Brauer-Siegel* par

$$\mathfrak{Bs}(E/K) := \frac{\log\left(\#Ш(E/K)\cdot \mathrm{Reg}(E/K)\right)}{\log H(E/K)}.$$

Le ratio de Brauer-Siegel d'une courbe elliptique n'a de sens que si l'on suppose que le groupe de Tate-Shafarevich de celle-ci est fini (*cf.* Conjecture 1.2.10). D'après [KT03] (voir Théorème 1.4.10), la finitude du groupe de Tate-Shafarevich $Ш(E/K)$ est équivalente aux conjectures de Birch et Swinnerton-Dyer pour E/K.

Comme on l'a expliqué en détail dans l'Introduction de cette thèse, cet invariant naît principalement de la volonté de savoir à quel point la majoration

$$\forall \varepsilon > 0, \qquad \#Ш(E/K)\cdot \mathrm{Reg}(E/K) \ll_\varepsilon H(E/K)^{1+\varepsilon} \tag{1.19}$$

conjecturée par Lang est optimale (voir [Lan83a, Conjecture 1]). L'enjeu est donc d'obtenir un *encadrement* du ratio de Brauer-Siegel : une majoration de celui-ci par $1+\varepsilon$ permet de démontrer l'inégalité (1.19) et une minoration par $1-\varepsilon$ donnerait que (1.19) est « optimale ».

Remarque 1.6.3. On peut, plus généralement, donner un sens au ratio de Brauer-Siegel d'une variété abélienne A définie sur un corps de fonctions $K = \mathbb{F}_q(C)$, pour peu que son groupe de Tate-Shafarevich $Ш(A/K)$ soit fini (*cf.* [HP16, Definition 1.2]). C'est d'ailleurs à ce niveau de généralité que se placent Hindry et Pacheco dans [HP16] : les résultats de cet article cités ci-dessous pour les courbes elliptiques valent également pour des variétés abéliennes de dimension plus grande.

Plus généralement encore, ce ratio pourrait aussi être défini pour une variété abélienne sur un corps de nombres (voir [Hin07]).

1.6.3 Lien avec la valeur spéciale

Pour étudier le ratio de Brauer-Siegel $\mathfrak{Bs}(E/K)$ d'une courbe elliptique E/K (variant dans une famille), nous ferons un usage constant du lien qui existe entre celui-ci et la valeur spéciale $L^*(E/K,1)$ de la fonction L de E/K.

Proposition 1.6.4. *Soit $\mathscr{E}$ une famille de courbes elliptiques définies sur un corps de fonctions $K = \mathbb{F}_q(C)$ fixé. On suppose que toutes les courbes elliptiques $E \in \mathscr{E}$ vérifient la conjecture de Birch et Swinnerton-Dyer (voir Section 1.4.4). Alors, lorsque $H(E/K) \to \infty$,*

$$\mathfrak{Bs}(E/K) = 1 + \frac{\log L^*(E/K,1)}{\log H(E/K)} + o(1),$$

la constante implicite ne dépendant que de q et g_C, le genre de C.

Démonstration. Soit $E \in \mathscr{E}$ une courbe elliptique. Il suffit de supposer que E/K satisfait à la conjecture de Birch et Swinnerton-Dyer « faible » pour qu'elle vérifie la conjecture « forte » (*cf.* Section 1.4.3). Auquel cas, la valeur spéciale de la fonction L de E/K s'exprime sous la forme :

$$L^*(E/K,1) = \frac{\#Ш(E/K)\cdot \mathrm{Reg}(E/K)}{\left(\#E(K)_{\mathrm{tors}}\right)^2}\cdot \mathcal{T}am(E/K)\cdot \frac{q^{1-g_C}}{H(E/K)}.$$

En passant au logarithme et en divisant par $\log H(E/K)$, on obtient que

$$\mathfrak{Bs}(E/K) = 1 + \frac{\log L^*(E/K,1)}{\log H(E/K)} + \frac{f(E/K)}{\log H(E/K)},$$

où l'on a posé $f(E/K) = 2\log \#E(K)_{\mathrm{tors}} - \log \mathcal{T}am(E/K) - \log q^{1-g_C}$. Pour terminer la preuve de la Proposition, il faut vérifier que $\frac{f(E/K)}{\log H(E/K)} = o(1)$ est bien un terme d'erreur. Ceci est une conséquence des encadrements exposés à la Section 1.5. En effet, il existe une constante T_{q,g_C} telle que, pour toute courbe elliptique E/K on a (*cf.* Théorème 1.5.2)

$$1 \leqslant \#E(K)_{\mathrm{tors}} \leqslant T_{q,g_C}.$$

En outre, d'après le Théorème 1.5.4, on a

$$0 \leqslant \log \mathcal{T}am(E/K) = o\big(\log H(E/K)\big),$$

la constante implicite ne dépendant que de q et g_C. Par suite, lorsque $H(E/K) \to \infty$, on a

$$o(1) + \frac{A_{q,g_C}}{\log H(E/K)} \leqslant \frac{f(E/K)}{\log H(E/K)} \leqslant \frac{B_{q,g_C}}{\log H(E/K)},$$

où $A_{q,g_C} = (g_C - 1)\log q$ et $B_{q,g_C} = 2\log T_{q,g_C} + A_{q,g_C}$ sont des constantes ne dépendant que de q et du genre de C. Par conséquent, $f(E/K) = o\big(\log H(E/K)\big)$ et on a bien la relation recherchée. □

Si l'on fixe un corps de fonctions K, la taille de la valeur spéciale $L^*(E/K, 1)$ de la fonction L d'une courbe elliptique E/K (qui vérifie la conjecture de Birch et Swinnerton-Dyer) gouverne donc la taille du ratio de Brauer-Siegel $\mathfrak{Bs}(E/K)$ de celle-ci.

1.6.4 Conjectures et résultats connus

Soit $K = \mathbb{F}_q(C)$ un corps de fonctions. En relation avec l'algorithme conjectural proposé par Manin ([Man71, Chapter II, §11]) pour calculer effectivement une base du groupe de Mordell-Weill $E(K)$ d'une courbe elliptique, Lang ([Lan83a, Conjecture 2]) a conjecturé la majoration suivante : si E est une courbe elliptique sur K dont le groupe de Tate-Shafarevich $Ш(E/K)$ est fini,

$$\forall \varepsilon > 0, \qquad \#Ш(E/K) \cdot \mathrm{Reg}(E/K) \ll_{K,\varepsilon} H(E/K)^{1+\varepsilon}.$$

La conjecture originale de Lang concerne uniquement les courbes elliptiques définies sur $\mathbb{Q}$, mais son extension à un corps de base plus général est immédiate (voir [Hin07, (5.6)] ou [HP16, Remark 1.14]). Une fois traduite en termes de ratio de Brauer-Siegel, cette conjecture s'écrit :

Conjecture 1.6.5 (Lang, Hindry)**.** *Soit K un corps de fonctions et E une courbe elliptique définie sur K. Si E/K a un groupe de Tate-Shafarevich fini, on a*

$$\mathfrak{Bs}(E/K) \leqslant 1 + o(1), \tag{1.20}$$

lorsque $H(E/K) \to \infty$.

Guidé par l'analogie avec le théorème de Brauer-Siegel classique, il est naturel de se demander si une minoration du même ordre de grandeur est vraie : *i.e.* a-t-on

$$1 - o(1) \leqslant \mathfrak{Bs}(E/K) \ ? \qquad (H(E/K) \to \infty) \tag{1.21}$$

C'est la conjecture « optimiste » initialement proposée par Hindry (voir [Hin07, Conjecture 5.5]). Cependant, son auteur indique (*cf.* [HP16, Observations 1.15 (b)]) ne plus croire en la véracité de celle-ci en général. Pour l'heure, il semble plus prudent d'avancer :

Conjecture 1.6.6 (Hindry)**.** *Soit K un corps de fonctions et E une courbe elliptique définie sur K. Si E/K a un groupe de Tate-Shafarevich fini, on a*

$$0 + o(1) \leqslant \mathfrak{Bs}(E/K), \tag{1.22}$$

lorsque $H(E/K) \to \infty$.

Nous reviendrons à la Section 1.6.6 sur des heuristiques qui suggèrent que (1.21) est même « bien trop optimiste » au sens fort suivant (voir [HP16, Conjecture 1.3]) :

Conjecture 1.6.7 (Hindry)**.** *Soit K un corps de fonctions. Lorsque E parcourt la famille de toutes les courbes elliptiques sur K (on suppose que leur groupe de Tate-Shafarevich est fini), on a*

$$0 = \liminf \mathfrak{Bs}(E/K). \tag{1.23}$$

Autrement dit, la minoration (1.22) de la Conjecture 1.6.6 ne peut pas être améliorée en général.

Les deux Conjectures 1.6.5 et 1.6.6 ont été démontrées conditionnellement à la finitude du groupe de Tate-Shafarevich (voir les preuves de [HP16, Theorem 1.10] et [HP16, Corollary 1.13]). Pour énoncer ce résultat, nous introduisons la notation suivante : si $K = \mathbb{F}_q(C)$ est un corps de fonctions, $\mathscr{E}\ell\ell_{/K}$ désigne la famille de toutes les courbes elliptiques définies sur K, ordonnée par hauteur croissante.

Théorème 1.6.8 (Hindry - Pacheco). *Soit $K = \mathbb{F}_q(C)$ un corps de fonctions fixé. On suppose que $Ш(E/K)$ est fini pour toute $E \in \mathscr{E}\ell\ell_{/K}$ (ou, de façon équivalente, que la conjecture de Birch et Swinnerton-Dyer est vraie pour toute $E \in \mathscr{E}$). Alors*

$$0 \leqslant \liminf_{E \in \mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) \leqslant \limsup_{E \in \mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) \leqslant 1.$$

Nous présenterons à la Section 1.6.5 une esquisse de la preuve de ce théorème. Les auteurs montrent également (voir [HP16, Theorem 7.12]) que l'inégalité tout à droite est optimale : Hindry et Pacheco exhibent une certaine famille infinie $\mathscr{E}_0$ de courbes elliptiques définie sur $K = \mathbb{F}_q(t)$ qui vérifie inconditionnellement

$$\limsup_{E \in \mathscr{E}_0} \mathfrak{Bs}(E/K) = \lim_{\substack{E \in \mathscr{E}_0 \\ H(E/K) \to \infty}} \mathfrak{Bs}(E/K) = 1.$$

Plus explicitement, ils prouvent :

Théorème 1.6.9 (Hindry - Pacheco). *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \geqslant 1$ premier à p, on considère la courbe elliptique E_d définie sur K par le modèle de Weierstrass affine*

$$E_d : \quad Y^2 + XY = X^3 - t^d.$$

Le groupe de Tate-Shafarevich $Ш(E_d/K)$ est fini. De plus, on a $\lim_{d\to\infty} \mathfrak{Bs}(E_d/K) = 1$. En d'autres termes, lorsque $d \to \infty$,

$$\log\big(\#Ш(E_d/K) \cdot \mathrm{Reg}(E_d/K)\big) \sim \log H(E_d/K) \sim \frac{\log q}{6} \cdot d.$$

Cette famille de courbes elliptiques fournit le *premier exemple inconditionnel* où il est possible de démontrer que le ratio de Brauer-Siegel a une limite et que cette limite vaut 1. La famille des courbes E_d ci-dessus avait déjà été étudiée en détail par Ulmer [Ulm02], qui a démontré que les courbes E_d vérifient la conjecture de Birch et Swinnerton-Dyer (*via* la construction de Shioda, *cf.* Théorème 1.4.15). Ce qui implique la finitude de $Ш(E_d/K)$ pour tout $d \in \mathbb{N}^*$ premier à q (voir Théorème 1.4.10).

1.6.5 Esquisse de la preuve du Théorème 1.6.8

Comme on l'a expliqué ci-avant (Proposition 1.6.4), la preuve d'un encadrement du ratio de Brauer-Siegel d'une courbe elliptique E/K vérifiant les conjectures de Birch et Swinnerton-Dyer peut se faire en encadrant la valeur spéciale $L^*(E/K, 1)$ de la fonction L associée à E/K. Fixons dans cette section un corps de fonctions $K = \mathbb{F}_q(C)$ et notons g_C le genre de la courbe C. Pour toute courbe elliptique E définie sur K, rappelons que la fonction $L(E/K, T)$ est une fraction rationnelle en T (et même un polynôme en T si E/K n'est pas constante) de degré $\deg L(E/K, T)$ noté $\mathfrak{b}_{E/K} := \deg \mathcal{N}(E/K) + 4g_C - 4$ (voir Théorème 1.3.11). Il sera commode d'écrire d'abord des encadrements de la valeur spéciale $L^*(E/K, 1)$ en termes de $\mathfrak{b}_{E/K}$ plutôt qu'en termes de $H(E/K)$.

On peut d'abord démontrer un « encadrement trivial » de la valeur spéciale (la minoration sera dite « de Liouville »).

Proposition 1.6.10 (Hindry - Pacheco). *Soit $K = \mathbb{F}_q(C)$ un corps de fonctions et E une courbe elliptique définie sur K. La valeur spéciale $L^*(E/K, 1)$ de la fonction L associée à E admet l'encadrement :*

$$-\frac{\log q}{2} \leqslant \frac{\log |L^*(E/K, 1)|}{\mathfrak{b}_{E/K}} \leqslant \big(1 + o(1)\big) \cdot \log 2, \tag{1.24}$$

lorsque $\mathfrak{b}_{E/K} = \deg L(E/K, T) \to \infty$.

Démonstration. Contentons-nous de démontrer ceci lorsque la courbe E/K n'est pas constante et renvoyons la lectrice à la preuve du [HP16, Lemma 7.1] pour le cas général. La valeur spéciale $L^*(E/K, 1)$ est, par définition, la valeur en $T = q^{-1}$ du polynôme $L^*(E/K, T)$ (*cf.* Définition 1.3.12). Ce dernier est à coefficients entiers et son degré vaut

$$\deg L^*(E/K, T) = \deg L(E/K, T) - r_{an}(E/K) \leqslant \mathfrak{b}_{E/K}.$$

Rappelons la « remarque de Liouville » suivante : si $L^*(T)$ est un polynôme à coefficients entiers de degré b alors, ou bien $L^*(q^{-1}) = 0$ ou bien $q^b \cdot L^*(q^{-1}) \in \mathbb{Z} \smallsetminus \{0\}$. Cette remarque donne dans un premier temps que

$$\big|q^{\mathfrak{b}_{E/K}} \cdot L^*(E/K, 1)\big| \geqslant 1.$$

En utilisant l'équation fonctionnelle satisfaite par $L(E/K,T)$ (*cf.* Théorème 1.3.11) et donc également par $L^*(E/K,T)$, la minoration ci-dessus peut être améliorée en

$$\left| q^{\left\lfloor \frac{\mathfrak{b}_{E/K}+1}{2} \right\rfloor} \cdot L^*(E/K,1) \right| \geqslant 1.$$

D'où la minoration donnée dans la proposition, en passant au logarithme. Pour prouver la majoration, on utilise le fait que la fonction L de E/K vérifie l'hypothèse de Riemann (*cf.* Théorème 1.3.11) : on peut fixer des entiers algébriques β_j ($j = 1, \dots, \mathfrak{b}_{E/K}$), de valeur absolue q dans tout plongement complexe, tels que

$$L(E/K,T) = \prod_{j=1}^{\mathfrak{b}_{E/K}} (1 - \beta_j \cdot T).$$

On utilise alors, sur chacun des facteurs, l'inégalité triangulaire : $\left|1 - \beta_j \cdot q^{-1}\right| \leqslant 1 + |\beta_j| \cdot |q|^{-1} = 2$. D'où la seconde inégalité recherchée car l'ordre d'annulation de $L(E/K,T)$ en $T = q^{-1}$ est négligeable devant $\mathfrak{b}_{E/K} = \deg L(E/K,T)$ (d'après la majoration du rang de Brumer [Bru92] ; Théorème 1.5.5). Plus précisément, notant $\mathcal{Z}$ l'ensemble des indices j tels que $\beta_j = q$, on a

$$|L^*(E/K,1)| = \left| \prod_{j \notin \mathcal{Z}} \left(1 - \beta_j \cdot q^{-1}\right) \right| \leqslant 2^{\mathfrak{b}_{E/K} - \#\mathcal{Z}} \leqslant 2^{\mathfrak{b}_{E/K} + o\left(\mathfrak{b}_{E/K}\right)},$$

où $\#\mathcal{Z} = \operatorname{ord}_{T=q^{-1}} L(E/K,T) = r_{an}(E/K)$. □

Si E/K est une courbe elliptique vérifiant la conjecture de Birch et Swinnerton-Dyer, on déduit de cet encadrement (et de la Proposition 1.6.4) que

$$-5 + o(1) \leqslant \mathfrak{Bs}(E/K) \leqslant 1 + \frac{12 \cdot \log 2}{\log q} + o(1) \qquad (\text{lorsque } H(E/K) \to \infty).$$

En effet, il est aisé de « traduire » l'encadrement (1.24) ci-dessus en un encadrement de $L^*(E/K,1)$ en termes de $H(E/K)$: d'après le Théorème 1.3.11 et la Remarque 1.1.14, on a

$$\begin{aligned} \mathfrak{b}_{E/K} = \deg \mathcal{N}(E/K) + 4g_C - 4 &\leqslant \deg \Delta_{\min}(E/K) + 4g_C = \frac{12}{\log q} \cdot \log H(E/K) + 4g_C \\ &\ll_{q,g_C} \log H(E/K), \end{aligned}$$

la constante implicite ne dépendant que de q et du genre g_C de C.

Pour compléter la preuve du Théorème 1.6.8, il faut à présent améliorer à la fois la majoration et la minoration. De ces deux points, la majoration est la plus simple à obtenir : avec des méthodes standards d'analyse complexe, Hindry et Pacheco démontrent (*cf.* [HP16, Theorem 7.5]) :

Proposition 1.6.11 (Hindry - Pacheco)**.** *Soit $K = \mathbb{F}_q(C)$ un corps de fonctions et E une courbe elliptique définie sur K. Il existe une constante β_K (ne dépendant que de K) telle que*

$$\frac{\log |L^*(E/K,1)|}{\mathfrak{b}_{E/K}} \leqslant \beta_K \cdot \frac{\log\log \mathfrak{b}_{E/K}}{\log \mathfrak{b}_{E/K}} = o(1),$$

lorsque $\mathfrak{b}_{E/K} = \deg L(E/K,T) \to \infty$.

De cette majoration plus forte, on déduit que $\log |L^*(E/K,1)| / \log H(E/K) \leqslant o(1)$ et que

$$\mathfrak{Bs}(E/K) \leqslant 0 + o(1) \qquad (\text{lorsque } H(E/K) \to \infty).$$

Cette majoration est donc suffisante pour démontrer la Conjecture 1.6.5 de Lang si E/K vérifie la conjecture de Birch et Swinnerton-Dyer.

Cependant, les méthodes analytiques ne suffisent pas, en général, pour améliorer la minoration « triviale » de $\mathfrak{Bs}(E/K)$. Un joli argument diophantien (*cf.* [HP16, Proposition 7.6]) permet tout de même de conclure la preuve du Théorème 1.6.8 :

Proposition 1.6.12 (Hindry - Pacheco). *Soit K un corps de fonctions et E une courbe elliptique définie sur K. Alors,*

$$0 - o(1) \leqslant \frac{\log \mathrm{Reg}(E/K)}{\log H(E/K)} \qquad (\textit{lorsque } H(E/K) \to \infty).$$

Nous ne reproduisons pas ici la preuve de [HP16, Proposition 7.6], préférant renvoyer le lecteur à cette référence. Notons cependant que l'inégalité est *inconditionnelle*, On peut alors utiliser la majoration triviale $\log \mathrm{Reg}(E/K)/\log H(E/K) \leqslant \mathfrak{Bs}(E/K)$ (qui, elle, est conditionnelle à la conjecture de Birch et Swinnerton-Dyer) et obtenir la minoration recherchée de $\mathfrak{Bs}(E/K)$:

$$0 - o(1) \leqslant \mathfrak{Bs}(E/K) \qquad (\text{lorsque } H(E/K) \to \infty).$$

Remarque 1.6.13. Mentionnons une approche alternative pour démontrer la Proposition 1.6.12 (suggérée par Ulmer). Il s'agit de montrer que pour toute courbe elliptique E/K, on a

$$\forall \varepsilon > 0, \qquad \mathrm{Reg}(E/K) \gg_\varepsilon H(E/K)^{-\varepsilon}.$$

Pour une telle courbe E/K, on note $\pi : \mathcal{E} \to C$ son modèle régulier minimal. Pour toute place v de K, on note Φ_v l'ensemble des composantes irréductibles de la fibre $\pi^{-1}(v)$, $E_v^0 \in \Phi_v$ la composante neutre et $f_v = \#\Phi_v$. On peut alors définir F_v le sous-groupe de $\mathrm{NS}(\mathcal{E})$ engendré par $\Phi_v \smallsetminus \{E_v^0\}$: c'est un groupe libre de rang $f_v - 1$. On peut alors restreindre la forme d'intersection sur $\mathcal{E}$ à F_v : soit δ_v le discriminant de cette forme bilinéaire restreinte (et on pose $\delta_v = 1$ si $f_v = 1$). Alors δ_v vaut 1 pour presque toute place v de K. Avec ces notations, on a [Ulm14a, Proposition 9.1]

$$\frac{\mathrm{Reg}(E/K) \cdot \prod_v \delta_v}{(\#E(K)_{\mathrm{tors}})^2} \in \mathbb{Z} \smallsetminus \{0\}.$$

Il est aisé de voir que la minoration souhaitée de $\mathrm{Reg}(E/K)$ suit de la majoration

$$\forall \varepsilon > 0, \qquad \prod_v \delta_v \ll_\varepsilon H(E/K)^\varepsilon,$$

majoration que l'on pourrait montrer en adaptant la preuve du Théorème 1.5.4, après étude au cas par cas de la valeur de δ_v en fonction du type de réduction de E en v (*cf.* la classification des réseaux F_v possibles dans [SS10, §6.2-§6.5]).

Remarque 1.6.14. À l'aide de la Proposition 1.6.12 et de la majoration du Théorème 1.6.8, on peut déduire que pour toute courbe elliptique E définie sur un corps de fonctions K et dont le groupe de Tate-Shafarevich est fini, on a

$$\#Ш(E/K) \ll_\varepsilon H(E/K)^{1+\varepsilon}.$$

Ceci est cohérent avec les résultats démontrés par Goldfeld et Szpiro (voir [GS95]) : si le j-invariant de E/K est séparable, ils ont en effet prouvé que

$$\#Ш(E/K) \ll_\varepsilon \left(q^{\deg \mathcal{N}(E/K)}\right)^{1/2+\varepsilon}.$$

Le lien entre $\deg \mathcal{N}(E/K)$ et $H(E/K)$ a déjà été mentionné à la Remarque 1.1.14.

1.6.6 Heuristiques

Comme on l'a déjà remarqué, les Conjectures 1.6.6 et 1.6.7 diffèrent de l'analogue le plus immédiat du théorème de Brauer-Siegel (Théorème 1.6.1) auquel on pourrait penser. Celui-ci s'écrirait :

$$\lim_{E \in \mathscr{E}\ell\ell_{/K}} \mathfrak{Bs}(E/K) = 1, \qquad (?)$$

où $\mathscr{E}\ell\ell_{/K}$ désigne la famille de toutes les courbes elliptiques sur un corps de fonctions K fixé. Nous nous placerons, pour la durée de cette section, dans le cas plus concret où $K = \mathbb{F}_q(t)$.

Hindry et Pacheco ([HP16, Conjecture 1.7]) conjecturent que la famille des tordues quadratiques d'une courbe elliptique fixée pourrait présenter un comportement inédit :

Conjecture 1.6.15 (Hindry - Pacheco). *Soit E une courbe elliptique définie sur un corps de fonctions K. On considère la famille $\mathscr{Q}_E$ formée par les tordues quadratiques $E^{(D)}/K$ de E par les polynômes sans facteurs carrés $D \in \mathbb{F}_q[t]$. On suppose que les groupes de Tate-Shafarevich des courbes $E' \in \mathscr{Q}_E$ sont finis. Alors*

$$0 = \liminf_{E^{(D)} \in \mathscr{Q}_E} \mathfrak{Bs}(E^{(D)}/K) \qquad \textit{et} \qquad \limsup_{E^{(D)} \in \mathscr{Q}_E} \mathfrak{Bs}(E^{(D)}/K) = 1.$$

Dans le cas où E/K n'est pas constante (voir [HP16, §7.5]), la taille du ratio de Brauer-Siegel $\mathfrak{Bs}(E^{(D)}/K)$ est en effet liée à la taille des coefficients de Fourier d'une certaine forme modulaire g_E de poids 3/2 (au moins dans le cas où $E^{(D)}$ est de rang 0). Or, les coefficients de Fourier de formes modulaires sont « usuellement » équidistribués dans l'intervalle où il se trouvent. Ce qui suggère que l'on ne peut pas avoir $\liminf_{E^{(D)}\in\mathscr{Q}_E} \mathfrak{Bs}(E^{(D)}/K) > 0$, sans quoi les coefficients de Fourier non nuls de g_E « éviteraient » un petit intervalle centré en 0. Pour autant, il y a très peu de résultats quant à la répartition des coefficients de Fourier d'une forme modulaire de poids demi-entier.

Dans le cas où E/K est constante, la conjecture ci-dessus admet une reformulation « élémentaire » (voir [HP16, §7.6]). Soit E_0 une courbe elliptique définie sur $\mathbb{F}_q$ et $E = E_0 \times_{\mathbb{F}_q} \mathbb{F}_q(t)$ la courbe elliptique constante correspondante. On note encore $E^{(D)}/K$ la tordue quadratique de E par un polynôme sans facteurs carrés $D \in \mathbb{F}_q[t]$, et $\mathscr{Q}_E$ la famille formée par les courbes $E^{(D)}$.

Alors E/K et ses tordues $E^{(D)}/K$ vérifient la conjecture de Birch et Swinnerton-Dyer par le Théorème 1.4.14 de Milne (voir [Mil68, Theorem 3]). De plus, Milne donne une formule explicite pour la valeur spéciale $L^*(E^{(D)}/K, 1)$ qui, dans ce contexte, a été traduite par Hindry et Pacheco en expression de $\mathfrak{Bs}(E^{(D)}/K)$ (*cf.* [HP16, Proposition 7.16]). Commençons par introduire quelques notations : pour tout polynôme sans facteurs carrés $D \in \mathbb{F}_q[t]$, on note C_D la courbe hyperelliptique définie sur $\mathbb{F}_q$ par l'équation

$$C_D : \ y^2 = D(x),$$

et g_D le genre de C_D. Un calcul classique montre que $g_D = g(C_D) = \left\lfloor \frac{\deg D - 1}{2} \right\rfloor$. On notera $L_D(T) \in \mathbb{Z}[T]$ le numérateur de la fonction zeta de C_D. Par ailleurs, comme E_0 est une courbe elliptique sur $\mathbb{F}_q$, on peut poser $a_0 := q + 1 - \#E_0(\mathbb{F}_q)$.

On définit alors $L_D^*(T) \in \mathbb{Z}[T]$, le polynôme obtenu à partir de $L_D(T)$ en lui retirant autant de facteurs $(1 - a_0T + qT^2)$ que possible, *i.e.* $L_D^*(T) = L_D(T)/(1 - a_0T + qT^2)^{r_D}$ avec $r_D \in \mathbb{N}$ maximal. En fait, il est possible de prouver que r_D est le rang de $E^{(D)}(K)$ (voir la discussion sous [Mil68, Theorem 3], ou [Oes90, §3.2] pour plus de détails). Comme $L_D(T)$ est de degré $2g_D$ et vérifie une équation fonctionnelle par rapport à $T \mapsto (qT)^{-1}$, il existe un unique polynôme unitaire $G_D(T) \in \mathbb{Z}[T]$ de degré g_D tel que

$$L_D(T) = T^{g_D} \cdot G_D\left(qT + \tfrac{1}{T}\right).$$

En outre, $L_D^*(T)$ vérifie également une équation fonctionnelle par rapport à $T \mapsto (qT)^{-1}$. Comme $\deg L_d^*(T) = g_D - r_D$, il existe un unique polynôme unitaire $G_D^*(T) \in \mathbb{Z}[T]$ tel que

$$L_D^*(T) = T^{g_D - r_D} \cdot G_D^*\left(qT + \tfrac{1}{T}\right).$$

Proposition 1.6.16 (Hindry - Pacheco)**.** *Avec les notations ci-dessus, on a*

$$\mathfrak{Bs}(E^{(D)}/K) = \frac{\log G_D^*(a_0)^2}{(g_D - r_D)\log q} + o(1) \qquad (\textit{lorsque } \deg D \to \infty).$$

Par construction, $G_D^*(T)$ est à coefficients entiers et ne s'annule pas en a_0. D'après l'hypothèse de Riemann (Théorème 1.3.2), les inverses des racines de $L_D(T)$ (et donc les inverses des racines de $L_D^*(T)$) sont de valeur absolue $\sqrt{q}$. Par un calcul rapide, il s'ensuit que toutes les racines γ de $G_D^*(T)$ sont réelles et qu'elles vérifient $|\gamma| \leqslant 2\sqrt{q}$. Par ailleurs, vu la borne sur le rang de $E^{(D)}(K)$ (Théorème 1.5.5), on a

$$\deg G_D^* = \frac{\deg D}{2} + o\big(\deg D\big) \qquad (\text{lorsque } \deg D \to \infty).$$

Quand $\deg D \to \infty$, on a donc $\deg G_D^*(T) \to \infty$: le polynôme $G_D^*(T)$ a de plus en plus de racines dans l'intervalle $[-2\sqrt{q}, 2\sqrt{q}]$. Or, le théorème de Hasse (Théorème 1.3.9) assure que $|a_0| \leqslant 2\sqrt{q}$ et par théorème de Honda-Tate (voir [WM71]), lorsque E_0 parcourt l'ensemble des courbes elliptiques définies sur $\mathbb{F}_q$, l'entier a_0 varie et prend presque toutes les valeurs possibles dans ce même intervalle $[-2\sqrt{q}, 2\sqrt{q}]$. Il est donc naturel de penser que $|G_D^*(a_0)| \in \mathbb{N}^*$ *pourrait* être aussi petit que possible. En d'autres termes, lorsque $D \in \mathbb{F}_q[t]$ parcourt l'ensemble des polynômes sans facteurs carrés et que E_0 parcourt l'ensemble des courbes elliptiques définies sur $\mathbb{F}_q$, a-t-on

$$\liminf_{E_0, D} \frac{\log G_D^*(a_0)^2}{\deg G_D^*} = 0 \ ?$$

Il est facile de construire des polynômes $G(T) \in \mathbb{Z}[T]$ de degré arbitrairement grand, dont toutes les racines sont dans l'intervalle $[-2\sqrt{q}, 2\sqrt{q}]$, qui ne s'annulent pas en a_0 et tels que $\log G(a_0)^2/\deg G$ soit arbitrairement petit (voir l'exemple proposé dans [HP16, §7.6]). Mais rien ne permet de démontrer que de tels polynômes $G(T)$ sont effectivement de la forme $G_D^*(T)$, pour un certain polynôme $D \in \mathbb{F}_q[t]$ sans facteurs carrés.

Remarque 1.6.17. Ajoutons la remarque suivante en faveur de la Conjecture 1.6.7. Soit $\mathscr{E}\ell\ell^{r=0}_{/K}$ la famille des courbes elliptiques de rang 0 sur K : pour celles-ci, le régulateur est trivial. Si la Conjecture 1.6.7 était fausse, il existerait une constante $\alpha_K > 0$ telle que, pour toute courbe $E \in \mathscr{E}\ell\ell^{r=0}_{/K}$ on ait

$$\#Ш(E/K) \gg_K H(E/K)^{\alpha_K}.$$

En particulier, il n'y aurait qu'un nombre fini de courbes elliptiques définies sur K, de rang 0 et dont le groupe de Tate-Shafarevich est trivial (ou plus généralement, pour tout $B \in \mathbb{N}^*$, il n'y aurait qu'un nombre fini de courbes elliptiques définies sur K, de rang 0 et telles que $\#Ш(E/K) \leqslant B$).

Pour les courbes elliptiques sur les corps de nombres, une telle borne semble peu vraisemblable : on s'attend à ce que « la moitié » des courbes soient de rang 0 *et* que l'ordre du groupe de Tate-Shafarevich puisse être arbitrairement grand. Il n'est pas déraisonnable de penser que le comportement des courbes elliptiques sur les corps de fonctions est similaire. Notons par exemple que le rang moyen des courbes elliptiques sur $\mathbb{F}_q(t)$ est borné (*cf.* [Bru92, Theorem 7.11]) et qu'une conjecture de Goldfeld prédit que « la moitié » des tordues quadratiques d'une courbe elliptique donnée sont de rang 0.

1.6.7 Conjectures sur les valeurs spéciales

Avec la Proposition 1.6.4, on peut reformuler les Conjectures 1.6.5, 1.6.6 et 1.6.7 en termes de valeurs spéciales (sans référence directe au ratio de Brauer-Siegel) pour les courbes elliptiques vérifiant la conjecture de Birch et Swinnerton-Dyer. Sous cette forme, celles-ci se généralisent à d'autres contextes. Commençons par poser la définition *ad hoc* suivante :

Définition 1.6.18. Soit E une courbe elliptique sur un corps de fonctions $K = \mathbb{F}_q(C)$. On définit la *hauteur analytique (exponentielle)* de E/K par

$$H_{an}(E/K) := q^{\deg L(E/K,T)},$$

où $\deg L(E/K,T)$ est le degré de la fonction $L(E/K,T)$, vue comme fraction rationnelle en T.

D'après le Théorème 1.3.11, on a $\deg L(E/K,T) = \deg \mathcal{N}(E/K) + 4g_C - 4$.

Remarque 1.6.19. Soit $K = \mathbb{F}_q(C)$ un corps de fonctions fixé et E est une courbe elliptique (variable) sur K dont l'invariant j est séparable. Alors, d'après la Remarque 1.1.14, il existe des constantes absolues telles que

$$\log H_{an}(E/K) \ll \log H(E/K) \ll \log H_{an}(E/K).$$

Si E vérifie de plus la conjecture de Birch et Swinnerton-Dyer, on peut réécrire les Conjectures 1.6.5 et 1.6.6 sous la forme d'un encadrement de la valeur spéciale $L^*(E/K,1)$ (voir Proposition 1.6.4) :

$$-1 + o(1) \leqslant \frac{\log L^*(E/K,1)}{\log H_{an}(E/K)} \leqslant 0 + o(1) \qquad (H_{an}(E/K) \to \infty). \tag{1.25}$$

Les Conjectures 1.6.6 et 1.6.5 ont été généralisées à d'autres contextes (voir [Zyk15, §5]). Mentionnons en particulier le cas suivant. Soit E_0 une courbe elliptique sur un corps de fonctions $K_0 = \mathbb{F}_q(C_0)$. Soit $\mathscr{C}$ une tour de courbes C_i de genres $g_i = g(C_i)$ ($i \in \mathbb{N}^*$) au-dessus de C_0, *i.e.* on a des morphismes non constants $C_0 \leftarrow C_1 \leftarrow C_2 \leftarrow \cdots \leftarrow C_i \leftarrow \ldots$ et $g_i \to \infty$. Soit alors, pour tout $i \in \mathbb{N}^*$, $K_i = \mathbb{F}_q(C_i)$ le corps des fonctions de C_i et $E_i = E_0 \times_{K_0} K_i$ la courbe elliptique sur K_i obtenue par changement de base.

Pour tout point fermé $x \in C_0$ et tout entier $d \in \mathbb{N}^*$, on note $\mathbb{F}_x$ le corps résiduel de C_0 en x et $\mathbb{F}_{x^d}$ l'extension de degré d de $\mathbb{F}_x$. On définit $\Phi_{d,x}(C_i)$ le nombre de points $x_i \in C_i$ qui sont au-dessus du point x (pour le morphisme $C_i \to C_0$) et dont le corps résiduel est de degré d sur $\mathbb{F}_x$. Alors, [Zyk15, Lemma 3.16] montre que les limites

$$\phi_{x,d} = \phi_{x,d}(\mathscr{C}) := \lim_{i\to\infty} \frac{\Phi_{d,x}(C_i)}{g(C_i)}$$

existent. On peut alors formuler (voir [Zyk15, Conjecture 5.26])

Conjecture 1.6.20 (Kunyavskiĭ-Tsfasman)**.** *Avec les notations et hypothèses ci-dessus, on a*

$$\lim_{i\to\infty} \frac{\log L^*(E_i/K_i,1)}{\log H_{an}(E_i/K_i)} = -\sum_{x\in|C_0|}\sum_{d=1}^{\infty} \phi_{d,x} \cdot \frac{\#\overline{(E_0)}_x(\mathbb{F}_{x^d})}{\#\mathbb{F}_{x^d}}.$$

Cette Conjecture, où la courbe E_0/K_0 est fixée et le corps de base K_i varie dans une tour, peut être vue comme le cas « orthogonal » à la situation étudiée aux Conjectures 1.6.5 et 1.6.6 (où le corps de base est fixé et la courbe parcourt une famille infinie). Le comportement de la valeur spéciale semble en tout cas très différent.

Dans cette direction, Kunyavskĭ et Tsfasman ont étudié le cas où la courbe E_0/K_0 est supposée constante (voir [KT08]) : ils démontrent le

Théorème 1.6.21 (Kunyavskĭ-Tsfasman). *Soit E_0 une courbe elliptique définie sur $\mathbb{F}_p$. Soit $\{K_i\}_{i\in\mathbb{N}}$ une tour de corps de fonctions, avec $g(C_i)\to\infty$. On note $E_i := E_0\times_{\mathbb{F}_p} K_i$ le changement de base de E_0 à K_i. Alors*

$$\lim_{i\to\infty}\frac{\log\left(\#Ш(E_i/K_i)\cdot\mathrm{Reg}(E_i/K_i)\right)}{\log p\cdot g(C_i)}\to 1-\sum_{m=1}^{\infty}\beta_m\cdot\log_p\left(\frac{\#E_0(\mathbb{F}_{p^m})}{p^m}\right),$$

où $\beta_m=\lim_{i\to\infty}\#C_i(\mathbb{F}_{p^m})/g(C_i)$ (on peut toujours supposer que ces limites existent, quitte à extraire une sous tour de $\{K_i\}_{i\in\mathbb{N}}$).

Il semble cependant que la preuve de ce théorème ne soit pas tout à fait juste (voir [KT10] et [Zyk15, §5]). Noter que la finitude du groupe de Tate Shafarevich des courbes constantes a été démontrée par Milne (cf. Section 1.4.4). Nous ne parlerons pas plus de cette situation ; mais mentionnons tout de même que [Zyk15, Conjecture 5.27] propose une conjecture « unifiée », où la courbe E *et* le corps de base K sont autorisés à varier.

1.6.8 Schéma des preuves

Dans la suite de ce travail (Chapitres 4, 5, 6, 7 et 8), nous nous intéressons à certaines familles spécifiques de courbes elliptiques sur $K=\mathbb{F}_q(t)$. Soit $\mathscr{E}$ une telle famille : pour étudier le comportement asymptotique du ratio de Brauer-Siegel $\mathfrak{Bs}(E/K)$ (avec $E\in\mathscr{E}$ et $H(E/K)\to\infty$) et démontrer que celui-ci a pour limite $\lim\mathfrak{Bs}(E/K)=1$, nous procédons ainsi :

(I) Dans un premier temps, pour donner un sens à l'étude de $\mathfrak{Bs}(E/K)$ pour $E\in\mathscr{E}$, il faut démontrer que le groupe de Tate-Shafarevich $Ш(E/K)$ est fini. Pour ce faire, nous ne connaissons pas d'autre moyen que de démontrer la conjecture de Birch et Swinnerton-Dyer pour chaque courbe elliptique E/K de la famille $\mathscr{E}$.

Pour éviter cette étape, on peut choisir la famille $\mathscr{E}$ parmi les familles infinies de courbes elliptiques vérifiant *a priori* la conjecture de Birch et Swinnerton-Dyer (*cf.* Section 1.4.4).

(II) Ensuite, il convient d'expliciter la hauteur de $E\in\mathscr{E}$, par exemple en fonction d'un paramètre entier que l'on utilise pour indexer la famille $\mathscr{E}$. Cette étape est relativement simple si l'on dispose d'un modèle de Weierstrass de E/K.

(III) Dans un troisième temps, nous explicitons la fonction L de E/K. Pour ce faire, nous avons donné deux techniques possibles (*cf.* Section 1.3.4). Afin d'éviter la construction explicite d'un modèle régulier minimal de E, qui peut s'avérer délicate, nous utilisons plutôt la méthode « des sommes de caractères ». Celle-ci permet d'expliciter complètement la factorisation de $L(E/K,T)$ et, donc, ses racines.

(IV) Pour $E\in\mathscr{E}$, comme la conjecture de Birch et Swinnerton-Dyer est vraie pour E et comme on a explicité les zéros de $L(E/K,T)$ à l'étape précédente, on peut donner une expression « combinatoire » du rang du groupe de Mordell-Weil $E(K)$ et expliciter la valeur spéciale $L^*(E/K,1)$ sous la forme d'un produit.

Nous utiliserons ici la majoration de $L^*(E/K,1)$ donnée par le Théorème 1.6.8 (Proposition 1.6.11), qui est suffisante pour démontrer que

$$\mathfrak{Bs}(E/K)\leqslant 1+o(1)\qquad(H(E/K)\to\infty).$$

(V) L'étape la plus délicate de l'étude est la minoration de $\mathfrak{Bs}(E/K)$. En effet, la meilleure minoration générale connue, [HP16, Proposition 7.6], donne seulement

$$\mathfrak{Bs}(E/K)\geqslant 0+o(1)\qquad(H(E/K)\to\infty).$$

Ainsi, il faut encore raffiner cette minoration : pour ce faire, nous développons (au Chapitre 3) des outils qui permettent, dans certains cas, de démontrer que

$$\mathfrak{Bs}(E/K)\geqslant 1-o(1)\qquad(H(E/K)\to\infty).$$

2

Sommes de caractères et fonctions zeta de certaines courbes

Dans ce chapitre, nous commençons par rappeler des faits classiques sur les caractères des corps finis et sur les sommes de caractères. En particulier, nous introduisons les sommes de Gauss et les sommes de Jacobi (Section 2.2.2). La majeure partie de la Section 2.1 est dédiée à la construction suivante : soit $\mathbb{F}_q$ un corps fini de caractéristique impaire p et $d \geqslant 2$ un entier premier à q, nous explicitons une famille $\{\mathbf{t}_m\}_{m\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}}$ de caractères non triviaux $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$, définis sur diverses extensions de $\mathbb{F}_q$, et dont l'ordre divise d. Nous utilisons ces caractères pour écrire un résultat assez général de « réindexation » de sommes formelles (Proposition 2.1.14).

Nous introduisons également les « sommes de Legendre » (Section 2.2.3) : pour tout $b \in \mathbb{F}_q$ et tout caractère $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$, on pose

$$\boldsymbol{S}_q(\chi; b) = -\sum_{x\in\mathbb{F}_q} \chi(x)\cdot\mu(x^2+2b\cdot x+1),$$

où $\mu : \mathbb{F}_q^\times \to \{\pm 1\}$ désigne l'unique caractère non trivial d'ordre 2 sur $\mathbb{F}_q^\times$. À propos de ces sommes, nous démontrons un analogue (Théorème 2.2.21) de la relation de Hasse-Davenport pour les sommes de Gauss (*cf.* Théorème 2.2.18). Précisément :

Théorème. *Soit $b \in \mathbb{F}_q \smallsetminus \{1,-1\}$ et $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère non trivial de $\mathbb{F}_q^\times$. Il existe deux nombres complexes $\alpha_b(\chi)$ et $\beta_b(\chi)$ tels que, pour tout entier $s \in \mathbb{N}^*$, notant $\chi^{(s)} : \mathbb{F}_{q^s}^\times \to \overline{\mathbb{Q}}^\times$ l'extension de χ à $\mathbb{F}_{q^s}^\times$ via la norme (i.e. $\chi^{(s)} = \chi\circ\mathbf{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$), on a*

$$\boldsymbol{S}_{q^s}(\chi^{(s)}, b) = \alpha_b(\chi)^s + \beta_b(\chi)^s.$$

De plus, on a $\alpha_b(\chi)\cdot\beta_b(\chi) = q$.

En montrant que les sommes de Legendre apparaissent dans les fonctions zeta de certaines courbes hyperelliptiques (Théorème 2.3.4), nous prouvons également un analogue de l'hypothèse de Riemann pour celles-ci (Corollaire 2.3.5).

Théorème. *Soit $b \in \mathbb{F}_q \smallsetminus \{0,1,-1\}$. Pour tout caractère non trivial $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$, les nombres complexes $\alpha_b(\chi)$ et $\beta_b(\chi)$ associés à $\boldsymbol{S}_q(\chi; b)$ comme ci-dessus vérifient :*

$$|\alpha_b(\chi)| = |\beta_b(\chi)| = \sqrt{q}.$$

En particulier, on a donc $|\boldsymbol{S}_q(\chi; b)| \leqslant 2\sqrt{q}$.

La dernière section du chapitre rappelle quelques cas dans lesquels on sait expliciter complètement les sommes de Jacobi. Nous y rappelons le théorème de Shafarevich et Tate, après avoir démontré un lemme arithmétique dont nous n'avons pas trouvé de preuve satisfaisante dans la littérature (Lemme 2.4.1 et Lemme 2.4.3).

Dans tout le reste de ce chapitre, p est un nombre premier $\geqslant 3$.

2.1 Caractères des corps finis

2.1.1 Notations et conventions

Soit $\mathbb{F}_q$ un corps fini de caractéristique p. Un *caractère* de $\mathbb{F}_q^\times$ est un morphisme de groupes $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$. Comme $\mathbb{F}_q^\times$ est un groupe cyclique d'ordre $q-1$, un tel morphisme est en fait à valeurs dans $\mu_{q-1} \subset \overline{\mathbb{Q}}^\times$, les racines $(q-1)$-ièmes de l'unité. Les caractères de $\mathbb{F}_q^\times$ forment un groupe fini, parfois noté $\widehat{\mathbb{F}_q^\times}$, qui est aussi cyclique d'ordre $q-1$. L'*ordre* d'un caractère χ est l'ordre de χ vu comme élément de ce groupe. L'inverse χ^{-1} d'un caractère χ dans le groupe $\widehat{\mathbb{F}_q^\times}$ est souvent noté $\overline{\chi}$. Dans toute la suite, on note $\mathbf{1} : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ le caractère trivial de $\mathbb{F}_q^\times$: c'est celui qui à tout $x \in \mathbb{F}_q^\times$ associe 1.

Il sera commode de prolonger les caractères à tout $\mathbb{F}_q$: si $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ n'est pas le caractère trivial, on pose $\chi(0) = 0$. On prolonge aussi le caractère trivial en posant $\mathbf{1}(0) = 1$. Les relations d'orthogonalité donnent :

– si $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ est un caractère, on a

$$\sum_{x \in \mathbb{F}_q} \chi(x) = \begin{cases} q & \text{si } \chi \text{ est trivial,} \\ 0 & \text{si } \chi \text{ est non trivial.} \end{cases}$$

– si $x \in \mathbb{F}_q$, on a

$$\sum_{\chi} \chi(x) = \begin{cases} 1 & \text{si } x = 0, \\ q-1 & \text{si } x = 1, \\ 0 & \text{sinon.} \end{cases}$$

la somme portant sur tous les caractères de $\mathbb{F}_q^\times$.

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. On prolonge le symbole de Legendre usuel $\left(\frac{\cdot}{\mathbb{F}_p}\right)$ à $\mathbb{F}_q$ de la façon suivante : pour tout $x \in \mathbb{F}_q$, on pose

$$\mu(x) = \left(\frac{\mathbf{N}_{\mathbb{F}_q/\mathbb{F}_p}(x)}{\mathbb{F}_p}\right) = \mathbf{t}(x)^{(q-1)/2}.$$

Ainsi définie, l'application $\mu : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ est un caractère de $\mathbb{F}_q^\times$, d'ordre exactement 2. C'est d'ailleurs l'unique tel caractère car $\mathbb{F}_q^\times$ est cyclique d'ordre pair (car on a supposé q impair et $\#\mathbb{F}_q = q-1$). Dans la suite, on notera toujours μ le caractère quadratique d'un corps fini $\mathbb{F}_q$, ou éventuellement μ_q si l'on a besoin de préciser le corps sur lequel il est défini.

Soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère et $\mathbb{F}_{q^n}/\mathbb{F}_q$ une extension finie. La norme $\mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ permet de prolonger χ à $\mathbb{F}_{q^n}^\times$ en une application

$$\chi^{(n)} = \chi \circ \mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n}^\times \to \overline{\mathbb{Q}}^\times.$$

Comme la norme $\mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$ est un morphisme de groupes surjectif, on voit que $\chi^{(n)}$ est un caractère de $\mathbb{F}_{q^n}^\times$ et que l'ordre de $\chi^{(n)}$ est le même que celui de χ. Pour plus de détails sur le contenu de ce paragraphe, on pourra par exemple consulter [IR90, Chap. 8, §1] ou [LN97, Chap. 5, §1].

Terminons ce paragraphe par un Lemme, qu'on pourrait résumer ainsi : « un caractère sur un corps fini est un carré si et seulement si il est pair ».

Lemme 2.1.1. *Soit $\mathbb{F}_q$ un corps fini de caractéristique p impaire. Pour un caractère $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$, on a $\chi(-1) = \pm 1$ et, si $d \in \mathbb{N}^*$ désigne l'ordre de χ,*

$$\chi(-1) = 1 \iff \exists \theta : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times,\ \chi = \theta^2.$$

D'autre part, $\chi(-1) = -1$ n'est possible que si d est pair et $(q-1)/d$ impair.

Démonstration. Notons ici $X = \widehat{\mathbb{F}_q^\times}$ le groupe cyclique formé par les caractères sur $\mathbb{F}_q^\times$. Soit $X_\square$ le sous-ensemble formé des caractères $\chi \in X$ tels qu'il existe $\theta \in X$ avec $\theta^2 = \chi$. Ainsi défini, $X_\square$ est un sous-groupe de X car c'est l'image du morphisme $\psi : \chi \in X \mapsto \chi^2$. De plus, $\#X_\square = \#X/\#\ker\psi$ et le noyau de ψ est formé de $\mathbf{1}$ et μ. Par conséquent, $X_\square$ est le sous-groupe cyclique d'ordre $(q-1)/2$ de X.

Le sous-ensemble $X_{pair} \subset X$ des caractères $\chi \in X$ tels que $\chi(-1) = 1$ est en fait un sous-groupe de X (c'est le noyau du morphisme $j : \chi \in X \mapsto \chi(-1)$). En tant que sous-groupe d'un groupe cyclique,

X_{pair} est lui-même cyclique d'ordre $(q-1)/\#\operatorname{Im} j$. Soit ξ_0 un générateur de X : c'est un caractère de $\mathbb{F}_q^\times$ d'ordre exactement $q-1$. En particulier, l'image d'un générateur g de $\mathbb{F}_q^\times$ est une racine primitive $(q-1)$-ième de l'unité notée $\zeta = \xi_0(g)$. Alors $\xi_0(-1) = \xi_0(g^{(q-1)/2}) = \xi_0(g)^{(q-1)/2} = \zeta^{(q-1)/2}$ est une racine carrée de 1 : ce ne peut être que -1 (sinon ζ ne serait pas primitive). On en déduit que $-1 = \xi_0(-1) = j(\xi_0) \in \operatorname{Im} j$ et que X_{pair} est le sous-groupe cyclique d'ordre $(q-1)/2$ de X.

Par cyclicité de X, les deux sous-groupes ci-dessus sont confondus : $X_{pair} = X_\square$! Ceci démontre l'équivalence souhaitée. Pour démontrer le deuxième point du Lemme, fixons un caractère $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ d'ordre $d \geqslant 2$ (notons que d divise $q-1$). Le caractère χ est alors à valeurs dans le groupe $\mu_d \subset \overline{\mathbb{Q}}$ des racines d-ièmes de l'unité : -1 n'est une racine de l'unité que si d est pair. Si maintenant g est un générateur de $\mathbb{F}_q^\times$, $\chi(g)$ est une racine primitive d-ième de l'unité, notons celle-ci ζ. Alors on a $\chi(-1) = \chi(g^{(q-1)/2}) = \chi(g)^{(q-1)/2} = \zeta^{(q-1)/2}$ et

$$\chi(-1) = -1 \iff \zeta^{(q-1)/2} = -1 \iff \frac{q-1}{2} \equiv \frac{d}{2} \bmod d \iff \frac{q-1}{d} \equiv 1 \bmod 2.$$

Donc $\chi(-1) = -1$ n'est possible que si d est pair et que $(q-1)/d$ impair. Dans tous les autres cas, $\chi(-1) = 1$ et, d'après le premier paragraphe, il existe $\theta \in X$ tel que $\chi = \theta^2$. □

2.1.2 Caractère de Teichmüller

On fixe une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$: tous les corps de nombres considérés seront implicitement vus comme des sous-corps de $\overline{\mathbb{Q}}$. Soit $\mathfrak{P}$ un idéal maximal de $\overline{\mathbb{Z}}$, l'anneau des entiers de $\overline{\mathbb{Q}}$, au-dessus de p. Le corps $\overline{\mathbb{Z}}/\mathfrak{P}$ est une clôture algébrique de $\mathbb{F}_p$, qu'on notera $\overline{\mathbb{F}_p}$ et tous les corps finis $\mathbb{F}_q$ sont vus comme des sous-corps de celle-ci. Soit $\mu_{p'} \subset \overline{\mathbb{Z}}$ le groupe des racines de l'unité d'ordre premier à p. La réduction modulo $\mathfrak{P}$ induit un isomorphisme entre $\mu_{p'}$ et le groupe multiplicatif $(\overline{\mathbb{Z}}/\mathfrak{P})^\times = \overline{\mathbb{F}_p}^\times$. On notera

$$\mathbf{t} : \overline{\mathbb{F}_p}^\times \xrightarrow{\sim} \mu_{p'} \hookrightarrow \overline{\mathbb{Q}}^\times$$

l'inverse de cet isomorphisme. En d'autres termes, pour tout $x \in \overline{\mathbb{Z}}$, on a

$$\mathbf{t}\left(x \bmod \mathfrak{P}\right) \equiv x \ (\mathrm{mod}\mathfrak{P}), \text{ ou encore } x - \mathbf{t}\left(x \bmod \mathfrak{P}\right) \in \mathfrak{P}.$$

On utilise la même notation $\mathbf{t}$ pour désigner la restriction de $\mathbf{t}$ à tous les corps finis $\mathbb{F}_q$. Le caractère $\mathbf{t}$ ainsi défini sera appelé *caractère de Teichmüller*. Voir [Kat81, §II] ou [Ulm02, §7] pour plus de détails.

Lemme 2.1.2. *Soit $\mathbb{F}_q$ un corps fini de caractéristique p. Tous les caractères $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ s'écrivent comme des puissances entières de $\mathbf{t}$. Autrement dit, $\mathbf{t}$ engendre le groupe $\widehat{\mathbb{F}_q^\times}$.*

Démonstration. Comme $\mathbb{F}_q^\times$ est cyclique d'ordre $q-1$, tous ses caractères ont un ordre divisant $q-1$. Si m_χ est un entier divisant $q-1$, on pose

$$\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times, \quad x \mapsto \mathbf{t}(x)^{(q-1)/m_\chi}.$$

Alors, pour tout $x \in \mathbb{F}_q^\times$, on a $\chi^{m_\chi}(x) = \mathbf{t}(x)^{q-1} = \mathbf{t}(x^{q-1}) = \mathbf{t}(1) = 1$. Ce qui montre que l'ordre de χ divise m_χ et il n'est pas difficile, en considérant l'image d'un générateur de $\mathbb{F}_q^\times$, de voir que l'ordre est en fait exactement m_χ.

Réciproquement, soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère, on note $m \in \mathbb{N}^*$ son ordre. Alors m divise $q-1$ d'après ce qu'on a dit plus haut sur la cyclicité de $\mathbb{F}_q^\times$. Puisque χ est d'ordre m, il est à valeurs dans $\mu_m(\overline{\mathbb{Q}}) \subset \mu_{p'}(\overline{\mathbb{Q}}) \subset \overline{\mathbb{Q}}^\times$. Mieux : l'image par χ d'un générateur g de $\mathbb{F}_q^\times$ est une racine primitive m-ième de l'unité. Ainsi, il existe un unique $a_\chi \in (\mathbb{Z}/d\mathbb{Z})^\times$ tel que $\mathbf{t}\big(g^{(q-1)/m}\big)$ – qui est aussi une racine primitive m-ième de l'unité – s'écrive, $\chi(g) = \mathbf{t}\big(g^{(q-1)/m}\big)^{a_\chi}$. Puisque g engendre $\mathbb{F}_q^\times$, ceci montre que $\chi = \mathbf{t}(\cdot)^{a_\chi \cdot (q-1)/m}$, qui est bien une puissance (entière) de $\mathbf{t}$. □

2.1.3 Caractères dont l'ordre divise d

Pour tous entiers n et q premiers entre eux, on notera $o_q(n)$ l'ordre (multiplicatif) de q modulo n :

$$o_q(n) := \mathrm{ord}^\times(q \bmod n).$$

De façon équivalente, $o_q(n)$ est l'ordre du sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$ engendré par $q \bmod n$.

Définition 2.1.3. Soit q une puissance d'un nombre premier impair et $d \geqslant 2$ un entier premier à p. Pour tout $m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$, on pose

$$u(m) := \min\left\{\nu \in \mathbb{N}^* \;\middle|\; q^\nu m \equiv m \bmod d\right\} = \min\left\{\nu \in \mathbb{N}^* \;\middle|\; d \mid (q^\nu - 1)m\right\} = o_q\left(\tfrac{d}{\operatorname{pgcd}(d,m)}\right).$$

Par définition de $o_q\big(d/\operatorname{pgcd}(d,m)\big)$, pour tout $m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$, les entiers $n \in \mathbb{N}^*$ tels que d divise $m(q^n-1)$ sont exactement les multiples de $u(m)$:

$$\left\{n \in \mathbb{N}^* \;\middle|\; d \mid m(q^n-1)\right\} = \{s \cdot u(m),\ s \in \mathbb{N}^*\}.$$

Dans les calculs de fonctions zeta et fonctions L de ce texte, nous aurons besoin « d'instancier » les caractères sur un corps fini $\mathbb{F}_q$ (et ses extensions) dont l'ordre divise un entier d (fixé).

Définition 2.1.4. Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $d \geqslant 2$ un entier premier à p. Pour tout $m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$, on définit le caractère $\mathbf{t}_m$ par

$$\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times, \quad x \mapsto \mathbf{t}(x)^{(q^{u(m)}-1)m/d}.$$

On démontre alors :

Propriété 2.1.5. *Le caractère $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ est d'ordre exactement $d/\operatorname{pgcd}(d,m)$.*

Par ailleurs, pour tout $j \in \mathbb{N}$, on a $u(q^j \cdot m) = u(m)$.

Démonstration. La restriction de $\mathbf{t}$ à $\mathbb{F}_{q^{u(m)}}^\times$ est un caractère d'ordre $q^{u(m)}-1$ par construction. Et $\mathbf{t}_m$ est la puissance e_m-ième de $\mathbf{t}$, où $e_m = (q^{u(m)}-1)m/d \in \mathbb{N}^*$, donc l'ordre de $\mathbf{t}_m$ vaut

$$\frac{q^{u(m)}-1}{\operatorname{pgcd}\left(e_m, q^{u(m)}-1\right)} = \frac{q^{u(m)}-1}{\operatorname{pgcd}\left((q^{u(m)}-1)m/d, q^{u(m)}-1\right)}.$$

Posons $d_m = \operatorname{pgcd}(d,m)$: on peut écrire $d = d_m d'$ et $m = d_m m'$ où m' et d' sont des entiers premiers entre eux. Par définition, $u(m) = o_q(d/d_m) = o_q(d')$, donc $q^{u(m)}-1$ est un multiple de d' : écrivons ceci $q^{u(m)}-1 = d'e_m$. Alors

$$\frac{(q^{u(m)}-1)m}{d} = \frac{(q^{u(m)}-1)m'}{d'} = \frac{d'm'e_m}{d'} = m'e_m.$$

Ainsi, l'ordre de $\mathbf{t}_m$ vaut

$$\frac{q^{u(m)}-1}{\operatorname{pgcd}\left((q^{u(m)}-1)m/d, q^{u(m)}-1\right)} = \frac{d'e_m}{\operatorname{pgcd}(m'e_m, d'e_m)} = \frac{d'e_m}{e_m \operatorname{pgcd}(d',m')} = d' = \frac{d}{\operatorname{pgcd}(d,m)}.$$

La preuve de la seconde assertion est immédiate : puisque d et q sont premiers entre eux, pour tout $m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$, on a $\operatorname{pgcd}(d,m) = \operatorname{pgcd}(d, q^j \cdot m)$, d'où $u(m) = u(q^j \cdot m)$ (car $u(m)$ s'écrit comme $o_q(d/\operatorname{pgcd}(d,m))$). □

Définition 2.1.6. Nous reprenons les notations de la définition précédente. Soit $m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$, et $s \in \mathbb{N}^*$. On note $n = s \cdot u(m)$. Alors $\mathbb{F}_{q^n}/\mathbb{F}_{q^{u(m)}}$ est une extension de degré s. On peut alors prolonger $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ en un caractère $\mathbf{t}_m^{(s)} : \mathbb{F}_{q^n}^\times \to \overline{\mathbb{Q}}^\times$ via la norme $\mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{u(m)}}}$, *i.e.*

$$\mathbf{t}_m^{(s)} = \mathbf{t}_m \circ \mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{u(m)}}}.$$

Par construction, $\mathbf{t}_m^{(s)}$ est un caractère de $\mathbb{F}_{q^n}^\times$ et son ordre est le même que celui de $\mathbf{t}_m$ (*cf.* Section 2.1.1), à savoir $d/\operatorname{pgcd}(d,m)$.

Remarque 2.1.7. Insistons sur le fait que les notations « $\mathbf{t}_m$ » et « $\mathbf{t}_m^{(s)}$ » ne font pas intervenir l'entier d, qu'il est pourtant nécessaire d'avoir fixé au préalable. Par ailleurs, bien que $\mathbf{t}_m$ et $\mathbf{t}_{q^j \cdot m}$ aient le même ordre, ils ne sont pas toujours égaux.

Si $\mathbb{F}_q$ est un corps fini de caractéristique p, et $d \geqslant 2$ est un entier premier à p, nous avons produit un ensemble de caractères $\mathbf{t}_m, \mathbf{t}_m^{(2)}, \mathbf{t}_m^{(3)}, \ldots$ (avec $m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$) définis sur diverses extensions de $\mathbb{F}_q$ et dont les ordres divisent d. La Proposition ci-dessous prouve qu'on a de cette manière écrit *tous* les caractères d'ordre divisant d définis sur les extensions de $\mathbb{F}_q$.

Définition 2.1.8. Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $d \geqslant 1$ un entier premier à p. Pour toute extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, on note

$$X(d, q^n) := \left\{ \chi : \mathbb{F}_{q^n}^\times \to \overline{\mathbb{Q}}^\times \mid \chi \neq \mathbf{1}, \chi^d = \mathbf{1} \right\},$$

l'ensemble des caractères non triviaux $\chi : \mathbb{F}_{q^n}^\times \to \overline{\mathbb{Q}}^\times$ dont la puissance d-ième est le caractère trivial (*i.e.* dont l'ordre divise d). Noter que $\#X(d, q^n) = \operatorname{pgcd}(d, q^n - 1) - 1$ car l'ensemble des caractères d'ordre divisant d est un sous-groupe (nécessairement cyclique) de $\widehat{\mathbb{F}_{q^n}^\times}$.

Proposition 2.1.9. *Soit $\mathbb{F}_q$ un corps fini de caractéristique p et $d \geqslant 2$ un entier premier à p. Avec les notations précédentes, on a*

$$\bigcup_{n \geqslant 1} X(d, q^n) = \bigcup_{m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}} \left\{ \mathbf{t}_m, \mathbf{t}_m^{(2)}, \mathbf{t}_m^{(3)}, \dots, \mathbf{t}_m^{(s)}, \dots \right\} = \bigcup_{m=1}^{d-1} \bigcup_{s \geqslant 1} \left\{ \mathbf{t}_m^{(s)} \right\}.$$

Démonstration. Soit $n \geqslant 1$ et $\chi \in X(d, q^n)$, on note $d_n = \operatorname{pgcd}(d, q^n - 1)$. Soit par ailleurs $\chi_0 : \mathbb{F}_{q^n}^\times \to \overline{\mathbb{Q}}$ le caractère donné par $\chi_0 = \mathbf{t}(\cdot)^{(q^n-1)/d_n}$. L'ordre de χ_0 est exactement d_n : par cyclicité de $\widehat{\mathbb{F}_{q^n}^\times}$, χ_0 engendre $X(d, q^n) \cup \{\mathbf{1}\}$. Comme $\chi^d = \mathbf{1}$ mais que $\chi \neq \mathbf{1}$, il existe un unique $j \in [\![1, d_n - 1]\!]$ tel que $\chi = {\chi_0}^j$, autrement dit :

$$\chi = \mathbf{t}(\cdot)^{\frac{(q^n-1)j}{d_n}} = \mathbf{t}(\cdot)^{\frac{(q^n-1)j \cdot d/d_n}{d}}.$$

On pose alors $m = j \cdot d/d_n \in \mathbb{N}^*$, comme $1 \leqslant j < d_n$, on a $1 \leqslant m < d$. Ainsi, d divise $m(q^n - 1)$ et $\chi = \mathbf{t}(\cdot)^{(q^n-1)m/d}$. On note $u(m) = o_q(d/\operatorname{pgcd}(d, m))$ comme précédemment : n s'écrit sous la forme $n = s \cdot u(m)$ pour un certain $s \in \mathbb{N}^*$ (car d divise $m(q^n - 1)$), ce qui donne finalement :

$$\chi = \mathbf{t}(\cdot)^{(q^n-1)m/d} = \mathbf{t}(\cdot)^{(q^{s \cdot u(m)}-1)m/d} = \mathbf{t}_m^{(s)}.$$

Réciproquement, pour $m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ et $s \geqslant 1$. Vérifions que $\mathbf{t}_m^{(s)}$ appartient à la réunion des $X(d, q^n)$. Soit $n = s \cdot u(m)$, le caractère $\mathbf{t}_m^{(s)} : \mathbb{F}_{q^n}^\times \to \overline{\mathbb{Q}}^\times$ est donné par

$$\mathbf{t}_m^{(s)}(x) = \mathbf{t}(x)^{(q^n-1)m/d}.$$

Il est clair que $\mathbf{t}_m^{(s)}$ est non trivial et que sa puissance d-ième est triviale puisque tout élément $x \in \mathbb{F}_{q^n}$ vérifie $x^{q^n-1} = 1$ et donc $x^{m(q^n-1)} = 1^m = 1$. Ainsi, on a $\mathbf{t}_m^{(s)} \in X(d, q^n)$. □

Remarque 2.1.10. La preuve de la Proposition précédente donne en fait un résultat plus précis : si $\mathbb{F}_{q^n}/\mathbb{F}_q$ est une extension finie donnée, on a

$$X(d, q^n) = \left\{ \mathbf{t}_m^{(s)},\ m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}, s \in \mathbb{N}^* \text{ tels que } s \cdot u(m) = n \right\}.$$

Terminons ce paragraphe par la définition suivante.

Définition 2.1.11. Soit q une puissance d'un nombre premier p impair et $d \geqslant 2$ un entier premier à q. Il y a une action naturelle de q sur $\mathbb{Z}/d\mathbb{Z}$ par multiplication. Dans cette action l'orbite de $0 \in \mathbb{Z}/d\mathbb{Z}$ est réduite à $\{0\}$. Nous noterons

$$\mathcal{O}'_q(d) := \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\big) \big/ \langle q \bmod d \rangle$$

l'ensemble des autres orbites de $\mathbb{Z}/d\mathbb{Z}$ sous l'action de q par multiplication.

Cette notation est en vigueur dans tout le reste de ce travail.

Remarque 2.1.12. Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $d \geqslant 2$ un entier premier à p. On note $\mu_d \subset \overline{\mathbb{F}_q}$ le groupe des racines d-ièmes de l'unité dans $\overline{\mathbb{F}_q}$: c'est un groupe cyclique d'ordre d. Les caractères $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ sur les extensions finies $\mathbb{F}_Q/\mathbb{F}_q$ dont l'ordre divise d sont exactement les caractères sur le groupe μ_d. Autrement dit, dans nos notations,

$$\{\mathbf{1}\} \cup \bigcup_{n \geqslant 1} X(d, q^n) = \widehat{\mu_d}.$$

Il y a une action naturelle du Frobenius $\mathrm{Fr}_q \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ sur $\widehat{\mu_d}$: celle-ci est donnée par $\chi \mapsto \mathrm{Fr}_q * \chi = \chi^q$. En tant que groupe cyclique d'ordre d, $\widehat{\mu_d}$ est naturellement isomorphe à $\mathbb{Z}/d\mathbb{Z}$:

si $\zeta \in \overline{\mathbb{F}_q}$ est une racine primitive d-ième de l'unité, on associe à $\chi \in \widehat{\mu_d}$ l'unique $a_\chi \in \mathbb{Z}/d\mathbb{Z}$ tel que $\chi(\zeta) = \exp\left(\frac{2i\pi}{d} \cdot a_\chi\right) \in \overline{\mathbb{Q}}^\times$. De cette identification $\widehat{\mu_d} \simeq \mathbb{Z}/d\mathbb{Z}$, on déduit une bijection entre l'ensemble des orbites de $\widehat{\mu_d}$ sous l'action de Fr_q à l'ensemble des orbites de $\mathbb{Z}/d\mathbb{Z}$ sous l'action de q par multiplication et

$$\left(\widehat{\mu_d} \smallsetminus \{\mathbf{1}\}\right) / \langle \mathrm{Fr}_q \rangle \simeq \left(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\right) / \langle q \bmod d \rangle = \mathcal{O}'_q(d).$$

L'ensemble d'orbites $\mathcal{O}'_q(d)$ est donc le pendant « combinatoire » de l'action du Frobenius Fr_q (*i.e.* l'action de $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$) sur $\mu_d \subset \overline{\mathbb{F}_q}$.

Remarque 2.1.13. Si d divise $q-1$, il existe un caractère de $\mathbb{F}_q^\times$ d'ordre exactement d : le caractère $\mathbf{t}_1$. Auquel cas,

$$X(d,q) = \left\{\mathbf{t}_1, \mathbf{t}_1^2, \ldots, \mathbf{t}_1^{d-1}\right\}.$$

Remarquons aussi que, si d divise $q-1$, on a $\mu_d \subset \mathbb{F}_q$.

2.1.4 Réindexation de sommes

Dans cette section, nous énonçons et démontrons un résultat de « réindexation de sommes ». Cet énoncé sera d'usage constant pour calculer les fonctions zeta et les fonctions L des courbes que nous étudions. Un premier exemple d'utilisation est visible à la Section 2.3.2 ci-dessous.

Proposition 2.1.14. *Soit $\mathbb{F}_q$ un corps fini et $d \geqslant 2$ un entier premier à q. Pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$, on note à nouveau*

$$X(d,Q) = \left\{\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times \;\middle|\; \chi^d = \mathbf{1} \text{ et } \chi \neq \mathbf{1}\right\}.$$

Soit, pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$ et tout caractère $\chi \in X(d,Q)$ un nombre complexe $\sigma(Q,\chi)$ tel que

$$\sigma(Q, \chi^q) = \sigma(Q,\chi).$$

On suppose que, pour un certain $K \in \mathbb{N}^*$ fixé, les nombres $\sigma(Q,\chi)$ satisfont « une relation de Hasse-Davenport à l'ordre K » au sens suivant : si $\chi \in X(d,Q)$ est un caractère (non trivial), il existe K nombres complexes $\alpha_1(\chi), \ldots, \alpha_K(\chi)$ (qui ne dépendent que de χ) tels que, pour tout $s \in \mathbb{N}^*$, si l'on note $\chi^{(s)} : \mathbb{F}_{Q^s}^\times \to \overline{\mathbb{Q}}^\times$ l'extension de χ à $\mathbb{F}_{Q^s}^\times$ via la norme (i.e. $\chi^{(s)} = \chi \circ \mathbf{N}_{\mathbb{F}_{Q^s}/\mathbb{F}_Q}$), on a

$$\sigma(Q^s, \chi^{(s)}) = (\alpha_1(\chi))^s + (\alpha_2(\chi))^s + \cdots + (\alpha_K(\chi))^s.$$

Alors on a

$$\sum_{n=1}^{\infty} \left(\sum_{\chi \in X(d,q^n)} \sigma(q^n, \chi) \right) \frac{T^n}{n} = \sum_{m \in \mathcal{O}'_q(d)} -\log\left(\prod_{i=1}^{K} \left(1 - \alpha_i(m) T^{u(m)}\right) \right),$$

où $\mathcal{O}'_q(d) = \left(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\right) / \langle q \bmod d \rangle$ et, pour toute orbite $m \in \mathcal{O}'_q(d)$, $\alpha_i(m)$ désigne $\alpha_i(\mathbf{t}_a)$ pour un quelconque choix de représentant $a \in \mathbb{Z}/d\mathbb{Z}$ de l'orbite m.

Dans la suite, nous désignerons souvent $\alpha_i(m)$ par $\alpha_i(\mathbf{t}_m)$.

Démonstration. Soit $\sigma(q^n,\chi)$ comme dans l'énoncé. La double somme à expliciter peut se « réindexer » grâce à la Proposition 2.1.9 :

$$\sum_{n=1}^{\infty} \sum_{\chi \in X(d,q^n)} \sigma(q^n,\chi) \frac{T^n}{n} = \sum_{m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}} \sum_{s=1}^{\infty} \sigma(q^{s \cdot u(m)}, \mathbf{t}_m^{(s)}) \frac{T^{s \cdot u(m)}}{s \cdot u(m)}.$$

Or, comme les nombres $\sigma(q^{u(m)}, \mathbf{t}_m)$ satisfont une relation de Hasse-Davenport à l'ordre K (l'entier K est indépendant de m), pour tout $m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$, on peut fixer $\alpha_1(\mathbf{t}_m), \ldots, \alpha_K(\mathbf{t}_m)$ tels que :

$$\forall s \geqslant 1, \quad \sigma(q^{su(m)}, \mathbf{t}_m^{(s)}) = \sigma\left(\left(q^{u(m)}\right)^s, \mathbf{t}_m^{(s)}\right) = \alpha_1(\mathbf{t}_m)^s + \alpha_2(\mathbf{t}_m)^s + \cdots + \alpha_K(\mathbf{t}_m)^s.$$

On a donc

$$\begin{aligned}\sum_{n=1}^{\infty}\sum_{\chi\in X(d,q^n)}\sigma(q^n,\chi)\frac{T^n}{n} &= \sum_{m\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}}\left(\sum_{s=1}^{\infty}\sigma(q^{s\cdot u(m)},\mathbf{t}_m^{(s)})\frac{T^{s\cdot u(m)}}{s\cdot u(m)}\right)\\ &= \sum_{m\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}}\left(\sum_{s=1}^{\infty}\left(\sum_{i=1}^{K}\alpha_i(\mathbf{t}_m)^s\right)\frac{T^{s\cdot u(m)}}{s\cdot u(m)}\right)\\ &= \sum_{m\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}}\frac{1}{u(m)}\cdot\sum_{i=1}^{K}\left(\sum_{s=1}^{\infty}\frac{\left(\alpha_i(\mathbf{t}_m)\cdot T^{u(m)}\right)^s}{s}\right)\\ &= \sum_{m\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}}\frac{1}{u(m)}\cdot\sum_{i=1}^{K}-\log\left(1-\alpha_i(\mathbf{t}_m)\cdot T^{u(m)}\right).\end{aligned}$$

Mais, pour tout $m\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ et tout $j\in\mathbb{N}^*$, par hypothèse sur les $\sigma(Q,\chi)$, on a

$$\sigma(q^{s\cdot u(m)},\mathbf{t}_m)=\sigma(q^{s\cdot u(m)},\mathbf{t}_m{}^q)=\sigma(q^{s\cdot u(m)},\mathbf{t}_{q\cdot m})=\cdots=\sigma(q^{s\cdot u(m)},\mathbf{t}_{q^j\cdot m}).$$

Par suite, quitte à renuméroter les α_i, on a $\alpha_i(m)=\alpha_i(q^j\cdot m)$ pour tout $j\in\mathbb{N}^*$. Ainsi, dans la somme

$$\sum_{m\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}}\frac{1}{u(m)}\cdot\sum_{i=1}^{K}-\log\left(1-\alpha_i(m)\cdot T^{u(m)}\right),$$

chaque terme $\sum_{i=1}^{K}-\log\left(1-\alpha_i(\mathbf{t}_m)\cdot T^{u(m)}\right)$ apparaît en fait $\#\{m,qm,q^2m,\dots,q^{u(m)-1}m\}=u(m)$ fois. On peut donc les regrouper par orbites $\left\{m,q\cdot m,q^2\cdot m,\dots,q^{u(m)-1}\cdot m\right\}$ sous l'action de q et noter, pour tout $i\in[\![1,K]\!]$, $\alpha_i(\widetilde{m})$ la valeur commune de $\alpha_i(\mathbf{t}_m)=\alpha_i(\mathbf{t}_{qm})=\cdots=\alpha_i(\mathbf{t}_{q^{u(m)-1}m})$. Ce qui conduit à l'expression affichée dans l'énoncé de la Proposition. □

Nous aurons par ailleurs besoin d'une variante de cette proposition sous la forme suivante.

Proposition 2.1.15. *Soit $\mathbb{F}_q$ un corps fini et $d\geqslant 2$ un entier premier à q. On fixe aussi ℓ un nombre premier. Pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$, on pose*

$$X^{(\ell)}(d,Q)=\left\{\chi:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times\;\middle|\;\chi^d=\mathbf{1}\text{ et }\chi^\ell\neq\mathbf{1}\right\}.$$

Soit, pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$ et tout caractère $\chi\in X^{(\ell)}(d,Q)$ un nombre complexe $\sigma(Q,\chi)$ tel que

$$\sigma(Q,\chi^q)=\sigma(Q,\chi).$$

On suppose que, pour un certain $K\in\mathbb{N}^*$ fixé, les $\sigma(Q,\chi)$ satisfont « une relation de Hasse-Davenport à l'ordre K » au sens de la Proposition précédente. Alors on a

$$\sum_{n=1}^{\infty}\left(\sum_{\chi\in X^{(\ell)}(d,q^n)}\sigma(q^n,\chi)\right)\frac{T^n}{n}=\sum_{m\in\mathcal{O}_q^{(\ell)}(d)}-\log\left(\prod_{i=1}^{K}\left(1-\alpha_i(m)T^{u(m)}\right)\right),$$

où

$$\mathcal{O}_q^{(\ell)}(d)=\begin{cases}\left(\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}\right)/\langle q \bmod d\rangle & \text{si } \ell \text{ ne divise pas } d,\\ \left(\mathbb{Z}/d\mathbb{Z}\smallsetminus\left\{0,\frac{d}{\ell},\frac{2d}{\ell},\dots,\frac{(\ell-1)d}{\ell}\right\}\right)/\langle q \bmod d\rangle & \text{si } \ell \text{ divise } d\end{cases}$$

et, pour toute orbite $m\in\mathcal{O}_q^{(\ell)}(d)$, $\alpha_i(m)$ désigne la valeur commune des $\alpha_i(\mathbf{t}_a)$ lorsque a parcourt l'orbite m. Dans la suite, nous désignerons souvent $\alpha_i(m)$ par $\alpha_i(\mathbf{t}_m)$.

Démonstration. Distinguons naturellement deux cas :

– Supposons d'abord que d n'est pas divisible par ℓ. Alors, pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$, on a $X^{(\ell)}(d,Q)=X(d,Q)$. En effet, on a clairement $X^{(\ell)}(d,Q)\subset X(d,Q)$ et, pour tout $\chi\in X(d,Q)$, la condition « $\chi^\ell\neq\mathbf{1}$ » est automatiquement satisfaite : si l'on fixe une relation de Bézout $u\ell+vd=1$ entre d et ℓ ($u,v\in\mathbb{Z}$), on a

$$\chi=\chi^1=\chi^{u\ell+vd}=(\chi^\ell)^u\cdot(\chi^d)^v=(\chi^\ell)^u,$$

où χ n'est pas trivial, c'est donc que $\chi^\ell\neq\mathbf{1}$.
Comme $X^{(\ell)}(d,Q)=X(d,Q)$ et que $\mathcal{O}_q^{(\ell)}(d)=\mathcal{O}'_q(d)$, la Proposition suit directement de la Proposition 2.1.14 dans ce cas.

– Supposons maintenant que d est divisible par ℓ. Pour une extension finie $\mathbb{F}_{q^n}/\mathbb{F}_q$, on a vu à la Remarque 2.1.10 (sous la Proposition 2.1.9) que

$$X(d,q^n) = \left\{ \mathbf{t}_m^{(s)},\ m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}, s \in \mathbb{N}^* \text{ tels que } s\cdot u(m) = n \right\}.$$

Soit $m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ et $s \in \mathbb{N}^*$ tels que $s\cdot u(m) = n$. Notons $\chi : \mathbb{F}_{q^n}^\times \to \overline{\mathbb{Q}}^\times$ le caractère non trivial $\chi = \mathbf{t}_m^{(s)}$. Comme on l'a vu à la Propriété 2.1.5, χ est d'ordre exactement $d/\operatorname{pgcd}(d,m)$. Par suite, $\chi^\ell = \mathbf{1}$ si et seulement si ℓ est un multiple de $d/\operatorname{pgcd}(d,m)$, c'est-à-dire quand $\ell = d/\operatorname{pgcd}(d,m)$ (car ℓ est premier). Ceci se produit lorsque (le relevé dans $[\![1, d-1]\!]$ de) $m \in \mathbb{Z}/d\mathbb{Z}$ est de la forme $m = k\cdot d/\ell$ avec $k \in [\![1, \ell-1]\!]$ (à nouveau car ℓ est premier). Soit donc $Z_\ell = \mathbb{Z}/d\mathbb{Z} \smallsetminus \left\{0, \frac{d}{\ell}, \frac{2d}{\ell}, \dots, \frac{(\ell-1)d}{\ell}\right\}$. On a prouvé que

$$\begin{aligned} X^{(\ell)}(d,q^n) &= X(d,q^n) \smallsetminus \left\{\chi \in X(d,q^n) \mid \chi^\ell = \mathbf{1}\right\} \\ &= \left\{ \mathbf{t}_m^{(s)},\ m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \left\{0, \tfrac{d}{\ell}, \tfrac{2d}{\ell}, \dots, \tfrac{(\ell-1)d}{\ell}\right\}, s \in \mathbb{N}^* \text{ tels que } s\cdot u(m) = n \right\} \\ &= \left\{ \mathbf{t}_m^{(s)},\ m \in Z_\ell, s \in \mathbb{N}^* \text{ tels que } s\cdot u(m) = n \right\}. \end{aligned}$$

D'où l'on déduit l'analogue de la Proposition 2.1.9 pour les ensembles $X^{(\ell)}(d,q^n)$:

$$\bigcup_{n\geqslant 1} X^{(\ell)}(d,q^n) = \bigcup_{m\in Z_\ell} \left\{ \mathbf{t}_m, \mathbf{t}_m^{(2)}, \mathbf{t}_m^{(3)}, \dots, \mathbf{t}_m^{(s)}, \dots \right\}.$$

On peut alors reprendre mot pour mot la preuve de la Proposition 2.1.14, en remplaçant $X(d,q^n)$ par $X^{(\ell)}(d,q^n)$, $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ par Z_ℓ et $\mathcal{O}'_q(d)$ par $\mathcal{O}_q^{(\ell)}(d)$.
Remarquons tout de même que Z_ℓ est stable sous l'action de q par multiplication. En effet, si $m = k_0 d/\ell$ (avec $k_0 \in [\![0, \ell-1]\!]$) et $j \in \mathbb{N}$, alors $q^j m$ est de la forme $k_j d/\ell$ où $k_j = q^j k_0 \in \mathbb{Z}$ et l'orbite entière de $m \in \left\{0, \frac{d}{\ell}, \frac{2d}{\ell}, \dots, \frac{(\ell-1)d}{\ell}\right\}$ sous l'action de q est contenue dans cet ensemble. Donc le complémentaire Z_ℓ de $\left\{0, \frac{d}{\ell}, \frac{2d}{\ell}, \dots, \frac{(\ell-1)d}{\ell}\right\}$ dans $\mathbb{Z}/d\mathbb{Z}$ est lui aussi stable sous l'action de q ; et la définition

$$\mathcal{O}_q^{(\ell)}(d) := \left(\mathbb{Z}/d\mathbb{Z} \smallsetminus \left\{0, \tfrac{d}{\ell}, \tfrac{2d}{\ell}, \dots, \tfrac{(\ell-1)d}{\ell}\right\}\right) / \langle q \bmod d \rangle$$

a bien un sens.
Ceci conclut la preuve de la Proposition 2.1.15. □

Insistons à nouveau sur le fait que nous ferons l'abus de notation de désigner par « $1-\alpha_i(\mathbf{t}_m)T^{u(m)}$ » ce qu'on devrait noter « $1-\alpha_i(\mathbf{t}_a)T^{u(a)}$ pour $a \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ un quelconque représentant de l'orbite $m \in \mathcal{O}'_q(d)$ ». Ceci ne posera pas de problème car on aura vérifié que $\alpha_i(\mathbf{t}_a) = \alpha_i(\mathbf{t}_{q^j a})$ (bien que $\mathbf{t}_a \neq \mathbf{t}_{q^j a}$ en général).

Remarque 2.1.16. Il y a une version « cohomologique » de ces Propositions. Elle est basée sur la Remarque 2.1.12 ci-dessus. La lectrice peut se référer à [Kat81, §1-§2], [Gor79, Lemma §2] ou [Ulm07b] pour plus de détails à ce propos.

2.2 Sommes de caractères

2.2.1 Nombre de solutions d'équations et sommes de caractères

Commençons par rappeler quelques dénombrements classiques du nombre de solutions de certaines équations monomiales dans les corps finis à l'aide de sommes de caractères. Dans toute cette section, $\mathbb{F}_q$ est un corps fini de caractéristique impaire.

Lemme 2.2.1. *Soit $z \in \mathbb{F}_q$. Alors $\#\left\{y \in \mathbb{F}_q \mid y^2 = z\right\} = 1 + \mu(z)$.*
Plus généralement, si $P \in \mathbb{F}_q[z]$ est un polynôme, on a

$$\#\left\{(y,z) \in \mathbb{F}_q^2 \mid y^2 = P(z)\right\} = \sum_{z\in\mathbb{F}_q} (1 + \mu(P(z))).$$

Lemme 2.2.2. *Soit $z \in \mathbb{F}_q$ et $d \in \mathbb{N}^*$ un entier premier à q. Alors*

$$\#\left\{y \in \mathbb{F}_q \mid y^d = z\right\} = \sum_{\chi^d = \mathbf{1}} \chi(z),$$

la somme portant sur les caractères $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ dont l'ordre divise d.

Le premier de ces Lemmes est une conséquence du deuxième. Il s'agit essentiellement d'une relation d'orthogonalité de caractères. La lectrice trouvera une preuve dans [IR90, Prop. 8.1.4, Prop. 8.1.5] ou [Hin08, Chap. 1, Exercice 6.11]. Noter que, dans l'énoncé du Lemme 2.2.2, on ne suppose pas que $d \mid q-1$. Terminons ce paragraphe par un résultat utile (voir [LN97, Theorem 5.48]).

Lemme 2.2.3. *Soit $Q(X) = aX^2 + bX + c$ un polynôme de degré 2 à coefficients dans $\mathbb{F}_q$ (rappelons que q est impair) avec $a \neq 0$. On pose $\delta = b^2 - 4ac$. Alors*

$$\sum_{x \in \mathbb{F}_q} \mu(ax^2 + bx + c) = \begin{cases} \mu(a) \cdot (q-1) & \text{si } \delta = 0, \\ -\mu(a) & \text{si } \delta \neq 0. \end{cases}$$

Démonstration. On commence par multiplier la somme $\sum_{x \in \mathbb{F}_q} \mu(Q(x))$ par $\mu(4a^2) = (\mu(2a))^2 = 1$ et on réindexe la somme après avoir factorisé Q :

$$\begin{aligned} \sum_{x \in \mathbb{F}_q} \mu(Q(x)) &= \mu(4a^2) \cdot \sum_{x \in \mathbb{F}_q} \mu(Q(x)) = \mu(a) \cdot \sum_{x \in \mathbb{F}_q} \mu(4a^2x^2 + 4abx + 4ac) \\ &= \mu(a) \cdot \sum_{x \in \mathbb{F}_q} \mu((2ax+b)^2 - \delta) = \mu(a) \cdot \sum_{y \in \mathbb{F}_q} \mu(y^2 - \delta). \end{aligned}$$

Pour $\delta = 0$, le résultat est maintenant clair :

$$\sum_{x \in \mathbb{F}_q} \mu(Q(x)) = \mu(a) \cdot \sum_{y \in \mathbb{F}_q} \mu(y)^2 = \mu(a) \cdot (q-1).$$

Si maintenant δ est non nul, on écrit

$$\sum_{y \in \mathbb{F}_q} \mu(y^2 - \delta) = -q + \sum_{x \in \mathbb{F}_q} \left(1 + \mu(x^2 - \delta)\right).$$

Comme $1 + \mu(x^2 - \delta)$ est le nombre de solutions $z \in \mathbb{F}_q$ de l'équation $z^2 = x^2 - \delta$, on obtient :

$$\sum_{y \in \mathbb{F}_q} \mu(y^2 - \delta) = -q + \#\left\{(x,z) \in \mathbb{F}_q^2 \mid z^2 = x^2 - \delta\right\}.$$

Le comptage des solutions de l'équation à droite est assez simple : si (x,z) est une telle solution, on pose $(u,v) = (x-z, x+z)$ et on remarque que l'application $(x,z) \mapsto (u,v)$ est une bijection entre les solutions de $z^2 = x^2 - \delta$ et les solutions de $uv = \delta$. En particulier,

$$\#\left\{(x,z) \in \mathbb{F}_q^2 \mid z^2 = x^2 - \delta\right\} = \#\left\{(u,v) \in \mathbb{F}_q^2 \mid uv = \delta\right\} = q - 1.$$

Ce qui donne finalement,

$$\sum_{x \in \mathbb{F}_q} \mu(Q(x)) = \mu(a) \cdot \sum_{y \in \mathbb{F}_q} \mu(y^2 - \delta) = \mu(a) \cdot (-q + (q-1)) = -\mu(a).$$

□

2.2.2 Sommes de Gauss et sommes de Jacobi

Soit $\mathbb{F}_q$ un corps fini de caractéristique p. On fixe une fois pour toute un caractère additif non trivial ψ_q de $\mathbb{F}_q$: nous choisissons le caractère additif standard défini par

$$\psi_q : x \in \mathbb{F}_q \mapsto \exp\left(\frac{2i\pi}{p} \cdot \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)\right).$$

Ce dernier est à valeurs dans le corps cyclotomique $\mathbb{Q}(\zeta_p) \subset \overline{\mathbb{Q}}$ engendré par les racines p-ièmes de l'unité.

Définition 2.2.4. Si $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ est un caractère de $\mathbb{F}_q^\times$, on définit la *somme de Gauss* associée par :

$$\mathbf{g}_q(\chi) := -\sum_{x\in\mathbb{F}_q^\times} \chi(x)\psi_q(x).$$

Au vu de sa définition, $\mathbf{g}_q(\chi)$ est un entier du corps cyclotomique $\mathbb{Q}(\zeta_p,\zeta_d) = \mathbb{Q}(\zeta_{pd})$, où d est l'ordre de χ. Noter la normalisation par un signe « $-$ » choisie ici, ainsi que le fait que la somme porte uniquement sur les éléments non nuls de $\mathbb{F}_q$. L'article [Kat81, §I - §II] propose une définition et une interprétation « cohomologiques » des sommes $\mathbf{g}_q(\chi)$. La Proposition suivante rappelle les propriétés de base des sommes de Gauss :

Proposition 2.2.5. *Soit $\mathbb{F}_q$ un corps fini et $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère.*

- *Si $\chi = \mathbf{1}$ est le caractère trivial, on a $\mathbf{g}_q(\mathbf{1}) = 1$.*
- *Si χ est un caractère non trivial, on a $\mathbf{g}_q(\chi)\cdot\mathbf{g}_q(\overline{\chi}) = \chi(-1)q$.*
- *Si χ est un caractère non trivial, on a $|\mathbf{g}_q(\chi)| = \sqrt{q}$. De plus, $\overline{\mathbf{g}_q(\chi)} = \chi(-1)\cdot\mathbf{g}_q(\overline{\chi})$.*

La preuve en est classique : on pourra par exemple consulter [Coh07, Chap. 2, §2.5.2], [IR90, Chap. 8, §2] [LN97, Chap. 5, §2] ou [Was97, Chap. 6, §1].

Définition 2.2.6. Soit $n \in \mathbb{N}$. Étant donnés $n+1$ caractères $\chi_0,\chi_1,\dots,\chi_n : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$, on définit la *somme de Jacobi* associée par :

$$\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_n) := (-1)^n \cdot \sum_{\substack{x_i\in\mathbb{F}_q \\ x_0+x_1+\cdots+x_n=1}} \chi_0(x_0)\chi_1(x_1)\cdot\cdots\cdot\chi_n(x_n).$$

On dira parfois que $\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_n)$ est une somme de Jacobi *de dimension* n.

Ainsi définie, il est clair que $\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_n)$ est un entier algébrique de $\mathbb{Q}(\mu_{q-1})$. Remarquer la normalisation avec un « $(-1)^n$ ». Pour $n=0$, on a $\mathbf{j}_q(\chi_0) = 1$ quelque soit $\chi_0 : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$. Notons enfin que la valeur de $\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_n)$ ne dépend pas de la numérotation des χ_i. La proposition ci-dessous explicite le lien entre sommes de Gauss et sommes de Jacobi. Sa preuve est elle aussi classique : voir par exemple [Coh07, Chap. 2, §2.5.3 - §2.5.4], [Hin08, Chap. 1, Exercice 6.11], [IR90, Chap. 8, §6 - §8], [LN97, Chap. 5, §3] ou [Was97, Chap. 6, §1].

Proposition 2.2.7. *Soit $n \geqslant 1$ et $\chi_0,\dots,\chi_n : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ des caractères de $\mathbb{F}_q^\times$.*

- *Si $\chi_0 = \chi_1 = \cdots = \chi_n = \mathbf{1}$, alors $\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_n) = (-1)^n q^n$.*
- *Si certains χ_i sont triviaux, mais pas tous, alors $\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_n) = 0$.*
- *Si tous les χ_i sont non triviaux et que le produit $\chi_0\cdot\chi_1\cdot\cdots\cdot\chi_n = \mathbf{1}$, on a*

$$\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_n) = \chi_n(-1)\cdot\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_{n-1}).$$

Dans ce cas, on a également : $\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_n) = \dfrac{1}{q}\cdot\mathbf{g}_q(\chi_0)\cdot\mathbf{g}_q(\chi_1)\cdot\cdots\cdot\mathbf{g}_q(\chi_n)$.

- *Enfin, si tous les χ_i sont non triviaux et que le produit $\chi_0\cdot\chi_1\cdot\cdots\cdot\chi_n \neq \mathbf{1}$, on a*

$$\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_n) = \frac{\mathbf{g}_q(\chi_0)\cdot\mathbf{g}_q(\chi_1)\cdot\cdots\cdot\mathbf{g}_q(\chi_n)}{\mathbf{g}_q(\chi_0\cdot\chi_1\cdot\cdots\cdot\chi_n)}.$$

Grâce à la Proposition 2.2.5, on remarque que, si $\chi_0,\chi_1,\dots,\chi_n$ sont non triviaux,

$$|\mathbf{j}_q(\chi_0,\chi_1,\dots,\chi_n)| = \begin{cases} q^{(n-1)/2} & \text{si } \chi_0\cdot\chi_1\cdot\cdots\cdot\chi_n = \mathbf{1}, \\ q^{n/2} & \text{si } \chi_0\cdot\chi_1\cdot\cdots\cdot\chi_n \neq \mathbf{1}. \end{cases} \tag{2.1}$$

Remarque 2.2.8. Nous aurons surtout besoin du cas où $n=1$. Si $\chi_1,\chi_2 : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ sont deux caractères non triviaux de $\mathbb{F}_q^\times$, alors la Proposition ci-dessus donne que $\mathbf{j}_q(\mathbf{1},\mathbf{1}) = -q$, que $\mathbf{j}_q(\chi_1,\mathbf{1}) = 0$ et que

$$\mathbf{j}_q(\chi_1,\chi_2) = \begin{cases} \chi_1(-1) & \text{si } \chi_1\chi_2 = \mathbf{1}, \\ \dfrac{\mathbf{g}_q(\chi_1)\cdot\mathbf{g}_q(\chi_2)}{\mathbf{g}_q(\chi_1\cdot\chi 2)} & \text{si } \chi_1\chi_2 \neq \mathbf{1}. \end{cases}$$

En particulier, la Proposition précédente (ou le Lemme 2.2.3) implique que

$$\mathbf{j}_q(\mu,\mu) = \mu(-1). \tag{2.2}$$

Rappelons enfin la relation suivante (*cf.* [Coh07, Prop. 2.5.18] ou [LN97, Exercice 5.43]).

Lemme 2.2.9. *Soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère non trivial. Alors*

$$\mathbf{j}_q(\chi, \mu) = \chi(4) \cdot \mathbf{j}_q(\chi, \chi).$$

Cette relation est fausse si χ est le caractère trivial. En effet, comme μ n'est pas trivial, on a $\mathbf{j}_q(\mathbf{1}, \mu) = 0$ mais $\mathbf{j}_q(\mathbf{1}, \mathbf{1}) = -q$.

2.2.3 Sommes de Legendre

Soit à nouveau $\mathbb{F}_q$ un corps fini de caractéristique p. Désignons à nouveau par $\mu = \mu_q : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ le caractère « de Legendre », *i.e.* l'unique caractère non trivial d'ordre 2 de $\mathbb{F}_q^\times$.

Définition 2.2.10. Soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère multiplicatif et soit $b \in \mathbb{F}_q$. On définit la *somme de Legendre* associée par :

$$\boldsymbol{S}_q(\chi; b) := -\sum_{x \in \mathbb{F}_q} \chi(x) \cdot \mu_q(x^2 + 2bx + 1).$$

Tel qu'elle est définie, la somme $\boldsymbol{S}_q(\chi; b)$ est un entier du corps cyclotomique $\mathbb{Q}(\zeta_d)$, où d est l'ordre du caractère χ.

Remarque 2.2.11. Ces sommes ont été introduites par R. Evans [Eva86, Eq. (2.3)] comme analogues sur les corps finis des fonctions (spéciales) de Legendre :

$$\forall n \in \mathbb{N}^*, \forall x \in \mathbb{R}, \quad H_n(x) = \frac{1}{2i\pi} \int_C \frac{1}{\sqrt{u^2 - 2xu + 1}} \cdot \frac{\mathrm{d}u}{u}.$$

Il suit ainsi le « programme » initié par J. Greene (voir [Gre87]) de trouver des analogues sur les corps finis des fonctions hypergéométriques, mais ne démontre aucun résultat sur $\boldsymbol{S}_q(\chi; b)$. Mentionnons également [Saw92], traitant plus spécifiquement des sommes $\boldsymbol{S}_q(\chi; b)$.

Ceci étant, nous n'avons pas trouvé dans la littérature existante les résultats dont nous avions besoin, à savoir : une « relation de Hasse-Davenport » pour les sommes $\boldsymbol{S}_q(\chi; b)$ et l'analogue de l'« hypothèse de Riemann » pour celles-ci. Nous démontrons ces relations aux Théorème 2.2.21 et Corollaire 2.3.5. De plus, nous montrons que les sommes de Legendre apparaissent naturellement dans les fonctions zeta de certaines courbes hyperelliptiques sur $\mathbb{F}_q$ (Théorème 2.3.4).

Commençons par donner quelques relations satisfaites par les sommes de Legendre.

Proposition 2.2.12. *Soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère.*

- *Si $b = \pm 1$ et si $\chi = \mathbf{1}$ est trivial, on a $\boldsymbol{S}_q(\mathbf{1}; b) = 1 - q$.*
- *Si $b = \pm 1$ et si χ n'est pas trivial, on a $\boldsymbol{S}_q(\chi; b) = \chi(-b)$.*
- *Si $b \neq 0, \pm 1$ et si $\chi = \mathbf{1}$, on a $\boldsymbol{S}_q(\mathbf{1}; b) = 1$.*
- *Pour tout $b \in \mathbb{F}_q$, on a $\boldsymbol{S}_q(\chi; -b) = \chi(-1) \cdot \boldsymbol{S}_q(\chi; b)$.*
- *Pour tout $b \in \mathbb{F}_q$, on a $\boldsymbol{S}_q(\chi; b) = \boldsymbol{S}_q(\overline{\chi}; b) = \overline{\boldsymbol{S}_q(\chi; b)}$.*

Démonstration. Commençons par supposer que $b = \pm 1$. Dans ce cas, on a $x^2 + 2bx + 1 = (x \pm b)^2$ et pour tout caractère $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$,

$$-\boldsymbol{S}_q(\chi; b) = \sum_{x \in \mathbb{F}_q} \chi(x)\mu(x + b)^2 = \sum_{x \neq -b} \chi(x) = -\chi(-b) + \sum_{x \in \mathbb{F}_q} \chi(x).$$

Par conséquent, si $\chi = \mathbf{1}$, on a $\boldsymbol{S}_q(\mathbf{1}; \pm 1) = 1 - q$ et, si $\chi \neq \mathbf{1}$, on a $\boldsymbol{S}_q(\chi; b) = \chi(-b)$. Dans le cas où $b = 0$, d'après le Lemme 2.2.3, on a

$$-\boldsymbol{S}_q(\chi; 0) = \sum_{x \in \mathbb{F}_q} 1 \cdot \mu(x^2 + 1) = -1.$$

Soit $b \in \mathbb{F}_q$ et $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère quelconque. Le changement de variables « $x' = -x$ » donne immédiatement

$$\begin{aligned} -\boldsymbol{S}_q(\chi; -b) &= \sum_{x \in \mathbb{F}_q} \chi(x)\mu(x^2 - 2bx + 1) = \sum_{x' \in \mathbb{F}_q} \chi(-x')\mu\big((-x')^2 + 2bx' + 1\big) \\ &= \chi(-1) \sum_{x' \in \mathbb{F}_q} \chi(x')\mu(x'^2 + 2bx' + 1) = -\chi(-1) \cdot \boldsymbol{S}_q(\chi; b). \end{aligned}$$

Démontrons ensuite que $\boldsymbol{S}_q(\chi;b)$ est réelle. C'est immédiat si $\chi=\mathbf{1}$ (et ce, quelque soit b) d'après ce qu'on vient de prouver. Concentrons-nous donc sur le cas où $\chi:\mathbb{F}_q^\times\to\overline{\mathbb{Q}}^\times$ n'est pas trivial. Alors, comme $x^2+2bx+1=x^2\cdot(x^{-2}+2bx^{-1}+1)$ pour tout $x\in\mathbb{F}_q^\times$, on a

$$\begin{aligned}-\overline{\boldsymbol{S}_q(\chi,b)}&=\sum_{x\in\mathbb{F}_q}\overline{\chi(x)}\mu(x^2+2bx+1)=\sum_{x\in\mathbb{F}_q^\times}\overline{\chi(x)}\mu(x^2+2bx+1)\\&=\sum_{x\in\mathbb{F}_q^\times}\chi(x^{-1})\mu(x^2+2bx+1)=\sum_{x'\in\mathbb{F}_q^\times}\chi(x')\mu(x'^2)\mu(x'^2+2bx'+1)\\&=-\boldsymbol{S}_q(\chi,b).\end{aligned}$$

De façon similaire, comme $\mu(x^2+2bx+1)$ est réel pour tout $x\in\mathbb{F}_q$, on voit que $\boldsymbol{S}_q(\overline{\chi},b)=\boldsymbol{S}_q(\chi,b)$. □

Dans le cas où $b=0$, on peut expliciter les sommes $\boldsymbol{S}_q(\chi;0)$ en termes de sommes de Jacobi :

Proposition 2.2.13. *Pour tout caractère non trivial $\chi:\mathbb{F}_q^\times\to\overline{\mathbb{Q}}^\times$, on a*

- *Si $\chi(-1)=-1$, alors $\boldsymbol{S}_q(\chi;0)=0$.*
- *Si $\chi(-1)=1$, alors il existe un caractère $\theta:\mathbb{F}_q^\times\to\overline{\mathbb{Q}}^\times$ tel que $\chi=\theta^2$ et*

$$\boldsymbol{S}_q(\chi;0)=\theta(-1)\cdot\mathbf{j}_q(\theta,\mu)+\mu(-1)\theta(-1)\cdot\mathbf{j}_q(\mu\theta,\mu).$$

Démonstration. D'après la Proposition précédente, on a $\boldsymbol{S}_q(\chi;0)=\chi(-1)\cdot\boldsymbol{S}_q(\chi;-0)$. On en déduit immédiatement que $\boldsymbol{S}_q(\chi;0)=0$ si $\chi(-1)=-1$. Passons donc au cas où $\chi(-1)=1$: d'après le Lemme 2.1.1, il existe un caractère $\theta:\mathbb{F}_q^\times\to\overline{\mathbb{Q}}^\times$ (nécessairement non trivial) tel que $\chi=\theta^2$. Alors, à l'aide du Lemme 2.2.1, on trouve :

$$\begin{aligned}-\boldsymbol{S}_q(\chi;0)&=\sum_{x\in\mathbb{F}_q}\chi(x)\mu(x^2+0+1)=\sum_{x\in\mathbb{F}_q}\theta^2(x)\mu(x^2+1)=\sum_{x\in\mathbb{F}_q}\theta(x^2)\mu(x^2+1)\\&=\sum_{s\in\mathbb{F}_q}\theta(s)\mu(s+1)\cdot\#\left\{x\in\mathbb{F}_q\;\middle|\;s=x^2\right\}=\sum_{s\in\mathbb{F}_q}\theta(s)\mu(s+1)\cdot(1+\mu(s))\\&=\sum_{s\in\mathbb{F}_q}\theta(s)\mu(s+1)+\sum_{s\in\mathbb{F}_q}\mu(s)\theta(s)\mu(s+1)\\&=\theta(-1)\sum_{s\in\mathbb{F}_q}\theta(-s)\mu(s+1)+\theta(-1)\mu(-1)\sum_{s\in\mathbb{F}_q}\theta\mu(-s)\mu(s+1)\\&=-\theta(-1)\cdot\mathbf{j}_q(\theta,\mu)-\theta(-1)\mu(-1)\cdot\mathbf{j}_q(\mu\theta,\mu).\end{aligned}$$

Comme il fallait démontrer. □

Notons également que les sommes $\boldsymbol{S}_q(\chi;b)$ admettent une expression qui ne fait pas intervenir le caractère μ.

Proposition 2.2.14. *Pour tout $b\in\mathbb{F}_q\smallsetminus\{-1,1\}$, on pose $a=(1-b)/2$. Soit $\chi:\mathbb{F}_q^\times\to\overline{\mathbb{Q}}^\times$ un caractère* non trivial. *On a*

$$\boldsymbol{S}_q(\chi;b)=-\sum_{\substack{x\in\mathbb{F}_q\\x\neq a}}\chi\left(\frac{x(x-1)}{x-a}\right)=-\sum_{x\in\mathbb{F}_q}\chi(x)\chi(x-1)\overline{\chi}(x-a).$$

Démonstration. Considérons l'application $f:\mathbb{P}^1\to\mathbb{P}^1$ définie par $f(x)=\frac{x(x-1)}{x-a}$. Vu les hypothèses sur b, l'application rationnelle f est de degré 2 (car $a\neq0,1$). Par commodité, on prolonge tout caractère non trivial χ à $\mathbb{P}^1(\mathbb{F}_q)=\mathbb{F}_q\cup\{\infty\}$ par $\chi(\infty)=0$. Avec ces notations, le membre de droite de l'égalité à démontrer vaut

$$\sum_{\substack{x\in\mathbb{F}_q\\x\neq a}}\chi\left(\frac{x(x-1)}{x-a}\right)=\sum_{x\in\mathbb{P}^1(\mathbb{F}_q)}\chi\left(f(x)\right)=\sum_{t\in\mathbb{P}^1(\mathbb{F}_q)}\chi\left(t\right)\cdot\#\left\{x\in\mathbb{P}^1(\mathbb{F}_q)\;\middle|\;f(x)=t\right\}.$$

Soit $t\in\mathbb{P}^1(\mathbb{F}_q)$, écrivons $\#\left\{x\in\mathbb{P}^1(\mathbb{F}_q)\;\middle|\;f(x)=t\right\}$ sous une forme plus manipulable. Si $t=\infty$, on a $\#\left\{x\in\mathbb{P}^1(\mathbb{F}_q)\;\middle|\;f(x)=\infty\right\}=2$ (les deux solutions en question sont $x=a$ et $x=\infty$). Sinon, pour tout $x\in\mathbb{F}_q$, on a

$$t=f(x)\iff x(x-1)=t(x-a)\iff x^2-(t+1)x+at=0.$$

Vue comme une équation quadratique en x, cette dernière égalité est vérifiée pour $1+\mu(\delta_t)$ valeurs de $x \in \mathbb{P}^1(\mathbb{F}_q)$, où δ_t est le discriminant

$$\delta_t = (t+1)^2 - 4at = t^2 + 2(1-2a)t + 1 = t^2 + 2bt + 1.$$

Par conséquent, $\#\left\{x \in \mathbb{P}^1(\mathbb{F}_q) \;\middle|\; f(x) = t\right\} = 1 + \mu(t^2+2bt+1)$ et

$$\begin{aligned}\sum_{\substack{x\in\mathbb{F}_q\\ x\neq a}} \chi\left(\frac{x(x-1)}{x-a}\right) &= \sum_{t\in\mathbb{P}^1(\mathbb{F}_q)} \chi(t)\cdot\big(1+\mu(t^2+2bt+1)\big)\\ &= \sum_{t\in\mathbb{F}_q} \chi(t)\cdot\big(1+\mu(t^2+2bt+1)\big)\\ &= \sum_{t\in\mathbb{F}_q} \chi(t) + \sum_{t\in\mathbb{F}_q} \chi(t)\,\mu(t^2+2bt+1)\\ &= 0 - \boldsymbol{S}_q(\chi;b).\end{aligned}$$

Nous avons utilisé que, par convention, $\chi(\infty)=0$ et que, comme χ est non trivial, $\sum_t \chi(t) = 0$. □

Remarque 2.2.15. Soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère *non trivial* et $b \in \mathbb{F}_q$ (quelconque). Alors

$$\sum_{x\in\mathbb{F}_q} \chi(x)\big(1+\mu(x^2+2bx+1)\big) = \sum_{x\in\mathbb{F}_q}\chi(x) + \sum_{x\in\mathbb{F}_q}\chi(x)\mu(x^2+2bx+1) = -\boldsymbol{S}_q(\chi;b).$$

Or, pour tout $x \in \mathbb{F}_q$, $1+\mu(x^2+2bx+1)$ est un entier pair. Ce qui montre que $\boldsymbol{S}_q(\chi;b) \equiv 0 \bmod 2$, au sens où $\boldsymbol{S}_q(\chi;b)/2$ est un entier algébrique.

2.2.4 Relations de Hasse-Davenport

Commençons par rappeler le « principe de Hasse-Davenport » (*cf.* [LN97, Chap. 5, pp. 195-196]).

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$, fixé pour le reste de cette section. On note $\Phi \subset \mathbb{F}_q[X]$, l'ensemble des polynômes unitaires à coefficients dans $\mathbb{F}_q$ et $\Phi_k \subset \Phi$, le sous-ensemble de ceux qui sont de degré k ($k \in \mathbb{N}^*$). De plus, on notera $\mathbb{P} \subset \Phi$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_q[X]$.

Définition 2.2.16. Soit $\lambda : \Phi \to \mathbb{C}$ une application. On dira que λ satisfait la *condition de Hasse-Davenport à l'ordre* $K \in \mathbb{N}^*$ si elle vérifie :

(i) $\lambda(1) = 1$,

(ii) $|\lambda(F)| \leqslant 1$ pour tout $F \in \Phi$,

(iii) $\lambda(FG) = \lambda(F)\lambda(G)$ pour tout $F, G \in \Phi$,

(iv) Pour tout $k > K$, $\sum_{F\in\Phi_k} \lambda(F) = 0$.

Avec cette définition, on peut démontrer le Théorème (formel) suivant.

Théorème 2.2.17 (« Principe de Hasse-Davenport »)**.** *Soit $\lambda : \Phi \to \mathbb{C}$ une application qui satisfait à la condition de Hasse-Davenport à l'ordre K (cf. Définition 2.2.16). Pour tout entier $s \geqslant 1$, on pose*

$$S(\lambda, s) := -\sum_{\substack{P\in\mathbb{P}\\ \deg P \mid s}} \deg(P)\lambda(P)^{s/\deg P}.$$

Alors il existe des nombres complexes $\omega_1, \ldots, \omega_K$ (qui ne dépendent que de λ) tels que

$$\forall s \geqslant 1, \qquad S(\lambda, s) = {\omega_1}^s + {\omega_2}^s + \cdots + {\omega_K}^s.$$

Démonstration. On pose $\Sigma_0(\lambda) = 1$ et pour tout $k \geqslant 1$, on définit $\Sigma_k(\lambda) = \sum_{F\in\Phi_k} \lambda(F)$. On considère la série formelle :

$$\mathcal{L}(\lambda, X) := \sum_{k=0}^{\infty} \Sigma_k(\lambda) X^k.$$

Comme $\#\Phi_k = q^k$ et que λ satisfait la condition (ii) de la Définition 2.2.16, on a $|\Sigma_k(\lambda)| \leqslant q^k$. La série $\mathcal{L}(\lambda, X)$ est donc convergente dans le disque ouvert $\{z \in \mathbb{C} \mid |z| < q^{-1}\}$. Par multiplicativité

de λ (condition (iii) de la Définition 2.2.16) et comme tout polynôme $F \in \Phi$ se décompose de façon unique en un produit de polynômes irréductibles unitaires, on peut écrire (par un argument usuel) :

$$\mathcal{L}(\lambda, X) = \prod_{P\in\mathbb{P}} \left(\sum_{n=0}^{\infty} \lambda(P^n) X^{n \deg P} \right) = \prod_{P\in\mathbb{P}} \left(\sum_{n=0}^{\infty} (\lambda(P) X^{\deg P})^n \right).$$

En sommant les séries géométriques qui apparaissent, on constate que $\mathcal{L}(\lambda, X)$ s'écrit comme produit eulérien :

$$\mathcal{L}(\lambda, X) = \prod_{P\in\mathbb{P}} \left(1 - \lambda(P) X^{\deg P}\right)^{-1}.$$

Le logarithme de ce produit eulérien s'écrit alors

$$\begin{aligned} -\log \mathcal{L}(\lambda, X) &= \sum_{P\in\mathbb{P}} \sum_{n=1}^{\infty} \frac{(\lambda(P) X^{\deg P})^n}{n} = \sum_{P\in\mathbb{P}} \deg P \cdot \sum_{n=1}^{\infty} \frac{(\lambda(P) X^{\deg P})^n}{n \deg P} \\ &= \sum_{n=1}^{\infty} \sum_{P\in\mathbb{P}} \deg P \cdot \frac{\lambda(P)^{n \deg P/ \deg P} X^{n \deg P}}{n \deg P} = \sum_{s=1}^{\infty} \sum_{\deg P | s} \deg P \cdot \frac{\lambda(P)^{s/ \deg P} X^s}{s} \\ &= \sum_{s=1}^{\infty} \left(\sum_{\deg P | s} \deg P \cdot \lambda(P)^{s/ \deg P} \right) \frac{X^s}{s} = -\sum_{s=1}^{\infty} S(\lambda, s) \frac{X^s}{s}. \end{aligned} \tag{2.3}$$

Par hypothèse, la condition (iv) de la Définition 2.2.16 est satisfaite : $\mathcal{L}(\lambda, X)$ est donc en fait un polynôme de degré $\leqslant K$ en X, tel que $\mathcal{L}(\lambda, 0) = 1$. On peut donc trouver des nombres complexes $\omega_1, \ldots, \omega_K$ tels que

$$\mathcal{L}(\lambda, X) = (1 - \omega_1 X)(1 - \omega_2 X) \ldots (1 - \omega_K X).$$

Le logarithme d'un tel polynôme s'écrit

$$-\log \mathcal{L}(\lambda, X) = \sum_{s=1}^{\infty} ({\omega_1}^s + {\omega_2}^s + \cdots + {\omega_K}^s) \frac{X^s}{s}. \tag{2.4}$$

Rapprochons les deux expressions (2.3) et (2.4) de $-\log \mathcal{L}(\lambda, X)$:

$$\sum_{s=1}^{\infty} S(\lambda, s) \frac{X^s}{s} = \sum_{s=1}^{\infty} ({\omega_1}^s + {\omega_2}^s + \cdots + {\omega_K}^s) \frac{X^s}{s}.$$

Par identification des coefficients de ces deux séries formelles, on trouve bien le résultat annoncé. En outre, remarquons que le coefficient dominant de $\mathcal{L}(\lambda, X)$ vaut

$$(-1)^K \cdot \prod_{k=1}^{K} \omega_k = \Sigma_K(\lambda) = \sum_{F\in\Phi_K} \lambda(F). \tag{2.5}$$

□

On pourra consulter [Kat81, §I - § II] pour une interprétation cohomologique de ce Théorème. On en déduit le résultat classique ci-dessous.

Théorème 2.2.18 (Relation de Hasse-Davenport pour les sommes de Gauss)**.** *Soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère non trivial et $\mathbb{F}_{q^s}/\mathbb{F}_q$ une extension finie de degré $s \in \mathbb{N}^*$. Comme ci-dessus, on note $\chi^{(s)} : \mathbb{F}_{q^s}^\times \to \overline{\mathbb{Q}}^\times$ le caractère déduit de χ par composition avec la norme (i.e. $\chi^{(s)} = \chi \circ \mathbf{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$). Alors*

$$\mathbf{g}_{q^s}(\chi^{(s)}) = \mathbf{g}_q(\chi)^s.$$

Démonstration. Soit χ un caractère non trivial de $\mathbb{F}_q^\times$, on note $\psi_q : \mathbb{F}_q \to \overline{\mathbb{Q}}$ le caractère additif standard de $\mathbb{F}_q$. Définissons $\lambda : \Phi \to \mathbb{C}$ l'application qui, à tout polynôme non constant $F = X^k + c_{k-1}X^{k-1} + \ldots c_1 X + c_0 \in \Phi_k$ $(k \geqslant 1)$ associe

$$\lambda(F) = \chi\left((-1)^{\deg F} c_0\right) \cdot \psi_q(-c_{k-1}).$$

On pose par ailleurs $\lambda(1) = 1$. Vérifions d'abord que λ satisfait la condition de Hasse-Davenport à l'ordre 1 (*cf.* Définition 2.2.16). On a $\lambda(1) = 1$ par définition et il est clair que $|\lambda(F)| \leqslant 1$ pour tout $F \in \Phi$. De plus, si $F, G \in \Phi$ sont deux polynômes non constants, mettons

$$F = X^k + c_{k-1}X^{k-1} + \cdots + c_1 X + c_0, \quad G = X^\ell + c'_{\ell-1}X^{\ell-1} + \cdots + c'_1 X + c'_0,$$

alors $FG = X^{k+\ell} + (c_{k-1} + c'_{\ell-1})X^{k+\ell-1} + \cdots + c_0 c'_0$ et

$$\begin{aligned}\lambda(FG) &= \chi\left((-1)^{\deg(FG)} c_0 c'_0\right) \cdot \psi_q(-c_{k-1} - c'_{\ell-1}) \\ &= \chi\left((-1)^{\deg F} c_0\right) \psi_q(-c_{k-1}) \cdot \chi\left((-1)^{\deg G} c'_0\right) \psi_q(-c'_{\ell-1}) \\ &= \lambda(F)\lambda(G).\end{aligned}$$

Il reste enfin à s'assurer que λ vérifie la condition (iv) de la définition 2.2.16 : soit $k > 1$, on a

$$\begin{aligned}\sum_{F \in \Phi_k} \lambda(F) &= \sum_{c_{k-1} \in \mathbb{F}_q} \sum_{c_{k-2} \in \mathbb{F}_q} \cdots \sum_{c_1 \in \mathbb{F}_q} \sum_{c_0 \in \mathbb{F}_q} \chi\left((-1)^k c_0\right) \psi_q(-c_{k-1}) \\ &= \chi(-1)^k q^{k-2} \cdot \sum_{c_{k-1} \in \mathbb{F}_q} \sum_{c_0 \in \mathbb{F}_q} \chi(c_0)\psi_q(-c_{k-1}) \\ &= \chi(-1)^k q^{k-2} \cdot \left(\sum_{c_{k-1} \in \mathbb{F}_q} \psi_q(-c_{k-1})\right)\left(\sum_{c_0 \in \mathbb{F}_q} \chi(c_0)\right) \\ &= \chi(-1)^k q^{k-2} \cdot 0 = 0.\end{aligned}$$

En effet, χ n'est pas le caractère trivial donc $\sum_{c_0} \chi(c_0) = 0$. Ce qui précède prouve que λ vérifie la condition de Hasse-Davenport à l'ordre 1. On peut donc appliquer le Théorème 2.2.17 : posons

$$\forall s \in \mathbb{N}^*, \quad S(\lambda, s) := -\sum_{\substack{P \in \mathbb{P} \\ \deg P | s}} \deg(P) \lambda(P)^{s/\deg P}.$$

Alors il existe un nombre complexe ω_1 tel que $S(\lambda, s) = {\omega_1}^s$ pour tout $s \in \mathbb{N}^*$; en particulier on sait que $\omega_1 = S(\lambda, 1)$. Il ne reste donc qu'à relier $S(\lambda, s)$ et $\mathbf{g}_{q^s}(\chi^{(s)})$.

Fixons à cet effet un entier $s \in \mathbb{N}^*$: on notera $\mathbb{P}_s$ l'ensemble des polynômes irréductibles unitaires dont le degré divise s. Pour tout $P = X^d + c_{d-1}X^{d-1} + \cdots + c_0 \in \mathbb{P}_s$ de degré d, on note $z_1, \ldots, z_d$ ses racines dans $\overline{\mathbb{F}_q}$. Si z est l'une d'entre elles (on a nécessairement $z \neq 0$, sinon $X \mid P$), les conjugués de z dans l'extension galoisienne $\mathbb{F}_{q^d}/\mathbb{F}_q$ sont $z_1, \ldots, z_d$ et on a $z^{q^d} = z$. De plus, les relations coefficients/racines donnent que $(-1)^d c_0 = z_1 z_2 \ldots z_n$ et $c_{d-1} = -(z_1 + z_2 + \cdots + z_d)$. Ce qui entraîne,

$$\mathbf{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(z) = \prod_{i=0}^{s-1} z^{q^i} = (z_1 z_2 \ldots z_d)^{s/d} = (-1)^s c_0^{s/d}, \tag{2.6}$$

$$\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(z) = \sum_{i=0}^{s-1} z^{q^i} = \frac{s}{d}\left(z_1 + z_2 + \cdots + z_d\right) = -\frac{s}{d} c_{d-1}. \tag{2.7}$$

Ainsi, comme χ est multiplicatif et ψ_q additif, on a

$$\begin{aligned}\lambda(P)^{s/d} &= \left(\chi((-1)^d c_0)\psi_q(-c_{d-1})\right)^{s/d} = \chi\left((-1)^s c_0^{s/d}\right) \cdot \psi_q\left(-\frac{s}{d} c_{d-1}\right) \\ &= \chi \circ \mathbf{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(z) \cdot \psi_q \circ \mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(z) = \chi^{(s)}(z) \cdot \psi_{q^s}(z).\end{aligned}$$

Lorsque l'on somme cette identité sur les racines $z_1, \ldots, z_d$ de P, on obtient

$$\sum_{\substack{z \in \overline{\mathbb{F}_q} \\ P(z)=0}} \chi^{(s)}(z) \cdot \psi_{q^s}(z) = \sum_{i=1}^{d} \chi^{(s)}(z_i) \cdot \psi_{q^s}(z_i) = d \cdot \lambda(P)^{s/d}$$

car, les z_i étant conjugués, ils ont même trace et même norme. On peut alors sommer cette dernière identité pour $P \in \mathbb{P}_s$ en remarquant que

$$\prod_{P \in \mathbb{P}_s} P = \prod_{\substack{P \in \mathbb{P} \\ \deg P | s}} P = X^{q^s} - X. \tag{2.8}$$

On arrive donc à

$$\begin{aligned}-S(\lambda, s) &= \sum_{P \in \mathbb{P}_s} \deg P \cdot \lambda(P)^{s/\deg P} = \sum_{P \in \mathbb{P}_s} \sum_{\substack{z \in \overline{\mathbb{F}_q} \\ P(z)=0}} \chi^{(s)}(z) \cdot \psi_{q^s}(z) \\ &= \sum_{\substack{z \in \overline{\mathbb{F}_q} \\ z^{q^s} - z = 0}} \chi^{(s)}(z) \cdot \psi_{q^s}(z) = \sum_{z \in \mathbb{F}_{q^s}} \chi^{(s)}(z) \cdot \psi_{q^s}(z) = -\mathbf{g}_{q^s}(\chi^{(s)}).\end{aligned}$$

Dans la dernière égalité, il faut remarquer que le terme « $z = 0$ » ne contribue pas car $\chi^{(s)}$ n'est pas trivial. Ceci conclut la preuve. □

Remarque 2.2.19. Le lecteur pourra consulter [DH35] pour la preuve « historique », [LN97, Theorem 5.14] ou [Wei49] pour des preuves plus « modernes ». Noter l'absence de « $(-1)^s$ » dans la relation du Théorème 2.2.18. Ceci est dû à notre choix de normalisation pour les sommes de Gauss.

Du Théorème ci-dessus et de la Proposition 2.2.7, on déduit immédiatement que les sommes de Jacobi vérifient également une « relation de Hasse-Davenport à l'ordre 1 » ([LN97, Theorem 5.26] propose une preuve directe à partir du Théorème 2.2.17) :

Corollaire 2.2.20 (Relation de Hasse-Davenport pour les sommes de Jacobi)**.** *Soit $n \geqslant 1$ et $\chi_0, \chi_1, \dots, \chi_n : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ des caractères non tous triviaux. Soit aussi $\mathbb{F}_{q^s}/\mathbb{F}_q$ une extension finie de degré s. On prolonge les caractères χ_i en $\chi_i^{(s)} : \mathbb{F}_{q^s}^\times \to \overline{\mathbb{Q}}^\times$ de la même façon que précédemment. Alors*

$$\mathbf{j}_{q^s}\left(\chi_0^{(s)}, \chi_1^{(s)}, \dots, \chi_n^{(s)}\right) = \mathbf{j}_q(\chi_0, \chi_1, \dots, \chi_n)^s.$$

Enfin, à l'aide du Théorème 2.2.17, nous démontrons le théorème principal de cette section : c'est un résultat nouveau concernant les sommes de Legendre $\boldsymbol{S}_q(\chi; b)$ introduites à la Section 2.2.3. Plus précisément, nous prouvons que $\boldsymbol{S}_q(\chi; b)$ vérifie une « relation de Hasse-Davenport à l'ordre 2 ».

Théorème 2.2.21. *Soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère non trivial de $\mathbb{F}_q^\times$ et $b \in \mathbb{F}_q \smallsetminus \{1, -1\}$. Il existe deux nombres complexes $\alpha_b(\chi)$ et $\beta_b(\chi)$ (qui ne dépendent que de b et de χ) tels que, pour tout entier $s \in \mathbb{N}^*$, si l'on note $\chi^{(s)} : \mathbb{F}_{q^s}^\times \to \overline{\mathbb{Q}}^\times$ l'extension de χ à $\mathbb{F}_{q^s}^\times$ via la norme (i.e. $\chi^{(s)} = \chi \circ \mathbf{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}$), on a*

$$\boldsymbol{S}_{q^s}(\chi^{(s)}, b) = \alpha_b(\chi)^s + \beta_b(\chi)^s.$$

De plus, on a $\alpha_b(\chi) \cdot \beta_b(\chi) = q$.

Enfin, les nombres $\alpha_b(\overline{\chi})$ et $\beta_b(\overline{\chi})$ ainsi associés à la somme $\boldsymbol{S}_q(\overline{\chi}, b)$ sont, à permutation près, les mêmes que ceux associés à $\boldsymbol{S}_q(\chi, b)$:

$$\{\alpha_b(\overline{\chi}), \beta_b(\overline{\chi})\} = \{\alpha_b(\chi), \beta_b(\chi)\}.$$

Remarque 2.2.22. Nous verrons plus loin (Corollaire 2.3.5) que $|\alpha_b(\chi)| = |\beta_b(\chi)| = \sqrt{q}$. Ce fait est l'analogue de l'« hypothèse de Riemann » pour les sommes $\boldsymbol{S}_q(\chi; b)$ et n'est pas une conséquence du Théorème 2.2.21. Notons également que celui-ci ne se déduit pas d'autres relations de Hasse-Davenport pour des sommes de caractères classiques (par exemple celles démontrées dans [LN97, Chapter 5, §5]).

Démonstration (du Théorème 2.2.21). Avec les notations introduites au début de ce paragraphe, nous allons définir une application $\lambda : \Phi \to \mathbb{C}$ adaptée à nos besoins. Dans un premier temps, nous montrons que λ satisfait aux conditions de la Définition 2.2.16. Nous appliquons ensuite le Théorème 2.2.17 à celle-ci. Enfin, nous relions les sommes $S(\lambda, s)$ associées à λ aux sommes $\boldsymbol{S}_{q^s}(\chi^{(s)}; b)$ qui nous intéressent.

Soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère non trivial et $b \in \mathbb{F}_q \smallsetminus \{1, -1\}$. On notera $Q_b = X^2 + 2bX + 1 \in \mathbb{F}_q[X]$: c'est une forme quadratique dont le discriminant $\delta = 4(b^2 - 1)$ est non nul. Appelons y et y' les deux racines (distinctes) de Q_b dans $\overline{\mathbb{F}_q}$: celles-ci sont conjuguées et vérifient $y + y' = -2b$ et $yy' = 1$.

Soit alors $\lambda : \Phi \to \mathbb{C}$ définie par $\lambda(1) = 1$ et, pour tout polynôme $F \in \Phi$ non constant,

$$\lambda(F) := \chi\left((-1)^{\deg F} F(0)\right) \mu_q\left(F(y)F(y')\right).$$

Cette définition est licite : comme F est à coefficients $\mathbb{F}_q$-rationnels et que y et y' sont conjuguées, on a bien $F(y)F(y') \in \mathbb{F}_q$. Ainsi construite, l'application λ vérifie clairement les conditions (i) et (ii) de la Définition 2.2.16. Si $F, G \in \Phi$, on a

$$\begin{aligned}\lambda(FG) &= \chi\left((-1)^{\deg FG} FG(0)\right) \mu_q\left(FG(y)FG(y')\right) \\ &= \chi\left((-1)^{\deg F} F(0)\right) \chi\left((-1)^{\deg G} G(0)\right) \mu_q\left(F(y)F(y')\right) \mu_q\left(G(y)G(y')\right) \\ &= \lambda(F)\lambda(G),\end{aligned}$$

et la condition (iii) est également satisfaite par λ. Soit maintenant un entier $k \geqslant 2$; étudions de plus près les sommes $\Sigma_k(\lambda) := \sum_{F \in \Phi_k} \lambda(F)$. Pour tout $F \in \Phi_k$, écrivons la division euclidienne de F par

Q_b sous la forme $F = A \cdot Q_b + (\alpha X + \beta)$, où le reste est $\alpha X + \beta \in \mathbb{F}_q[X]$ et le quotient $A \in \mathbb{F}_q[X]$ est nécessairement unitaire de degré $k-2$. De plus, comme $Q_b(0) = 1$ et $Q_b(y) = Q_b(y') = 0$, on a

$$F(0) = A(0) + \beta \quad \text{et} \quad F(y)F(y') = (\alpha y + \beta)(\alpha y' + \beta) = \alpha^2 - 2b\alpha\beta + \beta^2.$$

En particulier, $\lambda(F) = \chi(-1)^k \cdot \chi(A(0)+\beta)\mu_q(\alpha^2 - 2b\alpha\beta + \beta^2)$. Réciproquement, étant donné $A \in \Phi_{k-2}$, $\alpha, \beta \in \mathbb{F}_q$, le polynôme $F = AQ_b + \alpha X + \beta$ est un élément de Φ_k. Nous venons d'établir une bijection $r : \Phi_k \to \Phi_{k-2} \times \mathbb{F}_q \times \mathbb{F}_q$.

Si $k = 2$, l'ensemble $\Phi_{k-2} = \Phi_0$ est réduit au polynôme $1 = X^0$ et

$$\begin{aligned}
\Sigma_2(\lambda) &= \sum_{F \in \Phi_2} \lambda(F) = \sum_{A \in \Phi_0} \sum_{\alpha \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \lambda(AQ_b + \alpha X + \beta) \\
&= \chi(-1)^2 \cdot \sum_{A \in \Phi_0} \sum_{\alpha \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \chi(A(0) + \beta)\mu_q(\alpha^2 - 2b\alpha\beta + \beta^2) \\
&= \sum_{\beta \in \mathbb{F}_q} \chi(1+\beta) \left(\sum_{\alpha \in \mathbb{F}_q} \mu_q(\alpha^2 - 2b\alpha\beta + \beta^2) \right).
\end{aligned}$$

Or, pour tout $\beta \in \mathbb{F}_q$, la somme $\sum_{\alpha \in \mathbb{F}_q} \mu_q(\alpha^2 - 2b\alpha\beta + \beta^2)$ se calcule aisément (Lemme 2.2.3) :

$$\sum_{\alpha \in \mathbb{F}_q} \mu_q(\alpha^2 - 2b\alpha\beta + \beta^2) = \begin{cases} -\mu(1) & \text{si } 4\beta^2(b^2-1) \neq 0 \\ (q-1)\mu(1) & \text{si } 4\beta^2(b^2-1) = 0. \end{cases}$$

Comme $b^2 \neq 1$ et $\mu(1) = 1$, on a

$$\begin{aligned}
\Sigma_2(\lambda) &= \sum_{\beta \neq 0} \chi(1+\beta) \cdot (-1) + \chi(1+0) \cdot (q-1) = -\sum_{\beta \in \mathbb{F}_q} \chi(1+\beta) + \chi(1) + \chi(1) \cdot (q-1) \\
&= q - \sum_{\beta' \in \mathbb{F}_q} \chi(\beta') = q.
\end{aligned}$$

Ce qui montre que $\Sigma_2(\lambda) = q$ (car, χ étant non trivial, $\sum_{\beta'} \chi(\beta') = 0$). Supposons maintenant $k > 2$: de façon similaire, on obtient

$$\begin{aligned}
\Sigma_k(\lambda) &= \sum_{F \in \Phi_k} \lambda(F) = \sum_{A \in \Phi_{k-2}} \sum_{\alpha \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \lambda(AQ_b + \alpha X + \beta) \\
&= \chi(-1)^k \cdot \sum_{A \in \Phi_{k-2}} \sum_{\alpha \in \mathbb{F}_q} \sum_{\beta \in \mathbb{F}_q} \chi(A(0) + \beta)\mu_q(\alpha^2 - 2b\alpha\beta + \beta^2) \\
&= \chi(-1)^k \cdot \sum_{A \in \Phi_{k-2}} \sum_{\beta \in \mathbb{F}_q} \chi(A(0) + \beta) \left(\sum_{\alpha \in \mathbb{F}_q} \mu_q(\alpha^2 - 2b\alpha\beta + \beta^2) \right) \\
&= \chi(-1)^k \cdot \sum_{A \in \Phi_{k-2}} \left(-\sum_{\beta \neq 0} \chi(A(0) + \beta) + (q-1)\chi(A(0)+0) \right) \\
&= \chi(-1)^k \cdot \sum_{A \in \Phi_{k-2}} \left(-\sum_{\beta \in \mathbb{F}_q} \chi(A(0) + \beta) + q\chi(A(0)) \right) \\
&= \chi(-1)^k \cdot \sum_{A \in \Phi_{k-2}} \left(-\sum_{\beta' \in \mathbb{F}_q} \chi(\beta') + q\chi(A(0)) \right) = \chi(-1)^k q \cdot \sum_{A \in \Phi_{k-2}} \chi(A(0)).
\end{aligned}$$

Mais, si $A \in \Phi_{k-2}$ s'écrit $A = X^{k-2} + a_{k-3}X^{k-3} + \cdots + a_0$, on a $A(0) = a_0$ et

$$\sum_{A \in \Phi_{k-2}} \chi(A(0)) = \sum_{a_{k-3} \in \mathbb{F}_q} \cdots \sum_{a_1 \in \mathbb{F}_q} \sum_{a_0 \in \mathbb{F}_q} \chi(a_0) = q^{k-3} \cdot \sum_{a_0 \in \mathbb{F}_q} \chi(a_0) = 0.$$

Par suite, pour tout $k > 2$ on a $\Sigma_k(\lambda) = 0$. L'application $\lambda : \Phi \to \mathbb{C}$ vérifie donc la condition (iv) de la Définition 2.2.16 avec $K = 2$. Ainsi, λ satisfait la condition de Hasse-Davenport : on pourra lui appliquer le Théorème 2.2.17. Avant de ce faire, nous remarquons que $\Sigma_1(\lambda) = -\boldsymbol{S}_q(\chi; b)$. En effet,

on a $\Phi_1 = \{X - \beta,\ \beta \in \mathbb{F}_q\}$ et, pour $F = X - \beta$:$F(0) = -\beta$ et $F(y)F(y') = (y-\beta)(y'-\beta) = Q_b(\beta)$. Donc $\lambda(F) = \chi((-1)^1(-\beta))\mu(Q_b(\beta)) = \chi(\beta)\mu(Q_b(\beta))$. Par conséquent, on a bien

$$\Sigma_1(\lambda) = \sum_{F\in\Phi_1} \lambda(F) = \sum_{\beta\in\mathbb{F}_q} \lambda(X-\beta) = \sum_{\beta\in\mathbb{F}_q} \chi(\beta)\mu(Q_b(\beta)) = -\boldsymbol{S}_q(b;\chi).$$

Dans les notations de la preuve du Théorème 2.2.17, on a

$$\mathcal{L}(\lambda, X) = \sum_{k=1}^{\infty} \Sigma_k(\lambda) X^k = 1 - \boldsymbol{S}_q(\chi; b)\cdot X + qX^2.$$

On applique à présent le Théorème 2.2.17 sus-mentionné à l'application λ avec $K = 2$: il existe deux nombres complexes ω_1, ω_2 (ne dépendant que de χ et b) tels que

$$\forall s \in \mathbb{N}^*, \qquad S(\lambda, s) = \omega_1^s + \omega_2^s.$$

De plus, ces nombres ω_1, ω_2 vérifient $\mathcal{L}(\lambda, X) = (1-\omega_1 X)(1-\omega_2 X)$. En particulier $\Sigma_1(\lambda) = -\omega_1 - \omega_2$ et $\omega_1\omega_2 = q$. Posons $\omega_1 = \alpha_b(\chi)$ et $\omega_2 = \beta_b(\chi)$.

Il ne reste qu'à exprimer les sommes $S(\lambda, s)$ du Théorème 2.2.17 en termes des sommes $\boldsymbol{S}_{q^s}(\chi^{(s)}; b)$ qui nous intéressent. Soit donc $s \in \mathbb{N}^*$, nous souhaitons étudier :

$$S(\lambda, s) = -\sum_{\substack{P\in\mathbb{P}\\ \deg P | s}} \deg P \cdot \lambda(P)^{s/\deg P}.$$

Comme dans la preuve du Théorème 2.2.18, notons $\mathbb{P}_s$ l'ensemble des polynômes irréductibles unitaires de degré divisant s. Soit $s \in \mathbb{N}^*$ et $P = X^d + c_{d-1}X^{d-1} + \cdots + c_0 \in \mathbb{P}_s$ de degré d. Si z est une racine de P dans $\overline{\mathbb{F}_q}$, on trouve (*cf.* (2.6))

$$\mathbf{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(z) = (-1)^s c_0^{s/d},$$

D'autre part, si l'on note $z = z_1, z_2, \ldots, z_d$ les racines de P, on a

$$\begin{aligned}\mathbf{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(Q_b(z)) &= \prod_{i=0}^{s-1} Q_b(z)^{q^i} = \prod_{i=0}^{s-1} Q_b\left(z^{q^i}\right) \text{ car } Q_b \in \mathbb{F}_q[x]\\ &= \prod_{i=0}^{s-1} \left(z^{q^i} - y\right)\left(z^{q^i} - y'\right) = \left(\prod_{j=1}^{d} (z_j - y)(z_j - y')\right)^{s/d} = (P(y)P(y'))^{s/d}.\end{aligned}$$

Ainsi, comme χ et μ_q sont multiplicatifs, par définition de λ, on a

$$\begin{aligned}\lambda(P)^{s/d} &= \chi\left((-1)^d c_0\right)^{s/d} \cdot \mu_q\left(P(y)P(y')\right)^{s/d} = \chi\left((-1)^s c_0^{s/d}\right)\cdot \mu_q\left((P(y)P(y'))^{s/d}\right)\\ &= \chi\circ\mathbf{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(z)\cdot\mu_q\circ\mathbf{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(Q_b(z)) = \chi^{(s)}(z)\cdot\mu_{q^s}(Q_b(z)).\end{aligned}$$

On peut alors sommer cette identité sur les d racines $z_i \in \overline{\mathbb{F}_q}$ de P (qui sont toutes conjuguées, donc de même norme) et l'on obtient

$$\sum_{\substack{z\in\overline{\mathbb{F}_q}\\ P(z)=0}} \chi^{(s)}(z)\cdot\mu_{q^s}(Q_b(z)) = \deg P\cdot\lambda(P)^{s/d}.$$

Finalement, par (2.8), on a

$$\begin{aligned}-S(\lambda, s) &= \sum_{P\in\mathbb{P}_s} \deg P\cdot\lambda(P)^{s/\deg P} = \sum_{P\in\mathbb{P}_s}\sum_{\substack{z\in\overline{\mathbb{F}_q}\\ P(z)=0}} \chi^{(s)}(z)\cdot\mu_{q^s}(Q_b(z))\\ &= \sum_{\substack{z\in\overline{\mathbb{F}_q}\\ z^{q^s}-z=0}} \chi^{(s)}(z)\cdot\mu_{q^s}(Q_b(z)) = \sum_{z\in\mathbb{F}_{q^s}} \chi^{(s)}(z)\cdot\mu_{q^s}(Q_b(z)) = -\boldsymbol{S}_{q^s}(\chi^{(s)}).\end{aligned}$$

Nous avons donc démontré que, pour tout $s \geqslant 1$,

$$S(\lambda, s) = \boldsymbol{S}_{q^s}(\chi^{(s)}; b) = \alpha_b(\chi)^s + \beta_b(\chi)^s \quad \text{avec} \quad \alpha_b(\chi)\cdot\beta_b(\chi) = q.$$

La dernière assertion suit de la Proposition 2.2.12, où l'on a vu que $\boldsymbol{S}_q(\overline{\chi}; b) = \boldsymbol{S}_q(\chi; b)$. □

2.3 Hypothèse de Riemann pour les sommes de Legendre

À la section précédente (Théorème 2.2.21), nous avons vu que, pour tout caractère non trivial $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ et tout $b \in \mathbb{F}_q \smallsetminus \{1, -1\}$, il existe deux nombres complexes $\alpha_b(\chi)$, $\beta_b(\chi)$ tels que la somme de Legendre $\boldsymbol{S}_q(\chi; b)$ se décompose sous la forme :

$$\boldsymbol{S}_q(\chi; b) = \alpha_b(\chi) + \beta_b(\chi) \quad \text{avec} \quad \alpha_b(\chi) \cdot \beta_b(\chi) = q.$$

De plus, comme $\boldsymbol{S}_q(\chi; b)$ est réelle (dans tout plongement de $\mathbb{Q}(\zeta_{q-1})$ dans $\mathbb{C}$), les nombres $\alpha_b(\chi)$ et $\beta_b(\chi)$ sont conjugués. Dans cette section, nous démontrons en outre que $|\alpha_b(\chi)| = |\beta_b(\chi)| = \sqrt{q}$ (dans tout plongement complexe de $\overline{\mathbb{Q}}$) : c'est le Corollaire 2.3.5. Pour ce faire, nous prouvons que $\alpha_b(\chi)$ et $\beta_b(\chi)$ apparaissent naturellement comme racines (inverses) de la fonction zeta $Z(D_d/\mathbb{F}_q, T)$ d'une certaine courbe hyperelliptique D_d définie sur $\mathbb{F}_q$ (Théorème 2.3.4).

2.3.1 Fonction zeta des courbes $y^2 = ax^d + b$

Citons tout d'abord un théorème de A. Weil (voir [Wei49]) avec nos notations. Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $d \geqslant 2$ un entier premier à q. On fixe $a, b \in \mathbb{F}_q^\times$ et on considère la courbe hyperelliptique $C_d \subset \mathbb{P}^2$ définie sur $\mathbb{F}_q$ dont un ouvert affine a pour équation

$$C_d : \qquad Y^2 = aX^d + b.$$

Les conditions imposées à a, b et d assurent la lissité de C_d. Le genre de cette courbe est $g(C_d) = \left\lfloor \frac{d-1}{2} \right\rfloor$ (*cf.* [Mum84, Chapter 2]). Notons que, lorsque $d > 3$, la clotûre de Zariski (dans $\mathbb{P}^2$) de la courbe affine ci-dessus n'est pas lisse : la courbe C_d est plutôt obtenue par recollement comme suit. On écrit $d = 2g + 1 + \delta$ avec $\delta \in \{0, 1\}$ (suivant que d est impair ou pair). Soit alors $C_1 \subset \mathbb{A}^2$ la courbe affine d'équation $Y^2 = aX^d + b$ et $C_2 \subset \mathbb{A}^2$ la courbe d'équation $V^2 = aU^{1-\delta} + bU^{2g+2}$, on recolle ces deux courbes affines par $(U, V) = (X^{-1}, YX^{-g-1})$. Ce recollement donne une courbe projective dont on peut vérifier la lissité. Lorsque d est impair, C_d possède un unique point à l'infini, qui est $\mathbb{F}_q$-rationnel. Lorsque d est pair, C_d possède ou bien deux points à l'infini $\mathbb{F}_q$-rationnels (si a est un carré dans $\mathbb{F}_q$), ou bien aucun point à l'infini $\mathbb{F}_q$-rationnel (si a n'est pas un carré de $\mathbb{F}_q$).

Rappelons également les notations introduites à la Section 2.1.3 : on fixe un idéal premier $\overline{\mathfrak{P}}$ de $\overline{\mathbb{Z}}$ pour disposer du caractère de Teichmüller $\mathbf{t} : \overline{\mathbb{F}_q}^\times \to \overline{\mathbb{Q}}^\times$. Pour la donnée de $d \geqslant 2$ premier à p, nous avons construit $d-1$ caractères non triviaux $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ définis sur diverses extensions $\mathbb{F}_{q^{u(m)}}\mathbb{F}_q$ et dont l'ordre divise d (m parcourant $\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$). Le théorème de A. Weil peut alors s'écrire :

Théorème 2.3.1 (Weil). *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $a, b \in \mathbb{F}_q^\times$. Pour tout entier $d \geqslant 2$ premier à q, on considère la courbe hyperelliptique définie sur $\mathbb{F}_q$ et dont un ouvert affine a pour équation $C_d : y^2 = ax^d + b$. La fonction zeta de $C_d/\mathbb{F}_q$, notée $Z(C_d/\mathbb{F}_q, T)$, est donnée par :*

$$Z\big(C_d/\mathbb{F}_q, T\big) = \frac{1}{(1-T)(1-qT)} \cdot \prod_{m \in \mathcal{O}_q^{(2)}(d)} \Big(1 - \boldsymbol{\beta}(m) \cdot T^{u(m)}\Big),$$

où le produit porte sur l'ensemble d'orbites $\mathcal{O}_q^{(2)}(d)$:

$$\mathcal{O}_q^{(2)}(d) = \begin{cases} \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/2\}\big)/\langle q \bmod d\rangle & \text{si } d \text{ est pair,} \\ \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\big)/\langle q \bmod d\rangle & \text{si } d \text{ est impair,} \end{cases}$$

et où $\boldsymbol{\beta}(m)$ est, à multiplication par une racine de l'unité près, une somme de Jacobi :

$$\boldsymbol{\beta}(m) = \mathbf{t}_a(-4a/b)\mu_q(b)^{u(m)} \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_a, \mathbf{t}_a),$$

pour un choix quelconque de représentant $a \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ de l'orbite m.

Nous ne rappelons pas la démonstration de ce théorème car nous allons effectuer un calcul assez similaire ci-dessous. Le lecteur peut consulter le limpide [Wei49].

Remarque 2.3.2. Désignons par $L_d(T)$ le numérateur de la fonction zeta $Z(C_d/\mathbb{F}_q, T)$. Le Théorème 2.3.1 montre que le polynôme $L_d(T)$ s'annule en $t \in \mathbb{C}$ si et seulement si

$$\exists m \in \mathcal{O}_q^{(2)}(d), \quad \boldsymbol{\beta}(m) = t^{-u(m)}.$$

L'« hypothèse de Riemann » pour $Z(C_d/\mathbb{F}_q, T)$ (*cf.* Théorème 1.3.2) implique alors que, pour un tel zéro $t \in \mathbb{C}$, on a $|t| = q^{-1/2}$. Ce qui redémontre que $|\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)| = q^{u(m)/2}$ dans tout plongement complexe de $\mathbb{Q}(\zeta_d)$ (voir Proposition 2.2.7).

Exemple 2.3.3. Si $a=-1$ et $b=1/4$, on obtient que, pour tout $d\geqslant 2$ premier à q, la fonction zeta de $C_d/\mathbb{F}_q$ s'écrit

$$Z\big(C_d/\mathbb{F}_q,T\big)=\frac{\prod_{m\in\mathcal{O}_q^{(2)}(d)}\big(1-\mathbf{J}(m)\cdot T^{u(m)}\big)}{(1-T)(1-qT)},$$

où

$$\mathbf{J}(m)=\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m)=-\sum_{x\in\mathbb{F}_{q^{u(m)}}}\mathbf{t}_m(x)\mathbf{t}_m(1-x).$$

2.3.2 Fonction zeta des courbes $y^2=ax^{2d}+2bx^d+a$

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p\geqslant 3$, on fixe $a,b\in\mathbb{F}_q$ et $d\geqslant 2$ un entier premier à q. On considère dans cette section la courbe hyperelliptique $D_d\subset\mathbb{P}^2$ définie sur $\mathbb{F}_q$ et dont un ouvert affine a pour équation

$$D_d:\qquad y^2=ax^{2d}+2bx^d+a.$$

On suppose en outre que $a\neq 0$ et que $b^2-a^2\neq 0$: ces hypothèses assurent que la courbe $D_d/\mathbb{F}_q$ est lisse et irréductible. Rajoutons l'hypothèse que $b\neq 0$ (si b était égal à 0, la courbe D_d serait isomorphe à C_{2d} de la section précédente). Le genre de la courbe D_d est $g(D_d)=d-1$. En outre, comme le degré du polynôme $aX^{2d}+2bX^d+a$ est pair, la courbe D_d possède 2 ou 0 points à l'infini $\mathbb{F}_q$-rationnels suivant, respectivement, que a est un carré de $\mathbb{F}_q^\times$ ou non.

Avec les notations de la Section 2.1.3 (que nous avons rappelées à la section précédente), nous démontrons le théorème suivant.

Théorème 2.3.4. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p\geqslant 3$ et $a,b\in\mathbb{F}_q^\times$ tels que $a^2-b^2\neq 0$. Pour tout entier $d\geqslant 2$ premier à q, on considère la courbe hyperelliptique D_d définie sur $\mathbb{F}_q$ dont un ouvert affine a pour équation*

$$D_d:\qquad y^2=ax^{2d}+2bx^d+a.$$

La fonction zeta de $D_d/\mathbb{F}_q$, notée $Z\big(D_d/\mathbb{F}_q,T\big)$, est donnée par :

$$Z\big(D_d/\mathbb{F}_q,T\big)=\frac{1}{(1-T)(1-qT)}\cdot\prod_{m\in\mathcal{O}'_q(d)}\Big(1-\boldsymbol{\gamma}(m)\cdot T^{u(m)}+q^{u(m)}T^{2u(m)}\Big),$$

où le produit porte sur l'ensemble d'orbites $\mathcal{O}'_q(d)=\big(\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}\big)\big/\langle q \bmod d\rangle$ et $\boldsymbol{\gamma}(m)$ est, à multiplication par ±1 près, une somme de Legendre :

$$\boldsymbol{\gamma}(m)=\mu_{q^{u(m)}}(a)\cdot\boldsymbol{S}_{q^{u(m)}}\left(\mathbf{t}_q;\tfrac{b}{a}\right)=-\mu_{q^{u(m)}}(a)\cdot\sum_{x\in\mathbb{F}_{q^{u(m)}}}\mathbf{t}_q(x)\cdot\mu\left(x^2+\tfrac{2b}{a}x+1\right),$$

pour un choix quelconque de représentant $a\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ de l'orbite m.

Démonstration. Nous séparons la preuve de ce théorème en deux parties. Dans la première, nous « comptons » les points $\mathbb{F}_{q^n}$-rationnels sur D_d pour toute extension finie $\mathbb{F}_{q^n}/\mathbb{F}_q$. Dans la seconde, nous utilisons ce décompte de points pour exprimer les coefficients de la série génératrice définissant $Z(D_d/\mathbb{F}_q,T)$ et conclure.

Comptage de solutions. Dans cette première partie de la preuve, nous démontrons la relation suivante : pour toute extension finie $\mathbb{F}_{q^n}/\mathbb{F}_q$, le nombre de points $\mathbb{F}_{q^n}$-rationnels de D_d est donné par

$$\#D_d(\mathbb{F}_{q^n})=q^n+1-\sum_{\chi\in X(d,q^n)}\mu(a)\cdot\boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right),\tag{2.9}$$

où $X(d,q^n)$ désigne l'ensemble des caractères non triviaux de $\mathbb{F}_{q^n}^\times$ dont la puissance d-ième est triviale.

Preuve de (2.9). Si $\mathbb{F}_{q^n}/\mathbb{F}_q$ est une extension finie, on notera $N_\infty(q^n)$ le nombre de points à l'infini $\mathbb{F}_{q^n}$-rationnels de D_d. D'après la discussion ci-dessus, on a

$$N_\infty(q^n)=\begin{cases}0 & \text{si } a \text{ n'est pas un carré de } \mathbb{F}_{q^n}^\times,\\ 2 & \text{si } a \text{ est un carré de } \mathbb{F}_{q^n}^\times.\end{cases}$$

Autrement dit, on a $N_\infty(q^n)=1+\mu_{q^n}(a)$. Nos hypothèses sur a,b (qui assurent entre autres la lissité de D_d) se réécrivent sous la forme : $a\neq 0, b\neq 0$ et $b^2\neq a^2 \iff a\neq 0$ et $\frac{b}{a}\neq 0,1,-1$. Après

avoir pris en compte les $N_\infty(q^n)$ points $\mathbb{F}_{q^n}$-rationnels à l'infini, il ne reste qu'à dénombrer les points affines de D_d. On utilise pour cela le Lemme 2.2.1 (qui permet de « compter » les solutions d'équations quadratiques) :

$$\begin{aligned}
\#D_d(\mathbb{F}_{q^n}) &= N_\infty(q^n) + \#\left\{(x,y)\in\mathbb{F}_{q^n}^2 \;\middle|\; y^2 = ax^{2d}+2bx^d+a\right\}\\
&= N_\infty(q^n) + \sum_{x\in\mathbb{F}_{q^n}} \#\left\{y\in\mathbb{F}_{q^n} \;\middle|\; y^2 = ax^{2d}+2bx^d+a\right\}\\
&= N_\infty(q^n) + \sum_{x\in\mathbb{F}_{q^n}} 1+\mu\left(ax^{2d}+2bx^d+a\right)\\
&= q^n + N_\infty(q^n) + \sum_{x\in\mathbb{F}_{q^n}} \mu\left(ax^{2d}+2bx^d+a\right)\\
&= q^n + N_\infty(q^n) + \mu_{q^n}(a)\cdot\sum_{x\in\mathbb{F}_{q^n}} \mu\left(x^{2d}+\tfrac{2b}{a}x^d+1\right).
\end{aligned}$$

On « réindexe » alors la somme en posant « $z=x^d$ » à l'aide du Lemme 2.2.2, on obtient

$$\begin{aligned}
\sum_{x\in\mathbb{F}_{q^n}} \mu\left(x^{2d}+\tfrac{2b}{a}x^d+1\right) &= \sum_{z\in\mathbb{F}_{q^n}} \mu\left(z^2+\tfrac{2b}{a}z+1\right)\cdot\#\left\{x\in\mathbb{F}_{q^n} \;\middle|\; z=x^d\right\}\\
&= \sum_{z\in\mathbb{F}_{q^n}} \left(\sum_{\chi^d=\mathbf{1}}\chi(z)\right)\mu\left(z^2+\tfrac{2b}{a}z+1\right)\\
&= \sum_{\chi^d=\mathbf{1}}\left(\sum_{z\in\mathbb{F}_{q^n}}\chi(z)\mu\left(z^2+2\tfrac{b}{a}z+1\right)\right)\\
&= \sum_{\chi^d=\mathbf{1}} -\boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right) = -\sum_{\chi^d=\mathbf{1}}\boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right).
\end{aligned}$$

Les sommes écrites ci-dessus portent sur l'ensemble des caractères $\chi:\mathbb{F}_{q^n}^\times\to\overline{\mathbb{Q}}^\times$ dont la puissance d-ième est triviale. Parmi ces caractères figure le caractère trivial $\mathbf{1}$ dont la contribution à la somme est $\boldsymbol{S}_{q^n}\left(\mathbf{1};\frac{b}{a}\right)=1$ (*cf.* Proposition 2.2.12, nous sommes dans le cas où $b/a\in\mathbb{F}_q\smallsetminus\{0,1,-1\}$). En isolant ce terme et en utilisant l'expression obtenue plus haut pour $N_\infty(q^n)$, on obtient finalement

$$\begin{aligned}
\#D_d(\mathbb{F}_{q^n}) &= q^n + N_\infty(q^n) + \mu_{q^n}(a)\cdot\sum_{x\in\mathbb{F}_{q^n}}\mu\left(x^{2d}+\tfrac{2b}{a}x^d+1\right)\\
&= q^n + N_\infty(q^n) - \mu_{q^n}(a)\cdot\sum_{\chi^d=\mathbf{1}}\boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right)\\
&= q^n + N_\infty(q^n) - \mu_{q^n}(a)\cdot 1 - \mu_{q^n}(a)\cdot\sum_{\substack{\chi^d=\mathbf{1}\\ \chi\neq\mathbf{1}}}\boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right)\\
&= q^n + (1+\mu_{q^n}(a)) - \mu_{q^n}(a)\cdot 1 - \mu_{q^n}(a)\cdot\sum_{\substack{\chi^d=\mathbf{1}\\ \chi\neq\mathbf{1}}}\boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right)\\
&= q^n + 1 - \sum_{\chi\in X(q,q^n)}\mu_{q^n}(a)\cdot\boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right).
\end{aligned}$$

C'est la relation (2.9) qu'il fallait démontrer. □

Réindexation des caractères et fonction zeta Par définition de la fonction zeta de $D_d/\mathbb{F}_q$ (*cf.* Section 1.3.2), on a

$$\log Z\big(D_d/\mathbb{F}_q,T\big) = \sum_{n=1}^{\infty}\frac{\#D_d(\mathbb{F}_{q^n})}{n}T^n.$$

Mais, pour toute extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, nous avons prouvé au paragraphe précédent que :

$$\#D_d(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{\chi\in X(d,q^n)}\mu_{q^n}(a)\cdot\boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right).$$

En remplaçant $\#D_d(\mathbb{F}_{q^n})$ par son expression dans la série formelle $\log Z\big(D_d/\mathbb{F}_q, T\big)$, il suit que

$$\begin{aligned}\log Z\big(D_d/\mathbb{F}_q, T\big) &= \sum_{n=1}^{\infty}\left(q^n+1-\sum_{\chi\in X(d,q^n)}\mu_{q^n}(a)\cdot \boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right)\right)\frac{T^n}{n}\\ &= \sum_{n=1}^{\infty}\frac{(qT)^n}{n}+\sum_{n=1}^{\infty}\frac{T^n}{n}-\sum_{n=1}^{\infty}\left(\sum_{\chi\in X(d,q^n)}\mu_{q^n}(a)\cdot \boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right)\right)\frac{T^n}{n}\\ &= -\log(1-qT)-\log(1-T)-\sum_{n=1}^{\infty}\left(\sum_{\chi\in X(d,q^n)}\mu_{q^n}(a)\cdot \boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right)\right)\frac{T^n}{n}.\end{aligned}$$

La somme à droite est de la forme

$$\sum_{n=1}^{\infty}\left(\sum_{\chi\in X(d,q^n)}\sigma(q^n,\chi)\right)\frac{T^n}{n},$$

avec $\sigma(q^n,\chi)=\mu_{q^n}(a)\cdot \boldsymbol{S}_{q^n}\left(\chi;\frac{b}{a}\right)$. Prouvons à présent que les $\sigma(q^n,\chi)$ vérifient les hypothèses de la Proposition 2.1.14. Déjà, nous constatons que $\sigma(q^n,\chi)=\sigma(q^n,\chi^q)$ car $x\mapsto x^q$ est une bijection de $\mathbb{F}_{q^n}$. Soit maintenant $\mathbb{F}_Q/\mathbb{F}_q$ une extension quelconque et $\chi\in X(d,Q)$, soit de plus $\mathbb{F}_{Q^s}/\mathbb{F}_Q$ une extension de degré $s\in\mathbb{N}^*$. D'après le Théorème 2.2.21, il existe deux nombres complexes $\alpha_{b/a}(\chi)$ et $\beta_{b/a}(\chi)$ tels que

$$\boldsymbol{S}_{Q^s}\left(\chi^{(s)};\tfrac{b}{a}\right)=\big(\alpha_{b/a}(\chi)\big)^s+\big(\beta_{b/a}(\chi)\big)^s.$$

Par suite, comme $a\in\mathbb{F}_q\subset\mathbb{F}_Q$, on a

$$\sigma(Q^s,\chi^{(s)})=\mu_{Q^s}(a)\cdot \boldsymbol{S}_{Q^s}\left(\chi^{(s)};\tfrac{b}{a}\right)=\big(\mu_Q(a)\cdot\alpha_{b/a}(\chi)\big)^s+\big(\mu_Q(a)\cdot\beta_{b/a}(\chi)\big)^s.$$

Cette dernière identité est bien une relation de Hasse-Davenport à l'ordre $K=2$, avec

$$\alpha_1(\chi):=\mu_Q(a)\cdot\alpha_{b/a}(\chi)\quad\text{ et }\quad\alpha_2(\chi):=\mu_Q(a)\cdot\beta_{b/a}(\chi).$$

Nous sommes donc en mesure d'appliquer la Proposition 2.1.14 :

$$\sum_{n=1}^{\infty}\left(\sum_{\chi\in X(d,q^n)}\mu_{q^n}(a)\cdot \boldsymbol{S}_{q^n}\left(\chi;\tfrac{b}{a}\right)\right)\frac{T^n}{n}=-\sum_{m\in\mathcal{O}'_q(d)}\log\Big(\Big(1-\alpha_1(\mathbf{t}_m)T^{u(m)}\Big)\Big(1-\alpha_2(\mathbf{t}_m)T^{u(m)}\Big)\Big).$$

Ainsi,

$$\log Z\big(D_d/\mathbb{F}_q,T\big)=\log\left(\frac{\prod_{m\in\mathcal{O}'_q(d)}\big(1-\alpha_1(\mathbf{t}_m)T^{u(m)}\big)\big(1-\alpha_2(\mathbf{t}_m)T^{u(m)}\big)}{(1-T)(1-qT)}\right).$$

Il reste à expliciter un peu les facteurs dans le produit : pour toute orbite $m\in\mathcal{O}'_q(d)$, on a $\alpha_1(\mathbf{t}_m)+\alpha_2(\mathbf{t}_m)=\boldsymbol{\gamma}(m)$ et $\alpha_1(\mathbf{t}_m)\cdot\alpha_2(\mathbf{t}_m)=q^{u(m)}$ (*cf.* Théorème 2.2.21). Par conséquent,

$$\begin{aligned}\Big(1-\alpha_1(\mathbf{t}_m)T^{u(m)}\Big)\Big(1-\alpha_2(\mathbf{t}_m)T^{u(m)}\Big)&=1-\big(\alpha_1(\mathbf{t}_m)+\alpha_2(\mathbf{t}_m)\big)T^{u(m)}+\alpha_1(\mathbf{t}_m)\alpha_2(\mathbf{t}_m)\cdot T^{2u(m)}\\&=1-\boldsymbol{\gamma}(m)T^{u(m)}+q^{u(m)}\cdot T^{2u(m)}.\end{aligned}$$

Ce qui donne bien le résultat annoncé.

□

2.3.3 Conséquence

Soit $b\in\mathbb{F}_q\smallsetminus\{0,1,-1\}$ et $\chi:\mathbb{F}_q^\times\to\overline{\mathbb{Q}}^\times$ un caractère non trivial. Par définition, on a

$$|\boldsymbol{S}_q(\chi;b)|=\left|\sum_{x\in\mathbb{F}_q}\chi(x)\mu(x^2+2bx+1)\right|\leqslant q.$$

On peut en fait démontrer une majoration bien plus forte :

Corollaire 2.3.5. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $b \in \mathbb{F}_q \smallsetminus \{0, 1, -1\}$. Pour tout caractère non trivial $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$, les nombres complexes $\alpha_b(\chi)$ et $\beta_b(\chi)$ associés à $\boldsymbol{S}_q(\chi; b)$ par le Théorème 2.2.21 vérifient*

$$|\alpha_b(\chi)| = |\beta_b(\chi)| = \sqrt{q}.$$

En particulier, on a donc $|\boldsymbol{S}_q(\chi; b)| \leqslant 2\sqrt{q}$.

Démonstration. Soit b et χ comme dans l'énoncé du Corollaire. Nous reprenons les notations des Sections 2.1.2 et 2.1.3. Soit d l'ordre de χ, c'est un diviseur de $\#\mathbb{F}_q^\times = q-1$. Par conséquent, l'ensemble des orbites $\mathcal{O}'_q(d)$ de $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ modulo l'action de q par multiplication est en bijection avec $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ lui-même. Ceci implique que $u(m) = 1$ pour tout $m \in \mathcal{O}'_q(d)$. De plus, comme $\mathbf{t}_1 = \mathbf{t}^{(q-1)/d} : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ engendre le groupe des caractères d'ordre d de $\mathbb{F}_q^\times$, il existe $z_\chi \in (\mathbb{Z}/d\mathbb{Z})^\times$ tel que $\chi = (\mathbf{t}_1)^{z_\chi} = \mathbf{t}_{z_\chi}$. Soit maintenant $D/\mathbb{F}_q$ la courbe hyperelliptique d'équation affine

$$D : \quad y^2 = x^{2d} + 2bx^d + 1.$$

Le Théorème 2.3.4 permet d'écrire la fonction zeta de D sous la forme d'un produit :

$$Z\big(D/\mathbb{F}_q, T\big) = \frac{1}{(1-T)(1-qT)} \cdot \prod_{m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}} (1 - \alpha_b(\mathbf{t}_m)T)\,(1 - \beta_b(\mathbf{t}_m)T)\,.$$

L'hypothèse de Riemann pour les courbes projectives lisses sur les corps finis (*cf.* Théorème 1.3.2) affirme que les zéros $t \in \mathbb{C}$ de la fraction rationnelle $t \mapsto Z\big(D/\mathbb{F}_q, t\big)$ sont de la forme $t = q^{-1/2} \cdot \mathrm{e}^{i\theta}$ (avec $\theta \in [0, 2\pi[$). Ici, il est clair que, pour $t \in \mathbb{C}$,

$$\prod_{m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}} (1 - \alpha_b(\mathbf{t}_m)t)\,(1 - \beta_b(\mathbf{t}_m)t) = 0 \iff \exists m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\} \text{ tel que } t = \alpha_b(\mathbf{t}_m)^{-1} \text{ ou } \beta_b(\mathbf{t}_m)^{-1}.$$

De là, il suit que $|\alpha_b(\mathbf{t}_m)| = |\beta_b(\mathbf{t}_m)| = \sqrt{q}$ pour tout $m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$. En particulier, pour $m = z_\chi \in (\mathbb{Z}/d\mathbb{Z})^\times$, on a bien

$$|\alpha_b(\chi)| = |\alpha_b(\mathbf{t}_{z_\chi})| = \sqrt{q} = |\beta_b(\mathbf{t}_{z_\chi})| = |\beta_b(\chi)|.$$

La borne sur $|\boldsymbol{S}_q(\chi; b)|$ en découle directement car $\boldsymbol{S}_q(\chi; b) = \alpha_b(\chi) + \beta_b(\chi)$. □

Proposition 2.3.6. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $b \in \mathbb{F}_q \smallsetminus \{0, 1, -1\}$. Pour tout caractère non trivial $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$, les nombres complexes $\alpha_b(\chi)$ et $\beta_b(\chi)$ associés à $\boldsymbol{S}_q(\chi; b)$ par le Théorème 2.2.21 sont des entiers algébriques.*

Démonstration. Notons d l'ordre de χ : comme $\chi \neq \mathbf{1}$, on a $d \geqslant 2$. Soit également $f(T) := qT^2 - \boldsymbol{S}_q(\chi; b)T + 1$ et $g(T) := T^2 f(1/T)$. Par construction de $\alpha_b(\chi)$ et $\beta_b(\chi)$, on a

$$f(T) = (1 - \alpha_b(\chi)T)(1 - \beta_b(\chi)T),$$

de sorte que $g(T) = (T - \alpha_b(\chi))(T - \beta_b(\chi)) = T^2 - \boldsymbol{S}_q(\chi; b)T + q$. Or, la somme $\boldsymbol{S}_q(\chi; b)$ est un entier algébrique : mieux, d'après sa définition (Définition 2.2.10), $\boldsymbol{S}_q(\chi; b)$ est un entier de $\mathbb{Q}(\zeta_d)$. Soit $K = \mathbb{Q}(\zeta_d)$ et $\mathcal{O}_K$ son anneau des entiers ($\mathcal{O}_K = \mathbb{Z}[\zeta_d]$). Alors le polynôme g est à coefficients dans $\mathcal{O}_K$ et est unitaire. De plus, clairement, g admet $\alpha_b(\chi)$ et $\beta_b(\chi)$ comme racines. Ainsi, $\alpha_b(\chi)$ et $\beta_b(\chi)$ sont entiers sur $\mathcal{O}_K$, donc sur $\mathbb{Z}$. □

Remarque 2.3.7. Si $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ n'est pas le caractère trivial, on a

$$|\boldsymbol{S}_q(\chi; b)| = 2\sqrt{q} \text{ si et seulement si } \alpha_b(\chi) = \beta_b(\chi) = \pm\sqrt{q}.$$

Autrement dit, la somme $\boldsymbol{S}_q(\chi; b)$ est maximale (resp. minimale) si et seulement si $\alpha_b(\chi)$ et $\beta_b(\chi)$ sont réels et positifs (resp. négatifs). On note par ailleurs que, $\zeta := \boldsymbol{S}_q(\chi; b)/2\sqrt{q}$ est une racine de l'unité (dans $\overline{\mathbb{Q}}$) si et seulement si $\boldsymbol{S}_q(\chi; b) = \pm 2\sqrt{q}$. Autrement dit, si $\zeta = \boldsymbol{S}_q(\chi; b)/2\sqrt{q}$, ou bien $\zeta = \pm 1$ ou bien ζ n'est pas une racine de l'unité. De même, la somme $\boldsymbol{S}_q(\chi; b)$ est nulle si et seulement si $\alpha_b(\chi)$ et $\beta_b(\chi)$ sont imaginaires purs. Ils sont nécessairement conjugués car $\boldsymbol{S}_q(\chi; b)$ est toujours réelle (Proposition 2.2.12).

Remarquons enfin que la majoration obtenue $|\boldsymbol{S}_q(\chi; b)| \leqslant 2\sqrt{q}$ est « optimale en exposant », aux sens des deux lemmes suivants :

Lemme 2.3.8. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. On suppose que $q \geqslant 5$. Il existe une constante $c_q > 0$ (ne dépendant que de q) telle que, pour tout $b \in \mathbb{F}_q \smallsetminus \{1, -1\}$, il existe un caractère non trivial $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ avec $|\boldsymbol{S}_q(\chi; b)| \geqslant c_q\sqrt{q}$. De plus, on peut prendre $c_q = 2/\sqrt{5} \simeq 0,89....$*

Démonstration. Commençons par remarquer que, pour $b \in \mathbb{F}_q \smallsetminus \{1,-1\}$ fixé, on a

$$0 \leqslant \sum_{\chi \neq \mathbf{1}} \boldsymbol{S}_q(\chi;b)^2 \leqslant (q-2)\cdot \max_{\chi\neq\mathbf{1}} \boldsymbol{S}_q(\chi;b)^2.$$

Posons $Q_b := X^2+2bX+1 \in \mathbb{F}_q[X]$. Notons δ le discriminant de cette forme quadratique : $\delta = 4(b^2-1) \neq 0$. Alors Q_b admet $1+\mu(\delta)$ zéros dans $\mathbb{F}_q$ (*cf.* Lemme 2.2.1). Pour tout caractère non trivial χ, on a $\boldsymbol{S}_q(\chi;b) = \boldsymbol{S}_q(\overline{\chi};b)$ et, par orthogonalité des caractères, on trouve :

$$\begin{aligned}\sum_{\chi\neq\mathbf{1}} \boldsymbol{S}_q(\chi;b)^2 &= \sum_{\chi\neq\mathbf{1}}\sum_{x,y\neq 0} \chi(x)\overline{\chi}(y)\mu(Q_b(x)Q_b(y)) = \sum_{x,y\neq 0}\left(\sum_{\chi\neq\mathbf{1}}\chi(x)\overline{\chi}(y)\right)\mu(Q_b(x)Q_b(y))\\ &= \sum_{x,y\neq 0}\left(\sum_{\chi}\chi(x)\overline{\chi}(y) - \mathbf{1}(xy)\right)\mu(Q_b(x)Q_b(y))\\ &= (q-1)\sum_{x\neq 0}\mu(Q_b(x)^2) - \left(\sum_{x\neq 0}\mu(Q_b(x))\right)^2.\end{aligned}$$

D'où, avec le Lemme 2.2.3,

$$\begin{aligned}\sum_{\chi\neq\mathbf{1}} \boldsymbol{S}_q(\chi;b)^2 &= (q-1)\left(\sum_{x\in\mathbb{F}_q}\mu(Q_b(x)^2) - \mu(Q_b(0))\right) - \left(\sum_{x\in\mathbb{F}_q}\mu(Q_b(x)) - \mu(Q_b(0))\right)^2\\ &= (q-1)\left(q-(1+\mu(\delta))-1\right) - (-1-1)^2 = (q-1)\left(q-2-\mu(\delta)\right)-4.\end{aligned}$$

Pour $q \geqslant 5$, on en déduit par une rapide étude de fonctions, que

$$\begin{aligned}\max_{\chi\neq\mathbf{1}} \boldsymbol{S}_q(\chi;b)^2 &\geqslant \frac{1}{q-2}\sum_{\chi\neq\mathbf{1}} \boldsymbol{S}_q(\chi;b)^2 = \frac{(q-1)\left(q-2-\mu(\delta)\right)-4}{q-2} \geqslant \frac{(q-1)(q-3)-4}{(q-2)}\\ &\geqslant \frac{(q-2)^2-5}{q-2} = (q-2) \geqslant \frac{4}{5}\cdot q.\end{aligned}$$

Ainsi, il existe un caractère $\chi \neq \mathbf{1}$ tel que $|\boldsymbol{S}_q(\chi;b)| \geqslant \frac{2}{\sqrt{5}}\cdot\sqrt{q}$. Le cas où $q=3$ serait à traiter à part : le seul caractère non trivial de $\mathbb{F}_3^\times$ est le caractère μ d'ordre 2. De plus, le seul élément $b \in \mathbb{F}_3 \smallsetminus \{-1,1\}$ est $b=0$. Auquel cas, on a $\boldsymbol{S}_3(\mu;0)=0$ car $\mu(-1) = (-1)^{(3-1)/2} = -1$. □

Et la même remarque vaut dans le sens « orthogonal » :

Lemme 2.3.9. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. On suppose que $q \geqslant 5$. Il existe une constante $c'_q > 0$ (ne dépendant que de q) telle que, pour un caractère non trivial fixé $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$, il existe un élément $b \in \mathbb{F}_q \smallsetminus \{1,-1\}$ avec $|\boldsymbol{S}_q(\chi;b)| \geqslant c'_q\sqrt{q}$. De plus, on peut prendre $c'_q = 1/2$.*

Démonstration. Un calcul assez similaire à celui effectué à la remarque précédente conduit en effet à

$$\sum_{\substack{b\in\mathbb{F}_q\\ b\neq\pm 1}} \boldsymbol{S}_q(\chi;b)^2 = \begin{cases} q^2-2q-3 & \text{si } \chi=\mu,\\ q^2-3q-2 & \text{si } \chi\neq\mu.\end{cases}$$

Voir également [LN97, Exercise 5.56, p. 262]. Dans les deux cas, on a $q^2-2q-3 \geqslant q^2-3q-2$ et après une rapide étude de fonctions, on trouve que, pour $q \geqslant 5$,

$$\max_{b\neq\pm1} \boldsymbol{S}_q(\chi;b)^2 \geqslant \frac{1}{q-2}\sum_{\substack{b\in\mathbb{F}_q\\ b\neq\pm1}} \boldsymbol{S}_q(\chi;b)^2 \geqslant \frac{q^2-3q-2}{q-2} = q\cdot\frac{q^2-3q-2}{q(q-2)} \geqslant \frac{1}{4}\cdot q.$$

Ainsi, il existe un élément $b \in \mathbb{F}_q \smallsetminus \{1,-1\}$ tel que $|\boldsymbol{S}_q(\chi;b)| \geqslant \frac{1}{2}\sqrt{q}$. Ici encore, le cas où $q=3$ serait à traiter à part car la somme $\sum_{b\neq\pm1}\boldsymbol{S}_3(\chi;b)^2$ ne porte que sur un seul terme $\boldsymbol{S}_3(\mu;0)^2$ et $\boldsymbol{S}_3(\mu;0)=0$. □

2.4 Sommes de Jacobi explicites

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$, les entiers $d \geqslant 2$ tels que d divise $q^n + 1$ pour un certain $n \in \mathbb{N}^*$ occupent une place particulière dans l'étude des courbes de Fermat sur $\mathbb{F}_q$ (voir par exemple [SK79], [Shi86], [TŠ67], ...). Nous donnons quelques résultats les concernant avant d'en donner des corollaires relatifs aux sommes de Jacobi.

2.4.1 Lemmes préliminaires

Lemme 2.4.1. *Soit $q \geqslant 3$ un entier impair et $d \geqslant 3$ premier à q. On suppose qu'il existe un entier $n \in \mathbb{N}^*$ tel que $d \mid q^n + 1$ et l'on note n_0 le plus petit tel entier. Alors l'ordre de q modulo d est pair et*

$$o_q(d) = \mathrm{ord}^\times(q \bmod d) = 2n_0.$$

Démonstration. Tout d'abord, on remarque que $q^{2n} \equiv 1 \bmod d$ donc que l'ordre de q modulo d divise $2n_0$. De plus,

$$1 \equiv (q^{o_d(d)})^{n_0} \equiv (q^{n_0})^{o_d(d)} \equiv (-1)^{o_q(d)} \bmod d,$$

ce qui force $o_q(d)$ à être pair (car d est > 2). On peut alors définir

$$e = \mathrm{pgcd}(n_0, o_q(d)/2).$$

Comme d divise à la fois $q^{2n_0} - 1$ et $q^{o_q(d)} - 1$, il divise aussi leur plus grand commun diviseur

$$\mathrm{pgcd}(q^{2n_0} - 1, q^{o_q(d)} - 1) = q^{\mathrm{pgcd}(2n_0, o_q(d))} - 1 = q^{2e} - 1,$$

et ceci implique que $2e$ est un multiple de $o_q(d)$. Par définition, $2e$ divise $o_q(d)$ et l'on a ainsi

$$o_q(d) = 2e = 2\,\mathrm{pgcd}(n_0, o_q(d)/2).$$

Il s'agit donc maintenant de voir que $e = n_0$. Posons donc $d_1 = \mathrm{pgcd}(d, q^e + 1)$ et écrivons $d = d_1 d_2$ et $q^e + 1 = d_1 Q$ avec d_2 et Q premiers entre eux. Notons que $(q^e - 1)(q^e + 1) = q^{2e} - 1 \equiv 0 \bmod d$ alors que $q^e - 1 \not\equiv 0 \bmod d$. Ainsi, d_1 ne peut pas être égal à 1 : nécessairement, $d_1 > 1$. D'autre part, $Q(q^e - 1) \equiv 0 \bmod d_2$ donc d_2 divise $q^e - 1$. Or, e divise n_0 et $-1 \equiv q^{n_0} \equiv (q^e)^{n_0/e} \equiv 1 \bmod d_2$. Donc d_2 vaut 1 ou 2. Ecrivons maintenant d sous la forme $d = 2^s d'$ avec $s \geqslant 0$ et d' impair et distinguons trois cas :

- Si $s = 0$, *i.e.* si d est impair, d_2 ne peut être autre que 1 et $q^e + 1 = d_1 Q = dQ \equiv 0 \bmod d$. Par minimalité de n_0, $n_0 \leqslant e$ mais, par définition, $e \leqslant n_0$. Ainsi on a $e = n_0$ et $o_q(d) = 2e = 2n_0$, ce qu'il fallait démontrer.
- Si maintenant $s = 1$, alors $d = 2d'$ divise $q^n \pm 1$ si et seulement si d' divise $q^n \pm 1$ pour tout n. Ce qui implique que l'ordre de q modulo $d = 2d'$ est égal à celui de q modulo d'. De plus, l'hypothèse du Lemme que d divise $q^n + 1$ pour un certain n est aussi valable avec d' (avec le même n_0) et l'on peut utiliser le résultat du cas précédent : en particulier, l'ordre de q modulo d' est pair et égal à $2n_0$.
- Supposons enfin $s \geqslant 2$. Commençons par remarquer que n_0 est impair. En effet, si n_0 était pair, comme $q^2 \equiv 1 \bmod 4$, on aurait $q^{n_0} \equiv 1 \bmod 4$ et donc $q^{n_0} + 1 \equiv 2 \bmod 4$, ce qui serait contraire à l'hypothèse que 4 divise $q^{n_0} + 1$ (car 4 divise $2^s d' = d$ dans ce cas). Ecrivons alors que

  $$q^{n_0} + 1 = q^{n_0} - (-1)^{n_0} = (q+1)(q^{n_0-1} - q^{n_0-2} + \cdots + q^2 - q + 1) \equiv 0 \bmod 2^s,$$

  où le second facteur est impair. Ainsi $q + 1 \equiv 0 \bmod 2^s$ et $q^2 \equiv 1 \bmod 2^s$, ce qui prouve que $o_q(2^s) = 2$.
  Si $d' = 1$, *i.e.* si $d = 2^s$, on a donc montré que $n_0 = 1$ et $o_q(d) = 2 = 2n_0$. Si $d' > 1$, on a $d' \geqslant 3$ et on peut appliquer les résultats précédemment démontrés : l'ordre $o_q(d')$ est pair et vaut $o_q(d') = 2n'_0$ où n'_0 est l'entier minimal tel que d' divise $q^{n'_0} + 1$. Comme d' divise $q^{n_0} + 1$ où n_0 est impair et que $n_0 \equiv n'_0 \bmod o_q(d')$ avec $o_q(d')$ pair, on en déduit que n'_0 est aussi impair. Auquel cas, on a $q^{n'_0} + 1 \equiv (-1)^{n'_0} + 1 \equiv 0 \bmod 2^s$, ce qui montre que d divise $q^{n'_0} + 1$ et donc que $n'_0 = n_0$. Finalement, on a $o_q(d) = o_q(d') = 2n'_0 = 2n_0$.

□

Une conséquence de ce Lemme apparaît dans [Ulm02, Lemma 8.2] :

Lemme 2.4.2. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. Pour tout entier $d \geqslant 3$, on note à nouveau $\mathcal{O}_q^{(2)}(d)$ l'ensemble d'orbites suivant :*

$$\mathcal{O}_q^{(2)}(d) := \begin{cases} \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/2\}\big)/\langle q \bmod d\rangle & \text{si } d \text{ est pair,} \\ \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\big)/\langle q \bmod d\rangle & \text{si } d \text{ est impair.} \end{cases}$$

Pour tout $m \in \mathcal{O}_q^{(2)}(d)$, on note $u(m)$ le cardinal de l'orbite m. On suppose à nouveau que d divise $q^n + 1$ pour un certain entier $n \in \mathbb{N}^*$. Alors, pour tout $m \in \mathcal{O}_q^{(2)}(d)$, $u(m)$ est pair et d divise $m(q^{u(m)/2} + 1)$.

Démonstration. Soit $a \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ (on suppose également que $a \neq d/2$ si d est pair). On pose $d_a = d/\operatorname{pgcd}(d, a)$ de sorte que, notant m l'orbite de a, $u(m) = o_q(d_a) = o_q(d_m)$. Comme d_a est un diviseur de d et que d divise $q^{n_0} + 1$, la première partie de la preuve qui précède (Lemme 2.4.1) montre que $u(m)$ est pair. En effet, on a bien $d_a > 2$ car $d_a = 1$ si et seulement si $a \equiv 0 \bmod d$; et $d_a = 2$ si et seulement si d est pair et $a \equiv d/2 \bmod d$. La première assertion est donc vraie. Démontrons la seconde. L'entier $d_a > 2$ est un diviseur de d qui divise $q^{n_0} + 1$. On peut donc appliquer le Lemme précédent avec $d' = d_a$: l'ordre $u(m)$ de q modulo d_a vaut $2n'_m$ où n'_m est l'entier minimal n' tel que d_a divise $q^{n'} + 1$. Ceci montre en particulier que d_a divise $q^{n'_m} + 1 = q^{u(m)/2} + 1$. Cette dernière relation de divisibilité implique facilement que d divise $m(q^{u(m)/2} + 1)$ car $d_a = d_m = d/\operatorname{pgcd}(d, a)$. □

2.4.2 Une version étendue du Lemme 2.4.1

Dans cette section, on note $\Phi_m(X) \in \mathbb{Z}[X]$ le m-ième polynôme cyclotomique (voir [Hin08, Chapitre II, §6]). Dans le cas où $m = \ell$ est un nombre premier impair, celui-ci admet une expression simple : $\Phi_\ell(X) = X^{\ell-1} + X^{\ell-2} + \cdots + X + 1 = (X^\ell - 1)/(X - 1)$. En particulier, $\Phi_\ell(1) = \ell$ et, pour tout entier $a \in \mathbb{Z}$,

$$\Phi_\ell(a) \equiv 0 \bmod \ell \iff a \equiv 1 \bmod \ell. \tag{2.10}$$

Nous avons trouvé une version plus générale du Lemme 2.4.1, sous la forme suivante :

Lemme 2.4.3. *Soit $q \geqslant 3$ un entier impair et $d \geqslant 3$ premier à q. On suppose qu'il existe un nombre premier impair ℓ tel que $d \neq \ell$ et que $d \mid \Phi_\ell(q^n)$ pour un certain entier $n \in \mathbb{N}$. On note n_0 le plus petit tel entier. Alors l'ordre de q modulo d est un multiple de ℓ et*

$$o_q(d) = \operatorname{ord}^\times(q \bmod d) = \ell \cdot n_0.$$

Le cas où $\ell = 2$ a déjà été traité au Lemme 2.4.1.

Démonstration. Remarquons tout d'abord que d divise $q^{\ell n_0} - 1 = (q^{n_0} - 1) \cdot \Phi_\ell(q^{n_0})$. Par suite, l'ordre $o_q(d)$ de q modulo d divise ℓn_0. Il s'agit donc de démontrer que, réciproquement, ℓn_0 divise $o_q(d)$. Si d divisait $q^{n_0} - 1$, on aurait

$$0 \equiv \Phi_\ell(q^{n_0}) \equiv \Phi_\ell(1) \equiv \ell \bmod d,$$

ce qui impliquerait que d divise ℓ, et ceci contredirait la primalité de ℓ. Ainsi, ℓ divise $o_q(d)$ et l'on peut définir

$$e := \operatorname{pgcd}(n_0, o_q(d)/\ell).$$

Pour conclure la preuve, il faut voir que $e = n_0$. Puisque d divise à la fois $q^{\ell n_0} - 1$ et $q^{o_q(d)} - 1$, il divise leur plus grand commun diviseur. Or,

$$\operatorname{pgcd}\left(q^{\ell n_0} - 1, q^{o_q(d)} - 1\right) = q^{\operatorname{pgcd}(\ell n_0, o_q(d))} - 1.$$

Donc d divise $q^{\operatorname{pgcd}(\ell n_0, o_q(d))} - 1$ et, par définition de l'ordre, $o_q(d)$ divise $\operatorname{pgcd}(\ell n_0, o_q(d)) = \ell \cdot e$. Mais, par construction, $\ell \cdot e$ divise $o_q(d)$. Donc on a $o_q(d) = \ell \cdot e$.

Par ailleurs, d divise le produit $\Phi_\ell(q^e)(q^e - 1)$, mais pas $q^e - 1$. On peut donc définir l'entier $d_1 := \operatorname{pgcd}(\Phi_\ell(q^e), d)$, qui vérifie $d_1 \geqslant 2$. Écrivons d sous la forme $d = d_1 d_2$ et $\Phi_\ell(q^e)$ sous la forme $\Phi_\ell(q^e) = d_1 \Psi$, avec $\operatorname{pgcd}(d_2, \Psi) = 1$. On a maintenant $\Psi \cdot (q^e - 1) \equiv 0 \bmod d_2$, donc d_2 divise $q^e - 1$. Or, par définition, e divise n_0. Donc

$$0 \equiv \Phi_\ell(q^{n_0}) \equiv \Phi_\ell(1) \equiv \ \ell \bmod d_2.$$

Ce qui impose $d_2 = 1$ ou $d_2 = \ell$. On distingue alors deux cas :

– Si d n'est pas divisible par ℓ, on a nécessairement $d_2 = 1$. Ainsi d divise $\Phi_\ell(q^e)$ et, comme n_0 est minimal parmi les entiers n tels que d divise $\Phi_\ell(q^n)$, on a $e \geqslant n_0$. Mais e divise n_0, on a donc $e = n_0$ et $o_q(d) = \ell \cdot e = \ell \cdot n_0$.
– Si maintenant $d = \ell^s d'$ avec $s \geqslant 1$ et d' premier à ℓ, on montre dans un premier temps que s vaut nécessairement 1. En effet, si pour un certain entier $a \in \mathbb{Z}$, ℓ^2 divisait $\Phi_\ell(a)$ alors on aurait $a \equiv 1 \bmod \ell$. On écrirait alors $a = 1 + \ell a'$ et on obtiendrait

$$0 \equiv \Phi_\ell(a) = \sum_{i=0}^{\ell-1}(1+\ell a')^i \equiv \sum_{i=0}^{\ell-1}(1+i\ell a') \equiv \ell + \ell a' \frac{\ell(\ell-1)}{2} \equiv \ell \bmod \ell^2.$$

Ce qui est absurde. En particulier, comme d divise $\Phi_\ell(q^{n_0})$, on a $d = \ell^1 \cdot d'$ avec d' premier à ℓ. Considérons à présent n' le plus petit entier n tel que d' divise $\Phi_\ell(q^n)$. D'après ce qui précède, l'ordre $o_q(d')$ de q modulo d' vaut $o_q(d') = \ell \cdot n'$. Par conséquent, comme ℓ ne divise pas $o_q(\ell)$, on a

$$o_q(d) = \mathrm{ppcm}(o_q(\ell), o_q(d')) = \mathrm{ppcm}(o_q(\ell), \ell \cdot n') = \ \ell \cdot \mathrm{ppcm}(o_q(\ell), n').$$

Soit $n \in \mathbb{N}^*$ tel que $o_q(\ell)$ divise n. Comme $\Phi_\ell(q^{o_q(\ell)})$ divise $\Phi_\ell(q^n)$, on a $\Phi_\ell(q^n) \equiv 0 \bmod \ell$. De même, si n' divise n, on a $\Phi_\ell(q^n) \equiv 0 \bmod d'$. Si on note $m := \mathrm{ppcm}(o_q(\ell), n')$, on a donc $\Phi_\ell(q^m) \equiv 0 \bmod \ell d' \equiv 0 \bmod d$. Par minimalité de n_0, on a $n_0 \leqslant m$. Cependant, $o_q(d) = \ell \cdot \mathrm{ppcm}(o_q(\ell), n') = \ell \cdot m$ divise $\ell \cdot n_0$. Ainsi $m = \mathrm{ppcm}(o_q(\ell), n_0)$ divise n_0 et est donc *égal* à n_0. Nous en concluons donc que $o_q(d) = \ell \cdot n_0$.

□

2.4.3 Théorème de Shafarevich-Tate et conséquences

Théorème 2.4.4 (Shafarevich-Tate)**.** *Soit $\mathbb{F}_{Q^2}/\mathbb{F}_Q$ une extension quadratique de corps finis de caractéristique $p \geqslant 3$. Soit $\chi : \mathbb{F}_{Q^2}^\times \to \overline{\mathbb{Q}}^\times$ un caractère non trivial. On suppose que la restriction de χ à $\mathbb{F}_Q^\times$ est triviale. Alors la somme de Gauss $\mathbf{g}_{Q^2}(\chi)$ s'écrit*

$$\mathbf{g}_{Q^2}(\chi) = -\chi(-c) \cdot Q = -\chi(-c) \cdot \sqrt{Q^2},$$

où $c \in \mathbb{F}_{Q^2}$ est un élément tel que $\mathrm{Tr}_{\mathbb{F}_{Q^2}/\mathbb{F}_Q}(c) = 0$.

Démonstration. Nous renvoyons la lectrice à [TŠ67, Lemma] pour la preuve originale, ou bien à [Ulm02, Lemma 8.3], ou encore à [LN97, Theorem 5.16]. □

On fixe un corps fini $\mathbb{F}_q$ de caractéristique impaire. Reprenons les notations introduites à la Section 2.1.3 : pour tout entier $d \geqslant 3$ premier à q, on dispose de caractères non triviaux $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ dont l'ordre divise d (où m parcourt $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$). Pour écourter les énoncés, si $m \in \mathcal{O}'_q(d)$ est une orbite de $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ sous l'action de q par multiplication, nous noterons $\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)$ la somme de Jacobi que nous devrions noter $\mathbf{j}_{q^{u(m)}}(\mathbf{t}_a, \mathbf{t}_a)$ (pour un choix quelconque d'un représentant $a \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ de l'orbite m).

Corollaire 2.4.5. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. Soit $d \geqslant 2$ un entier premier à q, on suppose qu'il existe $n \in \mathbb{N}^*$ tel que d divise $q^n + 1$. Alors, pour tout $m \in \mathcal{O}_q^{(2)}(d)$, $u(m)$ est pair et l'on a*

$$\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m) = -q^{u(m)/2} \qquad \text{et} \qquad \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mu_{q^{u(m)}}) = -q^{u(m)/2},$$

où $\mu_{q^{u(m)}} : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ désigne le caractère non trivial d'ordre 2.

Démonstration. Soit $m \in \mathcal{O}_q^{(2)}(d)$ comme dans l'énoncé, on note $d_m = d/\gcd(d, m)$ (où $\gcd(d, m)$ désigne la valeur commune des $\gcd(d, a)$ pour $a \in m$) et $K_m = \mathbb{Q}(\zeta_{d_m})$. On a vu (Proposition 2.1.5) que $\mathbf{t}_m$ est d'ordre d_m et à valeurs dans le corps cyclotomique K_m. Ici, comme $m \in \mathcal{O}_q^{(2)}(d)$, on a $d_m > 2$. D'après les Lemme 2.4.1 et Lemme 2.4.2, l'orbite m est de cardinal $u(m)$ pair et d divise $m(q^{u(m)/2} + 1)$ (sous l'hypothèse que d divise $q^n + 1$ pour un certain $n \in \mathbb{N}^*$). Soit alors $Q = q^{u(m)/2}$, l'extension $\mathbb{F}_{Q^2}/\mathbb{F}_Q$ est quadratique et $\mathbf{t}_m : \mathbb{F}_{Q^2}^\times \to \overline{\mathbb{Q}}^\times$ est un caractère non trivial dont la restriction à $\mathbb{F}_Q^\times$ est triviale. En effet, $(Q+1)m/d$ est un entier et par construction de $\mathbf{t}_m$, on a

$$\forall x \in \mathbb{F}_Q^\times, \quad \mathbf{t}_m(x) = \mathbf{t}(x)^{(Q^2-1)m/d} = \mathbf{t}(x^{Q-1})^{(Q+1)m/d} = 1.$$

De plus, $\mathbf{t}_m^2$ vérifie les mêmes hypothèses : $\mathbf{t}_m^2$ n'est pas trivial (car l'ordre d_m de $\mathbf{t}_m$ est > 2) et sa restriction à $\mathbb{F}_Q^\times$ est triviale (puisque c'est le cas pour $\mathbf{t}_m$). On peut ainsi appliquer le Théorème de Shafarevich-Tate (Théorème 2.4.4) successivement à $\mathbf{t}_m$ et $\mathbf{t}_m^2$: pour tout $c \in \mathbb{F}_{Q^2}$ tel que $\mathrm{Tr}_{\mathbb{F}_{Q^2}/\mathbb{F}_Q}(c) = 0$, on a

$$\mathbf{g}_{Q^2}(\mathbf{t}_m) = -\mathbf{t}_m(-c)\cdot Q \quad \text{et} \quad \mathbf{g}_{Q^2}(\mathbf{t}_m^2) = -\mathbf{t}_m^2(-c)\cdot Q.$$

Or, par la Proposition 2.2.7, on a

$$\mathbf{j}_{Q^2}(\mathbf{t}_m, \mathbf{t}_m) = \frac{\mathbf{g}_{Q^2}(\mathbf{t}_m)\cdot \mathbf{g}_{Q^2}(\mathbf{t}_m)}{\mathbf{g}_{Q^2}(\mathbf{t}_m^2)} = \frac{(-\mathbf{t}_m(-c)\cdot Q)^2}{-\mathbf{t}_m^2(-c)\cdot Q} = -\frac{\mathbf{t}_m(-c)^2}{\mathbf{t}_m^2(-c)}\cdot Q = -Q = -q^{u(m)/2}.$$

Ce qui termine la preuve de la première identité.

Pour démontrer la seconde identité, commençons par faire la remarque suivante : notons encore $Q = q^{u(m)/2}$ et $\mu : \mathbb{F}_{Q^2}^\times \to \overline{\mathbb{Q}}^\times$ le caractère non trivial d'ordre 2 sur $\mathbb{F}_{Q^2}^\times$ et μ' sa restriction à $\mathbb{F}_Q^\times$. Alors l'ordre de μ' vaut (voir [LN97, Chapter 5, §1]) :

$$\frac{2}{\mathrm{pgcd}\left(2, \frac{q^{u(m)}-1}{q^{u(m)/2}-1}\right)} = \frac{2}{\mathrm{pgcd}\left(2, \frac{(q^{u(m)/2}-1)(q^{u(m)/2}+1)}{q^{u(m)/2}-1}\right)} = \frac{2}{\mathrm{pgcd}\left(2, q^{u(m)/2}+1\right)} = \frac{2}{\mathrm{pgcd}\left(2, Q+1\right)} = 1$$

car $Q+1$ est pair. Autrement dit, la restriction μ' de μ à $\mathbb{F}_Q^\times$ est triviale. On peut donc appliquer le Théorème de Shafarevich-Tate (Théorème 2.4.4) successivement à μ, $\mathbf{t}_m$ et $\mu\cdot\mathbf{t}_m$ (comme ci-dessus) : pour tout élément $c \in \mathbb{F}_{Q^2}$ tel que $\mathrm{Tr}_{\mathbb{F}_{Q^2}/\mathbb{F}_Q}(c) = 0$, on a

$$\mathbf{j}_{Q^2}(\mathbf{t}_m, \mu) = \frac{\mathbf{g}_{Q^2}(\mathbf{t}_m)\cdot \mathbf{g}_{Q^2}(\mu)}{\mathbf{g}_{Q^2}(\mu\cdot\mathbf{t}_m)} = \frac{(-\mathbf{t}_m(-c)Q)\cdot(-\mu(-c)Q)}{(-\mathbf{t}_m(-c)\mu(-c)Q)} = -Q = -q^{u(m)/2}.$$

Ce qui achève la démonstration. Noter que nous aurons souvent besoin de ce résultat sous la forme suivante : $\mathbf{j}_{Q^2}(\mathbf{t}_m, \mu)^2 = q^{u(m)}$. □

Corollaire 2.4.6. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. Soit $d \geqslant 2$ un entier premier à q, on suppose qu'il existe $n \in \mathbb{N}^*$ tel que d divise $q^n + 1$.*

Alors, pour tout $m \in \mathcal{O}_q^{(3)}(d)$, on a

$$\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) = q^{u(m)}.$$

Démonstration. Supposons que d divise q^n+1 pour un certain entier $n \in \mathbb{N}^*$. Pour tout $m \in \mathcal{O}_q^{(3)}(d)$, l'ordre de $\mathbf{t}_m$ est $d_m = d/\mathrm{pgcd}(d, m)$ et, comme m est différent de $0, d/3, 2d/3$ (si d est divisible par 3), on a $d_m > 3$. D'après les Lemmes 2.4.1 et 2.4.2, l'orbite m est de cardinal pair $u(m)$ et d divise $m(q^{u(m)/2}+1)$. Posons, comme à la preuve ci-dessus, $Q = q^{u(m)/2}$. Alors l'extension $\mathbb{F}_{Q^2}/\mathbb{F}_Q$ est quadratique et le caractère $\mathbf{t}_m : \mathbb{F}_{Q^2}^\times \to \overline{\mathbb{Q}}^\times$ vérifie l'hypothèse du Théorème de Shafarevich-Tate (Théorème 2.4.4), à savoir que $\mathbf{t}_m$ n'est pas trivial et que sa restriction à $\mathbb{F}_Q^\times$ est triviale (la démonstration en a été faite dans la preuve du Corollaire précédent). Il en est donc de même pour $\mathbf{t}_m^3$ car l'ordre d_m de $\mathbf{t}_m$ est > 3. D'où, en appliquant le Théorème 2.4.4 à $\mathbf{t}_m$ et $\mathbf{t}_m^3$:

$$\mathbf{g}_{Q^2}(\mathbf{t}_m) = -\mathbf{t}_m(-c)\cdot Q \quad \text{et} \quad \mathbf{g}_{Q^2}(\mathbf{t}_m^3) = -\mathbf{t}_m^3(-c)\cdot Q,$$

où $c \in \mathbb{F}_{Q^2}$ est un élément tel que $\mathrm{Tr}_{\mathbb{F}_{Q^2}/\mathbb{F}_Q}(c) = 0$. D'après la Proposition 2.2.7, on a

$$\mathbf{j}_{Q^2}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) = \frac{\mathbf{g}_{Q^2}(\mathbf{t}_m)^3}{\mathbf{g}_{Q^2}(\mathbf{t}_m^3)} = \frac{(-\mathbf{t}_m(-c)\cdot Q)^3}{-\mathbf{t}_m^3(-c)\cdot Q} = Q^2 = q^{u(m)}.$$

Ce qu'il fallait démontrer. □

3

Encadrement de « valeurs spéciales »

Ce chapitre développe les outils « analytiques » utilisés dans la suite de cette thèse pour encadrer les valeurs spéciales des fonctions L de certaines courbes elliptiques sur $K = \mathbb{F}_q(t)$. Soit $\mathscr{E}$ une famille de courbes elliptiques E_d définies sur $K = \mathbb{F}_q(t)$, indexée par l'ensemble des entiers $d \geqslant 2$ premiers à q. Supposons avoir écrit la fonction L d'une courbe $E_d \in \mathscr{E}$ sous la forme :

$$L(E_d/K, T) = \prod_{m \in \mathcal{O}'_q(d)} \left(1 - \omega(m) \cdot T^{u(m)}\right),$$

où le produit porte sur l'ensemble des orbites $\mathcal{O}'_q(d)$ de l'action de q par multiplication sur $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ et où, pour tout $m \in \mathcal{O}'_q(d)$, $\omega(m)$ est un entier algébrique explicite. Comme on l'a expliqué à la Section 1.6, nous avons besoin d'encadrer la valeur spéciale $L^*(E_d/K, 1)$ en fonction de la hauteur $H(E_d/K)$.

Dans la première section de ce chapitre, nous démontrons une majoration de la valeur spéciale pour une classe de fonctions L. Ce résultat est un cas particulier de [HP16, Theorem 6.5]. Notre majoration est d'application plus restreinte, mais elle est plus explicite et sa preuve plus élémentaire. Nous retrouvons aussi une forme explicite et effective de la majoration du rang obtenue par Brumer [Bru92, Proposition 6.9], dont la démonstration ne fait pas appel aux formules explicites de Weil. Nous obtenons (Proposition 3.1.8) :

Théorème. *Si $E_d \in \mathscr{E}$, on a*

$$\frac{\log |L^*(E_d/K, 1)|}{d \cdot \log q} \ll \frac{\log \log d}{\log d},$$

où la constante implicite est absolue (et effective).

Dans la seconde section, nous démontrons une minoration de la valeur spéciale de fonctions L satisfaisant quelques hypothèses supplémentaires. Nous supposons que $L(E_d/K, T)$ est telle que :

(i) Pour tout $m \in \mathcal{O}'_q(d)$, $\omega(m)$ est un entier du corps cyclotomique $\mathbb{Q}(\zeta_{d_m})$, où $d_m := d/\operatorname{pgcd}(d, m)$. En particulier, on a $\omega(m) \in \mathbb{Q}(\zeta_d)$.

(ii) Pour tout $t \in (\mathbb{Z}/d\mathbb{Z})^\times$, on note $\sigma_t \in \operatorname{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ l'automorphisme qui lui correspond dans l'identification $\operatorname{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \simeq (\mathbb{Z}/d\mathbb{Z})^\times$. Pour tout $m \in \mathcal{O}'_q(d)$, on a $\sigma_t(\omega(m)) = \omega(t \cdot m)$.

À l'aide de ces deux hypothèses, on démontre (voir Théorème 3.2.2) :

Théorème. *Si $E_d \in \mathscr{E}$ et si $L(E_d/K, T)$ vérifie les hypothèses ci-dessus, on a*

$$-\frac{W(d)}{d} \leqslant \frac{\log |L^*(E_d/K, 1)|}{d \cdot \log q},$$

où $W(d) > 0$ admet une expression explicite en fonction des « valuations p-adiques » des $\omega(m)$.

Pour préciser l'énoncé, fixons un idéal premier $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$ au-dessus de p. Pour tout $m \in \mathcal{O}'_q(d)$, on note $\mathfrak{p}_m = \mathbb{Q}(\zeta_{d_m}) \cap \overline{\mathfrak{P}}$. Alors $W(d)$ s'écrit comme une somme de termes de la forme

$$\max\left\{0, u(m) - \frac{\operatorname{ord}_{\mathfrak{p}_m} \omega(m)}{[\mathbb{F}_q : \mathbb{F}_p]}\right\}.$$

Dans tous les cas, on a $0 \leqslant W(d) \leqslant d$ et l'on en déduit la minoration « de Liouville » :

$$-1 \leqslant \frac{\log|L^*(E_d/K,1)|}{d\cdot\log q}.$$

La minoration de $L^*(E_d/K,1)$ devient meilleure que cette minoration « triviale » si l'on connaît une meilleure majoration de $W(d)$. Dans le cas où $\omega(m)$ est une somme de Jacobi (ou un produit de sommes de Jacobi), on peut expliciter complètement $W(d)$ en décrivant les valuations $\mathrm{ord}_{\mathfrak{p}_m}\omega(m)$. La troisième section est dédiée à ce calcul, basé sur le théorème de Stickelberger.

Une fois obtenue, à l'aide de ces calculs, une expression assez explicite de $W(d)$, nous aurons besoin d'un résultat d'équidistribution pour démontrer que $W(d) = o(d)$ (lorsque $d \to \infty$). La preuve du théorème ci-dessous (Théorème 3.4.1) et de ses corollaires occupe la dernière section de ce chapitre :

Théorème. *Soit I un intervalle de $[0,1]$ de longueur $\mu(I)$ et $\mathscr{D} \subset \mathbb{N}^*$ un ensemble infini d'entiers. Soit également, pour tout entier $d \in \mathscr{D}$, un sous-groupe H_d de $G_d = (\mathbb{Z}/d\mathbb{Z})^\times$ tel que « H_d n'est pas trop petit ». Alors, lorsque $d \to \infty$ (avec $d \in \mathscr{D}$), on a*

$$\frac{1}{\#G_d}\sum_{g\in G_d}\left|\mu(I) - \frac{1}{\#H_d}\cdot\#\left\{t\in H_d \;\middle|\; \left\{\tfrac{gt}{d}\right\}\in I\right\}\right| = o(1).$$

Notations

Nous utiliserons librement les résultats de base sur l'arithmétique des corps cyclotomiques : voir par exemple [Coh07, Chapter 3, §5], [IR90, Chapter 13, §2] et [Was97, Chapter 2]. Par ailleurs, pour tout $x \in \mathbb{R}$, on notera $\lfloor x\rfloor$ la partie entière de x et $\{x\} = x - \lfloor x\rfloor$ sa partie fractionnaire : c'est l'unique nombre réel de $[0,1[$ tel que $x - \{x\} \in \mathbb{Z}$.

Dans tout le chapitre, on fixe une puissance q d'un nombre premier $p \geqslant 3$. Pour tout entier $d \geqslant 2$ premier à p, on note à nouveau $\mathcal{O}'_q(d)$ l'ensemble des orbites de $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ sous l'action de $q \bmod d$ par multiplication :

$$\mathcal{O}'_q(d) := \big(\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}\big)\big/\langle q \bmod d\rangle.$$

Comme q est premier à d, l'entier $\gcd(d,m)$ est bien défini pour $m \in \mathcal{O}'_q(d)$: c'est la valeur commune de $\gcd(d,a)$ pour $a \in m$. On pose alors $d_m = d/\gcd(d,m)$. Pour toute orbite $m \in \mathcal{O}'_q(d)$, on définit par ailleurs :

$$u(m) = \#m = \min\left\{\nu\in\mathbb{N}^* \;\middle|\; \forall a\in m,\ q^\nu a \equiv a \bmod d\right\} = \mathrm{ord}^\times(q \bmod d_m),$$

où, comme précédemment, on a noté $o_q(d)$ l'ordre (multiplicatif) de q modulo d.

Pour tout entier $n \in \mathbb{N}^*$, on note $\zeta_n = \mathrm{e}^{2i\pi/n}$ et $K_n = \mathbb{Q}(\zeta_n)$ le n-ième corps cyclotomique.

Pour tout diviseur d' de d, on note $K_{d'}$ le corps cyclotomique $K_{d'} = \mathbb{Q}(\zeta_{d'})$ et $L = \mathbb{Q}(\zeta_d)$. On identifiera $\mathrm{Gal}(K_{d'}/\mathbb{Q})$ à $(\mathbb{Z}/d'\mathbb{Z})^\times$ via $t \in (\mathbb{Z}/d'\mathbb{Z})^\times \mapsto \sigma_t$, où $\sigma_t(\zeta_{d'}) = (\zeta_{d'})^t$. Par commodité, on fixe également un idéal premier $\mathfrak{P}$ de L au-dessus de p : celui qui est sous l'idéal $\overline{\mathfrak{P}}$ de $\overline{\mathbb{Z}}$ utilisé pour définir le caractère de Teichmüller à la Section 2.1.2. Pour tout diviseur d' de d, on note alors $\mathfrak{p}' = \overline{\mathfrak{P}}\cap\mathbb{Z}[\zeta_{d'}]$ l'idéal premier de $\mathbb{Q}(\zeta_{d'}) = K_{d'}$ qui est au-dessous de $\overline{\mathfrak{P}}$, donc au-dessus de p. Attirons l'attention du lecteur sur le fait que la notation $\mathfrak{p}'$ ne fait pas intervenir explicitement d'.

3.1 Calcul et majoration de valeurs spéciales

Dans cette section, nous démontrons une majoration de « valeurs spéciales » que nous utiliserons à plusieurs reprises de la façon suivante : si E est une courbe elliptique sur $K = \mathbb{F}_q(t)$ et que sa fonction L est de la forme (3.1) ci-dessous, alors

$$\frac{\log L^*(E/K,1)}{\log H(E/K)} \leqslant 0 + o(1) \qquad (H(E/K)\to\infty).$$

Sous cette forme, le résultat est un cas particulier de [HP16, Theorem 7.5]. Notre théorème est d'envergure beaucoup plus restreinte, mais sa preuve est plus élémentaire.

3.1.1 Cadre

Soit $d \geqslant 2$ un entier premier à q. On considère dans cette section des polynômes $L_d(T) \in \overline{\mathbb{Q}}[T]$ de la forme

$$L_d(T) = \prod_{m\in\mathcal{M}}\left(\prod_{k=1}^{K}\left(1-\omega_k(m)\cdot T^{u(m)}\right)\right), \tag{3.1}$$

où $\mathcal{M} \subset \mathcal{O}'_q(d)$ est un ensemble d'orbites, $K \in \mathbb{N}^*$ est un entier fixé indépendamment de d, et, pour tout $m \in \mathcal{M}$, $\omega_j(m) \in \overline{\mathbb{Q}}$ est un nombre algébrique tel que $|\omega_j(m)| = q^{u(m)}$ dans tout plongement complexe. Ces polynômes modélisent les fonctions L des courbes elliptiques que l'on étudiera.

Pour un tel polynôme $L_d(T)$, on appellera *rang de* $L_d(T)$ son ordre d'annulation en $T = q^{-1}$, noté $r = \mathrm{ord}_{T=q^{-1}} L(T)$. On pose de plus

$$L_d^*(T) = \frac{L_d(T)}{(1-qT)^r}.$$

On note que si $L_d(T)$ est à coefficients entiers, il en est de même pour $L_d^*(T)$. Pour tout $m \in \mathcal{M}$, on pose

$$g_m(T) = \prod_{k=1}^{K} (1 - \omega_k(m) \cdot T^{u(m)}).$$

Appelons $r_m = \mathrm{ord}_{T=q^{-1}} g_m(T)$ et posons $g_m^*(T) = g_m(T)/(1-qT)^{r_m}$. Alors $g_m^*(q^{-1}) \neq 0$ et la « valeur spéciale » de $L_d(T)$ s'écrit

$$L_d^*(q^{-1}) = \prod_{m \in \mathcal{M}} g_m^*(q^{-1}).$$

3.1.2 Lemmes préliminaires

Commençons par prouver quelques résultats sur l'action de q sur $\mathbb{Z}/d\mathbb{Z}$. Pour ce faire, nous aurons besoin du Lemme ci-dessous.

Lemme 3.1.1. *Il existe une constante $C > 0$ telle que, pour tout entier $n \in \mathbb{N}^*$, $n \geqslant 2$, on a*

$$\sum_{\substack{d|n \\ d \geqslant 2}} \frac{\phi(d)}{\log d} \leqslant C \cdot \frac{n}{\log n}.$$

La constante C est effective, on peut choisir $C \leqslant 4$.

Démonstration. Soit $n \geqslant 2$ un entier et $X \in \mathbb{R}$ un paramètre à choisir dans l'intervalle $2 \leqslant X \leqslant n$. Séparons la somme à majorer en deux parties :

$$\sum_{\substack{d|n \\ d \geqslant 2}} \frac{\phi(d)}{\log d} = \sum_{\substack{d|n \\ 2 \leqslant d \leqslant X}} \frac{\phi(d)}{\log d} + \sum_{\substack{d|n \\ X < d}} \frac{\phi(d)}{\log d}.$$

Dans la seconde somme, par croissance de $x \mapsto \log x$, chaque terme est inférieur ou égal à $\phi(d)/\log X$ de sorte que

$$\sum_{\substack{d|n \\ X < d}} \frac{\phi(d)}{\log d} \leqslant \frac{1}{\log X} \sum_{\substack{d|n \\ X < d}} \phi(d) \leqslant \frac{1}{\log X} \sum_{d|n} \phi(d) = \frac{n}{\log X}.$$

Pour majorer le premier terme, on commence par remarquer que la fonction $x \mapsto (x-1)/\log x$ est croissante sur $[2, +\infty[$. Pour tout $d \in [2, X]$, sachant que $\phi(d) \leqslant d-1$, on obtient :

$$\sum_{\substack{d|n \\ 2 \leqslant d \leqslant X}} \frac{\phi(d)}{\log d} \leqslant \sum_{\substack{d|n \\ 2 \leqslant d \leqslant X}} \frac{d-1}{\log d} \leqslant \frac{X-1}{\log X} \sum_{\substack{d|n \\ 2 \leqslant d \leqslant X}} 1 \leqslant \frac{(X-1)^2}{\log X} \leqslant \frac{X^2}{\log X}.$$

Par suite,

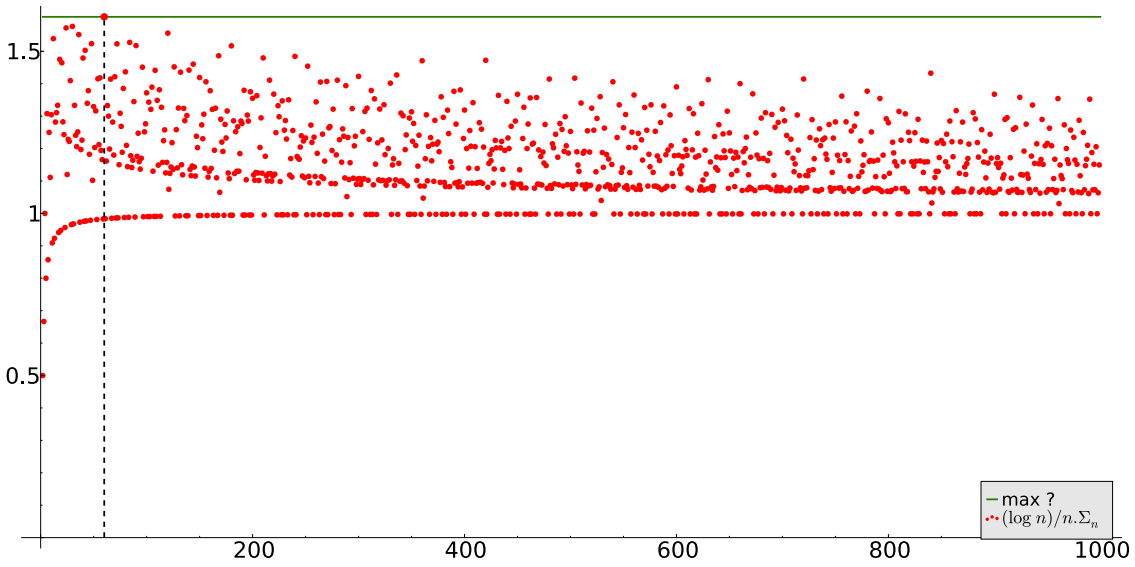
$$\sum_{\substack{d|n \\ X < d}} \frac{\phi(d)}{\log d} \leqslant \frac{X^2}{\log X} + \frac{n}{\log X}.$$

Le choix de $X = \sqrt{n}$ donne alors

$$\frac{X^2}{\log X} + \frac{n}{\log X} = \frac{n}{\log \sqrt{n}} + \frac{n}{\log \sqrt{n}} = \frac{4n}{\log n}.$$

Ce qui démontre l'existence d'une constante $C \leqslant 4$ telle que l'inégalité de l'énoncé est vérifiée. □

Remarque 3.1.2. Pour le moment, on ne sait pas démontrer mieux que $C = 4$. Cependant, des simulations numériques suggèrent que $C \simeq 1.61...$ serait un choix optimal. Ci-dessous, nous avons tracé (en rouge) la fonction $C : n \mapsto \frac{\log n}{n} \cdot \sum_{\substack{d|n \\ d\geqslant 2}} \frac{\phi(d)}{\log d}$ pour $n \in [\![1, 10^3]\!]$. Le maximum de cette fonction dans cet intervalle est atteint pour $n = 60$ et $C(60) \simeq 1.606272...$.



Soit maintenant q la puissance d'un nombre premier $p \geqslant 3$ et d un entier premier à q. On peut décomposer $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ comme une union disjointe

$$\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\} = \bigsqcup_{d'|d} \frac{d}{d'} \cdot (\mathbb{Z}/d'\mathbb{Z})^\times \tag{3.2}$$

en répartissant les éléments $m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ selon la valeur de $d' = d/\operatorname{pgcd}(d, m)$. L'action de q par multiplication sur $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ respecte cette décomposition puisque q est premier à d (au sens où, si $m \in \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$, $\operatorname{pgcd}(d, q \cdot m) = \operatorname{pgcd}(m, d)$: *i.e.* si $m \in \frac{d}{d'} \cdot (\mathbb{Z}/d'\mathbb{Z})^\times$ alors l'orbite entière de m est incluse dans $\frac{d}{d'} \cdot (\mathbb{Z}/d'\mathbb{Z})^\times$). Par conséquent, l'ensemble $\mathcal{O}'_q(d) = (\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\})/\langle q \bmod d\rangle$ des orbites de $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ sous l'action de q par multiplication admet lui-même une partition analogue à (3.2) :

$$\mathcal{O}'_q(d) = (\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\})/\langle q \bmod d\rangle = \bigsqcup_{d'|d} \frac{d}{d'} \cdot \left(\frac{(\mathbb{Z}/d'\mathbb{Z})^\times}{\langle q \bmod d'\rangle} \right). \tag{3.3}$$

Rappelons que pour tout entier n premier à q, on peut interpréter $o_q(n) = \operatorname{ord}^\times(q \bmod n)$ comme l'ordre du sous-groupe $\langle q\rangle_n$ de $(\mathbb{Z}/n\mathbb{Z})^\times$ engendré par q ; l'ensemble des orbites de l'action de q par multiplication sur $(\mathbb{Z}/n\mathbb{Z})^\times$ s'identifie au groupe quotient $(\mathbb{Z}/n\mathbb{Z})^\times/\langle q\rangle_n$. On a donc $o_q(n) \mid \phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. Par suite, pour tout entier $d' \geqslant 2$, on a $\#\left((\mathbb{Z}/d'\mathbb{Z})^\times/\langle q\rangle_{d'}\right) = \phi(d')/o_q(d')$. On obtient alors la relation importante :

$$\#\mathcal{O}'_q(d) = \sum_{\substack{d'|d \\ d'\geqslant 2}} \frac{\phi(d')}{o_q(d')}. \tag{3.4}$$

Dans la Proposition ci-dessous, nous donnons divers encadrements de $\#\mathcal{O}_q(d)$ et de quantités liées à l'action de q sur $\mathbb{Z}/d\mathbb{Z}$.

Proposition 3.1.3. *Soit $d \geqslant 2$ un entier premier à q. On note à nouveau $\mathcal{O}'_q(d)$ l'ensemble des orbites de $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ sous l'action de q par multiplication. On a les relations suivantes :*

(1) $\#O'_q(d) = \displaystyle\sum_{\substack{d'|d \\ d'\geqslant 2}} \frac{\phi(d')}{o_q(d')} \leqslant C \log q \cdot \frac{d}{\log d} = o\big(d\big).$

(2) $\displaystyle\sum_{m\in\mathcal{O}'_q(d)} u(m) = d - 1 \leqslant d.$

(3) $\displaystyle\sum_{m\in\mathcal{O}'_q(d)} \log u(m) \leqslant (C \log q + 1) \cdot \frac{d \cdot \log\log d}{\log d} = o\big(d\big).$

(4) À q fixé, lorsque $d \geqslant 2$ parcourt l'ensemble des entiers premiers à q, $\#\mathcal{O}_q(d)$ n'est pas borné. La constante C est la même que celle du Lemme 3.1.1.

Démonstration. Soit d' un entier $\geqslant 2$. Par définition de l'ordre, d' divise $q^{o_q(d')}-1$: en particulier, on a donc $\log d' \leqslant o_q(d')\log q$. On déduit alors du Lemme 3.1.1 la première majoration souhaitée :

$$\sum_{\substack{d'\mid d\\ d'\geqslant 2}} \frac{\phi(d')}{o_q(d')} \leqslant \log q \cdot \sum_{\substack{d'\mid d\\ d'\geqslant 2}} \frac{\phi(d')}{\log(d')} \leqslant C\log q \cdot \frac{d}{\log d}.$$

La seconde relation est une conséquence de la partition d'un ensemble comme réunion d'orbites disjointes sous une action : on a

$$\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\} = \bigsqcup_{m\in\mathcal{O}'_q(d)} m,$$

et il reste à remarquer que $\#m = u(m)$ pour tout $m \in \mathcal{O}'_q(d)$. Passons à la preuve de la troisième majoration : pour tout diviseur $d' \geqslant 2$ de d, on note $G_{d'} = (\mathbb{Z}/d'\mathbb{Z})^\times$ et $\langle q\rangle_{d'} \subset G_{d'}$ le sous-groupe engendré par q. En utilisant la partition (3.3) de $\mathcal{O}'_q(d)$, on remarque dans un premier temps que

$$\begin{aligned}\sum_{m\in\mathcal{O}'_q(d)} \log u(m) &= \sum_{\substack{d'\mid d\\ d'\geqslant 2}} \sum_{m'\in G_{d'}/\langle q\rangle_{d'}} \log u\left(\tfrac{d}{d'}m'\right) = \sum_{\substack{d'\mid d\\ d'\geqslant 2}} \sum_{m'\in G_{d'}/\langle q\rangle_{d'}} \log o_q(d')\\ &= \sum_{\substack{d'\mid d\\ d'\geqslant 2}} \frac{\#G_{d'}}{\#\langle q\rangle_{d'}} \log o_q(d') = \sum_{\substack{d'\mid d\\ d'\geqslant 2}} \frac{\phi(d')}{o_q(d')} \log o_q(d').\end{aligned}$$

Séparons cette dernière somme en deux parties en fonction d'un paramètre $Y \in [2,d]$ à choisir ci-après. En utilisant le fait que la fonction $y \mapsto (\log y)/y$ est décroissante sur $[2,+\infty[$ et la majoration de $\#O'_q(d)$ obtenue ci-dessus, on trouve que

$$\begin{aligned}\sum_{\substack{d'\mid d\\ d'\geqslant 2}} \frac{\phi(d')}{o_q(d')} \log o_q(d') &= \sum_{\substack{d'\mid d\\ 2\leqslant d'<Y}} \frac{\phi(d')}{o_q(d')} \log o_q(d') + \sum_{\substack{d'\mid d\\ Y\leqslant d'}} \frac{\phi(d')}{o_q(d')} \log o_q(d')\\ &\leqslant \log Y \cdot \sum_{\substack{d'\mid d\\ 2\leqslant d'<Y}} \frac{\phi(d')}{o_q(d')} + \frac{\log Y}{Y}\cdot \sum_{\substack{d'\mid d\\ Y\leqslant d'}} \phi(d')\\ &\leqslant \log Y \cdot \#\mathcal{O}'_q(d) + \frac{\log Y}{Y}\cdot \sum_{d'\mid d} \phi(d')\\ &\leqslant C\log q \cdot \frac{d}{\log d}\cdot \log Y + \frac{\log Y}{Y}\cdot d\\ &= d\cdot\left(\frac{C\log q\cdot\ \log Y}{\log d} + \frac{\log Y}{Y}\right).\end{aligned}$$

On choisit donc $Y = \log d < d$ et l'on obtient que

$$\sum_{m\in\mathcal{O}'_q(d)} \log u(m) \leqslant (C\log q+1)\cdot \frac{d\cdot\log\log d}{\log d} \ll_q \frac{d\cdot\log\log d}{\log d} = o\big(d\big),$$

la constante implicite ne dépendant que de q. Démontrons enfin la dernière assertion : on fixe q et il s'agit de produire une suite d'entiers d premiers à q tels que $\#\mathcal{O}'_q(d)\to\infty$. Pour tout entier $N\in\mathbb{N}^*$, on pose $d_N = q^N+1$, un entier pair et premier à q. Alors, le Lemme 2.4.1 s'applique : l'ordre de q modulo d_N vaut $o_q(d_N) = 2N$. De plus, pour tout diviseur $d'\geqslant 2$ de d_N, on a $o_q(d') \mid o_q(d_N) = 2N$. En particulier, on a

$$\#\mathcal{O}'_q(d_N) = \sum_{\substack{d'\mid d\\ d'\geqslant 2}} \frac{\phi(d')}{o_q(d')} \geqslant \frac{1}{o_q(d_N)}\cdot \sum_{\substack{d'\mid d\\ d'\geqslant 2}} \phi(d') = \frac{d_N-\phi(2)}{o_q(d_N)} \geqslant \frac{d_N-1}{2N}.$$

Mais, par construction, $\log d_N = \log(q^N + 1) \geqslant N \cdot \log q$. D'où l'on tire la minoration

$$\#\mathcal{O}'_q(d_N) \geqslant \frac{d_N - 1}{2N} \geqslant \frac{\log q}{2} \cdot \frac{d_N - 1}{\log d_N} \geqslant \frac{\log q}{3} \cdot \frac{d_N}{\log d_N}.$$

Ainsi, lorsque $N \to \infty$, le nombre $\#\mathcal{O}'_q(d_N)$ d'orbites tend également vers $+\infty$. Mieux, on a démontré que la majoration de l'item (1) de la Proposition est optimale ; au sens où, pour tout $N \in \mathbb{N}^*$,

$$\frac{\log q}{3} \cdot \frac{d_N}{\log d_N} \leqslant \#\mathcal{O}'_q(d_N) \leqslant C \log q \cdot \frac{d_N}{\log d_N}.$$

Ceci conclut la preuve de la Proposition. □

3.1.3 Majoration du rang et de la valeur spéciale

Soit $q \geqslant 3$ un entier impair et $d \geqslant 2$ premier à q. On considère un polynôme $L_d(T)$ de la forme (3.1). On a une majoration triviale de l'ordre d'annulation de $L_d(T)$ en $T = q^{-1}$ (son « rang ») :

$$\begin{aligned}\operatorname{ord}_{T=q^{-1}} L_d(T) \leqslant \deg L_d(T) &= \sum_{m \in \mathcal{M}} \deg g_m(T) = \sum_{m \in \mathcal{M}} K \cdot u(m) \\ &\leqslant K \cdot \sum_{m \in \mathcal{O}'_q(d)} u(m) = K(d-1) \ll_K d.\end{aligned}$$

La Proposition 3.1.5 ci-dessous raffine cette première borne (en $\mathcal{O}(d)$) en une majoration bien meilleure (en $\mathcal{O}(d/\log d)$). Commençons cependant par donner une expression explicite de l'ordre d'annulation de $L_d(T)$ en $T = q^{-1}$.

Lemme 3.1.4 (Expression du rang)**.** *Soit d un entier premier à q et $K \geqslant 1$ fixé. Pour tout polynôme $L_d(T)$ de la forme* (3.1)*, on a*

$$\operatorname{ord}_{T=q^{-1}} L_d(T) = \sum_{m \in \mathcal{M}} \#\left\{k \in [\![1, K]\!] \;\middle|\; \omega_k(m) = q^{u(m)}\right\}.$$

Démonstration. Par définition, $L_d(T)$ s'écrit comme un produit

$$L_d(T) = \prod_{m \in \mathcal{M}} g_m(T) \quad \text{où } g_m(T) = \prod_{k=1}^{K} \left(1 - \omega_k(m) \cdot T^{u(m)}\right).$$

On a immédiatement $\operatorname{ord}_{T=q^{-1}} L_d(T) = \sum_{m \in \mathcal{M}} \operatorname{ord}_{T=q^{-1}} g_m(T)$. Et, à $m \in \mathcal{M}$ fixé, il est clair que l'ordre d'annulation de $g_m(T)$ en $T = q^{-1}$ est égal au nombre de $\omega_k(m)$ égaux à $q^{u(m)}$ (pour $k \in [\![1, K]\!]$). □

Proposition 3.1.5 (Majoration du rang)**.** *Soit d un entier premier à q et $K \geqslant 1$ fixé. Pour tout polynôme $L_d(T)$ de la forme* (3.1)*, on a*

$$\operatorname{ord}_{T=q^{-1}} L_d(T) \leqslant C \log q \cdot K \cdot \frac{d}{\log d} \ll_{q,K} \frac{d}{\log d}.$$

Démonstration. D'après le Lemme ci-dessus, on a

$$\operatorname{ord}_{T=q^{-1}} L_d(T) = \sum_{m \in \mathcal{M}} \#\left\{k \in [\![1, K]\!] \;\middle|\; \omega_k(m) = q^{u(m)}\right\} \leqslant \#\mathcal{M} \cdot K \leqslant \#\mathcal{O}'_q(d) \cdot K.$$

La majoration de $\#\mathcal{O}'_q(d)$ obtenue à la Proposition 3.1.3 (item (1)) donne alors le résultat attendu. □

Remarque 3.1.6. On obtient ainsi facilement une version explicite de la borne de Brumer [Bru92, Proposition 6.9] pour le rang des courbes elliptiques sur $K = \mathbb{F}_q(t)$ dont les fonctions L sont de la forme (3.1).

Terminons cette section par des résultats sur les « valeurs spéciales » des polynômes de la forme (3.1).

Proposition 3.1.7 (Expression de la valeur spéciale)**.** *Soit d un entier premier à q et $K \geqslant 1$ fixé. Pour tout polynôme $L_d(T)$ de la forme* (3.1)*, on pose*

$$L_d^*(T) = \frac{L_d(T)}{(1-qT)^r} \text{ avec } r = \operatorname{ord}_{T=q^{-1}} L_d(T) \text{ comme ci-dessus.}$$

Pour toute orbite $m \in \mathcal{M}$, soit également $Z_m = \left\{k \in [\![1, K]\!] \mid \omega_k(m) = q^{u(m)}\right\}$. Alors

$$L_d^*(q^{-1}) = \prod_{m\in\mathcal{M}} \left(u(m)^{\#Z_m} \cdot \prod_{k\notin Z_m} \left(1 - \frac{\omega_k(m)}{q^{u(m)}}\right)\right).$$

Démonstration. On note à nouveau, pour toute orbite $m \in \mathcal{M} \subset \mathcal{O}'_q(d)$, le facteur

$$g_m(T) = \prod_{k=1}^{K} \left(1 - \omega_k(m) \cdot T^{u(m)}\right).$$

On pose alors $Z_m = \left\{k \in [\![1, K]\!] \mid \omega_k(m) = q^{u(m)}\right\}$. On constate que $r_m = \#Z_m = \operatorname{ord}_{T=q^{-1}} g_m(T)$. De plus, considérons $g_m^*(T) = g_m(T)/(1-qT)^{r_m}$. Un calcul rapide montre que

$$g_m^*(q^{-1}) = \prod_{k\in Z_m} u(m) \cdot \prod_{k\notin Z_m} \left(1 - \frac{\omega_k(m)}{q^{u(m)}}\right) = u(m)^{r_m} \cdot \prod_{k\notin Z_m} \left(1 - \frac{\omega_k(m)}{q^{u(m)}}\right).$$

Par construction, on a $r = \operatorname{ord}_{T=q^{-1}} L_d(T) = \sum_{m\in\mathcal{M}} r_m$ et $L_d^*(T) = \prod_{m\in\mathcal{M}} g_m^*(T)$. Donc, lorsque l'on évalue $L_d^*(T)$ en $T = q^{-1}$, on obtient le produit des $g_m^*(q^{-1})$ (m parcourant $\mathcal{M}$), quantités que l'on vient d'expliciter. □

Proposition 3.1.8 (Majoration de la valeur spéciale)**.** *Soit d un entier premier à q et $K \geqslant 1$ fixé. Pour tout polynôme $L_d(T)$ de la forme* (3.1)*, on pose*

$$L_d^*(T) = \frac{L_d(T)}{(1-qT)^r} \text{ avec } r = \operatorname{ord}_{T=q^{-1}} L_d(T) \text{ comme ci-dessus.}$$

Alors

$$\log|L_d^*(q^{-1})| \leqslant 3C \cdot K \log q \cdot \frac{d \cdot \log\log d}{\log d} \ll_{K,q} \frac{d \cdot \log\log d}{\log d}.$$

Démonstration. Reprenons les notations de la preuve précédente. Par hypothèse, pour tout $m \in \mathcal{M}$ et tout $k \in [\![1, K]\!]$, on a $|\omega_k(m)| = q^{u(m)}$ (dans tout plongement complexe de $\overline{\mathbb{Q}}$). Il suit que, pour tout $m \in \mathcal{M}$,

$$|g_m^*(q^{-1})| \leqslant u(m)^{r_m} \cdot \prod_{k\notin Z_m} 2 = u(m)^{r_m} \cdot 2^{K-r_m},$$

où $0 \leqslant r_m \leqslant K$. Par suite, on a

$$\begin{aligned}
|L_d^*(q^{-1})| = \prod_{m\in\mathcal{M}} |g_m^*(q^{-1})| &= \prod_{m\in\mathcal{M}} \left(u(m)^{r_m} \cdot \prod_{k\notin Z_m} \left|1 - \frac{\omega_k(m)}{q^{u(m)}}\right|\right) \\
&\leqslant \prod_{m\in\mathcal{M}} u(m)^{r_m} \cdot 2^{K-r_m} \leqslant \prod_{m\in\mathcal{M}} u(m)^K \cdot \prod_{m\in\mathcal{M}} 2^K \\
&\leqslant \prod_{m\in\mathcal{O}'_q(d)} u(m)^K \cdot \prod_{m\in\mathcal{O}'_q(d)} 2^K = 2^{K\cdot\#\mathcal{O}'_q(d)} \cdot \left(\prod_{m\in\mathcal{O}'_q(d)} u(m)\right)^K.
\end{aligned}$$

Par conséquent, après passage au logarithme, on obtient

$$\log|L_d^*(q^{-1})| \leqslant K\log 2 \cdot \#\mathcal{O}'_q(d) + K \cdot \sum_{m\in\mathcal{O}'_q(d)} \log u(m).$$

Les deux quantités relatives à $\mathcal{O}'_q(d)$ ont été majorées à la Proposition 3.1.3 (items (1) et (3)) :

$$\#O'_q(d) \leqslant C\log q \cdot \frac{d}{\log d} \quad \text{et} \quad \sum_{m\in\mathcal{O}'_q(d)} \log u(m) \leqslant (C\log q + 1) \cdot \frac{d \cdot \log\log d}{\log d}.$$

Finalement, en majorant grossièrement $\log 2 \leqslant \log\log d$, nous avons donc

$$\log|L_d^*(q^{-1})| \leqslant K \cdot (2C\log q + 1) \cdot \frac{d \cdot \log\log d}{\log d} \ll_{K,q} \frac{d \cdot \log\log d}{\log d}.$$

C'est bien la majoration annoncée. □

Exemple 3.1.9. Dans la pratique, nous aurons essentiellement besoin du cas où $K = 1$. Si $K = 1$ et que $d \geqslant 2$ est un entier premier à q, un polynôme $L_d(T)$ de la forme (3.1) s'écrit :

$$L_d(T) = \prod_{m\in\mathcal{M}} \left(1 - \omega(m) \cdot T^{u(m)}\right).$$

Au cours des preuves ci-dessus, on a donné une expression pour l'ordre d'annulation de $L_d(T)$ en $T = q^{-1}$:

$$\operatorname{ord}_{T=q^{-1}} L_d(T) = \#\mathcal{Z}_d \quad \text{où } \mathcal{Z}_d = \left\{m \in \mathcal{M} \;\middle|\; \omega(m) = q^{u(m)}\right\}.$$

D'autre part, on a

$$L_d^*(q^{-1}) = \prod_{m\in\mathcal{Z}_d} u(m) \cdot \prod_{m\notin\mathcal{Z}_d} \left(1 - \frac{\omega(m)}{q^{u(m)}}\right).$$

De plus, on a montré que

$$\frac{\log|L_d(q^{-1})|}{d} \leqslant (2C\log q + 1) \cdot \frac{\log\log d}{\log d} \ll_q \frac{\log\log d}{\log d}.$$

3.2 Minoration de valeurs spéciales

Soit $\mathbb{F}_q$ un corps fini et $d \geqslant 2$ un entier premier à q. Soit également $L_d(T)$ un polynôme de la forme (3.1). À la section précédente (Proposition 3.1.7), nous avons explicité la « valeur spéciale » associée à $L_d(T)$ sous la forme d'un produit : avec les notations précédemment introduites, on a

$$L_d^*(q^{-1}) = \prod_{m\in\mathcal{M}} \left(u(m)^{\#Z_m} \cdot \prod_{k\notin Z_m} \left(1 - \frac{\omega_k(m)}{q^{u(m)}}\right)\right).$$

Dans cette section, nous nous attachons à *minorer* ce produit (ou plutôt le logarithme de celui-ci). On peut d'ores et déjà mettre à part le terme $\prod_{m\in\mathcal{M}} u(m)^{\#Z_m} \in \mathbb{N}^*$, dont le logarithme est positif (et négligeable devant d, *cf.* Proposition 3.1.3, item (3)). Nous écrivons alors le terme restant sous la forme suivante :

$$\prod_{m\in\mathcal{M}} \prod_{k\notin Z_m} \left(1 - \frac{\omega_k(m)}{q^{u(m)}}\right) = \prod_{m\in\mathcal{M}} \left(1 - \frac{y(m)}{q^{u(m)}}\right), \tag{3.5}$$

où les $y(m)$ sont des entiers algébriques que l'on pourrait expliciter en termes des données $\omega_k(m)$. Notons que, lorsque $K = 1$, on a $\omega_k(m) = y(m)$.

Nous développons donc des outils pour minorer ce type de produit (3.5), en rajoutant des hypothèses sur la donnée des $y(m)$. Le but est d'obtenir une minoration de la forme

$$\frac{1}{d} \cdot \log\left|\prod_{m\in\mathcal{M}} \left(1 - \frac{y(m)}{q^{u(m)}}\right)\right| \geqslant -\log q \cdot \frac{W(y,\mathcal{M})}{d},$$

où $W(y,\mathcal{M}) \in \mathbb{Q}^*$ est un nombre positif explicite, qui doit être « facile » à *majorer* en termes de d. À la section suivante, nous expliciterons complètement $W(y,\mathcal{M})$ lorsque les $y(m)$ sont des sommes de Jacobi.

3.2.1 Cadre et hypothèses

Dans tout le reste de cette section, on fixe $q \in \mathbb{N}^*$ une puissance d'un nombre premier $p \geqslant 3$.

Soit $d \geqslant 2$ un entier premier à q et $L = \mathbb{Q}(\zeta_d)$ le corps cyclotomique correspondant. On suppose donné un couple $(y,\mathcal{M})$ formé de :

- une application $y : \mathcal{O}'_q(d) \to \mathbb{Q}(\zeta_d) = L$, *i.e.* un ensemble $\{y(m)\}_{m\in\mathcal{O}'_q(d)}$ d'éléments de L,
- un ensemble non vide d'orbites $\mathcal{M} \subset \mathcal{O}'_q(d)$.

Pour toute orbite $m \in \mathcal{O}'_q(d)$, on note $d_m = d/\operatorname{pgcd}(d,m)$. On rappelle également l'identification entre $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ et $(\mathbb{Z}/d\mathbb{Z})^\times$: à tout élément $t \in (\mathbb{Z}/d\mathbb{Z})^\times$, on associe $\sigma_t \in \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ défini par $\zeta_d \mapsto (\zeta_d)^t$.

On supposera que la donnée $(y, \mathcal{M})$ satisfait aux conditions suivantes :

(i) Pour tout $m \in \mathcal{O}'_q(d)$, $y(m)$ est un entier de $\mathbb{Q}(\zeta_{d'})$, où $d' = d_m$.
En particulier, $y(m) \in \mathbb{Q}(\zeta_d)$.

(ii) Pour tout $m \in \mathcal{O}'_q(d)$,
$$\forall t \in (\mathbb{Z}/d\mathbb{Z})^\times, \quad \sigma_t(y(m)) = y(t \cdot m).$$

(iii) Le produit
$$\pi^*_{\mathcal{M}} := \prod_{m \in \mathcal{M}} \left(1 - \frac{y(m)}{q^{u(m)}}\right)$$
est un nombre rationnel strictement positif.

En particulier, l'hypothèse (iii) requiert que $y(m) \neq q^{u(m)}$ pour tout $m \in \mathcal{M}$. Noter que nous ne supposons pas que $y(m)$ est un q-nombre de Weil de poids 2 (*i.e.* que $|y(m)| = q^{u(m)}$ dans tout plongement complexe de $\mathbb{Q}(\zeta_{d'})$).

On peut partitionner l'ensemble d'orbites $\mathcal{M}$ comme suit : pour tout diviseur d' de d, on notera $\mathcal{M}(d')$ l'ensemble des orbites $m \in \mathcal{M}$ telles que $\operatorname{pgcd}(d,m) = d/d'$:
$$\mathcal{M}(d') := \left\{ m \in \mathcal{M} \;\middle|\; \forall i \in m,\ \operatorname{pgcd}(d,i) = \tfrac{d}{d'} \right\}.$$
On a donc $\mathcal{M} = \bigsqcup_{d'|d} \mathcal{M}(d')$, avec $\mathcal{M}(1) = \varnothing$. Ainsi défini, pour $d' \geqslant 2$, l'ensemble $\mathcal{M}(d')$ est en bijection avec une partie du *groupe* quotient $(\mathbb{Z}/d'\mathbb{Z})^\times/\langle q\rangle_{d'}$, où $\langle q\rangle_{d'}$ désigne le sous-groupe de $(\mathbb{Z}/d'\mathbb{Z})^\times$ engendré par q (voir la Section précédente, et la partition (3.3) en particulier). On écrira donc aussi, $\mathcal{M}(d') = \frac{d}{d'}\mathcal{P}(d')$, où $\mathcal{P}(d')$ est une partie de $(\mathbb{Z}/d'\mathbb{Z})^\times/\langle q\rangle_{d'}$. Nous reviendrons plus en détail sur ce point à la Section 3.2.3.

3.2.2 Une minoration naïve et une minoration plus fine

Donnons une première minoration d'un produit $\pi^*_{\mathcal{M}}$ comme ci-dessus.

Proposition 3.2.1. *Soit $d \geqslant 2$ un entier premier à q et $(y, \mathcal{M})$ une donnée qui vérifie les hypothèses de la Section 3.2.1 ci-avant. Alors*
$$\log \pi^*_{\mathcal{M}} \geqslant -\log q \cdot d.$$

Démonstration. Pour tout $m \in \mathcal{O}'_q(d)$, le nombre algébrique $q^{u(m)} - y(m)$ est un entier de $L = \mathbb{Q}(\zeta_d)$ (par hypothèse (i)). En particulier, on a $\mathbf{N}_{L/\mathbb{Q}}(q^{u(m)} - y(m)) \in \mathbb{N}^*$ puisqu'on a en outre supposé que $y(m) \neq q^{u(m)}$. Par conséquent, pour tout $m \in \mathcal{O}'_q(d)$, on a
$$\mathbf{N}_{L/\mathbb{Q}}\left(1 - \frac{y(m)}{q^{u(m)}}\right) = \frac{\mathbf{N}_{L/\mathbb{Q}}(q^{u(m)} - y(m))}{\mathbf{N}_{L/\mathbb{Q}}(q^{u(m)})} \geqslant \frac{1}{q^{u(m)\cdot[L:\mathbb{Q}]}}.$$

Par ailleurs, le produit $\pi^*_{\mathcal{M}}$ est rationnel (hypothèse (iii)), c'est donc que
$$\begin{aligned}(\pi^*_{\mathcal{M}})^{[L:\mathbb{Q}]} = \mathbf{N}_{L/\mathbb{Q}}(\pi^*_{\mathcal{M}}) = \mathbf{N}_{L/\mathbb{Q}}\left(\prod_{m\in\mathcal{M}}\left(1 - \frac{y(m)}{q^{u(m)}}\right)\right) &= \prod_{m\in\mathcal{M}} \mathbf{N}_{L/\mathbb{Q}}\left(1 - \frac{y(m)}{q^{u(m)}}\right) \\ &\geqslant \prod_{m\in\mathcal{M}} \frac{1}{q^{u(m)[L:\mathbb{Q}]}} = q^{-[L:\mathbb{Q}]\cdot\sum_{m\in\mathcal{M}} u(m)}.\end{aligned}$$

Or, par construction de $\mathcal{O}'_q(d) \supset \mathcal{M}$, on a
$$1 \leqslant \sum_{m\in\mathcal{M}} u(m) \leqslant \sum_{m\in\mathcal{O}'_q(d)} u(m) = d - 1 \leqslant d.$$

D'où l'on tire que $\log \pi^*_{\mathcal{M}} \geqslant \log(q^{-d})$, comme annoncé. □

En termes d'un polynôme $L_d(T)$ de la forme (3.1), la minoration ci-dessus est une minoration « de Liouville » : si la valeur spéciale $L^*_d(q^{-1})$ de $L_d(T)$ vérifie les hypothèses de la Section 3.2.1, on a
$$\log |L^*_d(q^{-1})| \geqslant -\log q \cdot \deg L_d(T).$$

Cette minoration est insuffisante pour nos besoins. Pour l'améliorer, nous tenons compte des « simplifications » éventuelles dans le produit $\pi^*_{\mathcal{M}}$: la minoration précédente consiste essentiellement à écrire que

$$\forall m \in \mathcal{M}, \qquad q^{u(m)} \cdot \left(1 - \frac{y(m)}{q^{u(m)}}\right) \in \overline{\mathbb{Z}}.$$

Mais, si l'un des $y(m)$ est « très divisible » par q, le quotient $y(m)/q^{u(m)}$ est « presque » un entier algébrique : nul besoin alors de le multiplier par $q^{u(m)}$ pour obtenir un entier algébrique, une plus petite puissance de q suffit. Le Théorème ci-dessous met en forme cette intuition.

Rappelons que l'on a fixé une fois pour toute un idéal premier $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$ qui est au-dessus de p.

Théorème 3.2.2. *Soit $d \geqslant 2$ un entier premier à p. Pour tout diviseur $d' \geqslant 2$ de d, on notera $\mathfrak{p}'$ l'idéal premier de $\mathbb{Q}(\zeta_{d'})$ qui est en-dessous de $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$. Soit $\mathcal{M} \subset \mathcal{O}'_q(d)$ un ensemble d'orbites et une application $y : \mathcal{O}'_q(d) \to \mathbb{Q}(\zeta_d)$ satisfaisant aux hypothèses de la Section 3.2.1. Pour tout diviseur $d' \geqslant 1$ de d, on pose*

$$\mathcal{M}(d') := \left\{ m \in \mathcal{M} \;\middle|\; \forall i \in m,\ \operatorname{pgcd}(d,i) = \tfrac{d}{d'} \right\}.$$

Alors,

$$\log \pi^*_{\mathcal{M}} \geqslant -\log q \cdot \sum_{d'|d} \left(o_q(d') \cdot \sum_{m \in \mathcal{M}(d')} \max\left\{ 0, 1 - \frac{\operatorname{ord}_{\mathfrak{p}'} y\,(m)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]} \right\} \right). \tag{3.6}$$

Nous démontrons ce Théorème à la sous-section suivante. Remarquons tout d'abord que cette minoration est *a priori* meilleure que celle qui est présentée à la Proposition 3.2.1 car elle tient compte des « simplifications » éventuelles qui se produisent dans les fractions $y(m)/q^{u(m)}$. Ceci étant, la minoration (3.6) ne donne rien de nouveau si l'on ne dispose pas d'informations sur les valuations $\operatorname{ord}_{\mathfrak{p}'} y(m)$. Nous reviendrons sur celles-ci à la Section suivante. De ce Théorème, on tire une version plus faible, mais plus opérationnelle :

Corollaire 3.2.3. *Sous les mêmes hypothèses, on a*

$$\log \pi^*_{\mathcal{M}} \geqslant -\log q \cdot \sum_{d'|d} \left(o_q(d') \cdot \sum_{m' \in (\mathbb{Z}/d'\mathbb{Z})^\times / \langle q \rangle_{d'}} \max\left\{ 0, 1 - \frac{\operatorname{ord}_{\mathfrak{p}'} y\left(\frac{dm'}{d'}\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]} \right\} \right). \tag{3.7}$$

Dans ce Corollaire, la partie minorante ne dépend plus de $\mathcal{M}$ (mais encore de $y : \mathcal{O}'_q(d) \to \mathbb{Q}(\zeta_d)$). Afin de simplifier les notations, pour tout diviseur $d' \geqslant 2$ de d, on pose $G_{d'} = (\mathbb{Z}/d'\mathbb{Z})^\times$ et

$$W'(d') = o_q(d') \cdot \sum_{m' \in G_{d'}/\langle q \rangle_{d'}} \max\left\{ 0, o_q(d') - \frac{\operatorname{ord}_{\mathfrak{p}'} y\left(\frac{dm'}{d'}\right)}{[\mathbb{F}_q : \mathbb{F}_p]} \right\},$$

$W'(1) := 0$ et $W(d) := \sum_{d'|d} W'(d')$. Le Corollaire ci-dessus peut aussi s'écrire sous la forme :

$$\pi^*_{\mathcal{M}} \geqslant \frac{1}{q^{W(d)}}.$$

Remarque 3.2.4. Avec les notations introduites jusqu'à présent, on a

$$0 \leqslant W'(d') \leqslant \#(\mathbb{Z}/d'\mathbb{Z})^\times = \phi(d'),$$

de sorte que $0 \leqslant W(d) \leqslant d$. En effet, pour tout diviseur $d' \geqslant 2$ de d et tout $m' \in G_{d'}/\langle q \rangle_{d'}$, comme $y(m)$ est un entier de $\mathbb{Q}(\zeta_{d'})$, on a

$$0 \leqslant \max\left\{ 0, 1 - \frac{\operatorname{ord}_{\mathfrak{p}'} y\left(\frac{d}{d'}m'\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]} \right\} \leqslant \max\{0,1\} = 1.$$

Il s'ensuit que

$$0 \leqslant W'(d') \leqslant \sum_{m' \in G_{d'}/\langle q \rangle_{d'}} o_q(d') = \#\big(G_{d'}/\langle q \rangle_{d'}\big) \cdot o_q(d') = \frac{\phi(d')}{o_q(d')} \cdot o_q(d') = \phi(d').$$

Et la majoration de $W(d)$ est alors une conséquence de l'identité bien connue $\sum_{d'|d} \phi(d') = d$. En d'autres termes, une *majoration* triviale de $W(d)$ dans le Corollaire 3.2.3 donne la Proposition 3.2.1.

3.2.3 Preuve du Théorème 3.2.2

La preuve se déroule en quatre étapes, que l'on a séparées pour clarifier le raisonnement.

Premier regroupement de termes. Soit $\mathcal{M} \subset \mathcal{O}'_q(d)$ un ensemble d'orbites comme dans l'énoncé du Théorème 3.2.2. Pour tout diviseur d' de d, on pose

$$\mathcal{M}(d') := \left\{ m \in \mathcal{M} \;\middle|\; \forall i \in m,\ \operatorname{pgcd}(d,i) = \tfrac{d}{d'} \right\}.$$

Comme $0 \notin \mathcal{M} \subset \mathcal{O}'_q(d)$, on a $\mathcal{M}(1) = \varnothing$. On a clairement

$$\mathcal{M} = \bigsqcup_{\substack{d' \mid d \\ d' \geqslant 2}} \mathcal{M}(d') = \bigsqcup_{d' \mid d} \mathcal{M}(d'). \tag{3.8}$$

On a déjà mentionné le fait que l'on peut aussi écrire $\mathcal{M}(d')$ sous la forme $\frac{d}{d'} \cdot \mathcal{P}(d')$ où $\mathcal{P}(d')$ est une partie du *groupe* quotient $(\mathbb{Z}/d'\mathbb{Z})^\times / \langle q \rangle_{d'}$ (ce groupe est d'ordre $\#(\mathbb{Z}/d'\mathbb{Z})^\times / \langle q \rangle_{d'} = \phi(d')/o_q(d')$). On en déduit une seconde version de la partition (3.8) :

$$\mathcal{M} = \bigsqcup_{\substack{d' \mid d \\ d' \geqslant 2}} \frac{d}{d'} \cdot \mathcal{P}(d') = \bigsqcup_{d' \mid d} \frac{d}{d'} \cdot \mathcal{P}(d').$$

De plus, pour tout $m \in \mathcal{M}(d')$, l'entier $u(m)$ vaut $u(m) = \operatorname{ord}^\times \left(q \bmod (d/\operatorname{pgcd}(d,m)) \right) = o_q(d')$. La partition (3.8) permet alors d'écrire

$$\pi^*_{\mathcal{M}} = \prod_{m \in \mathcal{M}} \left(1 - \frac{y(m)}{q^{u(m)}}\right) = \prod_{d' \mid d} \left(\prod_{m \in \mathcal{M}(d')} \left(1 - \frac{y(m)}{q^{u(m)}}\right) \right) = \prod_{d' \mid d} \left(\prod_{m \in \mathcal{M}(d')} \left(1 - \frac{y(m)}{q^{o_q(d')}}\right) \right).$$

Sur ce, on démontre :

Lemme 3.2.5. *Pour chaque diviseur $d' \geqslant 2$ de d, sous les hypothèses* (i), (ii) *et* (iii) *de la Section 3.2.1, le produit*

$$\pi_{\mathcal{M}}(d') := \prod_{m \in \mathcal{M}(d')} \left(1 - \frac{y(m)}{q^{u(m)}}\right)$$

est rationnel et non nul.

Démonstration. Posons $x(m) = 1 - y(m)/q^{u(m)}$ pour tout $m \in \mathcal{M}$. A priori, par hypothèse (i), le produit $\pi_{\mathcal{M}}(d')$ est un élément de $\mathbb{Q}(\zeta_{d'}) \subset L = \mathbb{Q}(\zeta_d)$. Pour qu'il soit rationnel, il faut et il suffit que $\pi_{\mathcal{M}}(d')$ soit invariant par tous les automorphismes de $\operatorname{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/d\mathbb{Z})^\times$. Or, pour tout $t \in (\mathbb{Z}/d\mathbb{Z})^\times$, on a

$$\sigma_t\big(\pi_{\mathcal{M}}(d')\big) = \prod_{m \in \mathcal{M}(d')} \sigma_t\big(x(m)\big) = \prod_{m \in \mathcal{M}(d')} x(t \cdot m) = \prod_{n \in t \cdot \mathcal{M}(d')} x(n).$$

Il s'agit donc de montrer que $\mathcal{M}(d') \subset \mathcal{O}'_q(d)$ est stable par l'action de la multiplication par $(\mathbb{Z}/d\mathbb{Z})^\times$. Par hypothèse (iii), le produit $\pi^*_{\mathcal{M}} = \prod_{m \in \mathcal{M}} x(m)$ est rationnel et donc, par le même calcul que ci-dessus, l'ensemble $\mathcal{M}$ est stable par $(\mathbb{Z}/d\mathbb{Z})^\times$. Si maintenant $m \in \mathcal{M}(d')$, pour tout $t \in (\mathbb{Z}/d\mathbb{Z})^\times$ on a $t \cdot m \in \mathcal{M}$ et, comme t est premier à d,

$$\forall i \in m, \quad \operatorname{pgcd}(d, t \cdot m) = \operatorname{pgcd}(d, t \cdot i) = \operatorname{pgcd}(d,i) = \operatorname{pgcd}(d,m) = \frac{d}{d'}.$$

Donc $\mathcal{M}(d') \subset \mathcal{M}$ est aussi stable par $(\mathbb{Z}/d\mathbb{Z})^\times$ et $\sigma_t\big(\pi_{\mathcal{M}}(d')\big) = \pi_{\mathcal{M}}(d')$ pour tout $t \in (\mathbb{Z}/d\mathbb{Z})^\times$. Ce qui démontre la rationalité de $\pi_{\mathcal{M}}(d')$. □

Le lemme ci-dessus montre donc que, pour prouver le Théorème 3.2.2, il suffit d'étudier les produits $\pi_{\mathcal{M}}(d')$ pour tous les diviseurs $d' \geqslant 2$ de d. Noter que le produit $\pi_{\mathcal{M}}(1)$ vaut 1.

Norme de $1 - y(m)/q^{u(m)}$. Soit $d' \geqslant 2$ un diviseur de d et $m \in \mathcal{M}(d')$. Alors, par hypothèse (i), on a $y(m) \in \mathbb{Q}(\zeta_{d'})$. De plus, $u(m) = o_q(d')$ ne dépend pas de $m \in \mathcal{M}(d')$.

Lemme 3.2.6. *Soit $d' \geqslant 2$ un diviseur de d. On écrit $Q = q^{o_q(d')}$ sous la forme $Q = p^{v'}$ (avec $v' \in \mathbb{N}^*$) et l'on note $G_{d'} = (\mathbb{Z}/d'\mathbb{Z})^\times$ ainsi que $\langle p \rangle_{d'}$ le sous-groupe de $G_{d'}$ engendré par p. Sous les hypothèses et notations de la Section 3.2.1, pour tout $m \in \mathcal{M}(d')$, on a*

$$\log \mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}} \left(1 - \frac{y(m)}{q^{o_q(d')}}\right) \geqslant -\log p \cdot \left(o_p(d') \cdot \sum_{t \in G_{d'}/\langle p \rangle_{d'}} \max\{0, v' - \operatorname{ord}_{\mathfrak{p}'} y(t \cdot m)\} \right), \tag{3.9}$$

où le terme entre parenthèses est un entier positif.

Ce Lemme est l'outil qui nous permet de tenir compte des « simplifications » éventuelles évoquées sous l'énoncé du Théorème 3.2.2.

Démonstration. Le raisonnement est très proche de l'esprit de la preuve de [Shi87, Proposition 2.1]. Commençons par écrire la décomposition en produit d'idéaux premiers de l'idéal (entier) engendré par $Q = p^{v'}$ dans $\mathbb{Z}[\zeta_{d'}]$: elle se déduit de celle de $p \cdot \mathbb{Z}[\zeta_{d'}]$ (*cf.* [IR90, Chap. 13, §2, Theorem 2]). Comme p ne divise pas d', on a

$$Q \cdot \mathbb{Z}[\zeta_{d'}] = p^{v'} \cdot \mathbb{Z}[\zeta_{d'}] = \mathfrak{p}_1^{v'} \cdot \mathfrak{p}_2^{v'} \cdot \cdots \cdot \mathfrak{p}_{g'}^{v'},$$

où les idéaux premiers $\mathfrak{p}_i$ sont distincts, de degré résiduel $o_p(d')$ (en d'autres termes, $\mathbf{N}\mathfrak{p}_i = p^{o_p(d')}$) et $g' = \phi(d')/o_p(d')$. Quitte à renuméroter les $\mathfrak{p}_i$, on peut en outre supposer que $\mathfrak{p}_1 = \mathfrak{p}'$ est l'idéal au-dessous de $\widetilde{\mathfrak{P}}$. Rappelons que le sous-groupe de décomposition $D_{\mathfrak{p}'/p}$ de $\mathfrak{p}'$ au-dessus de p est isomorphe à $\langle p \rangle_{d'}$ dans l'isomorphisme $\mathrm{Gal}(K_{d'}/\mathbb{Q}) \simeq (\mathbb{Z}/d'\mathbb{Z})^\times$ et que le quotient $\mathrm{Gal}(K_{d'}/\mathbb{Q})/D_{\mathfrak{p}'/p}$ agit transitivement sur $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_{g'}\}$. En d'autres termes, une fois choisis des représentants $t_1 = 1$, $t_2, \ldots, t_g \in (\mathbb{Z}/d\mathbb{Z})^\times$ du quotient $(\mathbb{Z}/d'\mathbb{Z})^\times/\langle p \rangle_{d'}$, on peut numéroter les $\mathfrak{p}_i$ de sorte que $\mathfrak{p}_i = \sigma_{t_i}^{-1}(\mathfrak{p}')$ où $\sigma_{t_i} \in \mathrm{Gal}(K_{d'}/\mathbb{Q}) \simeq (\mathbb{Z}/d'\mathbb{Z})^\times$.

De façon similaire, écrivons la décomposition de l'idéal entier engendré par $y(m) \in \mathbb{Z}[\zeta_{d'}]$ sous la forme suivante :

$$y(m) \cdot \mathbb{Z}[\zeta_{d'}] = \mathfrak{p}_1^{\operatorname{ord}_{\mathfrak{p}_1} y(m)} \cdot \mathfrak{p}_2^{\operatorname{ord}_{\mathfrak{p}_2} y(m)} \cdot \cdots \cdot \mathfrak{p}_{g'}^{\operatorname{ord}_{\mathfrak{p}_{g'}} y(m)} \cdot \mathcal{Y}_m,$$

où $\mathcal{Y}_m$ est un idéal entier de $\mathbb{Z}[\zeta_{d'}]$ qui est premier aux $\mathfrak{p}_i$. Si $i \in [\![1, g']\!]$, on a (par hypothèse (ii)),

$$\operatorname{ord}_{\mathfrak{p}_i} y(m) = \operatorname{ord}_{\sigma_{t_i}^{-1}\mathfrak{p}'} y(m) = \operatorname{ord}_{\mathfrak{p}'} \sigma_{t_i}(y(m)) = \operatorname{ord}_{\mathfrak{p}'} y(t_i \cdot m).$$

Posons alors $\mathcal{I}_m \subset \mathbb{Z}[\zeta_{d'}]$, l'idéal entier défini par

$$\mathcal{I}_m := \prod_{i=1}^{g'} \mathfrak{p}_i^{\min\{v', \operatorname{ord}_{\mathfrak{p}_i} y(m)\}} = \prod_{i=1}^{g'} \mathfrak{p}_i^{\min\{v', \operatorname{ord}_{\mathfrak{p}'} y(t_i \cdot m)\}}.$$

Par construction, cet idéal divise l'idéal entier engendré par $Q - y(m)$ dans $\mathbb{Q}(\zeta_{d'})$. En particulier, la norme idéale de $\mathcal{I}_m$ divise, dans $\mathbb{Z}$, la norme de $Q - y(m)$. Par hypothèse (iii), $y(m) \neq Q = q^{u(m)}$ pour $m \in \mathcal{M}$. Il existe donc un entier $b_m \in \mathbb{N}^*$ tel que

$$\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}} \left(1 - \frac{y(m)}{Q}\right) = \frac{\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(Q - y(m))}{\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(Q)} = \frac{b_m \cdot \mathbf{N}\mathcal{I}_m}{\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(Q)} = \frac{b_m}{\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(Q) \cdot (\mathbf{N}\mathcal{I}_m)^{-1}}.$$

Mais, puisque la norme est multiplicative et que les idéaux $\mathfrak{p}_i$ ont tous la même norme $\mathbf{N}\mathfrak{p}_i = \mathbf{N}\mathfrak{p}' = p^{o_p(d')}$, on a

$$\begin{aligned} \mathbf{N}\mathcal{I}_m &= \mathbf{N}\left(\prod_{i=1}^{g'} \mathfrak{p}_i^{\min\{v', \operatorname{ord}_{\mathfrak{p}'} y(t_i \cdot m)\}} \right) = \prod_{i=1}^{g'} (\mathbf{N}\mathfrak{p}_i)^{\min\{v', \operatorname{ord}_{\mathfrak{p}'} y(t_i \cdot m)\}} \\ &= (\mathbf{N}\mathfrak{p}')^{\sum_{i=1}^{g'} \min\{v', \operatorname{ord}_{\mathfrak{p}'} y(t_i \cdot m)\}} = p^{o_p(d') \cdot \sum_{i=1}^{g'} \min\{v', \operatorname{ord}_{\mathfrak{p}'} y(t_i \cdot m)\}}. \end{aligned}$$

Or, comme $Q = p^{v'}$ est un entier, sa norme est aisée à calculer : $\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(Q) = Q^{[\mathbb{Q}(\zeta_{d'}):\mathbb{Q}]} = p^{v' \cdot \phi(d')}$. Ainsi,

$$\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(Q) \cdot (\mathbf{N}\mathcal{I}_m)^{-1} = p^{v'\phi(d')} \cdot p^{-o_p(d') \cdot \sum_{i=1}^{g'} \min\{v', \operatorname{ord}_{\mathfrak{p}'} y(t_i \cdot m)\}}.$$

D'où l'on tire que

$$\log \mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}\left(1-\frac{y(m)}{Q}\right) = \log\left(\frac{b_m}{\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(Q)\cdot(\mathbf{N}\mathcal{I}_m)^{-1}}\right) = \log b_m - \log\left(\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(Q)\cdot(\mathbf{N}\mathcal{I}_m)^{-1}\right)$$
$$\geqslant 0 - \log p\cdot\left(v'\phi(d') - o_p(d')\cdot\sum_{i=1}^{g'}\min\left\{v', \operatorname{ord}_{\mathfrak{p}'} y(t_i\cdot m)\right\}\right) = -\log p\cdot e(m).$$

Où l'on a appelé $e(m)\in\mathbb{Z}$ le terme entre parenthèses. Il ne reste qu'à écrire $e(m)$ sous la forme souhaitée : en remarquant que $g' = \phi(d')/o_p(d')$, on déduit que

$$\begin{aligned}
e(m) &= v'\phi(d') - o_p(d')\cdot\sum_{i=1}^{g'}\min\left\{v', \operatorname{ord}_{\mathfrak{p}'} y(t_i\cdot m)\right\}\\
&= v'o_p(d')\cdot g' - o_p(d')\cdot\sum_{i=1}^{g'}\min\left\{v', \operatorname{ord}_{\mathfrak{p}'} y(t_i\cdot m)\right\}\\
&= o_p(d')\cdot\sum_{i=1}^{g'}\left(v' - \min\left\{v', \operatorname{ord}_{\mathfrak{p}'} y(t_i\cdot m)\right\}\right) = o_p(d')\cdot\sum_{i=1}^{g'}\left(v' + \max\left\{-v', -\operatorname{ord}_{\mathfrak{p}'} y(t_i\cdot m)\right\}\right)\\
&= o_p(d')\cdot\sum_{i=1}^{g'}\max\left\{0, v' - \operatorname{ord}_{\mathfrak{p}'} y(t_i\cdot m)\right\} = o_p(d')\cdot\sum_{t\in(\mathbb{Z}/d'\mathbb{Z})^\times/\langle p\rangle_{d'}}\max\left\{0, v' - \operatorname{ord}_{\mathfrak{p}'} y(t\cdot m)\right\},
\end{aligned}$$

la dernière égalité venant du choix des $t_i\in(\mathbb{Z}/d'\mathbb{Z})^\times$. Ce qui conclut la preuve du Lemme. □

Minoration à $d'\mid d$ donné. En combinant les résultats des Lemmes 3.2.5 et 3.2.6, on obtient le Lemme ci-dessous. On se place toujours sous les hypothèses de la Section 3.2.1.

Lemme 3.2.7. *Soit $d'\geqslant 2$ un diviseur de d. On a*

$$\log|\pi_{\mathcal{M}}(d')| \geqslant -\log q\cdot\left(\sum_{m\in\mathcal{M}(d')}\max\left\{0, o_q(d') - \frac{\operatorname{ord}_{\mathfrak{p}'} y(m)}{[\mathbb{F}_q:\mathbb{F}_p]}\right\}\right). \tag{3.10}$$

Démonstration. Comme on l'a vu au Lemme 3.2.5, le produit $\pi_{\mathcal{M}}(d')$ (*a priori* un élément de $\mathbb{Q}(\zeta_{d'})$) est rationnel et non nul. Par suite, on a $\mathbf{N}_{Q(\zeta_{d'})/\mathbb{Q}}(\pi_{\mathcal{M}}(d')) = \left(\pi_{\mathcal{M}}(d')\right)^{[\mathbb{Q}(\zeta_{d'}):\mathbb{Q}]} = \left(\pi_{\mathcal{M}}(d')\right)^{\phi(d')}$. D'autre part,

$$\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(\pi_{\mathcal{M}}(d')) = \prod_{m\in\mathcal{M}(d')}\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}\left(1-\frac{y(m)}{q^{u(m)}}\right) = \prod_{m\in\mathcal{M}(d')}\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}\left(1-\frac{y(m)}{q^{o_q(d')}}\right).$$

Nous pouvons alors utiliser le Lemme 3.2.6 pour minorer le logarithme de chacun des termes de ce produit. On obtient :

$$\begin{aligned}
\log|\pi_{\mathcal{M}}(d')| &= \frac{1}{\phi(d')}\log\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}(\pi_{\mathcal{M}}(d')) = \frac{1}{\phi(d')}\sum_{m\in\mathcal{M}(d')}\log\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}\left(1-\frac{y(m)}{q^{o_q(d')}}\right)\\
&\geqslant -\log p\cdot\left(\frac{o_p(d')}{\phi(d')}\sum_{m\in\mathcal{M}(d')}\sum_{t\in(\mathbb{Z}/d'\mathbb{Z})^\times/\langle p\rangle_{d'}}\max\{0, v' - \operatorname{ord}_{\mathfrak{p}'} y(t\cdot m)\}\right)\\
&= -\log p\cdot\left(\frac{o_p(d')}{\phi(d')}\sum_{t\in(\mathbb{Z}/d'\mathbb{Z})^\times/\langle p\rangle_{d'}}\sum_{m\in\mathcal{M}(d')}\max\{0, v' - \operatorname{ord}_{\mathfrak{p}'} y(t\cdot m)\}\right).
\end{aligned}$$

Or, pour tout $t\in(\mathbb{Z}/d'\mathbb{Z})^\times$, comme $\mathcal{M}(d')$ est stable sous la multiplication par $(\mathbb{Z}/d'\mathbb{Z})^\times$, on a

$$\sum_{m\in\mathcal{M}(d')}\max\{0, v' - \operatorname{ord}_{\mathfrak{p}'} y(t\cdot m)\} = \sum_{m\in\mathcal{M}(d')}\max\{0, v' - \operatorname{ord}_{\mathfrak{p}'} y(m)\}.$$

Mais $\#\left((\mathbb{Z}/d'\mathbb{Z})^\times/\langle p\rangle_{d'}\right) = \phi(d')/o_p(d')$, on trouve donc que

$$\log|\pi_{\mathcal{M}}(d')| \geqslant -\log p\cdot\left(\sum_{m\in\mathcal{M}(d')}\max\{0, v' - \operatorname{ord}_{\mathfrak{p}'} y(m)\}\right).$$

Rappelons maintenant que $Q = q^{o_q(d')}$ s'écrit $Q = p^{v'}$ et que, par ailleurs, $q = p^{[\mathbb{F}_q:\mathbb{F}_p]}$. On a donc $v' = [\mathbb{F}_q : \mathbb{F}_p] \cdot o_q(d')$. Ceci permet d'écrire la dernière minoration sous la forme

$$\log|\pi_{\mathcal{M}}(d')| \geqslant -\log q \cdot \left(\sum_{m \in \mathcal{M}(d')} \max\left\{0, o_q(d') - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y(m)}{[\mathbb{F}_q : \mathbb{F}_p]}\right\}\right). \tag{3.11}$$

Ce qu'il fallait démontrer. □

Remarque 3.2.8. Tous les termes de la somme entre parenthèses dans (3.11) sont des entiers positifs. Comme on l'a vu plus haut, l'ensemble $\mathcal{M}(d')$ s'écrit $\frac{d}{d'} \cdot \mathcal{P}(d')$ où $\mathcal{P}(d')$ est une partie de $(\mathbb{Z}/d'\mathbb{Z})^\times/\langle q\rangle_{d'}$. On peut alors majorer le terme sommatoire de (3.11) par

$$\begin{aligned}
\sum_{m \in \mathcal{M}(d')} \max\left\{0, o_q(d') - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y(m)}{[\mathbb{F}_q : \mathbb{F}_p]}\right\} &= o_q(d') \cdot \sum_{m \in \frac{d}{d'}\cdot\mathcal{P}(d')} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y(m)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\} \\
&= o_q(d') \cdot \sum_{m' \in \mathcal{P}(d')} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{d}{d'} \cdot m'\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\} \\
&\leqslant o_q(d') \cdot \sum_{m' \in (\mathbb{Z}/d'\mathbb{Z})^\times/\langle q\rangle_{d'}} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{d}{d'} \cdot m'\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\}.
\end{aligned}$$

C'est cette version qui nous sera la plus utile en pratique.

Conclusion. Revenons à présent au produit $\pi^*_{\mathcal{M}}$ que nous souhaitons minorer. D'après la partition (3.8) et le Lemme 3.2.7, on a

$$\begin{aligned}
\log(\pi^*_{\mathcal{M}}) = \log \prod_{d'|d} |\pi_{\mathcal{M}}(d')| &= \sum_{d'|d} \log|\pi_{\mathcal{M}}(d')| \\
&\geqslant -\log q \cdot \sum_{d'|d} \left(o_q(d') \cdot \sum_{m \in \mathcal{M}(d')} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y(m)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\}\right) \\
&= -\log q \cdot \sum_{d'|d} \left(o_q(d') \cdot \sum_{m' \in \mathcal{P}(d')} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{dm'}{d'}\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\}\right).
\end{aligned}$$

C'est la minoration annoncée dans le Théorème. D'où l'on tire aussi la minoration plus faible du Corollaire 3.2.3 (avec la Remarque 3.2.8) : puisque $\mathcal{P}(d') \subset (\mathbb{Z}/d'\mathbb{Z})^\times/\langle q\rangle_{d'}$, on a

$$\begin{aligned}
\log(\pi^*_{\mathcal{M}}) &\geqslant -\log q \cdot \sum_{d'|d} \left(o_q(d') \cdot \sum_{m' \in \mathcal{P}(d')} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{dm'}{d'}\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\}\right) \\
&\geqslant -\log q \cdot \sum_{d'|d} \left(o_q(d') \cdot \sum_{m' \in (\mathbb{Z}/d'\mathbb{Z})^\times/\langle q\rangle_{d'}} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{dm'}{d'}\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\}\right).
\end{aligned}$$

Ceci achève la preuve du Théorème 3.2.2 et de son Corollaire.

3.3 Décomposition primaire des sommes de Jacobi

Dans le Théorème 3.2.2, on voit apparaître la nécessité de connaître suffisamment explicitement les valuations $\mathfrak{p}'$-adiques des entiers algébriques $y(m)$. Nous explicitons celles-ci dans le présent paragraphe lorsque $y(m)$ est une somme de Jacobi (ou un produit de telles sommes). Nous nous plaçons ici dans une généralité légèrement plus grande que nécessaire.

3.3.1 Rappels sur le Théorème de Stickelberger

Dans ce paragraphe, nous rappelons l'énoncé du théorème de Stickelberger (Théorème 3.3.3) sur les sommes de Gauss. Nous prenons soin de conserver les mêmes conventions qu'à la Section 2.2.

Rappelons que pour tout corps fini $\mathbb{F}_q$ et tout caractère $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$, on a défini (Définition 2.2.4) la somme de Gauss associée à χ par

$$\mathbf{g}_q(\chi) := -\sum_{x\in\mathbb{F}_q^\times} \chi(x)\psi_q(x),$$

où $\psi_q = \mathbb{F}_q \to \overline{\mathbb{Q}}^\times$ est le caractère additif standard de $\mathbb{F}_q$. Par ailleurs, à la Section 2.1.2, on a fixé un idéal premier $\mathfrak{P}$ de l'anneau des entiers $\overline{\mathbb{Z}}$ de $\overline{\mathbb{Q}}$ au-dessus de p. Ce choix nous a permis de définir un caractère $\mathbf{t} : \overline{\mathbb{F}_p}^\times \to \overline{\mathbb{Q}}^\times$ dont la restriction à toute extension finie $\mathbb{F}_q/\mathbb{F}_p$ engendre le groupe des caractères $\widehat{\mathbb{F}_q^\times}$.

Définition 3.3.1. Soit à nouveau $\mathbb{F}_q$ un corps fini de caractéristique p impaire et $d' \geqslant 2$ un entier premier à p, écrivons $Q = q^{o_q(d')}$. Par définition, Q est la plus petite puissance q^ν de q telle que $d' \mid q^\nu - 1$. Autrement dit, $\mathbb{F}_Q$ est la plus petite extension de $\mathbb{F}_q$ contenant les racines d'-ièmes de l'unité : $\mathbb{F}_Q = \mathbb{F}_q(\mu_{d'})$. $\boldsymbol{\omega} : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ le caractère donné par

$$\boldsymbol{\omega} : x \in \mathbb{F}_Q^\times \mapsto \mathbf{t}(x)^{(Q-1)/d'}.$$

Le caractère $\boldsymbol{\omega}$ est un caractère d'ordre exactement d' (*cf.* Section 2.1.3). Alors le sous-groupe de $\widehat{\mathbb{F}_Q^\times}$ formé des caractères d'ordre divisant d' est exactement $\{\boldsymbol{\omega}^a,\ a \in \mathbb{Z}/d'\mathbb{Z}\smallsetminus\{0\}\}$. Pour tout $a \in \mathbb{Z}/d'\mathbb{Z}$, la somme de Gauss $\mathbf{g}_Q(\boldsymbol{\omega}^a)$ est bien définie et c'est un entier algébrique du corps cyclotomique $\mathbb{Q}(\zeta_p, \zeta_{d'}) = \mathbb{Q}(\zeta_{pd'})$. Remarquons que $\boldsymbol{\omega}^a$ est le caractère trivial si et seulement si $a \equiv 0 \bmod d'$; et notons également que $\mathbf{g}_Q(\boldsymbol{\omega}^{q\cdot a}) = \mathbf{g}_Q(\boldsymbol{\omega}^{q\cdot a})$ (car $x \mapsto x^q$ est une bijection de $\mathbb{F}_Q^\times$).

Remarque 3.3.2. Faisons le lien entre $\boldsymbol{\omega}$ et les caractères $\mathbf{t}_m$ introduits à la Section 2.1.3. Si $m \in [\![1, d-1]\!]$, on a défini $d_m = d/\operatorname{pgcd}(d,m)$ et $u(m) = \operatorname{ord}^\times(q \bmod d_m) = o_q(d_m)$. De plus, le caractère $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ y a été défini par :

$$\forall x \in \mathbb{F}_{q^{u(m)}}, \qquad \mathbf{t}_m(x) = \mathbf{t}(x)^{(q^{u(m)}-1)m/d}.$$

Comme on l'a vu, l'ordre de $\mathbf{t}_m$ est exactement d_m (Propriété 2.1.5). On pose alors $d' = d_m$ et $m' = m/\operatorname{pgcd}(d,m)$ de sorte que $\frac{d}{d'}m' = m$ et m' est premier à d'. Notons $\boldsymbol{\omega} : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ le caractère associé à $d' = d_m$ à la Définition 3.3.1. On a

$$\mathbf{t}_m = \mathbf{t}^{(q^{u(m)}-1)m/d} = \mathbf{t}^{(q^{u(m)}-1)m'/d'} = \boldsymbol{\omega}^{m'}.$$

Ceci étant dit, on peut maintenant rappeler l'énoncé suivant :

Théorème 3.3.3 (Stickelberger)**.** *Soit $d' \geqslant 2$ un entier premier à q. On note $\wp$ l'unique idéal premier de $\mathbb{Q}(\zeta_p, \zeta_{d'}) = \mathbb{Q}(\zeta_{pd'})$ qui est au-dessous de $\mathfrak{P} \subset \overline{\mathbb{Z}}$ (cf. Section 2.1.2). On écrit aussi $Q = q^{o_q(d')}$ sous la forme $Q = p^v$ ($v \in \mathbb{N}^*$). Pour tout $a \in \mathbb{Z}/d'\mathbb{Z}\smallsetminus\{0\}$, on a*

$$\operatorname{ord}_\wp \mathbf{g}_Q(\boldsymbol{\omega}^a) = (p-1)\cdot\sum_{j=0}^{v-1}\left\{\frac{-ap^j}{d'}\right\}. \tag{3.12}$$

Démonstration. Voir [Sti90] pour l'article original, [IR90, Chap. 14, §3-4], [Was97, Chap. 6], [Coh07, Chap. 3, §6] pour des preuves plus modernes et [Lan94, Chap. IV, §3] pour une démonstration concise. Noter toutefois que notre normalisation des sommes de Gauss peut différer de celles utilisées dans les références citées. En particulier, l'objet que nous notons $\mathbf{g}_Q(\boldsymbol{\omega}^a)$ est plutôt noté $-\mathbf{g}_Q(\boldsymbol{\omega}^a)$ dans [IR90]. Quant à [Was97], le caractère trivial $\mathbf{1}$ y est prolongé par $\mathbf{1}(0) = 0$. □

Remarque 3.3.4. Sous les hypothèses du Théorème, la somme de Gauss $\mathbf{g}_Q(\boldsymbol{\omega}^a)$ est un entier de $\mathbb{Q}(\zeta_p, \zeta_{d'})$: en particulier, sa valuation $\wp$-adique est un entier naturel. Il n'est pas totalement évident que l'expression du membre de droite de (3.12) soit entière (c'est une somme de parties fractionnaires !). Reprenant les notations de l'énoncé, on pose $A = -a(Q-1)/d'$. Comme d' divise $Q-1$, on a $A \in \mathbb{Z}$

et $\left\{\frac{-ap^j}{d'}\right\} = \left\{\frac{Ap^j}{Q-1}\right\}$ pour tout $j \in [\![0, v-1]\!]$. Alors

$$\begin{aligned}(p-1)\cdot\sum_{j=0}^{v-1}\left\{\frac{-ap^j}{d'}\right\} &= (p-1)\cdot\sum_{j=0}^{v-1}\left\{\frac{Ap^j}{Q-1}\right\} = (p-1)\cdot\sum_{j=0}^{v-1}\left(\frac{Ap^j}{Q-1} - \left\lfloor\frac{Ap^j}{Q-1}\right\rfloor\right)\\ &= (p-1)\cdot\frac{A}{Q-1}\cdot\sum_{j=0}^{v-1}p^j - (p-1)\cdot\sum_{j=0}^{v-1}\left\lfloor\frac{Ap^j}{Q-1}\right\rfloor\\ &= A - (p-1)\cdot\sum_{j=0}^{v-1}\left\lfloor\frac{Ap^j}{Q-1}\right\rfloor.\end{aligned}$$

D'où l'on tire l'expression suivante de $\mathrm{ord}_\wp \mathbf{g}_Q(\boldsymbol{\omega}^a)$:

$$\mathrm{ord}_\wp \mathbf{g}_Q(\boldsymbol{\omega}^a) = \frac{-a(Q-1)}{d'} - (p-1)\cdot\sum_{j=0}^{v-1}\left\lfloor\frac{-ap^j}{d'}\right\rfloor, \tag{3.13}$$

dont le membre de droite est clairement un entier. Par ailleurs, sur l'expression (3.12) de $\mathrm{ord}_\wp \mathbf{g}_Q(\boldsymbol{\omega}^a)$, on constate (par définition de la partie fractionnaire) que

$$0 \leqslant \mathrm{ord}_\wp \mathbf{g}_Q(\boldsymbol{\omega}^a) \leqslant (p-1)\cdot v = (p-1)\cdot[\mathbb{F}_Q : \mathbb{F}_p]. \tag{3.14}$$

3.3.2 Valuation $\mathfrak{p}$-adique des sommes de Jacobi

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. Soit $d' \geqslant 2$ un entier premier à q. On pose à nouveau $Q = q^{o_q(d')}$ et on note encore $\boldsymbol{\omega} : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ le caractère d'ordre exactement d' défini au paragraphe précédent (Définition 3.3.1). Il sera commode d'utiliser les notations ci-dessous :

Définition 3.3.5. Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. Soit $d' \geqslant 2$ un entier premier à q. On notera

$$\mathfrak{A}^n(d') := \left\{\mathbf{a} = (a_0, a_1, \ldots, a_n, a_{n+1}) \in (\mathbb{Z}/d'\mathbb{Z})^{n+2} \;\middle|\; \forall i,\ a_i \neq 0 \text{ et } \textstyle\sum_{i=0}^{n+1} a_i = 0\right\}.$$

Pour tout $\mathbf{a} = (a_0, \ldots, a_{n+1}) \in \mathfrak{A}^n(d')$, on pose alors

$$\mathbf{J}_Q(\mathbf{a}) = \boldsymbol{\omega}^{-a_{n+1}}(-1)\cdot\mathbf{j}_Q(\boldsymbol{\omega}^{a_0}, \boldsymbol{\omega}^{a_1}, \ldots, \boldsymbol{\omega}^{a_n}).$$

Lorsque l'on considère une somme de Jacobi $\mathbf{j}_Q(\boldsymbol{\omega}^{a_0}, \boldsymbol{\omega}^{a_1}, \ldots, \boldsymbol{\omega}^{a_n})$ (avec $\mathbf{a} \in \mathfrak{A}^n(d')$), on peut toujours supposer que $\mathrm{pgcd}(d', a_0, \ldots, a_{n+1}) = 1$. Si ce n'est pas le cas, *i.e.* si $\delta = \mathrm{pgcd}(d, a_0, \ldots, a_{n+1}) \geqslant 2$, on peut remplacer $\mathbf{a}$ par $\mathbf{a}_r = \left(\frac{a_0}{\delta}, \frac{a_1}{\delta}, \ldots, \frac{a_{n+1}}{\delta}\right)$. Alors, $\mathbf{a}_r$ est un élément de $\mathfrak{A}^n(d'/\delta)$ avec $\mathrm{pgcd}\left(\frac{d'}{\delta}, \frac{a_0}{\delta}, \frac{a_1}{\delta}, \ldots, \frac{a_{n+1}}{\delta}\right) = 1$.

Remarque 3.3.6. Il convient de commenter l'apparition du facteur « $\boldsymbol{\omega}^{-a_{n+1}}(-1)$ ». Celui-ci intervient pour deux raisons. D'une part $\boldsymbol{\omega}^{-a_{n+1}}(-1)$ est une racine de l'unité dans $\mathbb{Q}(\zeta_{d'})$, en particulier il ne contribue pas à la valuation $\mathfrak{p}'$-adique de $\mathbf{J}_Q(\mathbf{a})$ (Théorème 3.3.7).

D'autre part, il permet d'obtenir une expression « symétrique » en les a_i de $\mathbf{J}_Q(\mathbf{a})$. Plus précisément, si $\mathbf{a} \in \mathfrak{A}^n(d')$ alors d' ne divise aucun des a_i ($i = 0, 1, \ldots, n, n+1$) : c'est donc que les caractères $\boldsymbol{\omega}^{a_0}, \boldsymbol{\omega}^{a_1}, \ldots, \boldsymbol{\omega}^{a_n}$ ne sont pas triviaux et que $\boldsymbol{\omega}^{a_0}\cdot\boldsymbol{\omega}^{a_1}\cdot\cdots\cdot\boldsymbol{\omega}^{a_n} = \boldsymbol{\omega}^{a_0+a_1+\cdots+a_n} = \boldsymbol{\omega}^{-a_{n+1}}$ n'est pas non plus trivial. La Proposition 2.2.7 permet alors d'écrire :

$$\mathbf{j}_Q(\boldsymbol{\omega}^{a_0}, \boldsymbol{\omega}^{a_1}, \ldots, \boldsymbol{\omega}^{a_n}) = \mathbf{g}_Q(\boldsymbol{\omega}^{a_0})\cdot\mathbf{g}_Q(\boldsymbol{\omega}^{a_1})\cdot\cdots\cdot\mathbf{g}_Q(\boldsymbol{\omega}^{a_n})\cdot\mathbf{g}_Q(\boldsymbol{\omega}^{-a_{n+1}})^{-1}.$$

D'autre part, la Proposition 2.2.5 donne la relation suivante :

$$\frac{1}{\mathbf{g}_Q(\boldsymbol{\omega}^{-a_{n+1}})} = \frac{\overline{\mathbf{g}_Q(\boldsymbol{\omega}^{-a_{n+1}})}}{|\mathbf{g}_Q(\boldsymbol{\omega}^{-a_{n+1}})|^2} = \frac{\boldsymbol{\omega}^{a_{n+1}}(-1)\cdot\mathbf{g}_Q(\boldsymbol{\omega}^{a_{n+1}})}{Q}.$$

D'où l'on tire finalement l'expression « symétrique » annoncée :

$$\begin{aligned}\mathbf{J}_Q(\mathbf{a}) &= \boldsymbol{\omega}^{-a_{n+1}}(-1)\mathbf{j}_Q(\boldsymbol{\omega}^{a_0}, \boldsymbol{\omega}^{a_1}, \ldots, \boldsymbol{\omega}^{a_n})\\ &= \frac{1}{Q}\cdot\mathbf{g}_Q(\boldsymbol{\omega}^{a_0})\cdot\mathbf{g}_Q(\boldsymbol{\omega}^{a_1})\cdot\cdots\cdot\mathbf{g}_Q(\boldsymbol{\omega}^{a_n})\cdot\mathbf{g}_Q(\boldsymbol{\omega}^{a_{n+1}}).\end{aligned} \tag{3.15}$$

Avec ces notations, on déduit du Théorème de Stickelberger ci-dessus une expression de la valuation $\mathfrak{p}'$-adique des sommes de Jacobi :

Théorème 3.3.7 (Stickelberger). *Soit $d' \geqslant 2$ un entier premier à q. On note $\mathfrak{p}'$ l'unique idéal premier de $\mathbb{Q}(\zeta_{d'})$ au-dessous de $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$. À nouveau, on écrit $Q = q^{o_q(d')} = p^v$. Soit $n \in \mathbb{N}^*$ et $\mathbf{a} \in \mathfrak{A}^n(d')$, on a :*

$$\operatorname{ord}_{\mathfrak{p}} \mathbf{J}_Q(\mathbf{a}) = \sum_{j=0}^{v-1} \left(-1 + \sum_{i=0}^{n+1} \left\{ \frac{-a_i p^j}{d'} \right\} \right). \tag{3.16}$$

Démonstration. Reprenons en partie les notations du Théorème 3.3.3 : $\wp$ désigne l'idéal premier de $\mathbb{Q}(\zeta_{pd'})$ au-dessous de $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$, et donc $\wp$ est un idéal premier au-dessus de $\mathfrak{p}' \subset \mathbb{Q}(\zeta_{d'}) \subset \mathbb{Q}(\zeta_{pd'})$.

Soit $\mathbf{a} \in \mathfrak{A}^n(d')$, d'après (3.15) ci-dessus, on peut écrire

$$\mathbf{J}_Q(\mathbf{a}) = \boldsymbol{\omega}^{-a_{n+1}}(-1)\mathbf{j}_Q(\boldsymbol{\omega}^{a_0}, \boldsymbol{\omega}^{a_1}, \dots, \boldsymbol{\omega}^{a_n}) = \frac{1}{Q} \cdot \mathbf{g}_Q(\boldsymbol{\omega}^{a_0}) \cdot \mathbf{g}_Q(\boldsymbol{\omega}^{a_1}) \cdot \dots \cdot \mathbf{g}_Q(\boldsymbol{\omega}^{a_n}) \cdot \mathbf{g}_Q(\boldsymbol{\omega}^{a_{n+1}}).$$

Dans cette dernière identité, on a $\operatorname{ord}_\wp(Q) = \operatorname{ord}_\wp(p^v) = v \cdot \operatorname{ord}_\wp(p)$. Appliquons maintenant le théorème de Stickelberger (Théorème 3.3.3) à ce produit :

$$\begin{aligned}
\operatorname{ord}_\wp \mathbf{J}_Q(\mathbf{a}) &= -\operatorname{ord}_\wp(Q) + \operatorname{ord}_\wp \left(\mathbf{g}_Q(\boldsymbol{\omega}^{a_0}) \cdot \mathbf{g}_Q(\boldsymbol{\omega}^{a_1}) \cdot \dots \cdot \mathbf{g}_Q(\boldsymbol{\omega}^{a_n}) \cdot \mathbf{g}_Q(\boldsymbol{\omega}^{a_{n+1}}) \right) \\
&= -\operatorname{ord}_\wp(Q) + \sum_{i=0}^{n+1} \operatorname{ord}_\wp \mathbf{g}_Q(\boldsymbol{\omega}^{a_i}) \\
&= -v \operatorname{ord}_\wp(p) + (p-1) \cdot \sum_{i=0}^{n+1} \left(\sum_{j=0}^{v-1} \left\{ \frac{-a_i p^j}{d'} \right\} \right).
\end{aligned}$$

Pour terminer la démonstration du théorème, il suffit de montrer que pour tout $x \in \mathbb{Q}(\zeta_{d'})$, on a

$$\operatorname{ord}_\wp(x) = (p-1) \operatorname{ord}_{\mathfrak{p}'}(x).$$

De façon générale, on a $\operatorname{ord}_\wp(x) = e(\wp/\mathfrak{p}') \cdot \operatorname{ord}_{\mathfrak{p}'}(x)$ où $e(\wp/\mathfrak{p}')$ désigne l'indice de ramification de $\wp/\mathfrak{p}'$ (*cf.* [Coh07, Chapter 3, §3.5], [Lan94, Chapter I, §7]) : il ne reste qu'à prouver $e(\wp/\mathfrak{p}') = p-1$. Par chance, la ramification de p est bien connue dans les corps cyclotomiques (voir [IR90, Chap. 13, §2] par exemple). Dans l'anneau des entiers de $\mathbb{Q}(\zeta_{d'})$, comme p ne divise pas $d' \geqslant 2$, l'idéal engendré par p se décompose en

$$p \cdot \mathbb{Z}[\zeta_{d'}] = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_g,$$

où $g = \phi(d')/o_p(d')$ et les idéaux $\mathfrak{p}_i$ sont des idéaux premiers distincts de degré résiduel $o_p(d')$ (*i.e.* $\mathbf{N}\mathfrak{p}_i = p^{o_p(d')}$). On peut en outre supposer que $\mathfrak{p}_1 = \mathfrak{p}'$. En particulier, on a $\operatorname{ord}_{\mathfrak{p}'}(p) = 1 = e(\mathfrak{p}'/p)$. D'autre part, dans $\mathbb{Z}[\zeta_{pd'}]$ cette fois (*cf.* [IR90, Chap. 13, §2, Proposition 13.2.9]), l'idéal engendré par p se décompose sous la forme

$$p \cdot \mathbb{Z}[\zeta_{pd'}] = (\wp_1 \cdot \wp_2 \cdot \dots \cdot \wp_g)^{p-1},$$

où g est le même entier que ci-dessus et les idéaux premiers $\wp_i$ sont distincts et de degré résiduel $o_p(d')$. On peut encore supposer que $\wp_1 = \wp$. En particulier, on a $e(\wp/\mathfrak{p}') = e(\wp/p)/e(\mathfrak{p}'/p) = p-1$ et $\operatorname{ord}_\wp(p) = p-1$. Ainsi, on a

$$\operatorname{ord}_{\mathfrak{p}'} \mathbf{J}_Q(\mathbf{a}) = \frac{1}{p-1} \operatorname{ord}_\wp \mathbf{J}_Q(\mathbf{a}) = -v + \sum_{i=0}^{n+1} \left(\sum_{j=0}^{v-1} \left\{ \frac{-a_i p^j}{d'} \right\} \right) = \sum_{j=0}^{v-1} \left(-1 + \sum_{i=0}^{n+1} \left\{ \frac{-a_i p^j}{d'} \right\} \right),$$

comme il fallait démontrer. □

3.3.3 Décomposition primaire des sommes de Jacobi

On garde les notations du paragraphe précédent. En outre, on note $\langle p \rangle_{d'}$ le sous-groupe de $(\mathbb{Z}/d'\mathbb{Z})^\times$ engendré par $p \bmod d'$: c'est un groupe d'ordre $o_p(d') = \operatorname{ord}^\times(p \bmod d')$. Dans l'isomorphisme entre $\operatorname{Gal}(\mathbb{Q}(\zeta_{d'})/\mathbb{Q})$ et $(\mathbb{Z}/d'\mathbb{Z})^\times$ donné par

$$t \in (\mathbb{Z}/d'\mathbb{Z})^\times \mapsto (\sigma_t : \zeta_{d'} \mapsto \zeta_{d'}^t) \in \operatorname{Gal}(\mathbb{Q}(\zeta_{d'})/\mathbb{Q}),$$

le sous groupe $\langle p\rangle_{d'} \subset (\mathbb{Z}/d'\mathbb{Z})^\times$ correspond au sous-groupe de décomposition $D_{\mathfrak{p}'/p} \subset \mathrm{Gal}(\mathbb{Q}(\zeta_{d'})/\mathbb{Q})$ en p. Pour $n \in \mathbb{N}^*$ fixé, il y a une action naturelle de $(\mathbb{Z}/d'\mathbb{Z})^\times$ sur l'ensemble $\mathfrak{A}^n(d')$ donnée, pour tout $t \in (\mathbb{Z}/d'\mathbb{Z})^\times$, par

$$\forall \mathbf{a} \in \mathfrak{A}^n(d'), \quad \mathbf{a} = (a_0, a_1, \dots, a_{n+1}) \mapsto t \cdot \mathbf{a} = (ta_0, ta_1, \dots, ta_{n+1}).$$

Il n'est pas difficile de vérifier que c'est bien une action de $(\mathbb{Z}/d'\mathbb{Z})^\times$ sur $\mathfrak{A}^n(d') \subset (\mathbb{Z}/d'\mathbb{Z})^{n+2}$. Cette action est la traduction « combinatoire » de l'action galoisienne sur les sommes de Jacobi :

Lemme 3.3.8. *L'action de* $\mathrm{Gal}(\mathbb{Q}(\zeta'_d)/\mathbb{Q}) \simeq (\mathbb{Z}/d'\mathbb{Z})^\times$ *sur les sommes de Jacobi* $\mathbf{J}_Q(\mathbf{a})$, $\mathbf{a} \in \mathfrak{A}^n(d')$ *est donnée par*

$$\forall t \in (\mathbb{Z}/d'\mathbb{Z})^\times, \quad \sigma_t\left(\mathbf{J}_Q(\mathbf{a})\right) = \mathbf{J}_Q(t \cdot \mathbf{a}).$$

Démonstration. Soit $\mathbf{a} \in \mathfrak{A}^n(d')$ et $t \in (\mathbb{Z}/d'\mathbb{Z})^\times$. Par définition, on a $\mathbf{J}_Q(\mathbf{a}) = \boldsymbol{\omega}^{a_{n+1}}(-1)\cdot\mathbf{j}_Q(\boldsymbol{\omega}^{a_0}, \dots, \boldsymbol{\omega}^{a_n})$. Comme $\boldsymbol{\omega}^{a_{n+1}}(-1) \in \mathbb{Q}(\zeta_{d'})$ est une racine (d'-ième) de l'unité, on a clairement

$$\sigma_t(\boldsymbol{\omega}^{a_{n+1}}(-1)) = (\boldsymbol{\omega}^{a_{n+1}}(-1))^t = \boldsymbol{\omega}^{t\cdot a_{n+1}}(-1).$$

D'autre part, par définition des sommes de Jacobi (Définition 2.2.6), on a

$$\begin{aligned}
\sigma_t(\mathbf{j}_Q(\boldsymbol{\omega}^{a_0}, \dots, \boldsymbol{\omega}^{a_n})) &= \sigma_t\left((-1)^n \cdot \sum_{\substack{x_i \in \mathbb{F}_Q \\ x_0+\cdots+x_n=1}} \boldsymbol{\omega}^{a_0}(x_0)\boldsymbol{\omega}^{a_1}(x_1)\cdot\dots\cdot\boldsymbol{\omega}^{a_n}(x_n)\right) \\
&= (-1)^n \cdot \sum_{\substack{x_i \in \mathbb{F}_Q \\ x_0+\cdots+x_n=1}} \sigma_t\left(\boldsymbol{\omega}^{a_0}(x_0)\boldsymbol{\omega}^{a_1}(x_1)\cdot\dots\cdot\boldsymbol{\omega}^{a_n}(x_n)\right) \\
&= (-1)^n \cdot \sum_{\substack{x_i \in \mathbb{F}_Q \\ x_0+\cdots+x_n=1}} \sigma_t(\boldsymbol{\omega}^{a_0}(x_0))\sigma_t(\boldsymbol{\omega}^{a_1}(x_1))\cdot\dots\cdot\sigma_t(\boldsymbol{\omega}^{a_n}(x_n)) \\
&= (-1)^n \cdot \sum_{\substack{x_i \in \mathbb{F}_Q \\ x_0+\cdots+x_n=1}} \boldsymbol{\omega}^{t\cdot a_0}(x_0)\boldsymbol{\omega}^{t\cdot a_1}(x_1)\cdot\dots\cdot\boldsymbol{\omega}^{t\cdot a_n}(x_n) \\
&= \mathbf{j}_Q(\boldsymbol{\omega}^{t\cdot a_0}, \boldsymbol{\omega}^{t\cdot a_1}, \dots, \boldsymbol{\omega}^{t\cdot a_n}).
\end{aligned}$$

D'où la relation annoncée. Notons par ailleurs que, comme $x \mapsto x^q$ définit une bijection de $\mathbb{F}_Q$, on a

$$\mathbf{j}_Q(\boldsymbol{\omega}^{q\cdot a_0}, \boldsymbol{\omega}^{q\cdot a_1}, \dots, \boldsymbol{\omega}^{q\cdot a_n}) = \mathbf{j}_Q(\boldsymbol{\omega}^{a_0}, \dots, \boldsymbol{\omega}^{a_n}).$$

□

Nous avons à présent tous les outils nécessaires pour donner la décomposition primaire explicite des sommes de Jacobi.

Théorème 3.3.9. *Soit* $d' \geqslant 2$ *un entier premier à* q. *On écrit à nouveau* $Q = q^{o_q(d')} = p^v$ *et on note* $\langle p\rangle_{d'}$ *le sous-groupe de* $(\mathbb{Z}/d'\mathbb{Z})^\times$ *engendré par* p. *On fixe des représentants* $t_1 = 1, t_2, \dots, t_g \in (\mathbb{Z}/d'\mathbb{Z})^\times$ *du quotient* $(\mathbb{Z}/d'\mathbb{Z})^\times/\langle p\rangle_{d'}$. *Les idéaux premiers de* $\mathbb{Q}(\zeta_{d'})$ *au-dessus de* p *sont donc les* $\mathfrak{p}_i = \sigma_{t_i}^{-1}(\mathfrak{p})$, $i \in [\![1, g]\!]$ *(cf. preuve du Lemme 3.2.6).*

Pour tout $\mathbf{a} \in \mathfrak{A}^n(d')$, *la décomposition en produit d'idéaux premiers de l'idéal engendré par* $\mathbf{J}_Q(\mathbf{a}) \in \mathbb{Z}[\zeta_{d'}]$ *dans l'anneau des entiers de* $\mathbb{Q}(\zeta_{d'})$ *est donnée par*

$$\mathbf{J}_Q(\mathbf{a})\cdot\mathbb{Z}[\zeta_{d'}] = \mathfrak{p}_1^{\alpha(t_1\cdot\mathbf{a})}\cdot\mathfrak{p}_2^{\alpha(t_2\cdot\mathbf{a})}\cdot\ldots\mathfrak{p}_g^{\alpha(t_g\cdot\mathbf{a})} = \prod_{t\in(\mathbb{Z}/d'\mathbb{Z})^\times/\langle p\rangle_{d'}} \mathfrak{p}_t{}^{\alpha(t\cdot\mathbf{a})},$$

où, pour tout $\mathbf{b} = (b_0, b_1, \dots, b_{n+1}) \in \mathfrak{A}^n(d')$, *on a défini* $\alpha(\mathbf{b}) \in \mathbb{N}$ *par*

$$\alpha(\mathbf{b}) = \sum_{j=0}^{v-1}\left(-1 + \sum_{i=0}^{n+1}\left\{\frac{-b_i\cdot p^j}{d'}\right\}\right).$$

Démonstration. Pour tout $\mathbf{a} \in \mathfrak{A}^n(d')$, l'entier algébrique $\mathbf{J}_Q(\mathbf{a})^2$ est de module $Q^n = p^{nv}$ dans tout plongement complexe de $\mathbb{Q}(\zeta_{d'})$ (*cf.* Proposition 2.2.7 et (2.1)). Par suite, $\mathbf{J}_Q(\mathbf{a})^2$ est une unité en tous les idéaux premiers $\mathfrak{l}$ de $\mathbb{Z}[\zeta_{d'}]$ de caractéristique résiduelle différente de p. Autrement dit, pour tout nombre premier ℓ et tout idéal premier $\mathfrak{l}$ de $\mathbb{Z}[\zeta_{d'}]$ au-dessus de ℓ, on a $\mathrm{ord}_\mathfrak{l}\,\mathbf{J}_Q(\mathbf{a})^2 = 0$. Par conséquent, on a aussi $\mathrm{ord}_\mathfrak{l}\,\mathbf{J}_Q(\mathbf{a}) = 0$. Ce qu'on pourrait résumer en : « l'idéal $\mathbf{J}_Q(\mathbf{a})\cdot\mathbb{Z}[\zeta_{d'}]$

est concentré en les idéaux premiers $\mathfrak{q} \subset \mathbb{Z}[\zeta_{d'}]$ au-dessus de p ». Pour caractériser l'idéal engendré par $\mathbf{J}_Q(\mathbf{a})$ dans $\mathbb{Z}[\zeta_{d'}]$, il reste donc à expliciter les valuations $\mathrm{ord}_{\mathfrak{q}} \mathbf{J}_Q(\mathbf{a})$ en les idéaux premiers $\mathfrak{q}$ de $\mathbb{Z}[\zeta_{d'}]$ au-dessus de p. Le Théorème 3.3.7 donne déjà $\mathrm{ord}_{\mathfrak{p}'} \mathbf{J}_Q(\mathbf{a})$ où $\mathfrak{p}' = \mathfrak{P} \cap \mathbb{Z}[\zeta_{d'}]$. Fixons à présent des représentants $t_1 = 1, t_2, \dots, t_g$ dans $(\mathbb{Z}/d'\mathbb{Z})^\times$ du quotient $(\mathbb{Z}/d'\mathbb{Z})^\times/\langle p \rangle_{d'}$ (on a donc $g = \phi(d')/o_p(d')$), la décomposition de l'idéal engendré par p est donnée par

$$p \cdot \mathbb{Z}[\zeta_{d'}] = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \dots \cdot \mathfrak{p}_g,$$

où $\mathfrak{p}_i = \sigma_{t_i}^{-1}(\mathfrak{p}')$ (*cf.* preuve du Lemme 3.2.6 ci-dessus ou [IR90, Chap. 13, §2, Theorem 2]). Or, si $x \in \mathbb{Q}(\zeta_{d'})$, on a $\mathrm{ord}_{\sigma^{-1}(\mathfrak{p}')}(x) = \mathrm{ord}_{\mathfrak{p}'}(\sigma(x))$ pour tout automorphisme $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{d'})/\mathbb{Q})$. En particulier, pour tout $t = t_i \in \{t_1, \dots, t_g\}$ et tout $\mathbf{a} \in \mathfrak{A}^n(d')$,

$$\mathrm{ord}_{\mathfrak{p}_i} \mathbf{J}_Q(\mathbf{a}) = \mathrm{ord}_{\sigma_{t_i}^{-1}(\mathfrak{p}')} \mathbf{J}_Q(\mathbf{a}) = \mathrm{ord}_{\mathfrak{p}'} \sigma_{t_i}\left(\mathbf{J}_Q(\mathbf{a})\right) = \mathrm{ord}_{\mathfrak{p}'} \mathbf{J}_Q(t_i \cdot \mathbf{a}).$$

La dernière égalité suit du Lemme 3.3.8. Or, le Théorème 3.3.7 explicite précisément la quantité tout à droite :

$$\forall t \in (\mathbb{Z}/d'\mathbb{Z})^\times, \quad \mathrm{ord}_{\mathfrak{p}'} \mathbf{J}_Q(t \cdot \mathbf{a}) = \sum_{j=0}^{v-1} \left(-1 + \sum_{i=0}^{n+1} \left\{ \frac{-t \cdot a_i p^j}{d'} \right\} \right).$$

Regroupant ce qui précède, on a

$$\begin{aligned} \mathbf{J}_Q(\mathbf{a}) \cdot \mathbb{Z}[\zeta_{d'}] &= \prod_{\mathfrak{l}} \mathfrak{l}^{\mathrm{ord}_{\mathfrak{l}} \mathbf{J}_Q(\mathbf{a})} = \prod_{\mathfrak{q} \mid p} \mathfrak{q}^{\mathrm{ord}_{\mathfrak{q}} \mathbf{J}_Q(\mathbf{a})} = \prod_{i=1}^{g} \mathfrak{p}_i{}^{\mathrm{ord}_{\mathfrak{p}_i} \mathbf{J}_Q(\mathbf{a})} \\ &= \prod_{i=1}^{g} \mathfrak{p}_i{}^{\mathrm{ord}_{\mathfrak{p}}(\sigma_{t_i} \mathbf{J}_Q(\mathbf{a}))} = \prod_{i=1}^{g} \mathfrak{p}_i{}^{\mathrm{ord}_{\mathfrak{p}'}(\mathbf{J}_Q(t_i \cdot \mathbf{a}))} = \prod_{i=1}^{g} \mathfrak{p}_i{}^{\alpha(t_i \cdot \mathbf{a})}. \end{aligned}$$

Ce qu'il fallait démontrer. □

Proposition 3.3.10. *Avec les notations du Théorème 3.3.9, pour tout* $\mathbf{b} = (b_0, b_1, \dots, b_{n+1}) \in \mathfrak{A}^n(d')$, *on a*

$$\alpha(\mathbf{b}) = \sum_{j=0}^{v-1} \left\lfloor \sum_{i=0}^{n} \left\{ \frac{-b_i p^j}{d'} \right\} \right\rfloor = \frac{[\mathbb{F}_Q : \mathbb{F}_p]}{\#\langle p \rangle_{d'}} \sum_{\pi \in \langle p \rangle_{d'}} \left\lfloor \sum_{i=0}^{n} \left\{ \frac{-b_i \pi}{d'} \right\} \right\rfloor.$$

En particulier, on a

$$0 \leqslant \alpha(\mathbf{b}) \leqslant nv = n \cdot [\mathbb{F}_Q : \mathbb{F}_p]. \tag{3.17}$$

Ce fait est cité sans preuve dans le cas où $p = q = Q$ dans [Shi87], [Yui94] et [SK79]. Le fait que les sommes portent sur $i \in [\![0, n]\!]$ et non $[\![0, n+1]\!]$ n'est pas une faute de frappe.

Démonstration. On peut supposer qu'il existe $i_0 \in [\![0, n+1]\!]$ tel que d' ne divise pas b_{i_0} (sinon, il n'y a rien à démontrer). Par définition, on a alors

$$\begin{aligned} \alpha(\mathbf{b}) &= \sum_{j=0}^{v-1} \left(-1 + \sum_{i=0}^{n+1} \left\{ \frac{-b_i \cdot p^j}{d'} \right\} \right) = \sum_{j=0}^{v-1} \left(-1 + \sum_{i \neq i_0} \left\{ \frac{-b_i \cdot p^j}{d'} \right\} + \left\{ \frac{-b_{i_0} \cdot p^j}{d'} \right\} \right) \\ &= \sum_{j=0}^{v-1} \left(\sum_{i \neq i_0} \left\{ \frac{-b_i \cdot p^j}{d'} \right\} + \left\{ \frac{b_{i_0} \cdot p^j}{d'} \right\} \right) = \sum_{j=0}^{v-1} \left(\sum_{i \neq i_0} \left\{ \frac{-b_i \cdot p^j}{d'} \right\} - \left\{ \sum_{i \neq i_0} \frac{-b_i \cdot p^j}{d'} \right\} \right). \end{aligned}$$

En effet, pour tout $y \in \mathbb{R} \smallsetminus \mathbb{Z}$, on a $\{-y\} = 1 - \{y\}$ (par choix de i_0, $b_{i_0} p^j / d'$ n'est pas entier car d' est premier à p). Pour tout $j \in [\![0, v-1]\!]$, on pose temporairement $c_i = -b_i p^j$ (pour $i \in [\![0, n+1]\!]$) de sorte que

$$\sum_{i \neq i_0} \left\{ \frac{-b_i \cdot p^j}{d'} \right\} - \left\{ \sum_{i \neq i_0} \frac{-b_i \cdot p^j}{d'} \right\} = \sum_{i \neq i_0} \left\{ \frac{c_i}{d'} \right\} - \left\{ \sum_{i \neq i_0} \frac{c_i \cdot p^j}{d'} \right\} = \sum_{i \neq i_0} \left\{ \frac{c_i}{d'} \right\} - \left\{ \sum_{i \neq i_0} \frac{c_i}{d'} \right\}.$$

Quitte à remplacer chaque c_i par un représentant $c_i' \in [\![1, d'-1]\!]$, on peut supposer que $\frac{c_i}{d'} = \left\{ \frac{c_i}{d'} \right\}$ pour tout $i \in [\![0, n]\!]$ (la fonction $x \in \mathbb{Z} \mapsto \{x/d'\}$ est d'-périodique). Ainsi,

$$\sum_{i \neq i_0} \left\{ \frac{c_i}{d'} \right\} - \left\{ \sum_{i \neq i_0} \frac{c_i}{d'} \right\} = \sum_{i \neq i_0} \left\{ \frac{c_i}{d'} \right\} - \left\{ \sum_{i \neq i_0} \left\{ \frac{c_i}{d'} \right\} \right\} = \left\lfloor \sum_{i \neq i_0} \left\{ \frac{c_i}{d'} \right\} \right\rfloor = \left\lfloor \sum_{i \neq i_0} \left\{ \frac{-b_i p^j}{d'} \right\} \right\rfloor.$$

Ce qui, après sommation sur j, démontre la première identité de la Proposition. Il faut remarquer que, par symétrie entre les b_i, on peut supposer que $i_0 = n+1$. Au passage, on a explicitement écrit $\alpha(\mathbf{b})$ comme une somme d'entiers ! De plus, pour tout $j \in [\![0, v-1]\!]$, on a

$$0 \leqslant s_j := \sum_{i=0}^{n} \left\{ \frac{-b_i p^j}{d'} \right\} < \sum_{i=0}^{n} 1 = n+1.$$

D'où l'on déduit que $0 \leqslant \lfloor s_j \rfloor \leqslant n$ et, en sommant sur $j \in [\![0, v-1]\!]$, on trouve (3.17).

Pour démontrer la deuxième égalité, il faut « se débarrasser » de v. Posons $v_0 = [\mathbb{F}_q : \mathbb{F}_p]$, *i.e.* $q = p^{v_0}$. On note à nouveau $o_q(d') = \mathrm{ord}^\times(q \bmod d')$ et $o_p(d') = \mathrm{ord}^\times(p \bmod d')$. On a $Q = q^{o_q(d')} = p^{v_0 o_q(d')} = p^v$, ou encore $v = v_0 o_q(d')$. Mais, comme q est une puissance de p, on a la relation suivante entre leurs ordres modulo d' :

$$o_q(d') = \mathrm{ord}^\times(q \bmod d') = \mathrm{ord}^\times(p^{v_0} \bmod d') = \frac{o_p(d')}{\mathrm{pgcd}(v_0, o_p(d'))}.$$

Ceci prouve que $v = v_0 o_q(d') = \mathrm{ppcm}(v_0, o_p(d'))$. En particulier, v est un multiple de $o_p(d')$ et $w = v/o_p(d')$ est entier. Mais alors, tout entier $j \in [\![0, v-1]\!]$ s'écrit de façon unique sous la forme

$$j = o_p(d')\alpha + \beta, \qquad \text{avec } \alpha \in [\![0, w-1]\!] \text{ et } \beta \in [\![0, o_p(d')-1]\!].$$

Et, par définition de l'ordre modulo d' et par d'-périodicité de $x \in \mathbb{Z} \mapsto \{x/d'\}$, pour tous $b \in \mathbb{Z}$, $\alpha, \beta \in \mathbb{N}$, on a $bp^{\alpha o_p(d')+\beta} \equiv bp^\beta \bmod d'$ et

$$\left\{ \frac{bp^{\alpha o_p(d')+\beta}}{d'} \right\} = \left\{ \frac{bp^\beta}{d'} \right\}.$$

Ainsi, la somme définissant $\alpha(\mathbf{b})$ se réécrit sous la forme :

$$\begin{aligned} \alpha(\mathbf{b}) &= \sum_{j=0}^{v-1} \left\lfloor \sum_{i=0}^{n} \left\{ \frac{-b_i p^j}{d'} \right\} \right\rfloor = \sum_{\alpha=0}^{w-1} \sum_{\beta=0}^{o_p(d')-1} \left\lfloor \sum_{i=0}^{n} \left\{ \frac{-b_i p^{o_p(d')\alpha+\beta}}{d'} \right\} \right\rfloor \\ &= \sum_{\alpha=0}^{w-1} \sum_{\beta=0}^{o_p(d')-1} \left\lfloor \sum_{i=0}^{n} \left\{ \frac{-b_i p^\beta}{d'} \right\} \right\rfloor = w \cdot \sum_{k=0}^{o_p(d')-1} \left\lfloor \sum_{i=0}^{n} \left\{ \frac{-b_i p^k}{d'} \right\} \right\rfloor. \end{aligned}$$

Notant encore $\langle p \rangle_{d'} \subset (\mathbb{Z}/d'\mathbb{Z})^\times$ le sous-groupe engendré par p, on a $\#\langle p \rangle_{d'} = o_p(d')$ et, par construction de $w \in \mathbb{N}$,

$$w = \frac{v}{o_p(d')} = \frac{[\mathbb{F}_Q : \mathbb{F}_p]}{\#\langle p \rangle_{d'}}. \tag{3.18}$$

Ce qui termine la preuve de la seconde égalité dans l'énoncé de la Proposition. □

Définition 3.3.11. Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. Soit $d' \geqslant 2$ un entier premier à q, on note $Q = q^{o_q(d')}$ et $\langle p \rangle_{d'} \subset (\mathbb{Z}/d'\mathbb{Z})^\times$ le sous-groupe engendré par p. Pour tout $n \in \mathbb{N}^*$ et tout $\mathbf{b} = (b_0, b_1, \ldots, b_n, b_{n+1}) \in \mathfrak{A}^n(d')$, on pose

$$\psi_{d'}(\mathbf{b}) = \sum_{\pi \in \langle p \rangle_{d'}} \left\lfloor \sum_{i=0}^{n} \left\{ \frac{-b_i \pi}{d'} \right\} \right\rfloor \in \mathbb{N}.$$

Par construction, on a

$$\alpha(\mathbf{b}) = \frac{[\mathbb{F}_Q : \mathbb{F}_p]}{\#\langle p \rangle_{d'}} \cdot \psi_{d'}(\mathbf{b}).$$

Remarque 3.3.12. En combinant un calcul similaire à celui du Lemme 3.2.6 avec le Théorème 3.3.9, on pourrait retrouver un résultat de Shioda [Shi87, Proposition 2.1]. Avec les notations introduites dans cette section, si $n \geqslant 2$ est un entier pair, pour tout $\mathbf{a} \in \mathfrak{A}^n(d')$, on a

$$\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}} \left(1 - \frac{\mathbf{J}_Q(\mathbf{a})}{Q^{n/2}} \right) \in \frac{1}{Q^{w(\mathbf{a})}} \cdot \mathbb{Z}, \tag{3.19}$$

avec

$$w(\mathbf{a}) = \sum_{t \in (\mathbb{Z}/d'\mathbb{Z})^\times / \langle p \rangle_{d'}} \max \left\{ 0, \frac{n}{2} \cdot \#\langle p \rangle_{d'} - \psi_{d'}(t \cdot \mathbf{a}) \right\} \in \mathbb{N}.$$

Les résultats ci-avant sont en fait nés de la nécessité de disposer de « minorations » plus générales que (3.19). Par exemple, pour $n \in \mathbb{N}^*$ quelconque et pour tous $\mathbf{a}', \mathbf{b}' \in \mathfrak{A}^n(d')$, on pourrait montrer que

$$\mathbf{N}_{\mathbb{Q}(\zeta_{d'})/\mathbb{Q}}\left(1 - \frac{\mathbf{J}_Q(\mathbf{a}') \cdot \mathbf{J}_Q(\mathbf{b}')}{Q^n}\right) \in \frac{1}{Q^{w_2(\mathbf{a}',\mathbf{b}')}} \cdot \mathbb{Z}, \tag{3.20}$$

avec

$$w_2(\mathbf{a}', \mathbf{b}') = \sum_{t \in (\mathbb{Z}/d'\mathbb{Z})^\times / \langle p \rangle_{d'}} \max\{0, n \cdot \#\langle p \rangle_{d'} - \psi_{d'}(t \cdot \mathbf{a}') - \psi_{d'}(t \cdot \mathbf{b}')\} \in \mathbb{N}.$$

3.4 Intermède sur l'équidistribution des sous-groupes de $(\mathbb{Z}/d\mathbb{Z})^\times$

Pour appliquer efficacement les résultats des sections précédentes, nous aurons besoin d'un théorème « d'équidistribution en moyenne des gros sous-groupes de $(\mathbb{Z}/d\mathbb{Z})^\times$ ». Plus précisément, nous démontrons dans la présente section le théorème ci-dessous, dont l'intérêt dépasse sûrement l'usage que l'on en fera.

Théorème 3.4.1. *Soit I un intervalle de $[0,1]$ de longueur $\mu(I)$ et $\mathscr{D} \subset \mathbb{N}^*$ un ensemble infini d'entiers. Soit également, pour tout entier $d \in \mathscr{D}$, un sous-groupe H_d de $G_d = (\mathbb{Z}/d\mathbb{Z})^\times$ tel que*

$$\frac{\#H_d}{\log\log d} \xrightarrow[d\to\infty]{} +\infty.$$

Alors, lorsque $d \to \infty$ (avec $d \in \mathscr{D}$), on a

$$\frac{1}{\#G_d} \sum_{g \in G_d} \left| \mu(I) - \frac{1}{\#H_d} \cdot \#\left\{t \in H_d \;\middle|\; \left\{\tfrac{gt}{d}\right\} \in I\right\} \right| \ll \left(\frac{\log\log d}{\#H_d}\right)^{1/6} = o(1).$$

La constante implicite dans « $\ll$ » est absolue et peut être choisie $\leqslant 3.52$.

Nous utiliserons ce Théorème pour démontrer que certaines familles de nombres $\{y(m)\}$ comme à la Section 3.2 vérifient

$$0 \leqslant \frac{w'(d', y)}{\phi(d')} = o(1) \qquad (d' \to \infty).$$

Remarque 3.4.2. La preuve du Théorème n'utilise pas la structure de groupe de H_d, seule la condition que « H_d n'est pas trop petit », au sens où $\#H_d / \log\log d \to +\infty$, est nécessaire.

Remarque 3.4.3. La moyenne extérieure sur G_d, elle, est cruciale. En effet, on ne peut espérer que chacun des termes

$$\left| \mu(I) - \frac{1}{\#H_d} \cdot \#\left\{t \in H_d \;\middle|\; \left\{\tfrac{gt}{d}\right\} \in I\right\} \right|$$

soit « petit » sans imposer plus de conditions sur I (ou sur H_d). Prenons en effet l'exemple suivant.

On fixe $P \geqslant 3$ un entier et $I =]2/3, 1]$, on pose également $\mathscr{D} = \{d = P^n - 1, n \in \mathbb{N}^*\}$. Pour tout $d \in \mathscr{D}$, on considère $H_d = \langle P \mod d \rangle = \{1, P, P^2, \dots, P^{N-1}\} \subset G_d$ le sous-groupe engendré par P modulo d. Dans cette situation, comme $\#H_d = \mathrm{ord}^\times(P \bmod d) = o_P(d)$, d divise $P^{\#H_d} - 1$ et

$$\frac{\#H_d}{\log\log d} \geqslant \frac{1}{\log P} \cdot \frac{\log d}{\log\log d} \xrightarrow[d\to\infty]{} +\infty.$$

Pour autant, pour tout $j \in [\![0, N-1]\!]$, on a

$$0 \leqslant \left\{\frac{P^j}{d}\right\} = \frac{P^j}{d} = \frac{P^j}{P^N - 1} \leqslant \frac{P^{N-1}}{P^N - 1} = \frac{1}{P} \cdot \frac{P^N}{P^N - 1} \leqslant \frac{1}{3} \cdot \frac{2}{2-1} = \frac{2}{3}.$$

Quelque soit $d \in \mathscr{D}$, le terme correspondant à $g = 1 \in G_d$ dans le Théorème 3.4.1 vaut donc $\mu(I) = 1/3$.

Remarque 3.4.4. Un théorème d'équidistribution similaire mais légèrement plus faible, est énoncé et démontré dans [HP16, §7.4] (voir [HP16, Lemma 7.10]). Notre preuve est toutefois assez différente : nous préférons avoir recours au Théorème d'Erdös-Turán afin de contourner l'argument délicat de [HP16] destiné à majorer le nombre d'« exceptions à l'équidistribution ».

Remarque 3.4.5. On pourra comparer le Théorème 3.4.1 et ses corollaires à d'autres résultats d'équidistribution. Par exemple, [Ulm07a, Proposition 2.6] ou [OU14, Lemma 5.1]

3.4.1 Équidistribution et transformée de Fourier sur $\mathbb{Z}/d\mathbb{Z}$

Le Théorème 3.4.1 est une assertion d'équidistribution « en moyenne » des $\left\{\frac{gt}{d}\right\}$ dans $[0,1]$ lorsque t parcourt H_d et g parcourt $(\mathbb{Z}/d\mathbb{Z})^\times$. Nous utiliserons donc un outil de mesure de l'équidistribution de suites dans $[0,1]$ (voir [KN74, Chapters 1 – 2]), à savoir :

Théorème 3.4.6 (Inégalité d'Erdös-Turán)**.** *Soit $\{x_t\}_{t\in H}$ une suite finie de points de $[0,1]$, indexée par un ensemble H. Alors, pour tout entier $K \in \mathbb{N}^*$,*

$$\sup_{I\subset[0,1]} \left|\mu(I) - \frac{1}{\#H}\cdot \#\left\{t\in H \;\middle|\; x_t \in I\right\}\right| \leqslant \frac{6}{K+1} + \frac{4}{\pi}\sum_{k=1}^{K}\frac{1}{k}\left|\frac{1}{\#H}\sum_{t\in H} \mathrm{e}^{2i\pi k\cdot x_t}\right|,$$

le « sup » étant pris sur tous les intervalles $I \subset [0,1]$, dont on note $\mu(I)$ la longueur.

Démonstration. La lectrice peut consulter l'ouvrage de Kuipers et Niederreiter [KN74, Chapter 2, §2, Theorem 2.5] ou le livre de Montgomery [Mon94, Chapter 1, §2, Theorem 1] pour de jolies preuves. □

Rappelons également qu'il y a une notion de transformée de Fourier pour les fonctions sur $\mathbb{Z}/d\mathbb{Z}$ (voir [Nat00, Chap. 4, §2]). On fixe un entier $d \geqslant 2$. Soit $f : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$ une fonction à valeurs complexes, on définit sa transformée de Fourier $\hat{f} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$ par :

$$\forall x \in \mathbb{Z}/d\mathbb{Z}, \qquad \hat{f}(x) := \sum_{y\in\mathbb{Z}/d\mathbb{Z}} f(y)\cdot \mathrm{e}^{-2i\pi xy/d}. \tag{3.21}$$

La plupart des résultats classiques sur la transformée de Fourier ont des analogues dans ce contexte : nous nous contentons de rappeler le Lemme suivant.

Lemme 3.4.7 (Formule de Plancherel)**.** *Soit $f : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$ une fonction et $\hat{f} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$ sa transformée de Fourier. Alors,*

$$\sum_{x\in\mathbb{Z}/d\mathbb{Z}} |\hat{f}(x)|^2 = d\cdot \sum_{y\in\mathbb{Z}/d\mathbb{Z}} |f(y)|^2.$$

C'est une conséquence de la relation d'orthogonalité des caractères sur $\mathbb{Z}/d\mathbb{Z}$: on pourra consulter [Nat00, Chap. 4, §2] pour le détail de la preuve. Si $g : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$ est une fonction, on note $\|g\|_\infty = \sup_{y\in\mathbb{Z}/d\mathbb{Z}} |g(y)|$ et $\mathrm{supp}(g)$ son support :

$$\mathrm{supp}(g) := \left\{z \in \mathbb{Z}/d\mathbb{Z} \;\middle|\; g(z) \neq 0\right\}.$$

À l'aide de ces résultats, prouvons le :

Lemme 3.4.8. *Soit $f : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$ une fonction et $\hat{f} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{C}$ sa transformée de Fourier. Pour tout $X > 0$, on a*

$$\#\left\{x \in \mathbb{Z}/d\mathbb{Z} \;\middle|\; |\hat{f}(x)| \geqslant X\right\} \leqslant \|f\|_\infty^2 \cdot \frac{d\cdot \#\,\mathrm{supp}(f)}{X^2}.$$

Démonstration. Dans la formule de Plancherel (Lemme 3.4.7), séparons les termes en fonction de leur taille par rapport au paramètre X :

$$\begin{aligned} d\cdot \sum_{y\in\mathbb{Z}/d\mathbb{Z}} |f(y)|^2 = \sum_{x\in\mathbb{Z}/d\mathbb{Z}} |\hat{f}(x)|^2 &= \sum_{\substack{x\in\mathbb{Z}/d\mathbb{Z} \text{ tq.}\\ |\hat{f}(x)|\geqslant X}} |\hat{f}(x)|^2 + \sum_{\substack{x\in\mathbb{Z}/d\mathbb{Z} \text{ tq.}\\ |\hat{f}(x)|< X}} |\hat{f}(x)|^2 \\ &\geqslant X^2\cdot \#\left\{x \in \mathbb{Z}/d\mathbb{Z} \;\middle|\; |\hat{f}(x)| \geqslant X\right\} + \sum_{\substack{x\in\mathbb{Z}/d\mathbb{Z} \text{ tq.}\\ |\hat{f}(x)|< X}} |\hat{f}(x)|^2 \\ &\geqslant X^2\cdot \#\left\{x \in \mathbb{Z}/d\mathbb{Z} \;\middle|\; |\hat{f}(x)| \geqslant X\right\}. \end{aligned}$$

Par ailleurs, il est clair que

$$\sum_{y\in\mathbb{Z}/d\mathbb{Z}} |f(y)|^2 = \sum_{y\in\mathrm{supp}(f)} |f(y)|^2 \leqslant \|f\|_\infty^2 \cdot \#\,\mathrm{supp}(f).$$

Le Lemme suit rapidement des deux dernières inégalités écrites. □

Exemple 3.4.9. En particulier, si f est la fonction indicatrice d'un sous-ensemble non vide $S \subset \mathbb{Z}/d\mathbb{Z}$, on a $\|f\|_\infty = 1$ et $\mathrm{supp}(f) = S$ (comme S est non vide, $\hat{f}$ n'est pas la fonction nulle). En outre, dans cette situation, on a $|\hat{f}(x)| \leqslant |\hat{f}(0)| = \#S = \|\hat{f}\|_\infty$. Par suite, pour tout $\alpha \in]0,1]$, le Lemme 3.4.8 (avec $X = \alpha \cdot \|\hat{f}\|_\infty$) donne

$$\#\left\{x \in \mathbb{Z}/d\mathbb{Z} \;\middle|\; |\hat{f}(x)| \geqslant \alpha\|\hat{f}\|_\infty\right\} \leqslant \frac{d}{\#S} \cdot \alpha^{-2}.$$

Pour $\alpha \geqslant \#S^{-1/2}$, cette majoration est meilleure que la majoration triviale :

$$\#\left\{x \in \mathbb{Z}/d\mathbb{Z} \;\middle|\; |\hat{f}(x)| \geqslant \alpha\|\hat{f}\|_\infty\right\} \leqslant \#\,\mathrm{supp}(\hat{f}) \leqslant d.$$

3.4.2 Preuve du Théorème 3.4.1

Soit, comme dans l'énoncé du Théorème, un intervalle I de $[0,1]$ et, pour tout entier $d \in \mathscr{D}$, un sous-groupe H_d de $G_d = (\mathbb{Z}/d\mathbb{Z})^\times$. Notons X_d la quantité à majorer :

$$X_d := \frac{1}{\#G_d}\sum_{g\in G_d}\left|\mu(I) - \frac{1}{\#H_d}\cdot\#\left\{t \in H_d \mid \left\{\tfrac{gt}{d}\right\} \in I\right\}\right|.$$

Il s'agit de montrer que X_d est un « o(1) » lorsque $d \to \infty$.

Démonstration. Pour tout $g \in G_d$, on pose

$$\Delta_I(g) := \left|\mu(I) - \frac{1}{\#H_d}\cdot\#\left\{t \in H_d \mid \left\{\tfrac{gt}{d}\right\} \in I\right\}\right|.$$

Soit $K \in \mathbb{N}^*$ un paramètre à fixer ultérieurement. Pour tout $g \in G_d$, l'inégalité d'Erdös-Turán (Théorème 3.4.6) appliquée à la suite $\left(\left\{\frac{gt}{d}\right\}\right)_{t\in H_d}$ donne

$$0 \leqslant \Delta_I(g) \leqslant \sup_{I'\subset[0,1]}\Delta_{I'}(g) \leqslant \frac{6}{K+1} + \frac{4}{\pi}\sum_{k=1}^{K}\frac{1}{k}\left|\frac{1}{\#H_d}\sum_{t\in H_d}\mathrm{e}^{2i\pi k\cdot\{gt/d\}}\right|,$$

le « sup » étant pris sur tous les intervalles I' de $[0,1]$. De plus, pour tout $k \in \mathbb{N}^*$ et tout $t \in H_d$, on a $\mathrm{e}^{2i\pi k\{gt/d\}} = \mathrm{e}^{2i\pi k\cdot gt/d}$. Sommant ces inégalités sur $g \in G_d$, on obtient

$$X_d = \frac{1}{\#G_d}\sum_{g\in G_d}\Delta_I(g) \leqslant \frac{6}{K+1} + \frac{4}{\pi}\sum_{k=1}^{K}\frac{1}{k}\left[\frac{1}{\#G_d}\sum_{g\in G_d}\left|\frac{1}{\#H_d}\sum_{t\in H_d}\mathrm{e}^{2i\pi k\cdot gt/d}\right|\right] \tag{3.22}$$

et il reste à majorer le terme entre crochets. Pour ce faire, notons $\mathbb{1} : \mathbb{Z}/d\mathbb{Z} \to \mathbb{R}$ la fonction indicatrice de H_d, vu comme une partie de $\mathbb{Z}/d\mathbb{Z}$. On remarque que

$$\forall y \in \mathbb{Z}/d\mathbb{Z}, \quad \widehat{\mathbb{1}}(y) = \sum_{t\in\mathbb{Z}/d\mathbb{Z}}\mathbb{1}(t)\cdot\mathrm{e}^{-2i\pi yt/d} = \sum_{t\in H_d}\mathrm{e}^{-2i\pi ty/d}.$$

En particulier, $\widehat{\mathbb{1}}(0) = \#H_d = \|\widehat{\mathbb{1}}\|_\infty$. Ainsi, pour tout $k \in \mathbb{N}^*$, on a

$$\forall g \in G_d, \qquad \left|\frac{1}{\#H_d}\sum_{t\in H_d}\mathrm{e}^{2i\pi k\cdot gt/d}\right| = \left|\frac{1}{\#H_d}\sum_{t\in H_d}\mathrm{e}^{-2i\pi k\cdot gt/d}\right| = \frac{|\widehat{\mathbb{1}}(gk)|}{\|\widehat{\mathbb{1}}\|_\infty}.$$

En remplaçant dans (3.22), on obtient

$$X_d \leqslant \frac{6}{K+1} + \frac{4}{\pi}\sum_{k=1}^{K}\frac{1}{k}\left[\frac{1}{\#G_d}\sum_{g\in G_d}\frac{|\widehat{\mathbb{1}}(gk)|}{\|\widehat{\mathbb{1}}\|_\infty}\right].$$

Démontrons alors :

Lemme 3.4.10. *Soit $k \in \mathbb{N}^*$. Avec les notations ci-dessus, on a*

$$\frac{1}{\#G_d}\sum_{g\in G_d}\frac{|\widehat{\mathbb{1}}(gk)|}{\|\widehat{\mathbb{1}}\|_\infty} \leqslant 2\left(\frac{d}{\phi(d)}\right)^{1/3}\cdot(\#H_d)^{-1/3}.$$

Démonstration. Soit $\alpha \in [0,1[$ un paramètre à déterminer ci-dessous. Séparons la somme à majorer en deux parties suivant que $|\widehat{\mathbb{1}}(mk)| < \alpha\|\widehat{\mathbb{1}}\|_\infty$ ou non. D'un côté, on a

$$\sum_{\substack{g\in G_d \text{ tq.}\\ |\widehat{\mathbb{1}}(gk)|<\alpha\|\widehat{\mathbb{1}}\|_\infty}} \frac{|\widehat{\mathbb{1}}(gk)|}{\|\widehat{\mathbb{1}}\|_\infty} \leqslant \sum_{\substack{g\in G_d \text{ tq.}\\ |\widehat{\mathbb{1}}(gk)|<\alpha\|\widehat{\mathbb{1}}\|_\infty}} \alpha \leqslant \#G_d \cdot \alpha.$$

De l'autre,

$$\sum_{\substack{g\in G_d \text{ tq.}\\ |\widehat{\mathbb{1}}(gk)|\geqslant\alpha\|\widehat{\mathbb{1}}\|_\infty}} \frac{|\widehat{\mathbb{1}}(gk)|}{\|\widehat{\mathbb{1}}\|_\infty} \leqslant \#\left\{g \in G_d \;\middle|\; |\widehat{\mathbb{1}}(gk)| \geqslant \alpha\|\widehat{\mathbb{1}}\|_\infty\right\} \cdot 1.$$

Comme on l'a vu à l'Exemple 3.4.9 (suite au Lemme 3.4.8), on peut majorer

$$\begin{aligned}\#\left\{g \in G_d \;\middle|\; |\widehat{\mathbb{1}}(gk)| \geqslant \alpha\|\widehat{\mathbb{1}}\|_\infty\right\} &\leqslant \#\left\{g \in \mathbb{Z}/d\mathbb{Z} \;\middle|\; |\widehat{\mathbb{1}}(gk)| \geqslant \alpha\|\widehat{\mathbb{1}}\|_\infty\right\}\\ &\leqslant \#\left\{x \in \mathbb{Z}/d\mathbb{Z} \;\middle|\; |\widehat{\mathbb{1}}(x)| \geqslant \alpha\|\widehat{\mathbb{1}}\|_\infty\right\}\\ &\leqslant \frac{d}{\#H_d} \cdot \alpha^{-2}.\end{aligned}$$

D'où l'on tire que

$$\begin{aligned}\frac{1}{\#G_d}\sum_{g\in G_d} \frac{|\widehat{\mathbb{1}}(gk)|}{\|\widehat{\mathbb{1}}\|_\infty} &\leqslant \alpha + \frac{1}{\#G_d} \cdot \#\left\{g \in G_d \;\middle|\; |\widehat{\mathbb{1}}(gk)| \geqslant \alpha\|\widehat{\mathbb{1}}\|_\infty\right\}\\ &\leqslant \alpha + \frac{d}{\#H_d \cdot \#G_d} \cdot \alpha^{-2}.\end{aligned}$$

Le choix (optimal) de $\alpha = \left(\frac{d}{\#G_d \cdot \#H_d}\right)^{1/3} = \left(\frac{d}{\phi(d)}\right)^{1/3} \cdot (\#H_d)^{-1/3}$ donne alors le résultat annoncé. □

Remarque 3.4.11. Il est bien connu que, pour tout entier $n \in \mathbb{N}^*$ (suffisamment grand),

$$\frac{n}{\phi(n)} \leqslant \mathrm{e}^\gamma \log\log n,$$

où γ est la constante d'Euler (voir [HW08, Theorem 328] pour une preuve et bien d'autres choses). La majoration obtenue au Lemme 3.4.10 se réécrit donc sous la forme :

$$\frac{1}{\#G_d}\sum_{g\in G_d} \frac{|\widehat{\mathbb{1}}(gk)|}{\|\widehat{\mathbb{1}}\|_\infty} \leqslant 2\mathrm{e}^{\gamma/3} \cdot \left(\frac{\log\log d}{\#H_d}\right)^{1/3}. \tag{3.23}$$

Notons alors $f(d) = \left(\frac{\log\log d}{\#H_d}\right)^{1/3}$ et reprenons les majorations de X_d avec la borne obtenue au Lemme 3.4.10 :

$$\begin{aligned}X_d &\leqslant \frac{6}{K+1} + \frac{4}{\pi}\sum_{k=1}^{K}\frac{1}{k}\left[\frac{1}{\#G_d}\sum_{g\in G_d}\frac{|\widehat{\mathbb{1}}(gk)|}{\|\widehat{\mathbb{1}}\|_\infty}\right] \leqslant \frac{6}{K+1} + \frac{4}{\pi}\sum_{k=1}^{K}\frac{1}{k} \cdot 2\mathrm{e}^{\gamma/3} \cdot \left(\frac{\log\log d}{\#H_d}\right)^{1/3}\\ &\leqslant \frac{6}{K+1} + \frac{8\mathrm{e}^{\gamma/3}}{\pi} \cdot f(d) \cdot \sum_{k=1}^{K}\frac{1}{k} \leqslant \frac{6}{K+1} + \frac{8\mathrm{e}^{\gamma/3}}{\pi} \cdot f(d) \cdot \log(K+1).\end{aligned}$$

Choisissons alors $K \in \mathbb{N}^*$ tel que

$$K+1 = \left\lfloor \frac{3\pi}{4\mathrm{e}^{\gamma/3} \cdot f(d)} \right\rfloor.$$

La majoration ci-dessus donne

$$0 \leqslant X_d \leqslant \frac{16\mathrm{e}^{\gamma/3}}{\pi} \cdot f(d) \cdot \log\left(\frac{3\pi}{4\mathrm{e}^{\gamma/3} \cdot f(d)}\right).$$

En remarquant que $y\log(1/y) \leqslant \sqrt{y}$ pour tout $y > 0$, nous obtenons la majoration plus faible suivante (dont nous nous contenterons) :

$$0 \leqslant X_d \ \leqslant 2\sqrt{\frac{8\mathrm{e}^{\gamma/3}}{\pi}} \cdot \left(\frac{\log\log d}{\#H_d}\right)^{1/6}.$$

Par hypothèse sur H_d, $f(d) = (\log\log d/\#H_d)^{1/3}$ tend vers 0 lorsque $d \to \infty$. Donc $X_d \to 0$, ce qu'il fallait démontrer. L'application numérique donne alors $2\sqrt{\frac{8\mathrm{e}^{\gamma/3}}{\pi}} \simeq 3.5138...$ □

3.4.3 Généralisation et corollaires

À peu de frais, on peut généraliser le Théorème 3.4.1 à toutes les fonctions Riemann-intégrables sur $[0,1]$ et non plus seulement les fonctions indicatrices d'intervalles :

Corollaire 3.4.12. *Soit $F : [0,1] \to \mathbb{R}$ une fonction Riemann-intégrable. On fixe un ensemble infini d'entiers $\mathscr{D} \subset \mathbb{N}^*$. Pour tout entier $d \in \mathscr{D}$, soit H_d un sous-groupe de $G_d = (\mathbb{Z}/d\mathbb{Z})^\times$ tel que*

$$\frac{\#H_d}{\log\log d} \xrightarrow[d\to\infty]{} +\infty.$$

Alors, lorsque $d \to \infty$ (et $d \in \mathscr{D}$), on a

$$\frac{1}{\#G_d}\sum_{g\in G_d}\left|\int_0^1 F(t)\mathrm{d}t - \frac{1}{\#H_d}\sum_{t\in H_d} F\left(\left\{\tfrac{gt}{d}\right\}\right)\right| = o(1).$$

Démonstration. Soit $F : [0,1] \to \mathbb{R}$ une fonction : on dira que F a la propriété $(\mathscr{E})$ si elle vérifie

$$(\mathscr{E}) : \quad \frac{1}{\#G_d}\sum_{g\in G_d}\left|\int_0^1 F(t)\mathrm{d}t - \frac{1}{\#H_d}\sum_{t\in H_d} F\left(\left\{\tfrac{gt}{d}\right\}\right)\right| \xrightarrow[d\to\infty]{} 0.$$

Le Théorème 3.4.1 montre que les fonctions indicatrices des intervalles $I \subset [0,1]$ ont la propriété $(\mathscr{E})$. De plus, il est clair qu'une combinaison linéaire (finie) de fonctions qui ont la propriété $(\mathscr{E})$ a la propriété $(\mathscr{E})$. Ainsi, toute fonction en escaliers sur $[0,1]$ a la propriété $(\mathscr{E})$. Comme toute fonction Riemann-intégrable est limite uniforme de fonctions en escaliers, on en déduit que les fonctions intégrables ont la propriété $(\mathscr{E})$. En effet, si $F : [0,1] \to \mathbb{R}$ est Riemman-intégrable, il existe une suite de fonctions en escaliers $(F_\nu)_{\nu\in\mathbb{N}}$ sur $[0,1]$ telle que $\|F - F_\nu\|_\infty \to 0$ lorsque $\nu \to \infty$ (la $\|.\|_\infty$ étant relative à $[0,1]$). Pour tout $\nu \in \mathbb{N}$, la fonction $F_\nu : [0,1] \to \mathbb{R}$ a la propriété $(\mathscr{E})$, *i.e.*

$$\frac{1}{\#G_d}\sum_{g\in G_d}\left|\int_0^1 F_\nu(t)\mathrm{d}t - \frac{1}{\#H_d}\sum_{t\in H_d} F_\nu\left(\left\{\tfrac{gt}{d}\right\}\right)\right| \xrightarrow[d\to\infty]{} 0.$$

Mais, par l'inégalité triangulaire, pour tout $\nu \in \mathbb{N}$ et tout $g \in G_d$, on a

$$\left|\int_0^1 F(t)\mathrm{d}t - \frac{1}{\#H_d}\sum_{t\in H_d} F\left(\left\{\tfrac{gt}{d}\right\}\right)\right| \leqslant 2\|F - F_\nu\|_\infty + \left|\int_0^1 F_\nu(t)\mathrm{d}t - \frac{1}{\#H_d}\sum_{t\in H_d} F_\nu\left(\left\{\tfrac{gt}{d}\right\}\right)\right|.$$

Pour tout $\varepsilon > 0$, il existe N_0 tel que pour tout $\nu \geqslant N_0$, le terme $2\|F - F_\nu\|_\infty$ est inférieur à $\varepsilon/2$. La moyenne de $2\|F - F_\nu\|_\infty$ sur G_d est donc également inférieure à $\varepsilon/2$. Et pour $\nu = N_0$ par exemple, si $d \in \mathscr{D}$ est suffisamment grand,

$$\frac{1}{\#G_d}\sum_{g\in G_d}\left|\int_0^1 F_\nu(t)\mathrm{d}t - \frac{1}{\#H_d}\sum_{t\in H_d} F_\nu\left(\left\{\tfrac{gt}{d}\right\}\right)\right| \leqslant \varepsilon/2.$$

Donc F a bien la propriété $(\mathscr{E})$. Noter que, sans hypothèse supplémentaire sur F, on ne peut rien dire de plus sur la « vitesse de convergence ». □

3.4.4 Une application

Soit $p \geqslant 3$ un entier impair et $q = p^v$ une puissance fixée de p, on notera $\mathscr{D}$ l'ensemble des entiers $d \geqslant 2$ qui sont premiers à p. On fixe également un intervalle $I \subset [0,1]$, dont on note $\mu(I)$ la longueur. Pour tout $d \in \mathscr{D}$, on note $G_d = (\mathbb{Z}/d\mathbb{Z})^\times$ et

$$\langle p\rangle_d := \langle p \bmod d\rangle \subset (\mathbb{Z}/d\mathbb{Z})^\times \quad \text{et} \quad \langle q\rangle_d := \langle q \bmod d\rangle \subset \langle p\rangle_d \subset (\mathbb{Z}/d\mathbb{Z})^\times.$$

Proposition 3.4.13. *Dans ces conditions, lorsque $d \to \infty$,*

$$\frac{1}{\#(G_d/\langle q\rangle_d)} \sum_{m\in G_d/\langle q\rangle_d} \left|\mu(I) - \frac{1}{\#\langle p\rangle_d} \cdot \#\left\{\pi \in \langle p\rangle_d \middle| \left\{\tfrac{m\pi}{d}\right\} \in I\right\}\right| \ll_{p,v} \left(\frac{\log\log d}{\log d}\right)^{1/6} = o(1),$$

la constante implicite dans le « $\ll$ » ne dépendant que de p.

Démonstration. Commençons par remarquer que, comme $\langle q\rangle_d = \langle p^v\rangle_d \subset \langle p\rangle_d$, on a

$$\begin{aligned}\sum_{g\in G_d} \left|\mu(I) - \frac{\#\left\{\pi \in \langle p\rangle_d \middle| \left\{\tfrac{m\pi}{d}\right\} \in I\right\}}{\#\langle p\rangle_d}\right| &= \sum_{m\in G_d/\langle q\rangle_d} \sum_{\beta\in\langle q\rangle_d} \left|\mu(I) - \frac{\#\left\{\pi \in \langle p\rangle_d \middle| \left\{\tfrac{g\cdot\beta\pi}{d}\right\} \in I\right\}}{\#\langle p\rangle_d}\right| \\ &= \sum_{m\in G_d/\langle q\rangle_d} \sum_{\beta\in\langle q\rangle_d} \left|\mu(I) - \frac{\#\left\{\pi' \in \langle p\rangle_d \middle| \left\{\tfrac{g\pi'}{d}\right\} \in I\right\}}{\#\langle p\rangle_d}\right| \\ &= \#\langle q\rangle_d \cdot \sum_{m\in G_d/\langle q\rangle_d} \left|\mu(I) - \frac{\#\left\{\pi' \in \langle p\rangle_d \middle| \left\{\tfrac{g\pi}{d}\right\} \in I\right\}}{\#\langle p\rangle_d}\right|.\end{aligned}$$

La somme à majorer peut donc s'écrire sous la forme :

$$\frac{1}{\#(G_d/\langle q\rangle_d)} \sum_{m\in G_d/\langle q\rangle_d} \left|\mu(I) - \frac{\#\left\{\pi' \in \langle p\rangle_d \middle| \left\{\tfrac{g\pi}{d}\right\} \in I\right\}}{\#\langle p\rangle_d}\right| = \frac{1}{\#G_d} \left|\mu(I) - \frac{\#\left\{\pi \in \langle p\rangle_d \middle| \left\{\tfrac{m\pi}{d}\right\} \in I\right\}}{\#\langle p\rangle_d}\right|.$$

Pour tout $d \in \mathscr{D}$, notons $H_d = \langle p\rangle_d \subset G_d$ et montrons que ce sous-groupe satisfait à l'hypothèse du Théorème 3.4.1 : il s'agit de voir que $\#H_d/\log\log d \to \infty$. Pour $d \in \mathscr{D}$ donné, H_d est le sous-groupe engendré par p : si l'on note θ_d l'ordre de p modulo d, on a $\theta_d = o_p(d) = \#H_d$ et d divise $p^{\theta_d} - 1$. En particulier, on a l'inégalité $2 \leqslant d \leqslant p^{\theta_d} - 1$ de laquelle on tire :

$$0 < \log d \leqslant \theta_d \cdot \log p = \log p \cdot \#H_d.$$

Il suit que

$$\frac{\#H_d}{\log\log d} \geqslant \frac{1}{\log p} \cdot \frac{\log d}{\log\log d} \xrightarrow[d\to\infty]{} +\infty.$$

On applique alors le Théorème 3.4.1 : il y a une constante absolue $\kappa > 0$ telle que

$$\frac{1}{\#(G_d/\langle q\rangle_d)} \sum_{m\in G_d/\langle q\rangle_d} \left|\mu(I) - \frac{\#\left\{\pi' \in \langle p\rangle_d \middle| \left\{\tfrac{g\pi}{d}\right\} \in I\right\}}{\#\langle p\rangle_d}\right| \leqslant \kappa \cdot \left(\frac{\log\log d}{\#H_d}\right)^{1/6} \leqslant \kappa'_p \cdot \left(\frac{\log\log d}{\log d}\right)^{1/6},$$

où $\kappa'_p = \kappa \cdot (\log p)^{1/6}$ est une constante ne dépendant que de p. Ce qu'il fallait démontrer. □

Dans les applications, nous aurons besoin de :

Corollaire 3.4.14. *Soit $F = [0,1] \to \mathbb{R}$ une fonction en escaliers. Avec les notations ci-dessus, lorsque $d \to \infty$,*

$$\frac{1}{\#(G_d/\langle q\rangle_d)} \sum_{m\in G_d/\langle q\rangle_d} \left|\int_0^1 F(t)\mathrm{d}t - \frac{1}{\#\langle p\rangle_d} \sum_{\pi\in\langle p\rangle_d} F\left(\left\{\tfrac{m\pi}{d}\right\}\right)\right| = o(1).$$

Ce corollaire est une conséquence immédiate de la Proposition 3.4.13 et du Corollaire 3.4.12.

Remarque 3.4.15. Soit $F : [0,1] \to \mathbb{R}$ est une fonction en escaliers à « N marches » : *i.e.* F est de la forme $F = \sum_{i=1}^N \lambda_i \cdot F_i$, où F_i est la fonction indicatrice d'un intervalle $I_i \subset [0,1]$. Le Théorème 3.4.1 appliqué à chacune des F_i donne alors que

$$\frac{1}{\#(G_d/\langle q\rangle_d)} \sum_{m\in G_d/\langle q\rangle_d} \left|\int_0^1 F(t)\mathrm{d}t - \frac{1}{\#\langle p\rangle_d} \sum_{\pi\in\langle p\rangle_d} F\left(\left\{\tfrac{m\pi}{d}\right\}\right)\right| \leqslant \kappa'_p \cdot N \cdot \|F\|_\infty \cdot \left(\frac{\log\log d}{\log d}\right)^{1/6},$$

lorsque $d \to \infty$, où κ'_p est une constante ne dépendant que de p.

Terminons cette section par un Lemme que nous utilisons à plusieurs reprises en lien avec ces questions d'équidistribution :

Lemme 3.4.16. *Soit $w' : \mathbb{N}^* \to \mathbb{R}_+$ une fonction. Pour tout $d \in \mathbb{N}^*$, on pose $w(d) = \sum_{d'|d} w'(d')$. On suppose que $w'(n)/\phi(n) \longrightarrow 0$ lorsque $n \to \infty$. Alors*

$$w(d) = o(d) \qquad (d \to \infty).$$

Démonstration. Soit $d \geqslant 2$ et $D \in [\![1, d]\!]$. Sous les hypothèses du Lemme, il existe une constante $C > 0$ telle que $w'(n) \leqslant C\phi(n)$ pour tout $n \in \mathbb{N}^*$. Soit $\varepsilon > 0$, par les hypothèses encore, il existe N_ε tel que $w'(n) \leqslant \frac{\varepsilon}{2}\phi(n)$ pour tout $n > N_\varepsilon$. Alors, si $d > N_\varepsilon$, on a

$$\begin{aligned} w(d) = \sum_{d'|d} w'(d') &= \sum_{\substack{d'|d \\ d' \leqslant N_\varepsilon}} w'(d') + \sum_{\substack{d'|d \\ d' > N_\varepsilon}} w'(d') \\ &\leqslant \sum_{\substack{d'|d \\ d' \leqslant N_\varepsilon}} C \cdot \phi(d') + \frac{\varepsilon}{2} \cdot \left(\sum_{\substack{d'|d \\ d' > N_\varepsilon}} \phi(d) \right) \leqslant C \cdot \sum_{\substack{d'|d \\ d' \leqslant N_\varepsilon}} d' + \frac{\varepsilon}{2} \cdot \left(\sum_{d'|d} \phi(d) \right) \\ &\leqslant C \cdot (N_\varepsilon)^2 + \frac{\varepsilon}{2} \cdot d = d \cdot \left(\frac{\varepsilon}{2} + \frac{CN_\varepsilon^2}{d} \right). \end{aligned}$$

Soit alors $M_\varepsilon \in \mathbb{N}^*$ tel que $M_\varepsilon > N_\varepsilon$ et $\frac{CN_\varepsilon^2}{n} \leqslant \frac{\varepsilon}{2}$ pour tout $n > M_\varepsilon$. En ce cas, pour tout $d > M_\varepsilon > N_\varepsilon$, on a

$$w(d) \leqslant d \cdot \left(\frac{\varepsilon}{2} + \frac{CN_\varepsilon^2}{d} \right) \leqslant d \cdot \left(\frac{\varepsilon}{2} + \frac{\varepsilon}{2} \right) = \varepsilon \cdot d.$$

□

4

Famille des courbes elliptiques « de Legendre »

Dans ce chapitre, nous étudions les courbes elliptiques « de Legendre » E_d définies sur $\mathbb{F}_q(t)$, dont un modèle de Weierstrass affine est :

$$E_d : Y^2 = X(X+1)(X+t^d),$$

où $d \in \mathbb{N}^*$ est un entier premier à la caractéristique p de $K = \mathbb{F}_q(t)$.

Dans une série d'articles ([Ulm14a], [CHU14] et [Ulm14b]), D. Ulmer étudie en détail ces courbes : il y démontre (entre autres) la conjecture de Birch et Swinnerton-Dyer pour les courbes E_d, il calcule leur fonction L et explicite leur rang et, sous des hypothèses supplémentaires sur d, calcule l'ordre de $Ш(E_d/K)$. Nous reprenons une partie de ses résultats, dans le but d'étudier le comportement du ratio de Brauer-Siegel de cette famille. Notons que notre approche diffère de celle de D. Ulmer : comme le titre de ses articles le suggère, il construit des points rationnels explicites sur la courbe E_d pour arriver (via la conjecture de Birch et Swinnerton-Dyer) à un bon encadrement de $\#Ш(E_d/K)$. Remarquons également que cet encadrement n'est valide, à q fixé, que pour un nombre fini d'entiers d. Au contraire, nous voulons éviter de considérer des points rationnels sur E_d et ainsi « séparer » les quantités $\#Ш(E_d/K)$ et $\mathrm{Reg}(E_d/K)$ dont le produit apparaît dans le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$. De plus, nous voulons estimer *asymptotiquement* $\mathfrak{Bs}(E_d/K)$ lorsque $d \to \infty$, à q fixé. Dans un but de cohérence, nos notations sont aussi proches que possible de celles utilisées dans [Ulm14a], [CHU14] et [Ulm14b]. Regroupons certains des résultats obtenus sur cette famille de courbes en un seul théorème :

Théorème. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \geqslant 2$ premier à p, on considère la courbe elliptique « de Legendre » E_d définie sur K dont un modèle de Weierstrass affine est*

$$E_d : \quad Y^2 = X(X+1)(X+t^d).$$

Les conjectures de Birch et Swinnerton-Dyer sont vraies pour la courbe E_d/K. En particulier, le groupe de Tate-Shafarevich $Ш(E_d/K)$ est fini et le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ a bien un sens. De plus, lorsque d tend vers l'infini, on a $H\big(E_d/K\big) \to +\infty$ et

$$\mathfrak{Bs}(E_d/K) \xrightarrow[d\to\infty]{} 1.$$

Autrement dit,

$$\log\big(\#Ш(E_d/K)\cdot \mathrm{Reg}(E_d/K)\big) \sim \log H\big(E_d/K\big) \sim \frac{d}{2}\log q \quad (d \to \infty).$$

Bien que cela n'apparaisse pas dans le résultat final, nous avons besoin de connaître la fonction L de E_d/K assez explicitement pour encadrer sa valeur spéciale $L^*(E_d/K, 1)$. C'est pourquoi, après avoir calculé hauteur et conducteur de E_d dans la première section (Proposition 4.1.4), nous donnons dans la seconde section l'expression de $L(E_d/K, T)$ (Théorème 4.2.1). Cette expression est, aux notations près, la même que celle de [CHU14, Theorem 3.2.1]. La section suivante démontre les conjectures de Birch et Swinnerton-Dyer pour la courbe E_d (Théorème 4.3.1 : nous nous contentons d'esquisser

brièvement la preuve, qui est contenue dans [Ulm14a]) et en tirons quelques conséquences quant au rang (Proposition 4.3.3) et à la valeur spéciale $L^*(E_d/K, 1)$ (Proposition 4.3.4). La dernière section, qui est la seule véritable contribution nouvelle du présent travail quant aux courbes E_d, est consacrée à l'étude proprement dite du ratio de Brauer-Siegel. Nous y démontrons la limite annoncée dans le Théorème ci-dessus.

4.1 Construction et invariants

La famille des courbes de Legendre est une des familles de courbes elliptiques les plus familières et les plus étudiées. Elle est souvent utilisée pour tester des conjectures et illustrer des théorèmes.

4.1.1 Courbes elliptiques dont la 2-torsion est rationnelle

Soit $\lambda(t) \in \mathbb{F}_q[t]$ un polynôme non constant. On peut considérer la courbe elliptique E_λ sur $K = \mathbb{F}_q(t)$ dont un modèle affine est

$$E_\lambda : \quad y^2 = x(x-1)(x-\lambda(t)).$$

Il est bien connu que E_λ/K est « la courbe elliptique universelle » sur $\mathbb{F}_q(t)$ munie de 4 points K-rationnels de 2-torsion (*cf.* [Hus04, Chapter 4, §1]). Plus précisément, on constate que les quatre points

$$P_0 = (0,0), \quad P_1 = (1,0), \quad P_2 = (\lambda, 0), \quad \mathcal{O}$$

sont des points K-rationnels de 2-torsion sur E_λ. Ceci nous incite à considérer :

Définition 4.1.1. Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. Pour $d \in \mathbb{N}^*$ un entier premier à p, on considère la courbe elliptique définie sur $K = \mathbb{F}_q(t)$ par le modèle de Weiestrass affine :

$$E_d : \quad y^2 = x(x+1)(x+t^d) = x^3 + (1+t^d)x^2 + t^d x. \tag{4.1}$$

Suivant [Ulm14a], dans toute la suite de ce chapitre, nous appelons E_d/K la *courbe de Legendre.*

Remarque 4.1.2. Soit E'_d la courbe elliptique définie sur K et donnée en coordonnées affines par :

$$E'_d : \quad y^2 = x(x-1)(x-t^d),$$

la « vraie » courbe de Legendre. On remarque, avec [Ulm14a, §2], que E_d est la tordue quadratique de E'_d. En effet, le changement de coordonnées $x' = -x$ dans (4.1) donne un isomorphisme explicite entre E_d et la tordue quadratique d'équation :

$$(-1)y^2 = x(x-1)(x-t^d)$$

de E'_d. Dès lors, si le corps des constantes $\mathbb{F}_q$ contient une racine primitive 4-ième de l'unité, il y a un isomorphisme $E_d \simeq E'_d$ défini sur $\mathbb{F}_q(t)$.

Le discriminant du modèle (4.1) de E_d donné ci-dessus se calcule aisément à l'aide du formulaire rappelé à la Section 1.1.2 : il vaut

$$\Delta = 16t^{2d}(t^d-1)^2 \in \mathbb{F}_q(t).$$

On peut aussi calculer l'invariant $j(E_d/K)$ de la courbe E_d/K :

$$j(E_d/K) = 16^2 \cdot \frac{(t^{2d}-t^d+1)^3}{t^{2d}(t^d-1)^2} = 2^8 \cdot \frac{(t^{3d}-1)^3}{t^{2d}(t^{2d}-1)(t^d+1)^2} \in K = \mathbb{F}_q(t).$$

On constate alors que $\deg j(E_d/K) = 2d > 0$: ceci montre que la courbe E_d n'est pas isotriviale (sinon on aurait $\deg j(E_d/K) = 0$). On remarque par ailleurs que $j(E_d/K) \notin K^p$ n'est pas une puissance p-ième. En d'autres termes, le morphisme $j : \mathbb{P}^1 \to \mathbb{P}^1$ défini par $t \mapsto j(E_d/K)(t)$ est non constant et séparable (car d est supposé premier à p). Remarquons dès à présent que le modèle (4.1) est un modèle entier de E_d.

4.1.2 Analyse de la mauvaise réduction

On voit sur l'expression du discriminant $\Delta = 16t^{2d}(t^d-1)^2$ du modèle (4.1) que les seules places de mauvaise réduction de E_d sont la place $v=0$, la place $v=\infty$ et les places v de K correspondant aux racines d-ièmes de l'unité (dans $\overline{\mathbb{F}_q}$). Plus précisément, on a :

Proposition 4.1.3. *Soit d un entier premier à q. Soit $\pi : \mathcal{E}_d \to \mathbb{P}^1$ le modèle régulier minimal de la courbe $E_d/\mathbb{F}_q(t)$. Alors les fibres singulières de π sont comme suit :*

- *au-dessus de $0 \in \mathbb{P}^1$, la fibre de π est de type $\mathbf{I}_{2d}$,*
- *au-dessus de $\zeta \in \mathbb{P}^1$, où $\zeta \in \mu_d(\overline{\mathbb{F}_q})$, la fibre de π est de type $\mathbf{I}_2$ (déployée),*
- *au-dessus de $\infty \in \mathbb{P}^1$, la fibre de π est de type* $\begin{cases} \mathbf{I}_{2d} \text{ déployée} & \text{si } d \text{ est pair} \\ \mathbf{I}^*_{2d} & \text{si } d \text{ est impair.} \end{cases}$

Démonstration. Reprenons le modèle affine de Weiestrass (4.1) de E_d :

$$y^2 = x^2 + (1+t^d)x^2 + t^d x,$$

dont le discriminant est $\Delta = 16t^{2d}(t^d-1)^2$. Pour calculer le type de la fibre $\pi^{-1}(v)$ en un point $v \in \mathbb{P}^1$, nous appliquons, place par place, l'algorithme de Tate (exposé en détail dans [Sil94, Chap. IV, §9] ou [Tat75]) :

- En la place $v=0$, on a $\operatorname{ord}_{v=0}\Delta = 2d$ et $\operatorname{ord}_{v=0} j(E_d) = -2d$. L'algorithme s'arrête donc à l'étape 1 : la réduction de E_d en $v=0$ est multiplicative, la fibre est singulière de type de Kodaira $\mathbf{I}_{2d}$. Un calcul rapide montre que la réduction modulo $v=0$ de (4.1) est d'équation affine $y^2 = x^3 + x^2 = x^2(x+1)$. La réduction est donc déployée. La contribution locale au discriminant minimal est donc $\operatorname{ord}_{v=0}\Delta_{\min}(E_d/K) = 2d$ et la contribution au conducteur est $\operatorname{ord}_{v=0}\mathcal{N}(E_d/K) = 1$. Comme la réduction est déployée, le nombre de Tamagawa local est $c_{v=0}(E_d/K) = 2d$.
- Soit $\zeta \in \overline{\mathbb{F}_q}$ tel que $\zeta^d = 1$. En la place v correspondant à $\zeta \in \mathbb{P}^1$, on a $\operatorname{ord}_{v=\zeta}\Delta = 2$ et $\operatorname{ord}_{v=\zeta} j(E_d) = -2$. Ici encore, l'algorithme s'arrête dès la première étape : la fibre du modèle régulier minimal de E_d au-dessus de $t=\zeta$ est singulière de type $\mathbf{I}_2$. Autrement dit, la réduction est multiplicative. L'étude de la réduction de (4.1) en $v=\zeta$ montre qu'elle est déployée si et seulement si -1 est un carré dans le corps résiduel $\mathbb{F}_v = \mathbb{F}_q(\zeta)$. Chacune des places $v=\zeta$ (avec $\zeta^d=1$) donne donc une contribution $\operatorname{ord}_{v=\zeta}\Delta_{\min}(E_d/K) = 2$ au discriminant minimal, une contribution $\operatorname{ord}_{v=\zeta}\mathcal{N}(E_d/K) = 1$ au conducteur et le nombre de Tamagawa local est $c_{v=\zeta}(E_d/K) = 2$ ou 1 suivant (respectivement) que -1 est un carré dans $\mathbb{F}_v$ ou non.
- Pour étudier la réduction de E_d en la place $v=\infty$, on commence par faire un changement de coordonnées $t = 1/u$ sur $\mathbb{P}^1$. Si $d' = \lceil d/2 \rceil$, après un changement de variables on obtient le modèle affine suivant pour $E_d/\mathbb{F}_q(u)$:

$$y'^2 = x'^3 + u^{2d'}(u^{-d}+1)x'^2 + u^{4d'-d}x'. \tag{4.2}$$

  Le discriminant de cette cubique est $\Delta' = -16u^{12d'-4d}(1-u^d)^2$. On distingue alors deux cas :
  - Si d est pair, le modèle (4.2) est

$$y^2 = x^3 + (1+u^d)x^2 + u^d x$$

    et l'on a $\operatorname{ord}_{u=0}\Delta' = 2d$ et $\operatorname{ord}_{t=\infty} j(E_d) = -\deg j(E_d) = -2d$. La réduction est donc multiplicative, de type de Kodaira $\mathbf{I}_{2d}$ et la contribution au conducteur est $\operatorname{ord}_{v=\infty}\mathcal{N}(E_d/K) = 1$ et $\operatorname{ord}_{v=\infty}\Delta_{\min}(E_d/K) = 2d$. De plus, la réduction de (4.2) est de la forme $y^2 = x^3+x^2 = x^2(x+1)$: la réduction est donc multiplicative déployée et le nombre de Tamagawa local est $c_\infty(E_d/K) = 2d$.
  - Si maintenant d est impair, le modèle (4.2) devient

$$y^2 = x^3 + u(1+u^d)x^2 + u^{d+2}x.$$

    L'algorithme de Tate s'arrête à l'étape 7 : la réduction de E_d est cette fois additive, de type de Kodaira $\mathbf{I}^*_{2d}$. La contribution au conducteur est par conséquent $\operatorname{ord}_{v=\infty}\mathcal{N}(E_d/K) = 2$, et celle au discriminant minimal $\operatorname{ord}_{v=\infty}\Delta_{\min}(E_d/K) = 2d+6$. Pour calculer le nombre de Tamagawa local et distinguer entre les cas $c_\infty(E_d/K) = 2$ ou 4, il faut suivre la « sous-procédure 7 » de Tate et l'on trouve facilement que $c_\infty(E_d/K) = 4$.

Ce qui termine l'analyse de la mauvaise réduction de $E_d/\mathbb{F}_q(t)$ et le calcul des invariants locaux. □

On pourra également consulter [Ulm11, Lecture 3, §2], où une construction explicite du modèle régulier minimal $\mathcal{E}_d \to \mathbb{P}^1$ de la courbe de Legendre E_d est proposée. Résumons dans un tableau synthétique les différentes informations trouvées dans la preuve ci-dessus :

Place	Type de réduction			$\operatorname{ord}_v \Delta_{\min}(E_d/K)$	$\operatorname{ord}_v \mathcal{N}(E_d/K)$	$c_v(E_d/K)$
$v=0$	$\mathbf{I}_{2d}$	déployée		$2d$	1	$2d$
$v=\zeta$	$\mathbf{I}_2$	déployée	si $\mu(-1)=1$	2	1	2
$(\zeta^d=1)$		non déployée	si $\mu(-1)=-1$	2	1	1
$v=\infty$	$\mathbf{I}_{2d}$	déployée	si d pair	$2d$	1	$2d$
	$\mathbf{I}^*_{2d}$		si d impair	$2d+6$	2	4

Dans ce tableau, pour toute place v de $K=\mathbb{F}_q(t)$ de mauvaise réduction pour E_d : on a noté $\operatorname{ord}_v(\Delta_{\min})$ la valuation en v du discriminant minimal de E_d, $\operatorname{ord}_v(\mathcal{N})$ la valuation du conducteur de E_d et $c_v(E_d/K)$ le nombre de Tamagawa local.

4.1.3 Calcul des invariants

Grâce à l'analyse de la mauvaise réduction de la courbe de Legendre E_d effectuée ci-dessus, on peut calculer les invariants « basiques » de E_d en fonction de $d\in\mathbb{N}^*$:

Proposition 4.1.4. *Soit d un entier premier à q et E_d la courbe de Legendre sur $K=\mathbb{F}_q(t)$ définie ci-dessus. Alors sa hauteur différentielle vaut :*

$$H(E_d/K)=q^{\left\lfloor\frac{d+1}{2}\right\rfloor}.$$

De plus, on a

$$\deg\mathcal{N}(E_d/K)=\begin{cases}d+2 & \text{si } d \text{ est pair,}\\ d+3 & \text{si } d \text{ est impair.}\end{cases}$$

Démonstration. Il suffit de reprendre les informations compilées dans le tableau ci-dessus. Pour une place v de $K=\mathbb{F}_q(t)$, on notera $\mathbb{F}_v$ le corps résiduel de K en v et $d_v=[\mathbb{F}_v:\mathbb{F}_q]$ le degré de v. On obtient alors

$$\begin{aligned}\deg\Delta_{\min}(E_d/K)&=\operatorname{ord}_{v=0}\Delta_{\min}\cdot d_0+\sum_{\zeta^d=1}\operatorname{ord}_{v=\zeta}\Delta_{\min}\cdot d_\zeta+\operatorname{ord}_{v=\infty}\Delta_{\min}\cdot d_\infty\\&=2d\cdot 1+2\cdot\sum_{\zeta^d=1}d_\zeta+\operatorname{ord}_{v=\infty}\Delta_{\min}.\\&=2d+2d+\operatorname{ord}_{v=\infty}\Delta_{\min}=4d+\operatorname{ord}_{v=\infty}\Delta_{\min}=\begin{cases}6d & \text{si } d \text{ est pair,}\\ 6(d+1) & \text{si } d \text{ est impair.}\end{cases}\end{aligned}$$

Remarquons en effet que

$$\sum_{\zeta^d=1}d_\zeta=\sum_{\substack{\zeta\in\overline{\mathbb{F}_q}\\ \zeta^d-1=0}}[\mathbb{F}_q(\zeta):\mathbb{F}_q]=\deg(X^d-1)=d. \tag{4.3}$$

Il suit immédiatement de ce calcul que

$$\frac{\deg\Delta_{\min}(E_d/K)}{12}=\begin{cases}\frac{d}{2} & \text{si } d \text{ est pair,}\\ \frac{d+1}{2} & \text{si } d \text{ est impair}\end{cases}=\left\lfloor\frac{d+1}{2}\right\rfloor.$$

D'où l'on peut déduire l'expression de la hauteur différentielle de E_d (par définition, $H(E_d/K)=q^{(\deg\Delta_{\min})/12}$). Enfin, un calcul très similaire à celui de $\deg\Delta_{\min}(E_d/K)$ permet de trouver l'expression du degré du conducteur $\mathcal{N}(E_d/K)$. □

D'après le *cf.* Théorème 1.3.11 de Grothendieck, comme E_d n'est pas isotriviale, sa fonction L est un polynôme à coefficients entiers. Mieux, on peut connaître le degré de $L\big(E_d/K,T\big)\in\mathbb{Z}[T]$ à partir de $\deg\mathcal{N}(E_d/K)$. Ici, on obtient :

$$\deg L\big(E_d/\mathbb{F}_q(t),T\big)=\deg\mathcal{N}(E_d/\mathbb{F}_q(t))+4\cdot g(\mathbb{P}^1)-4=\begin{cases}d-2 & \text{si } d \text{ est pair}\\ d-1 & \text{si } d \text{ est impair.}\end{cases}$$

Remarque 4.1.5. Ces résultats sont cohérents avec [Ulm14a, §7]. Si d est pair, [Ulm14a, Lemma 7.1] donne $\frac{1}{12}\deg\Delta_{\min}(E_d/K) = \frac{d}{2}$. La preuve du [Ulm14a, Lemma 7.1] utilise la construction explicite du modèle régulier minimal $\pi : \mathcal{E}_d \to \mathbb{P}^1$ de E_d/K, dont on note $\varepsilon : \mathbb{P}^1 \to \mathcal{E}_d$ la section neutre. Alors, $\frac{1}{12}\deg\Delta_{\min}(E_d/K)$ est le degré du faisceau $s^*\Omega^1_{\mathcal{E}_d/\mathbb{P}^1}$.

4.1.4 Torsion et nombre de Tamagawa

Soit d un entier premier à q. Comme on l'a vu, la courbe elliptique $E_d/\mathbb{F}_q(t)$ n'est pas isotriviale. Des théorèmes généraux (*cf.* Théorème 1.5.2, Théorème 1.5.4) montrent alors que, lorsque $H(E_d/K) \to \infty$,

$$\#E_d(K)_{\mathrm{tors}} \ll_q 1 \quad \text{et} \quad \log \mathcal{T}am(E_d/K) = o\big(\log H(E_d/K)\big).$$

Dans notre situation, on peut cependant être plus précis : les deux propositions ci-dessous donnent des bornes explicites. Pour le détail de la preuve de la première, nous renvoyons la lectrice à [Ulm14a, Proposition 6.1].

Proposition 4.1.6 (Ulmer)**.** *Soit $d \geqslant 2$ un entier premier à q. Le sous-groupe de torsion du groupe de Mordell-Weil de la courbe de Legendre E_d sur $K = \mathbb{F}_q(t)$ est comme suit :*

$$E_d(K)_{\mathrm{tors}} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{si } d \text{ est pair} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{si } d \text{ est impair.} \end{cases}$$

En particulier, pour tout entier $d \geqslant 2$ premier à q, on a $\#E_d(K)_{\mathrm{tors}} \leqslant 8$.

Dans le modèle de Weierstrass affine (4.1), il y a trois points évidents sur E_d :

$$Q_0 = (0,0), \quad Q_1 = (-1,0), \quad Q_t = (-t^d, 0).$$

Ces points sont $\mathbb{F}_q(t)$-rationnels et clairement de 2-torsion. Pour tout d premier à q, $E_d(K)_{\mathrm{tors}}$ contient donc un sous-groupe isomorphe à on a donc $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Si d est pair, on peut de plus poser $P = (t^{d/2}, t^{d/2}(t^{d/2}+1))$. Il est facile de voir que $P \in E_d(K)$, que $2P = Q_0$ et donc P est un point de 4-torsion. Ceci démontre que le sous-groupe de torsion $E_d(K)_{\mathrm{tors}}$ est au moins aussi gros que ce qu'on a annoncé. La preuve que l'on a énuméré ainsi toute la torsion K-rationnelle sur E_d est détaillée dans [Ulm14a, Proposition 6.1]. Nous reviendrons sur des arguments similaires dans les chapitres suivants.

Par ailleurs, à défaut d'avoir une expression exacte du nombre de Tamagawa $\mathcal{T}am(E_d/K)$, on dispose d'un encadrement assez précis :

Proposition 4.1.7. *Soit $d \geqslant 2$ un entier premier à q et E_d la courbe de Legendre sur $\mathbb{F}_q(t)$. On a*

$$\mathcal{T}am\big(E_d/\mathbb{F}_q(t)\big) = 2d \cdot (2d)^{1-\theta(d)} \cdot 4^{\theta(d)} \cdot 2^{\varepsilon(d)},$$

où $\theta(d) \in \{0,1\}$ est défini par $d \equiv \theta(d) \bmod 2$ et $\varepsilon(d) \in \mathbb{N}$ vérifie $\varepsilon(d)/d \to 0$ lorsque $d \to +\infty$.

En particulier, ceci implique qu'il existe des constantes dépendant au plus de q telles que

$$\frac{\log d}{d} \ll_q \frac{\log \mathcal{T}am\big(E_d/\mathbb{F}_q(t)\big)}{\log H\big(E_d/\mathbb{F}_q(t)\big)} \ll_q \frac{\log d}{d}.$$

Démonstration. Concaténons les nombres de Tamagawa locaux $c_v(E_d/K)$ obtenus à la preuve de la Proposition 4.1.3 : on a

$$\mathcal{T}am(E_d/K) = \prod_{v|\Delta} c_v(E_d/K) = c_0(E_d/K) \cdot \prod_{v|(X^d-1)} c_v(E_d/K) \cdot c_\infty(E_d/K),$$

Où $c_0(E_d/K) = 2d$, $c_\zeta(E_d/K) \in \{1,2\}$ pour toute racine d-ième de l'unité $\zeta \in \overline{\mathbb{F}_q}$ et $c_\infty(E_d/K) = 2d$ (resp. $c_\infty(E_d/K) = 4$) si d est pair (resp. si d est impair). Afin d'expliciter le produit $\prod_{v|(X^d-1)} c_v(E_d/K)$, rappelons que l'on a

$$X^d - 1 = \prod_{d'|d} \Phi_{d'}(X),$$

où $\Phi_{d'}(X) \in \mathbb{F}_q[X]$ désigne le d'-ième polynôme cyclotomique, dont on connaît la forme de la décomposition en facteurs irréductibles unitaires dans $\mathbb{F}_q[X]$: $\Phi_{d'}(X)$ est un produit de $g' = \phi(d')/o_q(d')$ facteurs irréductibles unitaires, tous de degré $o_q(d')$ où, comme avant, on a noté $o_q(d')$ l'ordre multiplicatif de q modulo d' (*cf.* [Hin08, Théorème 6.2.8]). Appelons $V_{d',1}, \dots, V_{d',g'} \in \mathbb{F}_q[X]$ ces polynômes irréductibles unitaires et, pour tout $i \in [\![1, g']\!]$, on fixe $\zeta_{d',i} \in \overline{\mathbb{F}_q}$ une des racines de $V_{d',i}$: on a

$[\mathbb{F}_q(\zeta_{d',i}) : \mathbb{F}_q] = \deg V_{d',i} = o_q(d')$. On pose alors $\varepsilon(d',i) = 1$ si -1 est un carré dans $\mathbb{F}_q(\zeta_{d',i})$ et $\varepsilon(d',i) = 0$ sinon. Les places v de K telles que $v \mid X^d - 1$ sont alors en bijection avec l'ensemble des $\zeta_{d',i}$ (où $d' \mid d$ et $i \in [\![1, g']\!]$) et l'on trouve que :

$$\begin{aligned}\prod_{v|X^d-1} c_v(E_d/K) &= \prod_{d'|d} \prod_{v|\Phi_{d'}(X)} c_v(E_d/K) = \prod_{d'|d} \prod_{i=1}^{g'} c_{\zeta_{d',i}}(E_d/K) \\ &= \prod_{d'|d} \prod_{i=1}^{g'} 2^{\varepsilon(d',i)} = 2^{\sum_{d'|d} \sum_{i=1}^{g'} \varepsilon(d',i)} = 2^{\varepsilon(d)},\end{aligned}$$

où l'on a posé $\varepsilon(d) := \sum_{d'|d} \sum_{i=1}^{g'} \varepsilon(d',i) \in \mathbb{N}$. On a donc :

$$\mathcal{T}am(E_d/K) = \begin{cases} 2d \cdot 2^{\varepsilon(d)} \cdot 2d & \text{si } d \text{ est pair} \\ 2d \cdot 2^{\varepsilon(d)} \cdot 4 & \text{si } d \text{ est impair.} \end{cases} \tag{4.4}$$

Il reste à démontrer que $\varepsilon(d) = o(d)$ lorsque $d \to \infty$. Or, on a

$$0 \leqslant \varepsilon(d) = \sum_{d'|d} \sum_{i=1}^{g'} \varepsilon(d',i) \leqslant \sum_{d'|d} \sum_{i=1}^{g'} 1 = \sum_{d'|d} g' = \sum_{d'|d} \frac{\phi(d')}{o_q(d')}.$$

Et il suit de la Proposition 3.1.3 que la quantité la plus à droite vérifie, lorsque $d \to \infty$,

$$\sum_{d'|d} \frac{\phi(d')}{o_q(d')} \leqslant C \log q \cdot \frac{d}{\log d} = o\big(d\big),$$

où $C > 0$ est une constante absolue. Ce qui prouve que $\varepsilon(d) = o\big(d\big)$. Par ailleurs, l'égalité (4.4) conduit à

$$\log 8 + \log d \leqslant \log \mathcal{T}am(E_d/K) \leqslant \log 4 + \varepsilon(d) \log 2 + 2 \log d,$$

duquel on déduit l'encadrement annoncé dans l'énoncé de la Proposition car $H(E_d/K) = q^{\lfloor \frac{d+1}{2} \rfloor}$. □

4.2 Calcul de la fonction L des courbes E_d

Dans cette section, nous explicitons la fonction L de la courbe de Legendre E_d. Nous reprenons les notations et définitions des Sections 2.1.2 et 2.1.3 : une fois fixé un idéal premier $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$ au-dessus de p, on dispose du caractère de Teichmüller $\mathbf{t} : \overline{\mathbb{F}_q}^\times \to \overline{\mathbb{Q}}^\times$. De plus, pour tout entier $d \geqslant 2$, on a construit des caractères $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ dont l'ordre divise d (m parcourant $[\![1, d-1]\!]$). Avec ces notations, on a :

Théorème 4.2.1 (Conceição - Hall - Ulmer). *Soit $d \geqslant 2$ un entier premier à q. On note*

$$\mathcal{O}_q^{(2)}(d) = \begin{cases} \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/2\}\big)/\langle q \bmod d \rangle & \text{si } d \text{ est pair} \\ \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\big)/\langle q \bmod d \rangle & \text{si } d \text{ est impair.} \end{cases}$$

La fonction L de la courbe de Legendre E_d définie sur $K = \mathbb{F}_q(t)$ s'exprime sous la forme

$$L(E_d/K, T) = \prod_{m \in \mathcal{O}_q^{(2)}(d)} \Big(1 - \mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 T^{u(m)}\Big),$$

où, pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$, on a noté $\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)$ la somme de Jacobi suivante :

$$\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m) = -\sum_{x \in \mathbb{F}_{q^{u(m)}}} \mathbf{t}_m(x) \cdot \mathbf{t}_m(1-x).$$

Ce calcul est présenté en détail dans [CHU14] : pour le confort de lecture, nous rappelons ici la preuve de [CHU14, Theorem 3.2.1]. Ceci nous permet de mettre le théorème en conformité avec nos notations et d'illustrer le fonctionnement des outils de la Section 2.1.4. La preuve du Théorème occupe les deux sous-sections qui suivent.

4.2.1 Décompte des points rationnels

On utilise l'approche « directe » du calcul de la fonction L : il s'agit de revenir à la définition de $L(E_d/\mathbb{F}_q(t), T)$ comme produit eulérien sur les places v de K, on calcule le nombre de points rationnels sur les réductions $\overline{(E_d)}_v$ de E_d en toutes les places v et l'on concatène ces informations pour obtenir $L(E_d/K, T)$ sous la forme d'un polynôme.

Soit $d \geqslant 2$ un entier premier à q, que l'on considère fixé pour le reste de la section. Soit $n \geqslant 1$ et $\mathbb{F}_Q = \mathbb{F}_{q^n}$ l'extension de degré n de $\mathbb{F}_q$. Pour tout point $\tau \in \mathbb{P}^1(\mathbb{F}_Q)$, on notera

$$A(\tau, Q) := Q + 1 - \#\overline{(E_d)}_\tau(\mathbb{F}_Q),$$

où $\overline{(E_d)}_\tau$ désigne la réduction d'un modèle entier minimal de E_d en la place v_τ de K correspondant à τ. La courbe $\overline{(E_d)}_\tau$ est donc une cubique plane irréductible (éventuellement singulière) définie sur le corps résiduel $\mathbb{F}_{v_\tau} \subset \mathbb{F}_Q$ de K en v_τ. Comme on l'a expliqué à la Section 4.1.1, le modèle de Weierstrass affine :

$$E_d : \quad y^2 = x(x+1)(x+t^d)$$

est entier et minimal en toute place v de K, sauf en la place ∞. On peut d'ores et déjà calculer $A(\infty, Q)$: puisque la réduction de E_d en $v = \infty$ est multiplicative déployée (resp. additive) lorsque d est pair (resp. impair), on a :

$$A(\infty, Q) = \begin{cases} 1 & \text{si } d \text{ est pair} \\ 0 & \text{si } d \text{ est impair} \end{cases} = \frac{1 + (-1)^d}{2}.$$

Commençons par démontrer la Proposition suivante :

Proposition 4.2.2. *Soit $\mathbb{F}_Q/\mathbb{F}_q$ une extension finie. Alors*

$$\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_Q)} A(\tau, Q) = -\sum_{\chi \in Y(d,Q)} \mathbf{j}_Q(\chi, \mu)^2 = -\sum_{\chi \in Y(d,Q)} \chi(16) \cdot \mathbf{j}_Q(\chi, \chi)^2,$$

les sommes portant sur l'ensemble suivant de caractères :

$$Y(d, Q) = \left\{ \chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times \;\middle|\; \chi^d = \mathbf{1},\ \chi \neq \mathbf{1}, \mu \right\}.$$

Démonstration. Soit $\tau \in \mathbb{F}_Q$ (*i.e.* $\tau \in \mathbb{P}^1(\mathbb{F}_Q) \smallsetminus \{\infty\}$), on note à nouveau $\overline{(E_d)}_\tau$ la réduction de E_d en τ : une équation de la partie affine de celle-ci est donc :

$$\overline{(E_d)}_\tau : \quad y^2 = x(x+1)(x+\tau^d).$$

Pour compter le nombre de points $\mathbb{F}_Q$-rationnels sur cette courbe, une fois pris en compte son (unique) point à l'infini, on utilise le Lemme 2.2.1 : désignant par $\mu : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ l'unique caractère non trivial d'ordre 2 sur $\mathbb{F}_Q^\times$, on a

$$\begin{aligned} \#\overline{(E_d)}_\tau(\mathbb{F}_Q) &= 1 + \#\left\{(x,y) \in \mathbb{F}_Q^2 \;\middle|\; y^2 = x(x+1)(x+\tau^d)\right\} \\ &= 1 + \sum_{x \in \mathbb{F}_Q} \#\left\{y \in \mathbb{F}_Q \;\middle|\; y^2 = x(x+1)(x+\tau^d)\right\} \\ &= 1 + \sum_{x \in \mathbb{F}_Q} \big(1 + \mu\big(x(x+1)(x+\tau^d)\big)\big) \\ &= Q + 1 + \sum_{x \in \mathbb{F}_Q} \mu\big(x(x+1)(x+\tau^d)\big). \end{aligned}$$

Par suite, pour tout $\tau \in \mathbb{F}_Q$, on a

$$A(\tau, Q) = Q + 1 - \#\overline{(E_d)}_\tau(\mathbb{F}_Q) = -\sum_{x \in \mathbb{F}_Q} \mu\big(x(x+1)(x+\tau^d)\big).$$

Dès lors, la somme à calculer s'écrit :

$$\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_Q)} A(\tau, Q) = A(\infty, Q) + \sum_{\tau \in \mathbb{F}_Q} A(\tau, Q) = A(\infty, Q) - \sum_{\tau \in \mathbb{F}_Q} \sum_{x \in \mathbb{F}_Q} \mu\big(x(x+1)(x+\tau^d)\big).$$

On « réindexe » ensuite la somme portant sur $\tau \in \mathbb{F}_Q$ à l'aide du Lemme 2.2.2 :

$$\begin{aligned}\sum_{\tau\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\mu\big(x(x+1)(x+\tau^d)\big) &= \sum_{x\in\mathbb{F}_Q}\sum_{\tau\in\mathbb{F}_Q}\mu\big(x(x+1)(x+\tau^d)\big)\\ &= \sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\#\big\{\tau\in\mathbb{F}_Q \;\big|\; \tau^d=z\big\}\cdot\mu\big(x(x+1)(x+z)\big)\\ &= \sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\left(\sum_{\chi^d=\mathbf{1}}\chi(z)\right)\mu\big(x(x+1)(x+z)\big)\\ &= \sum_{\chi^d=\mathbf{1}}\left(\sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\chi(z)\mu\big(x(x+1)(x+z)\big)\right),\end{aligned}$$

où $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ parcourt l'ensemble des caractères de $\mathbb{F}_Q^\times$ dont la puissance d-ième est triviale (*i.e.* les caractères dont l'ordre divise d). Explicitons maintenant les doubles sommes internes en termes de sommes de Jacobi :

Lemme 4.2.3. *Soit $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ un caractère (quelconque). Alors :*

$$\sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\chi(z)\mu\big(x(x+1)(x+z)\big) = \mathbf{j}_Q(\chi,\mu)^2.$$

Démonstration. Soit donc χ un caractère, cherchons à expliciter :

$$\sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\chi(z)\mu\big(x(x+1)(x+z)\big) = \sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\chi(z)\mu(x)\mu(x+1)\mu(x+z).$$

Commençons par remarquer que les termes avec « $x = 0$ » ne contribuent pas à la somme car $\mu(0) = 0$. On peut donc réindexer la somme interne en posant « $z = x \cdot v$ » :

$$\begin{aligned}\sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\chi(z)\mu\big(x(x+1)(x+z)\big) &= \sum_{x\in\mathbb{F}_Q^\times}\sum_{z\in\mathbb{F}_Q}\chi(z)\mu\big(x(x+1)(x+z)\big)\\ &= \sum_{x\in\mathbb{F}_Q^\times}\sum_{v\in\mathbb{F}_Q}\chi(xv)\mu\big(x(x+1)(x+xv)\big)\\ &= \sum_{x\in\mathbb{F}_Q^\times}\sum_{v\in\mathbb{F}_Q}\chi(x)\chi(v)\mu(x^2)\mu((x+1)(1+v))\\ &= \sum_{x\in\mathbb{F}_Q^\times}\sum_{v\in\mathbb{F}_Q}\chi(x)\chi(v)\mu((x+1)(v+1)),\end{aligned}$$

car $\mu(x^2) = 1$ pour tout $x \neq 0$. Cette dernière expression se factorise sous la forme :

$$\begin{aligned}\sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\chi(z)\mu\big(x(x+1)(x+z)\big) &= \sum_{x\in\mathbb{F}_Q^\times}\chi(x)\mu(x+1)\left(\sum_{v\in\mathbb{F}_Q}\chi(v)\mu(1+v)\right)\\ &= \left(\sum_{x\in\mathbb{F}_Q^\times}\chi(x)\mu(x+1)\right)\left(\sum_{v\in\mathbb{F}_Q}\chi(v)\mu(v+1)\right).\end{aligned}$$

L'intérêt de cette transformation est alors évident : on reconnaît (presque) une somme de Jacobi dans chacun des facteurs. Plus précisément, on a

$$\sum_{v\in\mathbb{F}_Q}\chi(v)\mu(1+v) = \sum_{w\in\mathbb{F}_Q}\chi(-v)\mu(1-w) = \chi(-1)\cdot\sum_{w\in\mathbb{F}_Q}\chi(v)\mu(1-v) = -\chi(-1)\cdot\mathbf{j}_Q(\chi,\mu).$$

De façon très similaire, le premier facteur vaut

$$\sum_{x\in\mathbb{F}_Q^\times}\chi(x)\mu(x+1) = -\chi(-1)\cdot\sum_{x'\neq 0}\chi(x')\mu(1-x') = -\chi(-1)\cdot\mathbf{j}_Q(\chi,\mu).$$

La dernière égalité suit de la Proposition 2.2.7 en distinguant deux cas suivant que χ est trivial ou non. Ceci conclut la preuve du Lemme car $\chi(-1)^2 = 1$. □

En particulier, si $\chi = \mathbf{1}$ est le caractère trivial, on a (*cf.* Proposition 2.2.7) :

$$\sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\mathbf{1}(z)\mu\big(x(x+1)(x+z)\big) = \mathbf{j}_Q(\mathbf{1},\mu)^2 = 0.$$

D'après la même Proposition 2.2.7, pour $\chi = \mu$, on a

$$\sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\mu(z)\mu\big(x(x+1)(x+z)\big) = \mathbf{j}_Q(\mu,\mu)^2 = \mu(-1)^2 = 1.$$

Par conséquent, si l'on introduit l'ensemble $X(d,Q)$ des caractères *non triviaux* $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ dont l'ordre divise d, on a démontré que

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) = A(\infty,Q) - \sum_{\chi^d=\mathbf{1}} \mathbf{j}_Q(\chi,\mu)^2 = A(\infty,Q) - \sum_{\chi\in X(d,Q)} \mathbf{j}_Q(\chi,\mu)^2.$$

Comme dans l'énoncé de la Proposition, soit maintenant

$$Y(d,Q) := \left\{\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times \;\middle|\; \chi^d = \mathbf{1},\ \chi \neq \mathbf{1}, \mu\right\}.$$

Pour conclure la preuve de la Proposition 4.2.2, distinguons deux cas :

- Si d est impair, on a $A(\infty,Q) = 0$ et $Y(d,Q) = X(d,Q)$ car le caractère μ n'est pas dans $X(d,Q)$ (comme d est impair et μ d'ordre exactement 2, on a $\mu^d = \mu \neq \mathbf{1}$). On a donc, dans ce cas,

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) = 0 - \sum_{\chi\in X(d,Q)} \mathbf{j}_Q(\chi,\mu)^2 = -\sum_{\chi\in Y(d,Q)} \mathbf{j}_Q(\chi,\mu)^2.$$

- Si maintenant d est pair, on a $A(\infty,Q) = 1$ et $\mu \in X(d,Q)$. Ainsi, $Y(d,Q) = X(d,Q) \smallsetminus \{\mu\}$ et, comme on vient de voir que $\mathbf{j}_Q(\mu,\ mu)^2 = 1$, on a

$$\begin{aligned}\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) &= 1 - \sum_{\chi\in X(d,Q)} \mathbf{j}_Q(\chi,\mu)^2 = 1 - \mathbf{j}_Q(\mu,\mu)^2 - \sum_{\chi\in Y(d,Q)} \mathbf{j}_Q(\chi,\mu)^2 \\ &= -\sum_{\chi\in Y(d,Q)} \mathbf{j}_Q(\chi,\mu)^2.\end{aligned}$$

Il ne reste finalement qu'à utiliser le Lemme 2.2.9 : pour tout caractère non trivial χ de $\mathbb{F}_Q^\times$, on a

$$\mathbf{j}_Q(\mu,\chi) = \chi(4)\cdot\mathbf{j}_Q(\chi,\chi).$$

□

4.2.2 Réindexation des caractères et conclusion

Pour toute extension finie $\mathbb{F}_{q^n}/\mathbb{F}_q$, la Proposition 4.2.2 donne que

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau,q^n) = -\sum_{\chi\in Y(d,q^n)} \chi(16)\cdot\mathbf{j}_{q^n}(\chi,\chi)^2,$$

la somme portant sur un ensemble de caractères. Par définition (*cf.* Lemme 1.3.15), on a

$$\log\big(L(E_d/\mathbb{F}_q(t),T)\big) = \sum_{n=1}^{\infty}\left(\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau,q^n)\right)\frac{T^n}{n}.$$

Ainsi, on a prouvé que

$$\log L\big(E_d/\mathbb{F}_q(t),T\big) = -\sum_{n=1}^{\infty}\left(\sum_{\chi\in Y(d,q^n)} \chi(16)\cdot\mathbf{j}_{q^n}(\chi,\chi)^2\right)\frac{T^n}{n}.$$

Dans le membre de droite, on reconnaît le genre de sommes étudiées à la Proposition 2.1.15 (avec $\ell = 2$) : pour toute extension $\mathbb{F}_Q/\mathbb{F}_q$ et tout caractère non trivial $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$, on pose :

$$\sigma(\chi,Q) = \chi(16)\cdot\mathbf{j}_Q(\chi,\chi)^2.$$

Montrons maintenant que cette donnée satisfait aux hypothèses de la Proposition sus-citée. Pour toute extension $\mathbb{F}_{Q^s}/\mathbb{F}_Q$, on note $\chi^{(s)} = \chi \circ \mathbf{N}_{\mathbb{F}_{Q^s}/\mathbb{F}_Q}$ le caractère sur $\mathbb{F}_{Q^s}^\times$ déduit de χ : comme les sommes de Jacobi satisfont une relation de Hasse-Davenport à l'ordre 1 (Théorème 2.2.20) et que $16 \in \mathbb{F}_q \subset \mathbb{F}_Q$, on a

$$\sigma(\chi^{(s)}, Q^s) = \chi^{(s)}(16) \cdot \mathbf{j}_{Q^s}(\chi^{(s)}, \chi^{(s)})^2 = \chi(16^s) \cdot (\mathbf{j}_Q(\chi,\chi))^{2s} = \sigma(\chi, Q)^s.$$

De plus, comme $\sigma(\chi, Q)$ est (le carré d') une somme portant sur les éléments de $\mathbb{F}_Q$, on a clairement $\sigma(\chi^q, Q) = \sigma(\chi, Q)$ (puisque $x \mapsto x^q$ est une permutation de $\mathbb{F}_Q$). Les deux hypothèses de la Proposition 2.1.15 étant vérifiées (avec $\ell = 2$ et $K = 1$), on a donc :

$$\sum_{n=1}^{\infty} \left(\sum_{\chi \in Y(d,q^n)} \sigma(\chi, Q) \right) \frac{T^n}{n} = \sum_{m \in \mathcal{O}_q^{(2)}(d)} -\log\left(1 - \sigma(\mathbf{t}_m, q^{u(m)}) \cdot T^{u(m)}\right),$$

où $\mathcal{O}_q^{(2)}(d)$ désigne l'ensemble des orbites de $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ sous l'action de q par multiplication, sauf l'orbite $\{d/2\}$ si d est pair. Remarquer que l'on a ici désigné par $\sigma(\mathbf{t}_m, q^{u(m)})$ ce qu'on aurait dû, en toute rigueur, noter « $\sigma(\mathbf{t}_a, q^{u(a)})$ pour un choix quelconque de $a \in m$ ». On en tire l'égalité suivante :

$$\log L\big(E_d/\mathbb{F}_q(t), T\big) = \log \left(\prod_{m \in \mathcal{O}_q^{(2)}(d)} \left(1 - \sigma(\mathbf{t}_m, q^{u(m)}) \cdot T^{u(m)}\right) \right).$$

Il ne reste qu'à expliciter $\sigma(\mathbf{t}_m, q^{u(m)}) = \mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2$ et à prendre l'exponentielle de cette identité pour avoir l'expression attendue de $L(E_d/K, T)$:

$$L\big(E_d/K, T\big) = \prod_{m \in \mathcal{O}_q^{(2)}(d)} \left(1 - \sigma(\mathbf{t}_m, q^{u(m)}) \cdot T^{u(m)}\right).$$

Ceci conclut la preuve du Théorème 4.2.1.

Remarque 4.2.4. La fonction L obtenue est bien un polynôme en T, de degré (voir l'item (ii) de la Proposition 3.1.3)

$$\deg L(E_d/K, T) = \sum_{m \in \mathcal{O}_q^{(2)}(d)} u(m) = \begin{cases} d-2 & \text{si } d \text{ est pair} \\ d-1 & \text{si } d \text{ est impair.} \end{cases}$$

Ceci est cohérent avec la Remarque suivant la Proposition 4.1.4.

Remarque 4.2.5. Nous avons ici choisi d'écrire la fonction L de E_d comme un produit de facteurs

$$1 - \mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 \cdot T^{u(m)}.$$

Les auteurs de [CHU14] ont préféré écrire $L(E_d/K, T)$ comme un produit de

$$1 - \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mu_{q^{u(m)}})^2 \cdot T^{u(m)},$$

où $\mu_{q^{u(m)}} : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ est l'unique caractère non trivial d'ordre 2 sur $\mathbb{F}_{q^{u(m)}}$. Les deux produits portent sur le même ensemble d'orbites $m \in \mathcal{O}_q^{(2)}(d)$ et les deux facteurs écrits ci-dessus sont en fait égaux (nous l'avons démontré au Lemme 2.2.9).

Remarque 4.2.6. Notons que, lorsque l'entier $d \geqslant 2$ divise $q-1$, on obtient une expression bien plus simple de $L(E_d/K, T)$ comme suit : comme d divise $q-1 = \#\mathbb{F}_q^\times$, il existe un caractère $\chi_0 : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ d'ordre exactement d. Alors $\mathcal{O}'_q(d) = \mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ (car $q \equiv 1 \bmod d$) et

$$L\big(E_d/K, T\big) = \prod_{\substack{n=1 \\ n \neq d/2}}^{d-1} \left(1 - \chi_0(16)^n \mathbf{j}_q({\chi_0}^n, {\chi_0}^n)^2 \cdot T\right).$$

Ceci étant, nous ne pouvons nous contenter de $d \mid q-1$: nous nous intéressons en effet au comportement asymptotique de $\mathfrak{Bs}(E_d/\mathbb{F}_q(t))$ lorsque $H(E_d/K) \sim q^{d/2} \to +\infty$. Pour cela, il faut que d puisse être arbitrairement grand, à q fixé.

4.3 Rang et valeur spéciale de E_d

4.3.1 La conjecture de Birch et Swinnerton-Dyer

Théorème 4.3.1 (Ulmer). *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$. Pour tout entier $d \in \mathbb{N}^*$, premier à p, on note à nouveau E_d la courbe elliptique de Legendre sur $K = \mathbb{F}_q(t)$ donnée par* (4.1).

La conjecture de Birch et Swinnerton-Dyer (Conjecture 1.4.1) est vraie pour la courbe elliptique E_d/K. En particulier, le groupe de Tate-Shafarevich $Ш(E_d/K)$ est fini et le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ est fini.

Nous renvoyons le lecteur à [Ulm14a, §11] et [Ulm13, §7], plus particulièrement [Ulm14a, Corollary 11.3] pour la preuve de ce Théorème. Les points importants de la preuve sont les suivants : la courbe E_d est isogène, après une extension finie $k'/\mathbb{F}_q$ du corps des constantes, à la courbe elliptique E'_d, définie sur $K = \mathbb{F}_q(t)$, dont un modèle affine est

$$E'_d : \quad y^2 + xy + t^d y = x^3 + t^d x^2.$$

Or, la conjecture de Birch et Swinnerton-Dyer « faible » est démontrée pour E'_d dans [Ulm13, §7], à l'aide des résultats de [Ber08]. Comme la véracité de la conjecture de Birch et Swinnerton-Dyer est invariante par isogénie et par « descente » finie du corps des constantes (*cf.* le point (4) de [Ulm11, Lecture 3, Theorem 8.1]), on en déduit que la conjecture « faible » est vérifiée par E_d/K. On peut alors invoquer les résultats rappelés à la Section 1.4.3 pour en conclure que la conjecture de Birch et Swinnerton-Dyer « forte » est vraie pour E_d/K.

4.3.2 Rang et valeur spéciale de E_d/K

Soit $d \geqslant 2$ un entier premier à la caractéristique de $K = \mathbb{F}_q(t)$. Nous avons vu (Théorème 4.2.1) que la fonction L de la courbe « de Legendre » E_d/K s'écrit sous la forme d'un produit :

$$L(E_d/K, T) = \prod_{m \in \mathcal{O}_q^{(2)}(d)} \left(1 - \mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 \cdot T^{u(m)}\right).$$

Ceci incite à poser la définition suivante :

Définition 4.3.2. Pour tout entier $d \geqslant 2$ premier à q, on pose :

$$\mathcal{Z}_q(d) := \left\{ m \in \mathcal{O}_q^{(2)}(d) \;\middle|\; \mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 = q^{u(m)} \right\}$$

et son complémentaire $\mathcal{V}_q^*(d) := \mathcal{O}_q^{(2)}(d) \smallsetminus \mathcal{Z}_q(d)$.

Munis de ces notations, on a :

Proposition 4.3.3 (Ulmer). *Soit $d \geqslant 2$ un entier premier à q. On considère à nouveau la courbe « de Legendre » E_d sur $K = \mathbb{F}_q(t)$ donnée par le modèle de Weierstrass* (4.1). *Le rang du groupe de Mordell-Weil $E_d(K)$ s'exprime sous la forme*

$$\operatorname{rang} E_d(K) = \#\mathcal{Z}_q(d) = \# \left\{ m \in \mathcal{O}_q^{(2)}(d) \;\middle|\; \mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 = q^{u(m)} \right\}.$$

Démonstration. Pour simplifier les écritures, notons ici $L(T) = L(E_d/K, T)$ et, pour tout $m \in \mathcal{O}_q^{(2)}(d)$, $\omega(m) = \mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2$. Il suit immédiatement du Lemme 3.1.4 (voir aussi l'Exemple 3.1.9) que

$$\operatorname{ord}_{T=q^{-1}} L(T) = \# \left\{ m \in \mathcal{O}_q^{(2)}(d) \;\middle|\; \omega(m) = q^{u(m)} \right\} = \#\mathcal{Z}_q(d).$$

De plus, la conjecture de Birch et Swinnerton-Dyer étant vraie pour E_d/K (Théorème 4.3.1), il y a égalité entre rangs algébrique et analytique, *i.e.* $\operatorname{rang} E_d(K) = \operatorname{ord}_{T=q^{-1}} L(T)$. □

Proposition 4.3.4. *Soit $d \geqslant 2$ un entier premier à q. La valeur spéciale en $T = q^{-1}$ de la fonction L de la courbe elliptique de Legendre E_d/K s'écrit sous la forme :*

$$L^*(E_d/K, 1) = \prod_{m \in \mathcal{Z}_q(d)} u(m) \cdot \prod_{m \in \mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2}{q^{u(m)}}\right).$$

Démonstration. Le calcul a été essentiellement effectué à la Section 3.1 (*cf.* Exemple 3.1.9). Pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$, on pose $g_m(T) = 1 - \omega(m) \cdot T^{u(m)}$. Alors, $L(E_d/K, T) = \prod_{m \in \mathcal{O}_q^{(2)}(d)} g_m(T)$ et $g_m(q^{-1}) = 0$ si et seulement si $m \in \mathcal{Z}_q(d)$. D'où,

$$\frac{L(E_d/K, T)}{(1-qT)^r} = \prod_{m \in \mathcal{Z}_q(d)} \frac{g_m(T)}{1-qT} \cdot \prod_{m \in \mathcal{V}_q^*(d)} g_m(T).$$

L'évaluation de ce polynôme en $T = q^{-1}$ fournit bien, par définition de la valeur spéciale (Définition 1.3.12), l'expression annoncée. □

Remarquons que, comme E_d/K vérifie la conjecture de Birch et Swinnerton-Dyer, la valeur spéciale $L^*(E_d/K, 1)$ s'écrit comme

$$L^*(E_d/K, 1) = \frac{\#Ш(E_d/K) \cdot \mathrm{Reg}(E_d/K)}{\left(\#E_d(K)_{\mathrm{tors}}\right)^2} \cdot \mathcal{T}am(E_d/K) \cdot \frac{q}{H(E_d/K)},$$

un produit de nombres rationnels strictement positifs. Donc $L^*(E_d/K, 1)$ est elle-même rationnelle et strictement positive.

4.3.3 Commentaires

Dans [Ulm14a], D. Ulmer démontre :

Proposition 4.3.5 (Ulmer)**.** *Lorsque d parcourt l'ensemble des entiers premier à p, le rang des courbes de Legendre E_d sur $K = \mathbb{F}_q(t)$ n'est pas borné :*

$$\limsup_{\mathrm{pgcd}(d,q)=1} \mathrm{rang}\, E_d(K) = +\infty.$$

C'est un cas particulier de [Ulm07b, Theorem 4.7] (voir aussi [Ulm11, Lecture 4, Theorem 3.1.1] et [Ber08, Theorem 4.1]). Comme c'est ici une conséquence facile de la Proposition 4.3.3 et du Théorème de Shafarevich-Tate (Théorème 2.4.4), nous en donnons la preuve.

Démonstration. Il suffit de démontrer que, pour $d \in \mathbb{N}^*$ premier à p bien choisi, « beaucoup » de sommes de Jacobi sont « triviales ». Nous reprenons les notations introduites ci-dessus. On se place dans le cas où $d = d_N = q^N + 1$ (avec $N \in \mathbb{N}^*$) : le Corollaire 2.4.5 donne que

$$\forall m \in \mathcal{O}_q^{(2)}(d), \quad \mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 = q^{u(m)}.$$

Ainsi, pour $d_N = q^N + 1$, on a $\mathcal{Z}_q(d_N) = \#\mathcal{O}_q^{(2)}(d_N)$ et

$$\mathrm{rang}\, E_{d_N}(\mathbb{F}_q(t)) = \#\mathcal{Z}_q(d_N) = \#\mathcal{O}_q^{(2)}(d_N).$$

On peut par ailleurs facilement minorer $\#\mathcal{O}_q^{(2)}(d_N)$ (voir le Lemme 2.4.1) :

$$\#\mathcal{O}_q^{(2)}(d_N) = \#\mathcal{O}'_q(d_N) - 1 = \sum_{\substack{d' \mid d_N \\ d' > 2}} \frac{\phi(d')}{o_q(d')} \geqslant \frac{1}{o_q(d_N)} \cdot \sum_{\substack{d' \mid d_N \\ d' > 2}} \phi(d') = \frac{d_N - 1}{o_q(d_N)} = \frac{d_N - 1}{2N}.$$

Vu que $\log d_N \geqslant N \cdot \log q$, ceci conduit alors à

$$\mathrm{rang}\, E_{d_N}(\mathbb{F}_q(t)) \geqslant \frac{d_N - 1}{2N} \geqslant \log\sqrt{q} \cdot \frac{d_N - 1}{\log d_N} \gg_q \frac{d_N}{\log d_N},$$

la constante implicite ne dépendant que de q. Comme la quantité à droite tend vers $+\infty$ avec $N \in \mathbb{N}^*$, la Proposition est démontrée. □

Dans la situation où $d = d_N = q^N + 1$, la Proposition 4.3.4 implique immédiatement que la valeur spéciale $L^*(E_{d_N}/K, 1)$ est un entier :

$$L^*(E_{d_N}/K, 1) = \prod_{m \in \mathcal{O}_q^{(2)}(d_N)} u(m) \in \mathbb{N}^*.$$

En particulier, $\log L^*(E_{d_N}/K, 1) \geqslant 0$ et, anticipant quelque peu sur la Section ci-dessous, on trouve que pour $d = d_N = q^N + 1$,

$$\mathfrak{Bs}(E_{d_N}/K, 1) \geqslant 1 + o(1) \qquad (N \to \infty).$$

4.4 Étude du ratio de Brauer-Siegel des courbes de Legendre

Dans cette section, nous utilisons les résultats des pages précédentes pour démontrer le Théorème principal de ce chapitre, à savoir :

Théorème 4.4.1. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \geqslant 2$ premier à q, on considère la courbe elliptique « de Legendre » E_d sur K, dont un modèle de Weierstrass affine est*

$$E_d : \quad Y^2 = X(X+1)(X+t^d).$$

Lorsque $d \to +\infty$ (i.e. $H(E_d/K) \to +\infty$), le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ admet une limite et celle-ci vaut 1 :

$$\mathfrak{Bs}(E_d/K) \xrightarrow[\substack{\mathrm{pgcd}(d,q)=1 \\ d\to+\infty}]{} 1.$$

Comme la conjecture de Birch et Swinnerton-Dyer est vraie pour la courbe E_d (Théorème 4.3.1), qui n'est pas isotriviale, on peut utiliser la Proposition 1.6.4 de la Section 1.6.3 : lorsque $H(E_d/K) \to +\infty$, on a

$$\mathfrak{Bs}(E_d/K) = 1 + \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} + o(1). \tag{4.5}$$

Pour estimer la limite qui nous intéresse, il faut donc donner un encadrement de la valeur spéciale $L^*(E_d/K,1)$. Plus précisément, vu l'énoncé du Théorème 4.4.1 et la relation (4.5), nous devons démontrer :

– une majoration :

$$\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \leqslant 0 + o\big(1\big) \qquad (d \to \infty),$$

ce que nous faisons à la Proposition 4.4.2.

– puis une minoration « forte » :

$$\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \geqslant 0 - o\big(1\big) \qquad (d \to \infty).$$

C'est la partie la plus difficile de la preuve (*cf.* Proposition 4.4.3).

La combinaison de ces deux inégalités et de (4.5) donne alors le résultat escompté :

$$1 - o(1) \leqslant \mathfrak{Bs}(E_d/K) \leqslant 1 + o(1) \qquad (d \to \infty).$$

Il ne reste donc qu'à démontrer la majoration et la minoration annoncées ci-dessus. Ceci occupe le reste de la Section.

4.4.1 Majoration de la valeur spéciale

Proposition 4.4.2. *Soit $d \geqslant 2$ un entier premier à q. Lorsque $d \to \infty$, la valeur spéciale $L^*(E_d/K,1)$ de la fonction L associée à la courbe de Legendre E_d admet la majoration suivante :*

$$\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \leqslant 0 + o\big(1\big) \qquad (d \to \infty).$$

Cette Proposition est un cas particulier de [HP16, Theorem 7.5] mais nous pouvons en donner une preuve directe avec les outils développés à la Section 3.1. Nous obtenons en fait une inégalité plus explicite :

$$\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \leqslant c' \cdot \frac{\log\log d}{\log d} \qquad (d \to \infty),$$

où $c' > 0$ est une constante absolue, que l'on peut prendre $\leqslant 30$.

Démonstration. À la Proposition 4.3.4, nous avons démontré que

$$L^*(E_d/K,1) = \prod_{m \in \mathcal{Z}_q(d)} u(m) \cdot \prod_{m \in \mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2}{q^{u(m)}}\right),$$

où $\mathcal{Z}_q(d)$ et $\mathcal{V}_q^*(d)$ sont les ensembles d'orbites $\subset \mathcal{O}_q^{(2)}(d)$ définis à la Section 4.3. Comme on l'a déjà remarqué plus haut, la fonction $L(E_d/K,T)$ est un polynôme de la forme étudiée à la Section 3.1. On en déduit donc (Proposition 3.1.8 avec $K=1$) :

$$\log L^*(E_d/K,1) \leqslant 3C\log q \cdot \frac{d\log\log d}{\log d},$$

où $C>0$ est une constante absolue. D'autre part, on a $\log H(E_d/K) = \left\lfloor \frac{d+1}{2} \right\rfloor \cdot \log q$ (Proposition 4.1.4). Ce qui donne

$$\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \leqslant 3C \cdot \frac{d\log\log d}{\log d} \cdot \frac{1}{\left\lfloor \frac{d+1}{2} \right\rfloor} \leqslant 3C \cdot \frac{\log\log d}{\log d} \cdot \frac{2d}{d+1} \leqslant 6C \cdot \frac{\log\log d}{\log d} = o\big(1\big).$$

Ce qui conclut la preuve. □

4.4.2 Minoration de la valeur spéciale

Pour minorer la valeur spéciale $L^*(E_d/K,1)$, nous utilisons les outils mis en place à la Section 3.2.

Proposition 4.4.3. *Soit $d \geqslant 2$ un entier premier à q. Lorsque $d \to \infty$, la valeur spéciale $L^*(E_d/K,1)$ de la fonction L associée à la courbe de Legendre E_d vérifie :*

$$\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \geqslant 0 + o\big(1\big) \qquad (d\to\infty).$$

Ce résultat se réécrit sous la forme compacte suivante : pour tout entier $d \geqslant 2$ premier à q, la valeur spéciale est « asymptotiquement presque entière » au sens où elle est de la forme

$$L^*(E_d/K,1) = \frac{(\text{entier})}{q^{o(d)}} \qquad (d\to\infty).$$

Démonstration. En premier lieu, remarquons que pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$, on a $u(m) = \#m \in \mathbb{N}^*$ et qu'on l'on peut d'ores et déja minorer la valeur spéciale $L^*(E_d/K,1)$ comme suit :

$$\begin{aligned}
\log L^*(E_d/K,1) &= \log \prod_{m\in\mathcal{Z}_q(d)} u(m) + \log \prod_{m\in\mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{t}_m(16)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m)^2}{q^{u(m)}}\right) \\
&\geqslant \log 1 + \log \prod_{m\in\mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{t}_m(16)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m)^2}{q^{u(m)}}\right) \\
&\geqslant \log \prod_{m\in\mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{t}_m(16)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m)^2}{q^{u(m)}}\right). \qquad (4.6)
\end{aligned}$$

Pour tout $m \in \mathcal{O}_q^{(2)}(d)$, on pose $y(m) = \mathbf{t}_m(16)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m)^2$. On notera $\mathcal{M} = \mathcal{V}_q^*(d)$. Vérifions que cette donnée satisfait aux hypothèses (i), (ii) et (iii) de la Section 3.2.1 :

(i) Pour toute $m \in \mathcal{M}$, on a $y(m) \in \mathbb{Q}(\zeta_{d'}) \subset \mathbb{Q}(\zeta_d)$ où $d' = d/\operatorname{pgcd}(d,m)$. En effet, pour $m \in [\![1, d-1]\!]$, le caractère $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ est d'ordre $d/\operatorname{pgcd}(d,m)$ et, comme $m \neq d/2$, on a $d' > 2$. Par définition, la somme de Jacobi $\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m)$ est un entier de $\mathbb{Q}(\zeta_{d'})$. Notons par ailleurs que pour tout $m \in \mathcal{O}_q^{(2)}(d)$, on a $|y(m)| = q^{u(m)}$ dans tout plongement complexe de $\mathbb{Q}(\zeta_{d'})$ car $\mathbf{t}_m$ n'est ni le caractère trivial, ni le caractère quadratique de $\mathbb{F}_{q^{u(m)}}^\times$.

(ii) Pour $m \in \mathcal{O}_q^{(2)}(d)$ et $a \in (\mathbb{Z}/d\mathbb{Z})^\times$, si l'on note $\sigma_a \in \operatorname{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ l'automorphisme de $\mathbb{Q}(\zeta_d)$ correspondant à a, on a (*cf.* Lemme 3.3.8)

$$\sigma_a\big(\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m)\big) = \mathbf{j}_{q^{u(m)}}(\sigma_a(\mathbf{t}_m),\sigma_a(\mathbf{t}_m)) = \mathbf{j}_{q^{u(m)}}(\mathbf{t}_{a\cdot m},\mathbf{t}_{a\cdot m}).$$

D'où l'on tire immédiatement que $\sigma_a(y(m)) = y(a\cdot m)$.

(iii) Enfin, par construction de $\mathcal{V}_q^*(d)$, le produit

$$\prod_{m\in\mathcal{M}} \left(1 - \frac{y(m)}{q^{u(m)}}\right) = \prod_{m\in\mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{t}_m(16)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m)^2}{q^{u(m)}}\right)$$

est non nul. Il est de plus rationnel car la valeur spéciale $L^*(E_d/K,1)$ l'est et que

$$\prod_{m\in\mathcal{M}} \left(1 - \frac{y(m)}{q^{u(m)}}\right) = \frac{L^*(E_d/K,1)}{\prod_{m\in\mathcal{Z}_q(d)} u(m)} \in \mathbb{Q}.$$

Nous sommes donc dans le cadre décrit à la Section 3.2 : on peut appliquer le Théorème 3.2.2. Rappelons tout d'abord quelques notations. Pour tout diviseur $d' > 2$ de d, soit $K_{d'} = \mathbb{Q}(\zeta_{d'})$ et $\mathfrak{p}'$ l'idéal premier de $K_{d'}$ qui est en-dessous de $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$. On identifiera à nouveau $\mathrm{Gal}(K_{d'}/\mathbb{Q})$ et $(\mathbb{Z}/d'\mathbb{Z})^\times$. On note de plus $G_{d'} = (\mathbb{Z}/d'\mathbb{Z})^\times$ et $\langle p\rangle_{d'}$ (resp. $\langle q\rangle_{d'}$) le sous-groupe de $G_{d'}$ engendré par p (resp. par q). On pose alors

$$w'(d') := o_q(d') \cdot \sum_{m' \in G_{d'}/\langle q\rangle_{d'}} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{d}{d'}m'\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\}.$$

Remarquons que $o_q(d') = \#\langle q\rangle_{d'}$ est un diviseur de $\phi(d') = \#G_{d'}$. L'application du Théorème 3.2.2 donne que

$$\log \prod_{m \in \mathcal{V}_q^*(d)} \left(1 - \frac{y(m)}{q^{u(m)}}\right) \geqslant -\log q \cdot \sum_{\substack{d' \mid d \\ d' > 2}} w'(d'). \tag{4.7}$$

Pour obtenir la minoration souhaitée, il nous reste à *majorer* les nombres $w'(d')$ pour tous les diviseurs $d' \geqslant 2$ de d. Commençons par expliciter (en partie) ceux-ci.

Lemme 4.4.4. *Pour tout diviseur $d' > 2$ de d, $w'(d')$ admet l'expression suivante :*

$$w'(d') = 2 \cdot o_q(d') \cdot \sum_{m' \in G_{d'}/\langle q\rangle_{d'}} \max\left\{0, \frac{1}{2} - \frac{\#\left\{\pi \in \langle p\rangle_{d'} \,\middle|\, \left\{\frac{m'\pi}{d'}\right\} \in]0, 1/2]\right\}}{\#\langle p\rangle_{d'}}\right\}.$$

Démonstration. On notera $\theta = o_q(d') = \#\langle q\rangle_{d'}$. Par définition, on a

$$w'(d') = \theta \cdot \sum_{m' \in G_{d'}/\langle q\rangle_{d'}} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{d}{d'}m'\right)}{[\mathbb{F}_{q^\theta} : \mathbb{F}_p]}\right\}$$

et il s'agit d'expliciter $\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{d}{d'}m'\right)$ pour tout $m' \in (\mathbb{Z}/d'\mathbb{Z})^\times/\langle q\rangle_{d'}$. Or, pour tout $m' \in (\mathbb{Z}/d'\mathbb{Z})^\times/\langle q\rangle_{d'}$, si l'on pose $m = dm'/d' \in \mathcal{O}_q^{(2)}(d)$, on a

$$y\left(\tfrac{d}{d'}m'\right) = \mathbf{t}_m(16) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 = \mathbf{t}(16)^{(q^\theta-1)m'/d'} \cdot \left(\mathbf{j}_{q^\theta}\left(\mathbf{t}^{(q^\theta-1)m'/d'}, \mathbf{t}^{(q^\theta-1)m'/d'}\right)\right)^2,$$

où $\mathbf{t}(16)^{(q^\theta-1)m'/d'}$ est une racine de l'unité. On applique alors le Théorème 3.3.9 (et la Proposition 3.3.10) donnant la valuation $\mathfrak{p}'$-adique des sommes de Jacobi :

$$\begin{aligned}
\mathrm{ord}_{\mathfrak{p}'}\, y\left(\tfrac{d}{d'}m'\right) &= 2 \cdot \mathrm{ord}_{\mathfrak{p}'}\, \mathbf{j}_{q^\theta}\left(\mathbf{t}^{(q^\theta-1)m'/d'}, \mathbf{t}^{(q^\theta-1)m'/d'}\right) \\
&= 2 \cdot \frac{[\mathbb{F}_{q^\theta} : \mathbb{F}_p]}{\#\langle p\rangle_{d'}} \cdot \sum_{\pi \in \langle p\rangle_{d'}} \left\lfloor \left\{\frac{-m'\pi}{d'}\right\} + \left\{\frac{-m'\pi}{d'}\right\}\right\rfloor \\
&= 2 \cdot \frac{[\mathbb{F}_{q^\theta} : \mathbb{F}_p]}{\#\langle p\rangle_{d'}} \cdot \sum_{\pi \in \langle p\rangle_{d'}} \left\lfloor 2 - 2\left\{\frac{m'\pi}{d'}\right\}\right\rfloor,
\end{aligned}$$

car, pour tout réel $y \notin \mathbb{Z}$, on a $\{-y\} = 1 - \{y\}$. Ce qu'on peut appliquer ici, car pour tout $\pi \in \langle p\rangle_{d'}$, $m' \in (\mathbb{Z}/d'\mathbb{Z})^\times$ et d' est premier à p donc $\frac{m'\pi}{d'} \notin \mathbb{Z}$. Dès lors, remarquons que, pour tout $y \in]0, 1]$, on a

$$\lfloor 2 - 2\{y\}\rfloor = \lfloor 2 - 2y\rfloor = \begin{cases} 1 & \text{si } y \in]0, 1/2] \\ 0 & \text{si } y \in]1/2, 1]. \end{cases}$$

D'où l'on déduit que $\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{d}{d'}m'\right)$ est, à un facteur près, une « fonction de comptage » :

$$\mathrm{ord}_{\mathfrak{p}'}\, y\left(\tfrac{d}{d'}m'\right) = 2 \cdot \frac{[\mathbb{F}_{q^\theta} : \mathbb{F}_p]}{\#\langle p\rangle_{d'}} \cdot \#\left\{\pi \in \langle p\rangle_{d'} \;\middle|\; \left\{\tfrac{m'\pi}{d'}\right\} \in]0, 1/2]\right\}.$$

L'expression attendue de $w'(d')$ est une conséquence immédiate de cette dernière égalité. □

On peut maintenant utiliser les résultats d'équidistribution développés à la Section 3.4 :

Lemme 4.4.5. *Pour tout diviseur $d' > 2$ de d, la quantité $w'(d')$ définie ci-dessus vérifie :*

$$\frac{w'(d')}{\phi(d')} \xrightarrow[d'\to\infty]{} 0.$$

De plus, on a

$$\frac{1}{d} \cdot \sum_{\substack{d'|d \\ d'>2}} w'(d') \xrightarrow[d\to\infty]{} 0. \tag{4.8}$$

Démonstration. Définissons $F : [0,1] \to \mathbb{R}$ la fonction indicatrice de l'intervalle $]0,1/2]$, de sorte que $\int_{[0,1]} F = \frac{1}{2}$. Pour toute orbite $m' \in G_{d'}/\langle q\rangle_{d'}$, on a

$$\frac{1}{2} - \frac{\#\left\{\pi \in \langle p\rangle_{d'} \,\middle|\, \left\{\frac{m'\pi}{d'}\right\} \in]0,1/2]\right\}}{\#\langle p\rangle_{d'}} = \int_{[0,1]} F - \frac{1}{\#\langle p\rangle_{d'}} \sum_{\pi\in\langle p\rangle_{d'}} F\left(\left\{\frac{m'\pi}{d'}\right\}\right)$$

et, puisque $\max\{0,y\} \leqslant |y|$ pour tout réel y, on en déduit que

$$\max\left\{0, \frac{1}{2} - \frac{\#\left\{\pi \in \langle p\rangle_{d'} \,\middle|\, \left\{\frac{m'\pi}{d'}\right\} \in]0,1/2]\right\}}{\#\langle p\rangle_{d'}}\right\} \leqslant \left|\int_{[0,1]} F - \frac{1}{\#\langle p\rangle_{d'}} \sum_{\pi\in\langle p\rangle_{d'}} F\left(\left\{\frac{m'\pi}{d'}\right\}\right)\right|.$$

D'après le Lemme précédent, on a donc :

$$\begin{aligned}
0 \leqslant \frac{w'(d')}{\phi(d')} &= 2\frac{o_q(d')}{\phi(d')} \cdot \sum_{m'\in G_{d'}/\langle q\rangle_{d'}} \max\left\{0, \int_{[0,1]} F - \frac{1}{\#\langle p\rangle_{d'}} \sum_{\pi\in\langle p\rangle_{d'}} F\left(\left\{\frac{m'\pi}{d'}\right\}\right)\right\} \\
&\leqslant 2\frac{o_q(d')}{\phi(d')} \cdot \sum_{m'\in G_{d'}/\langle q\rangle_{d'}} \left|\int_{[0,1]} F - \frac{1}{\#\langle p\rangle_{d'}} \sum_{\pi\in\langle p\rangle_{d'}} F\left(\left\{\frac{m'\pi}{d'}\right\}\right)\right| \\
&= \frac{2}{\#(G_{d'}/\langle q\rangle_{d'})} \cdot \sum_{m'\in G_{d'}/\langle q\rangle_{d'}} \left|\int_{[0,1]} F - \frac{1}{\#\langle p\rangle_{d'}} \sum_{\pi\in\langle p\rangle_{d'}} F\left(\left\{\frac{m'\pi}{d'}\right\}\right)\right|.
\end{aligned}$$

On applique alors la Proposition 3.4.13 (corollaire du Théorème 3.4.1) : lorsque $d' \to +\infty$, on a

$$\frac{1}{\#(G_{d'}/\langle q\rangle_{d'})} \cdot \sum_{m'\in G_{d'}/\langle q\rangle_{d'}} \left|\int_{[0,1]} F - \frac{1}{\#\langle p\rangle_{d'}} \sum_{\pi\in\langle p\rangle_{d'}} F\left(\left\{\frac{m'\pi}{d'}\right\}\right)\right| = o(1). \tag{4.9}$$

La constante implicite ne dépend que de q. Ceci démontre bien que $w'(d')/\phi(d') \longrightarrow 0$ lorsque $d' \to \infty$. Noter qu'on pourrait être plus précis ici : la Proposition 3.4.13 donne en fait une estimation de la « vitesse de convergence » de $w'(d')/\phi(d')$ vers 0. Dans tous les cas, on peut alors déduire (4.8) de (4.9) par le Lemme 3.4.16. Ce qui achève la preuve du Lemme. □

Finalement, d'après le calcul de la hauteur de E_d (à la Proposition 4.1.4), on voit que

$$\frac{\log H(E_d/K)}{d} = \log q \cdot \frac{1}{d} \cdot \left\lfloor \frac{d+1}{2} \right\rfloor \leqslant \frac{(d+1)\cdot\log q}{2d}$$

et, en combinant (4.6), (4.7) et (4.8), d'en conclure que

$$\begin{aligned}
\frac{\log L^*\big(E_d/K,1\big)}{\log H\big(E_d/K\big)} = \frac{d}{\log H\big(E_d/K\big)} \cdot \frac{\log L^*\big(E_d/K,1\big)}{d} &\geqslant -\frac{2d}{(d+1)\log q} \cdot \log q \cdot \frac{1}{d} \sum_{\substack{d'|d \\ d'>2}} w'(d') \\
&\geqslant -\frac{2d}{(d+1)} \cdot \frac{1}{d} \sum_{\substack{d'|d \\ d'>2}} w'(d') \geqslant -\frac{1}{d} \sum_{\substack{d'|d \\ d'>2}} w'(d') = o\big(1\big).
\end{aligned}$$

Ce qu'il fallait démontrer. □

Ceci termine la preuve que, lorsque $d \to \infty$, on a

$$\mathfrak{Bs}(E_d/K) \xrightarrow[\substack{\mathrm{pgcd}(d,q)=1 \\ d\to\infty}]{} 1.$$

5

Famille des courbes elliptiques « Hessiennes »

Dans ce chapitre, nous étudions les courbes elliptiques « hessiennes » H_d sur le corps $K = \mathbb{F}_q(t)$, dont un modèle de Weierstrass affine est

$$H_d : \quad Y^2 + 3t^d XY + Y = X^3,$$

avec $d \in \mathbb{N}^*$ premier à la caractéristique $p \geqslant 5$ de K.

Un résultat assez classique affirme que ces courbes sont les « courbes elliptiques universelles » sur K munies d'un point de 3-torsion K-rationnel. Après avoir étudié les courbes de Legendre (Chapitre 4), il semble donc naturel de considérer ces courbes. Résumons quelques résultats obtenus dans ce chapitre en un théorème :

Théorème. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \geqslant 2$, premier à p, on considère la courbe elliptique (dite « Hessienne ») définie sur K par le modèle affine suivant :*

$$H_d : \qquad Y^2 + 3t^d XY + Y = X^3.$$

La hauteur différentielle de H_d/K vaut $H\big(H_d/K\big) = q^d$. La courbe H_d vérifie les conjectures de Birch et Swinnerton-Dyer. En particulier, le groupe de Tate-Shafarevich $Ш(H_d/K)$ est fini et le ratio de Brauer-Siegel $\mathfrak{Bs}(H_d/K)$ également. De plus, lorsque $d \to +\infty$ (toujours en étant premier à p), on a $H\big(H_d/K\big) \to +\infty$ et

$$\mathfrak{Bs}\big(H_d/K\big) \xrightarrow[\substack{\mathrm{pgcd}(d,q)=1 \\ d\to+\infty}]{} 1.$$

Autrement dit,

$$\log\big(\#Ш\big(H_d/K\big) \cdot \mathrm{Reg}\,\big(H_d/K\big)\big) \sim d \cdot \log q \quad (d \to \infty).$$

Ainsi, les courbes Hessiennes $H_d/\mathbb{F}_q(t)$ ci-dessus vérifient un analogue « complet » du Théorème de Brauer-Siegel :

$$\forall \varepsilon > 0, \quad H\big(H_d/K\big)^{1-\varepsilon} \ll_\varepsilon \#Ш(H_d/K) \cdot \mathrm{Reg}(H_d/K) \ll_\varepsilon H\big(H_d/K\big)^{1+\varepsilon} \quad (d \to \infty).$$

L'organisation de ce chapitre est assez similaire à celle du chapitre précédent. Nous commençons par construire les courbes H_d à partir de leur définition « modulaire » (Section 5.1.1). Puis nous calculons les invariants classiques associés à H_d : conducteur, hauteur (Proposition 5.1.5) et nombres de Tamagawa (Proposition 5.1.7). Pour ce faire, nous menons une analyse assez détaillée de la réduction de H_d en les « mauvaises places » de K (Proposition 5.1.4).

La deuxième Section est dédiée au calcul de la fonction $L\big(H_d/K, T\big)$ sous la forme d'un produit explicite. À notre connaissance, un tel calcul n'avait jamais été mené. La technique utilisée se base sur des évaluations de sommes de caractères sur les corps finis, à partir de la définition de la fonction L comme série génératrice. Comme au chapitre précédent, nous faisons apparaître des sommes de Jacobi (*cf.* Théorème 5.2.1 et Lemme 5.2.5). Nous expliquons aussi pourquoi la conjecture de Birch et Swinnerton-Dyer est vérifiée par H_d/K (Théorème 5.3.1). Enfin, la dernière section contient la preuve de l'assertion sur la limite de $\mathfrak{Bs}\big(H_d/K\big)$ (Théorème 5.4.1), le résultat principal de ce chapitre.

5.1 Courbes hessiennes H_d

5.1.1 Construction des courbes Hessiennes

Soit E une courbe elliptique sur $K = \mathbb{F}_q(t)$, elle admet un modèle de Weierstrass affine de la forme

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \tag{5.1}$$

On suppose que E possède, outre l'origine $\mathcal{O}$ du groupe $E(K)$, un point K-rationnel de 3-torsion P. Quitte à effectuer des translations, on peut supposer que $P = (0,0)$ est K-rationnel, *i.e.* que $a_6 = 0$. Un calcul simple montre alors que la tangente en $(0,0)$ est de pente a_4/a_3. Comme la courbe est lisse en $(0,0)$, on ne peut avoir simultanément $a_4 = 0$ et $a_3 = 0$. Si $a_3 = 0$, la tangente à E en $(0,0)$ est verticale et $(0,0)$ serait de 2-torsion (on obtiendrait alors les courbes de Legendre, voir Chapitre 4).

Si $P = (0,0)$ n'est pas de 2-torsion, on a $a_3 \neq 0$ et un changement de variables $(X', Y') = \left(X, Y - \frac{a_4}{a_3}X\right)$ transforme l'équation (5.1) en

$$Y'^2 + a'_1X'Y' + a_3Y' = X'^3 + a'_2X'^2, \qquad \left(a'_1 = a_1 + 2\frac{a_3}{a_4}, a'_2 = a_2 - a_1\frac{a_3}{a_4} - \frac{a_3^2}{a_4^2}\right) \tag{5.2}$$

où la tangente au point $P = (0,0)$ est alors horizontale. Utilisons maintenant la condition que P est d'ordre 3 : la courbe E doit intersecter sa tangente en P en un autre point P'. Après calcul, on voit que $P = (0,0)$ est d'ordre 3 si et seulement si $a_3 \neq 0$ et $a_2 = 0$. Le modèle affine de E se réduit donc à

$$Y^2 + a'_1XY + a'_3Y = X^3. \tag{5.3}$$

Pour simplifier, on suppose ici que a'_3 *est un cube dans* $\mathbb{F}_q(t)$. Comme $a'_3 \neq 0$ est « de poids 3 », on peut faire un nouveau changement de coordonnées et normaliser par $a'_3 = 1$, on écrit alors a'_1 sous la forme $a'_1 = 3 \cdot A$ (avec $A \in K$) et l'on obtient un modèle de Weierstrass affine de la forme

$$E_A : \quad Y^2 + 3A \cdot XY + Y = X^3,$$

dont le discriminant vaut $\Delta = 27(A^3 - 1)$ et l'invariant j s'écrit $j = -\frac{27A^3(9A^3-8)^3}{A^3-1}$. Nous obtenons ainsi, pour tout polynôme $A \in \mathbb{F}_q[t]$ ($A^3 \neq 1$), une courbe E_A définie sur $K = \mathbb{F}_q(t)$. La courbe E_A est lisse si et seulement si $A^3 \neq 1$: c'est le cas par exemple si l'on suppose $\deg A > 0$. Si E_A est lisse, c'est une courbe elliptique sur K munie d'un point rationnel de 3-torsion. Celui-ci est $P = (0,0)$ et $2P = (0,-1) = -P$. Nous renvoyons la lectrice à [Hus04, Chapter 4, §2] pour de plus amples informations (notamment sur les conditions supplémentaires à imposer à $A \in \mathbb{F}_q[t]$ et q pour que E_A possède 9 points K-rationnels de 3-torsion).

Dans ce chapitre, nous nous concentrons exclusivement sur le cas où a'_3 est un cube (dans les notations de (5.3)) et où le paramètre $A(t)$ est le monôme $A(t) = t^d \in \mathbb{F}_q[t]$, avec $d \geqslant 2$ un entier premier à q. Nous noterons alors simplement $H_d = E_{t^d}$:

Définition 5.1.1. Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \in \mathbb{N}^*$, on considère la courbe elliptique H_d définie sur K par le modèle affine :

$$Y^2 + 3t^d \cdot XY + Y = X^3. \tag{5.4}$$

Dans tout ce chapitre, nous appellerons H_d/K la d-ième *courbe Hessienne*.

Remarque 5.1.2. Il y a d'autres modèles classiques de la courbe Hessienne. Notamment, pour tout $d \in \mathbb{N}^*$ premier à p, on peut considérer la courbe projective H'_d définie sur $K = \mathbb{F}_q(t)$ par l'équation

$$H'_d : x_0^3 + x_1^3 + x_2^3 = 3t^d \cdot x_0x_1x_2,$$

où l'on a noté $[x_0 : x_1 : x_2] \in \mathbb{P}^2$ les coordonnées sur $\mathbb{P}^2$. L'application rationnelle $\phi_d : H'_d \to H_d$ donnée par

$$\phi_d([x_0 : x_1 : x_2]) = \left(\frac{x_0x_1}{x_2^2}, -\frac{x_0^3}{x_2^3}\right) = (X, Y)$$

se prolonge en un morphisme dominant $H'_d \to H_d$ de degré 3. On vérifie que ϕ_d est en fait une 3-isogénie entre H'_d et H_d.

Par ailleurs, Ulmer nous a fait remarquer que l'hypothèse parasite que « a'_3 est un cube » (voir (5.3)) n'a pas d'interprétation « modulaire » simple : dans (5.3), il vaudrait mieux normaliser a'_1 par $a'_1 = 1$ lorsque celui-ci est non nul (ce qui est toujours possible car a'_1 est « de poids 1 »). Nous

reviendrons au Chapitre 7 sur la famille qu'on obtiendrait alors. La famille des courbes E_A (pour $A \in \mathbb{F}_q[t] \smallsetminus \mu_3$) données par :

$$E_A : \quad Y^2 + 3A \cdot XY + Y = X^3,$$

représente environ « un tiers » de la famille de toutes les courbes elliptiques $E/\mathbb{F}_q(t)$ munies d'un point de 3-torsion $\mathbb{F}_q(t)$-rationnel.

Remarque 5.1.3. Les méthodes développées ci-dessous permettraient de traiter le cas un peu plus général suivant. Pour tout $a \in \mathbb{F}_q \smallsetminus \{0\}$ et tout entier d premier à p, on définit une courbe elliptique $H_{d,a}$ sur $K = \mathbb{F}_q(t)$ par le modèle affine

$$H_{d,a} : \quad Y^2 + 3at^d \cdot XY + Y = X^3.$$

Les résultats majeurs de ce chapitre sont aussi valables pour la courbe $H_{d,a}$, avec les modifications appropriées. Notons que $H_{d,a}$ est $\overline{\mathbb{F}_q}(t)$-isomorphe à $H_{d,1} = H_d$.

5.1.2 Analyse de la mauvaise réduction

Soit d un entier premier à q, considérons la courbe Hessienne H_d définie sur $K = \mathbb{F}_q(t)$ par le modèle affine suivant :

$$H_d : \quad Y^2 + 3t^d XY + Y = X^3. \tag{5.5}$$

Le discriminant de ce modèle se calcule facilement (à l'aide du formulaire rappelé en 1.1.2) :

$$\Delta = 3^3(t^{3d} - 1).$$

Pour toute place finie v de K, on voit que $0 \leqslant \operatorname{ord}_v \Delta \leqslant 1$: le modèle (5.5) est donc entier et minimal en v. Avec ce formulaire, on obtient aussi l'invariant j de la courbe H_d :

$$j(H_d/\mathbb{F}_q(t)) = \frac{3^3 t^{3d}(9t^{3d} - 8)^3}{t^{3d} - 1}.$$

Ce dernier est une fraction rationnelle en t, de degré $9d > 0$. En particulier, la courbe H_d ne peut pas être isotriviale car son invariant j n'est pas constant. On constate aussi que $j(H_d/\mathbb{F}_q(t))$ est séparable, au sens où l'application rationnelle $j : \mathbb{P}^1 \to \mathbb{P}^1$ correspondante est séparable.

Les places v de $K = \mathbb{F}_q(t)$ en lesquelles H_d a mauvaise réduction sont exactement celles qui divisent Δ. C'est-à-dire, d'une part les places v correspondant à $\zeta \in \overline{\mathbb{F}_q}$, où ζ est une racine $3d$-ième de l'unité ($\zeta^{3d} = 1$) et d'autre part (éventuellement) la place $v = \infty$.

Proposition 5.1.4. *Soit $d \geqslant 2$ premier à q, on note $\pi : \mathcal{H}_d \to \mathbb{P}^1$ le modèle régulier minimal de la courbe H_d/K. Le morphisme π a les fibres singulières suivantes :*

- *Au-dessus des points $v = \zeta \in \mu_{3d}(\overline{\mathbb{F}_q})$ (i.e. $\zeta^{3d} = 1$), la fibre $\pi^{-1}(v)$ est irréductible (de type $\mathbf{I}_1$).*
- *En $v = \infty$, la fibre $\pi^{-1}(\infty)$ admet $9d$ composantes irréductibles arrangées en une configuration $\mathbf{I}_{9d}$.*

Démonstration. Les points v de $\mathbb{P}^1$ où la fibre $\pi^{-1}(v)$ est singulière sont ceux qui annulent le discriminant Δ d'un modèle de $H_d/\mathbb{F}_q(t)$, vu comme un morphisme $\Delta : \mathbb{P}^1 \to \mathbb{P}^1$. Comme annoncé, il n'y a que le point $\infty \in \mathbb{P}^1$ et les points $v = \zeta$, où ζ parcourt les racines $3d$-ièmes de l'unité (dans $\overline{\mathbb{F}_q}$). Pour déterminer le type de singularité de la fibre de π en v, nous utilisons l'algorithme décrit par Tate [Tat75] et expliqué en détail dans [Sil09, Chap. IV, §9].

- En $v = \zeta$ (où $\zeta \in \mu_{3d}(\overline{\mathbb{F}_q})$), le discriminant du modèle (5.5) admet une racine simple en v et l'invariant j de H_d admet un pôle simple en v :

  $$\operatorname{ord}_{v=\zeta} \Delta = 1 \qquad \text{et} \qquad \operatorname{ord}_{v=\zeta} j(H_d) = -1.$$

  L'algorithme de Tate s'arrête à l'étape 1 : la réduction de H_d en v est de type $\mathbf{I}_1$. La place v correspondant à ζ donne alors une contribution $\operatorname{ord}_{v=\zeta} \Delta_{\min}(H_d/K) = 1$ au discriminant minimal de H_d, une contribution $\operatorname{ord}_{v=\zeta} \mathcal{N}(H_d/K) = 1$ au conducteur et le nombre de Tamagawa local est $c_\zeta(H_d/K) = 1$.
- Pour étudier la fibre en $v = \infty$, commençons par faire le changement de variables $t = 1/u$ dans (5.5), on obtient le modèle (affine) suivant :

  $$Y^2 + 3XY + u^{3d}Y = X^3.$$

  Ce dernier a pour discriminant $\Delta' = 3^3 u^{9d}(1 - u^{3d})$ et $\operatorname{ord}_{u=0} \Delta' = 9d$. Par ailleurs, on a

  $$\operatorname{ord}_{u=0} j(H_d/K) = \operatorname{ord}_{t=\infty} j(H_d/K) = -\deg j(H_d/K) = -9d.$$

Ainsi, l'algorithme de Tate s'arrête à nouveau à l'étape 1 : la réduction de H_d en $t = \infty$ (*i.e.* en $u = 0$) est multiplicative de type $\mathbf{I}_{9d}$. De plus, il est aisé de voir que les tangentes au point singulier sur la courbe réduite sont à coefficients $\mathbb{F}_q$-rationnels : la réduction est déployée. On en déduit que la place $v = \infty$ contribue pour $\operatorname{ord}_{v=\infty} \Delta_{\min}(H_d/K) = 9d$ au discriminant minimal de H_d, pour $\operatorname{ord}_{v=\infty} \mathcal{N}(H_d/K) = 1$ au conducteur et que le nombre de Tamagawa local est $c_\infty(H_d/K) = 9d$.

□

Résumons cette analyse dans un tableau :

Place	Type de réduction	$\operatorname{ord}_v \Delta_{\min}(H_d/K)$	$\operatorname{ord}_v \mathcal{N}(H_d/K)$	$c_v(H_d/K)$
$v = \zeta$ $(\zeta^{3d} = 1)$	$\mathbf{I}_1$ –	1	1	1
$v = \infty$	$\mathbf{I}_{9d}$ déployée	$9d$	1	$9d$

Pour toute place v de $\mathbb{P}^1$, on a noté $\operatorname{ord}_v \Delta_{\min}(H_d/K)$ la valuation en v du discriminant minimal de H_d, $\operatorname{ord}_v \mathcal{N}(H_d/K)$ la valuation du conducteur de H_d et $c_v(H_d/K)$ le nombre de Tamagawa local.

5.1.3 Calcul des invariants

A partir de l'analyse de la mauvaise réduction menée à la section précédente, on peut expliciter les invariants de la courbe hessienne H_d.

Proposition 5.1.5. *Soit d un entier premier à q, $K = \mathbb{F}_q(t)$ et H_d la courbe elliptique définie sur K par* (5.5)*. Celle-ci est de hauteur différentielle (exponentielle) :*

$$H\big(H_d/\mathbb{F}_q(t)\big) = q^d.$$

D'autre part, on a $\deg \mathcal{N}\big(H_d/\mathbb{F}_q(t)\big) = 3d + 1$.

Démonstration. Reprenons les informations contenues dans le tableau ci-dessus. Pour une place v de K, on notera à nouveau $\mathbb{F}_v$ son corps résiduel et $d_v = [\mathbb{F}_v : \mathbb{F}_q]$ son degré. Pour alléger, nous notons simplement $\Delta_{\min}$ le discriminant minimal de H_d/K (vu comme diviseur sur $\mathbb{P}^1$). On obtient directement

$$\begin{aligned}\deg \Delta_{\min} &= \sum_v d_v \cdot \operatorname{ord}_v \Delta_{\min} = d_\infty \cdot \operatorname{ord}_{v=\infty} \Delta_{\min} + \sum_{\zeta^{3d}=1} d_\zeta \cdot \operatorname{ord}_{v=\zeta} \Delta_{\min} \\ &= 1 \cdot 9d + \sum_{\zeta^{3d}=1} d_\zeta \cdot 1 = 9d + 3d = 12d.\end{aligned}$$

Le fait que $\sum_{\zeta^{3d}=1} d_\zeta = 3d$ suit de la remarque faite durant la preuve de la Proposition 4.1.4 (*cf.* (4.3)). On en déduit l'expression annoncée pour $H\big(H_d/\mathbb{F}_q(t)\big)$ car, par définition, $H\big(H_d/\mathbb{F}_q(t)\big) = q^{(\deg \Delta_{\min})/12}$. Le calcul du degré du conducteur $\mathcal{N}(H_d/K)$ est très similaire. □

Le calcul de $\deg \mathcal{N}(H_d/K)$ permet d'anticiper le degré de la fonction L de la courbe H_d : comme H_d n'est pas isotriviale, $L\big(H_d/K, T\big)$ est un polynôme à coefficients entiers et la formule de Grothendieck-Ogg-Raynaud (Théorème 1.3.11) entraîne que

$$\deg_T L\big(H_d/\mathbb{F}_q(t), T\big) = \deg \mathcal{N}\big(H_d/\mathbb{F}_q(t)\big) + 4g(\mathbb{P}^1) - 4 = 3d - 3 = 3(d-1). \tag{5.6}$$

5.1.4 Torsion et nombre de Tamagawa

Pour tout entier d premier à q, la courbe elliptique H_d sur $K = \mathbb{F}_q(t)$ n'est pas isotriviale. Les Théorèmes 1.5.2 et 1.5.4 montrent que, lorsque $H\big(H_d/K\big) \to \infty$, on a des bornes :

$$\#H_d(K)_{\text{tors}} \ll_q 1 \quad \text{et} \quad \frac{\log \mathcal{T}am\,(H_d/K)}{\log H\big(H_d/K\big)} = o(1).$$

Ceci étant, dans la situation étudiée, on peut être bien plus explicite : ci-dessous, nous précisons la structure de $H_d(K)_{\text{tors}}$ et donnons une borne effective pour $\log \mathcal{T}am\,(H_d/K)$.

Proposition 5.1.6. *Soit d un entier premier à q. Le sous-groupe de torsion du groupe de Mordell-Weil de la courbe Hessienne H_d sur $K = \mathbb{F}_q(t)$ est comme suit :*

$$H_d(K)_{\mathrm{tors}} \simeq \mathbb{Z}/3\mathbb{Z}.$$

Démonstration. Par construction, le point $P_0 = (0,0)$ (donné en coordonnées affines sur le modèle (5.5)) est de 3-torsion et $2P_0 = -P_0 = (0,-1)$. On note $T = H_d(K)_{\mathrm{tors}}$ le sous-groupe de torsion du groupe de Mordell-Weil de H_d. D'après ce qui précède, on a $\langle P_0\rangle \subset T$ et T contient au moins un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

Pour toute place v de mauvaise réduction, on note G_v le groupe des composantes de la fibre en v du modèle de Néron de H_d (voir [SS10, §7]). Le formulaire [SS10, Lemma 7.3] montre que, si v est une place en laquelle la réduction de H_d est de type $\mathbf{I}_n$ ($n \in \mathbb{N}^*$), on a $G_v \simeq \mathbb{Z}/n\mathbb{Z}$. Avec l'analyse de la mauvaise réduction de H_d effectuée à la Proposition 5.1.4, on voit qu'ici $\prod_{v|\Delta} G_v \simeq G_\infty \simeq \mathbb{Z}/9d\mathbb{Z}$. Or, d'après [SS10, Corollary 7.5], il y a une injection de groupes $T \hookrightarrow \prod_{v|\Delta} G_v$, de laquelle on déduit que T est isomorphe à un sous-groupe de $\mathbb{Z}/9d\mathbb{Z}$. En particulier, T est cyclique d'ordre N, un diviseur de $9d$. Comme T contient un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z}$, N est de plus divisible par 3. D'autre part, la caractéristique p de K étant supposée être $\geqslant 5$ et d étant premier à p, N est lui-même premier à p (en particulier $H_d(K)_{\mathrm{tors}}$ a une partie p-primaire triviale, ce qu'on aurait pu également démontrer à l'aide de [Ulm11, Lecture 1, Proposition 7.3] car $j(H_d/K)$ est séparable).

Fixons à présent un point $Q \in T \subset H_d(K)$ d'ordre exactement N. D'après [KM85], il y a une courbe modulaire $X_1(N)$ irréductible définie sur $\overline{\mathbb{F}_p}$ classifiant les couples (E,P) de courbes elliptiques E munies d'un point rationnel d'ordre exactement N. Comme $X_1(N)$ est un « espace de modules grossier », la présence du point Q sur H_d implique l'existence d'un morphisme $j' : \mathbb{P}^1 \to X_1(N)$. Ce morphisme j' n'est pas constant, car H_d est non isotriviale, et j' est donc surjectif. Puisque le genre de $\mathbb{P}^1$ est 0, la formule de Riemann-Hurwitz implique que celui de $X_1(N)$ l'est également.

Or, le genre de $X_1(N)$ vaut 0 exactement quand $N \in \{1,2,3,4,5,6,7,8,9,10,12\}$ (*cf.* [Ser97, §5.4] ou [HS00, Theorem F.4.1.1]). Vu les restrictions sur N indiquées ci-dessus, on a donc $N \in \{3,6,9,12\}$. Pour compléter la démonstration, il reste à montrer que $H_d(K)$ n'a pas de 2-torsion et qu'il n'existe pas de point $P' \in H_d(K)$ tel que $3P' = P_0 = (0,0)$. Un point $P = (x,y) \in H_d(K)$ est de 2-torsion si et seulement si $-P = P$ et ceci est équivalent à

$$4x^3 + 9t^{2d}x^2 + 6t^d + 1 = 0. \tag{5.7}$$

Si $x \in \mathbb{F}_q(t)$ est une solution de cette relation, alors x n'a pas de pôle. Autrement dit $x \in \mathbb{F}_q[t]$ est un polynôme en t tel que $x^2(4x + 9t^{2d}) = 6t^d + 1$. En particulier, x^2 divise dans $\mathbb{F}_q[t]$ le polynôme $6t^d + 1$ qui, comme d est premier à p, n'a pas de facteurs carrés. Par suite, x est un polynôme constant, ce qui est impossible au vu de la relation (5.7). Donc $H_d(K)$ est sans 2-torsion et $N = \#T \in \{3,9\}$. Supposons à présent qu'il existe un point $Q = (u,v) \in T$ d'ordre exactement 9, on peut choisir Q de sorte que $3 \cdot Q = P_0 = (0,0)$. Un calcul facile mais fastidieux, à l'aide de la formule de triplication (*cf.* [Sil09, Chapter III, Exercice 3.7 (d)]), montre que $u \in \mathbb{F}_q(t)$ vérifie

$$0 = u^6 + 3(t^d+1)u^5 + 3(3t^{2d} - t^d + 3)u^4 + (3t^d+1)(3t^d+2)u^3 + 3(3t^{2d} + t^d + 1)u^2 + 6t^d u + 1$$
$$\text{ou } 0 = u^3 - 3(1+t^d)u^2 + 3t^d u + 1.$$

À nouveau, une fraction rationnelle $u \in \mathbb{F}_q(t)$ vérifiant l'une de ces relations ne peut avoir de pôle ; le polynôme $u \in \mathbb{F}_q[t]$ vérifie donc

$$-1 = u\big(u^5 + 3(t^d+1)u^4 + 3(3t^{2d} - t^d + 3)u^3 + (3t^d+1)(3t^d+2)u^2 + 3(3t^{2d} + t^d + 1)u + 6t^d\big)$$
$$\text{ou } -1 = u\big(u^2 - 3(1+t^d)u + 3t^d\big).$$

ce qui est contradictoire (car $\mathbb{F}_q[t]$ est un anneau factoriel). Ainsi, il n'y a pas de point de 9-torsion sur $H_d(K)$ et l'on a bien $N = 3$. □

Proposition 5.1.7. *Soit $d \geqslant 1$ un entier premier à q et H_d la courbe hessienne sur $K = \mathbb{F}_q(t)$. On a*

$$\mathcal{T}am\big(H_d/K\big) = 9d.$$

Par conséquent, il existe des constantes ne dépendant que de q telles que

$$\frac{\log d}{d} \ll_q \frac{\log \mathcal{T}am\big(H_d/K\big)}{\log H\big(H_d/K\big)} \ll_q \frac{\log d}{d}.$$

Démonstration. Le calcul du nombre de Tamagawa $\mathcal{T}am(H_d/K)$ est une conséquence immédiate de la Proposition 5.1.4 (*cf.* le tableau synthétique qui la suit). L'encadrement annoncé en découle facilement. □

5.2 Fonctions L des courbes H_d

Afin d'étudier le ratio de Brauer-Siegel des courbes hessiennes H_d/K, nous aurons besoin de disposer d'une expression suffisamment explicite de leur fonction L. Pour exprimer celle-ci, nous reprenons les notations des Sections 2.1.2 et 2.1.3. En particulier, nous fixons un idéal premier $\overline{\mathfrak{P}}$ de $\overline{\mathbb{Z}}$ au-dessus de p pour définir le caractère de Teichmüller $\mathbf{t} : \overline{\mathbb{F}_q}^\times \to \overline{\mathbb{Q}}^\times$. En outre, pour tout entier $d \geqslant 2$ premier à q, rappelons que l'on a défini à la Section 2.1.4 des caractères $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ dont l'ordre divise $3d$.

Une fois mises en place ces notations, nous pouvons énoncer :

Théorème 5.2.1. *Soit $d \geqslant 2$ un entier premier à q. La fonction L de la courbe elliptique « hessienne » H_d sur $K = \mathbb{F}_q(t)$, dont un modèle affine est*

$$Y^2 + 3t^d XY + Y = X^3,$$

s'écrit sous la forme :

$$L\big(H_d/\mathbb{F}_q(t), T\big) = \prod_{m \in \mathcal{O}_q^{(3)}(3d)} \Big(1 - \mathbf{t}_m(27) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) \cdot T^{u(m)}\Big)$$

où, $\mathcal{O}_q^{(3)}(3d)$ désigne l'ensemble des orbites de $\mathbb{Z}/3d\mathbb{Z} \smallsetminus \{0, d, 2d\}$ sous l'action de q par multiplication, $u(m)$ est le cardinal de l'orbite $m \in \mathcal{O}_q^{(3)}(3d)$ et

$$\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) = + \sum_{\substack{x,y,z \in \mathbb{F}_{q^{u(m)}} \\ x+y+z=1}} \mathbf{t}_m(x)\mathbf{t}_m(y)\mathbf{t}_m(z).$$

Nous attirons l'attention du lecteur sur le fait que les caractères $\mathbf{t}_m$ de la Section 2.1.3 qui apparaissent dans ce Théorème sont ceux dont l'ordre divise $3d$ (et non à d comme dans les autres chapitres de ce manuscrit).

Ce théorème semble nouveau. Pour la démonstration, nous utilisons des calculs élémentaires sur les sommes de caractères à partir de la série génératrice définissant $L\big(H_d/K, T\big)$. Le coeur de la preuve est le Lemme 5.2.5 où nous écrivons ces sommes sous la forme de sommes de Jacobi. Le reste de la présente section est consacré à la preuve du Théorème 5.2.1.

Remarque 5.2.2. L'apparition de sommes de Jacobi dans la fonction L des courbes hessiennes peut s'expliquer par voie « cohomologique ». En effet, le modèle régulier minimal $\mathcal{H}_d \to \mathbb{P}^1$ de la courbe H_d est (dominé par) un quotient de la surface de Fermat $\mathcal{F}_{3d}/\mathbb{F}_q$ (voir la Section 5.3.1) dont la fonction zeta fait classiquement apparaître les sommes de Jacobi (*cf.* [Wei49], [SK79] et [Yui94] par exemple).

Une analyse minutieuse de l'application rationnelle dominante $\mathcal{F}_{3d} \to \mathcal{H}_d$ devrait d'ailleurs permettre d'obtenir une autre preuve du Théorème 5.2.1. Par exemple, en adaptant la preuve de [Ulm02, Corollary 7.7] ou l'analyse de [Shi92, §2]. Notons que cette approche aurait l'avantage de fonctionner en caractéristique quelconque (à part en caractéristique 3 où la courbe H_d est singulière) : la méthode développée ici n'est pas valide en caractéristique 2.

5.2.1 Décompte de points

Entamons le calcul de la fonction L en « comptant » les points rationnels sur les réductions de H_d modulo les places v de degré $[\mathbb{F}_v : \mathbb{F}_q] \leqslant n$ de K. Soit $d \geqslant 2$ un entier premier à q, que l'on considère comme fixé dans toute la suite de cette section. Pour toute place $\tau \in \mathbb{P}^1(\overline{\mathbb{F}_q})$, on note $\overline{(H_d)}_\tau$ la réduction modulo τ d'un modèle minimal et entier de H_d en la place v_τ de K correspondant à τ. En particulier, $\overline{(H_d)}_\tau$ est une courbe cubique plane, éventuellement singulière, définie sur le corps résiduel $\mathbb{F}_{v_\tau} = \mathbb{F}_q(\tau)$. Pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$ et tout point $\tau \in \mathbb{P}^1(\mathbb{F}_Q)$, on note

$$A(\tau, Q) := Q + 1 - \#\overline{(H_d)}_\tau(\mathbb{F}_Q).$$

Pour pouvoir exprimer $A(\tau, Q)$, il nous faudra disposer d'un « bon » modèle de $\overline{(H_d)}_\tau$:

Lemme 5.2.3. *L'équation affine*

$$H'_d : \quad Y^2 = X^3 + 9t^{2d}X^2 + 24t^d X + 16 \tag{5.8}$$

détermine un modèle entier de la courbe hessienne H_d. Celui-ci est minimal en toute place $v \neq \infty$ de $K = \mathbb{F}_q(t)$.

Démonstration. Partons du modèle de Weierstrass (5.5) : en coordonnées affines (X, Y), la courbe hessienne est donnée par

$$Y^2 + 3t^d XY + Y = X^3.$$

Après le changement de variables $(X_1, Y_1) = \big(X, Y + (3t^d X + 1)/2\big)$, ce modèle devient :

$$Y_1^2 = X_1^3 + \frac{9t^{2d}}{4} X_1^2 + \frac{3t^d}{2} X_1 + \frac{1}{4}.$$

On ajuste alors l'échelle, *i.e.* poser $(X_2, Y_2) := (2^2 X_1, 2^3 Y_1)$ et l'on a

$$Y_2^2 = X_3^3 + +9t^{2d} X^2 + 24t^d X + 16.$$

Ce dernier modèle a pour discriminant $\Delta' = 2^{12} 3^3 \cdot (t^{3d} - 1)$. Il est donc entier (car les coefficients sont des entiers de K) et minimal en toute place v de K sauf en $v = \infty$ (car $2^{12} 3^3$ est une unité dans tous les corps résiduels de $\mathbb{F}_q(t)$). □

Prouvons alors l'identité suivante :

Proposition 5.2.4. *Soit $\mathbb{F}_Q/\mathbb{F}_q$ une extension finie. Alors*

$$\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_Q)} A(\tau, Q) = - \sum_{\chi \in Z(3d, Q)} \chi(27) \cdot \mathbf{j}_Q(\chi, \chi, \chi),$$

où la somme porte sur l'ensemble suivant de caractères de $\mathbb{F}_Q^\times$:

$$Z(3d, Q) := \Big\{ \chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times \;\Big|\; \chi^{3d} = \mathbf{1},\ \chi^3 \neq \mathbf{1} \Big\}.$$

Démonstration. Soit $\tau \in \mathbb{P}^1(\mathbb{F}_Q)$, on suppose que $\tau \neq \infty$ et on note à nouveau $\overline{(H_d)}_\tau$ la réduction de H_d en τ. C'est une courbe projective, dont un modèle affine est (*cf.* Lemme 5.2.3) :

$$\overline{(H_d)}_\tau : \quad Y^2 = X^3 + 9t^{2d} X^2 + 24t^d X + 16.$$

Dans un premier temps, dénombrons le nombre de points $\mathbb{F}_Q$-rationnels sur $\overline{(H_d)}_\tau$: il y a déjà le point à l'infini $[0 : 1 : 0]$, puis on utilise le Lemme 2.2.1 pour compter les points affines :

$$\begin{aligned}
\#\overline{(H_d)}_\tau(\mathbb{F}_Q) &= 1 + \#\left\{(x, y) \in \mathbb{F}_Q^2 \;\middle|\; y^2 = x^3 + 9\tau^{2d} x^2 + 24\tau^d x + 16\right\} \\
&= 1 + \sum_{x \in \mathbb{F}_Q} \#\left\{y \in \mathbb{F}_Q \;\middle|\; y^2 = x^3 + 9\tau^{2d} x^2 + 24\tau^d x + 16\right\} \\
&= 1 + \sum_{x \in \mathbb{F}_Q} \left(1 + \mu\left(x^3 + 9\tau^{2d} x^2 + 24\tau^d x + 16\right)\right) \\
&= Q + 1 + \sum_{x \in \mathbb{F}_Q} \mu\left(x^3 + 9\tau^{2d} x^2 + 24\tau^d x + 16\right).
\end{aligned}$$

Par suite, pour tout $\tau \in \mathbb{P}^1(\mathbb{F}_Q) \smallsetminus \{\infty\}$, on a

$$A(\tau, Q) = - \sum_{x \in \mathbb{F}_Q} \mu\left(x^3 + 9\tau^{2d} x^2 + 24\tau^d x + 16\right).$$

En la place $\tau = \infty$, la courbe H_d a réduction multiplicative déployée (*cf.* Proposition 5.1.4) : on a donc $A(\infty, Q) = 1$. Enfin, nous aurons besoin de séparer le terme correspondant à $\tau = 0$: la courbe H_d a bonne réduction en 0 et le calcul ci-dessus montre que

$$A(0, Q) = - \sum_{x \in \mathbb{F}_Q} \mu\left(x^3 + 16\right).$$

On somme alors ces quantités sur $\tau \in \mathbb{P}^1(\mathbb{F}_Q)$ et l'on sépare les termes correspondant à $\tau = 0$ et $\tau = \infty$. On réindexe ensuite la somme par $\gamma = \tau^{-1}$, on obtient :

$$\begin{aligned}
\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_Q)} A(\tau, Q) &= A(\infty, Q) + A(0, Q) + \sum_{\tau \in \mathbb{F}_Q^\times} A(\tau, Q) \\
&= A(\infty, Q) + A(0, Q) + \sum_{\gamma \in \mathbb{F}_Q^\times} A(\gamma^{-1}, Q) \\
&= A(\infty, Q) + A(0, Q) - \sum_{\gamma \in \mathbb{F}_Q^\times} \sum_{x \in \mathbb{F}_Q} \mu\left(x^3 + 9\gamma^{-2d} x^2 + 24\gamma^{-d} x + 16\right).
\end{aligned}$$

Manipulons alors la double somme pour se débarrasser des puissances négatives de $\gamma \in \mathbb{F}_Q^\times$ et faire apparaître des puissances multiples de $3d$:

$$\begin{aligned}\sum_{\gamma\in\mathbb{F}_Q^\times}\sum_{x\in\mathbb{F}_Q}\mu\left(x^3+9\gamma^{-2d}x^2+24\gamma^{-d}x+16\right) &= \sum_{\gamma\in\mathbb{F}_Q^\times}\sum_{x\in\mathbb{F}_Q}\mu(\gamma^{6d})\mu\left(x^3+9\gamma^{-2d}x^2+24\gamma^{-d}x+16\right)\\ &= \sum_{\gamma\in\mathbb{F}_Q^\times}\sum_{x\in\mathbb{F}_Q}\mu\left((\gamma^{2d}x)^3+9(\gamma^{2d}x)^2+24\gamma^{3d}(\gamma^{2d}x)+16\gamma^{6d}\right)\\ &= \sum_{\gamma\in\mathbb{F}_Q^\times}\sum_{x'\in\mathbb{F}_Q}\mu\left(x'^3+9x'^2+24\gamma^{3d}x'+16\gamma^{6d}\right),\end{aligned}$$

où l'on a posé $x' = \gamma^{2d}x$ pour tout $\gamma \neq 0$. On a alors

$$\sum_{\gamma\neq 0}\sum_{x'\in\mathbb{F}_Q}\mu\left(x'^3+9x'^2+24\gamma^{3d}x'+16\gamma^{6d}\right) = \sum_{\gamma,x'}\mu\left(x'^3+9x'^2+24\gamma^{3d}x'+16\gamma^{6d}\right) - \sum_{x'\in\mathbb{F}_Q}\mu\left(x'^3+9x'^2\right)$$

où

$$\sum_{x'\in\mathbb{F}_Q}\mu\left(x'^3+9x'^2\right) = \sum_{x'\in\mathbb{F}_Q}\mu(x'^2)\mu\left(x'+9\right) = \sum_{x'\neq 0}\mu\left(x'+9\right) = -\mu(9) = -1.$$

Nous pouvons maintenant utiliser le Lemme 2.2.2 et « réindexer » la somme sur $\gamma \in \mathbb{F}_Q$:

$$\begin{aligned}\sum_{\gamma\in\mathbb{F}_Q}\sum_{x'\in\mathbb{F}_Q}\mu\left(x'^3+9x'^2+24\gamma^{3d}x'+16\gamma^{6d}\right) &= \sum_{z\in\mathbb{F}_Q}\left(\sum_{\chi^{3d}=\mathbf{1}}\chi(z)\right)\sum_{x'\in\mathbb{F}_Q}\mu\left(x'^3+9x'^2+24zx'+16z^2\right)\\ &= \sum_{\chi^{3d}=\mathbf{1}}\left(\sum_{z\in\mathbb{F}_Q}\sum_{x'\in\mathbb{F}_Q}\chi(z)\mu\left(x'^3+9x'^2+24zx'+16z^2\right)\right),\end{aligned}$$

la somme portant sur l'ensemble des caractères $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ dont la puissance $3d$-ième est triviale. Pour un caractère quelconque $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$, définissons donc

$$M_Q(\chi) := \sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z)\mu\left(x^3+9x^2+24zx+16z^2\right).$$

Tâchons à présent d'identifier ces sommes $M_Q(\chi)$ sous la forme de sommes de Jacobi :

Lemme 5.2.5. *Soit $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ un caractère quelconque. Alors :*

$$M_Q(\chi) = \begin{cases}0 & \text{si } \chi \text{ est trivial,}\\ \chi(27)\cdot\mathbf{j}_Q(\chi,\chi,\chi) & \text{sinon.}\end{cases}$$

Pour clarifier l'argument, nous remettons la preuve de ce Lemme à la Section 5.2.2 ci-dessous. En tout état de cause, avec le calcul qui précède, si l'on applique ce Lemme aux caractères dont la puissance $3d$-ième est triviale, nous parvenons à

$$\begin{aligned}\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)}A(\tau,Q) &= A(0,Q)+A(\infty,Q)-\sum_{\gamma\in\mathbb{F}_Q^\times}\sum_{x\in\mathbb{F}_Q}\mu\left(x^3+9\gamma^{-2d}x^2+24\gamma^{-d}x+16\right)\\ &= A(0,Q)+A(\infty,Q)-\left(1+\sum_{\gamma\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\mu\left(x^3+9\gamma^{-2d}x^2+24\gamma^{-d}x+16\right)\right)\\ &= A(0,Q)+A(\infty,Q)-1-\sum_{\chi^{3d}=\mathbf{1}}M_Q(\chi)\\ &= A(0,Q)-\sum_{\substack{\chi^{3d}=\mathbf{1}\\ \chi\neq\mathbf{1}}}\chi(27)\cdot\mathbf{j}_Q(\chi,\chi,\chi),\end{aligned}$$

car $A(\infty,Q) = 1$. Pour conclure la preuve de la Proposition 5.2.4, il nous faut donc comprendre le terme $A(0,Q)$:

Lemme 5.2.6. *Soit $\xi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ un caractère non trivial d'ordre 3, s'il en existe. Alors on a*

$$A(0,Q) - \xi(27)\cdot \mathbf{j}_Q(\xi,\xi,\xi) - \xi^2(27)\cdot \mathbf{j}_Q(\xi^2,\xi^2,\xi^2) = 0.$$

S'il n'existe pas de tel ξ, on a $A(0,Q) = 0$.

Démonstration. Supposons d'abord qu'un tel ξ existe (ce qui est équivalent à supposer que $3 \mid q-1$). Alors $\xi\cdot\xi\cdot\xi = \mathbf{1}$ et un calcul classique de sommes de Jacobi (évoqué à la Proposition 2.2.7, *cf.* [IR90, Chap. 8, §6, Corollary 2]) implique que $\mathbf{j}_Q(\xi,\xi,\xi) = -\xi(-1)\cdot(-\mathbf{j}_Q(\xi,\xi)) = \xi(-1)\cdot\mathbf{j}_Q(\xi,\xi)$. Le même résultat vaut lorsque ξ est remplacé par ξ^2. Puisque $\xi(27) = \xi(3^3) = 1$, il vient

$$\xi(27)\cdot\mathbf{j}_Q(\xi,\xi,\xi) + \xi^2(27)\cdot\mathbf{j}_Q(\xi^2,\xi^2,\xi^2) = \xi(-1)\cdot\mathbf{j}_Q(\xi,\xi) + \xi^2(-1)\cdot\mathbf{j}_Q(\xi^2,\xi^2).$$

D'autre part, d'après le Lemme 2.2.2, on a

$$\begin{aligned}
-A(0,Q) &= \sum_{x\in\mathbb{F}_Q}\mu(x^3+16) = \sum_{y\in\mathbb{F}_Q}(1+\xi(y)+\xi^2(y))\cdot\mu(y+16)\\
&= \sum_{y\in\mathbb{F}_Q}\mu(y+16) + \sum_{y\in\mathbb{F}_Q}\xi(y)\cdot\mu(y+16) + \sum_{y\in\mathbb{F}_Q}\xi^2(y)\cdot\mu(y+16)\\
&= 0 - \xi(-16)\cdot\mathbf{j}_Q(\xi,\mu) - \xi^2(-16)\cdot\mathbf{j}_Q(\xi^2,\mu)\\
&= -\xi(-4^3)\cdot\mathbf{j}_Q(\xi,\xi) - \xi^2(-4^3)\cdot\mathbf{j}_Q(\xi^2,\xi^2)\\
&= -\xi(-1)\cdot\mathbf{j}_Q(\xi,\xi) - \xi^2(-1)\cdot\mathbf{j}_Q(\xi^2,\xi^2).
\end{aligned}$$

On a donc $A(0,Q) - \xi(27)\cdot\mathbf{j}_Q(\xi,\xi,\xi) - \xi^2(27)\cdot\mathbf{j}_Q(\xi^2,\xi^2,\xi^2) = 0$.

Supposons à présent qu'il n'existe pas de tel caractère ξ : alors 3 ne divise pas $q-1$ et l'application $\psi : x \mapsto x^3$ est une bijection du groupe cyclique $\mathbb{F}_q^\times$, qui se prolonge en une bijection $\psi : \mathbb{F}_q \to \mathbb{F}_q$. On peut ainsi « réindexer » la somme $A(0,Q)$:

$$-A(0,Q) = \sum_{x\in\mathbb{F}_q}\mu(x^3+16) = \sum_{x\in\mathbb{F}_q}\mu(\psi(x)+16) = \sum_{z\in\mathbb{F}_q}\mu(z+16) = 0.$$

La dernière égalité vient du fait que μ n'est pas le caractère trivial. □

Grâce à ce résultat, nous pouvons finalement réécrire la somme $\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q)$ sous la forme souhaitée :

$$\begin{aligned}
\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) &= A(0,Q) - \sum_{\substack{\chi^{3d}=\mathbf{1}\\ \chi\neq\mathbf{1}}}\chi(27)\cdot\mathbf{j}_Q(\chi,\chi,\chi)\\
&= -\sum_{\substack{\chi^{3d}=\mathbf{1}\\ \chi\neq\mathbf{1},\chi^3\neq\mathbf{1}}}\chi(27)\cdot\mathbf{j}_Q(\chi,\chi,\chi).
\end{aligned}$$

Il reste à définir, comme dans l'énoncé de la Proposition, l'ensemble $Z(3d,Q)$ des caractères non triviaux $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ dont la puissance $3d$-ième est triviale et tels que $\chi^3 \neq \mathbf{1}$. Nous avons bien obtenu l'expression annoncée à la Proposition 5.2.4. □

5.2.2 Preuve du Lemme 5.2.5

Soit $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ un caractère quelconque, on a posé

$$M_Q(\chi) := \sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z)\mu\left(x^3+9x^2+24zx+16z^2\right)$$

et l'on doit montrer que $M_Q(\chi)$ s'écrit comme une somme de Jacobi si χ n'est pas trivial (et $M_Q(\mathbf{1}) = 0$). Nous n'utilisons cette identité que dans le cas où l'ordre de χ divise $3d$.

Démonstration. Remarquons tout d'abord que, pour tous $x, z \in \mathbb{F}_Q$, on a

$$x^3+9x^2+24zx+16z^2 = x^3+(3x+4z)^2.$$

Ainsi, si l'on pose $(u,v) = (x, 3x+4z)$ (c'est-à-dire $x = u$ et $z = \frac{v-3u}{4}$), on peut réindexer la double somme $M_Q(\chi)$ de la façon suivante :

$$\begin{aligned} M_Q(\chi) &= \sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z)\mu\left(x^3+9x^2+24zx+16z^2\right) = \sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z)\mu\left(x^3+(3x+4z)^2\right) \\ &= \sum_{u\in\mathbb{F}_Q}\sum_{v\in\mathbb{F}_Q}\chi\left(\frac{v-3u}{4}\right)\mu\left(u^3+v^2\right) = \overline{\chi}(4)\sum_{u\in\mathbb{F}_Q}\sum_{v\in\mathbb{F}_Q}\chi\left(v-3u\right)\mu\left(u^3+v^2\right). \end{aligned}$$

Pour traiter cette double somme, on met à part les termes avec « $u = 0$ » des autres, pour lesquels on écrit « $v = uw$ ». On utilise à nouveau le fait que $\mu(v)^2 = 1$ pour tout $v \neq 0$:

$$\begin{aligned} \sum_{u\in\mathbb{F}_Q}\sum_{v\in\mathbb{F}_Q}\chi\left(v-3u\right)\mu\left(u^3+v^2\right) &= \sum_{v\in\mathbb{F}_Q}\chi\left(v\right)\mu\left(v^2\right) + \sum_{u\neq 0}\sum_{w\in\mathbb{F}_Q}\chi\left(uw-3u\right)\mu\left(u^3+u^2w^2\right) \\ &= \sum_{v\neq 0}\chi\left(v\right) + \sum_{u\neq 0}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\mu(u)^2\mu\left(u+w^2\right) \\ &= \sum_{v\neq 0}\chi\left(v\right) + \sum_{u\neq 0}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\mu\left(u+w^2\right). \end{aligned}$$

Pour expliciter le terme à droite, considérons la somme auxiliaire suivante :

$$S'_Q(\chi) := \sum_{u\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\left(1+\mu\left(u+w^2\right)\right).$$

D'une part, grâce au Lemme 2.2.1, on a

$$\begin{aligned} S'_Q(\chi) &= \sum_{u\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\cdot\#\left\{t\in\mathbb{F}_Q \;\middle|\; t^2 = u+w^2\right\} \\ &= \sum_{u\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\cdot\#\left\{t\in\mathbb{F}_Q \;\middle|\; u = (t-w)(t+w)\right\} \\ &= \sum_{t\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(t-w)\chi(t+w)\chi(w-3). \end{aligned}$$

On réindexe cette double somme en posant $(x,y,z) = \left(\frac{w-t}{6}, \frac{w+t}{6}, \frac{3-w}{3}\right)$ de sorte que $x+y+z = 1$ et $w = 3(x+y)$, $t = 3(y-x)$: on obtient

$$\begin{aligned} S'_Q(\chi) &= \sum_{t\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(t-w)\chi(t+w)\chi(w-3) = \sum_{x+y+z=1}\chi(-6x)\chi(6y)\chi(-3z) \\ &= \chi(3^3 2^2)\cdot\sum_{x+y+z=1}\chi(x)\chi(y)\chi(z) = \chi(3^3\cdot 4)\cdot\mathbf{j}_Q(\chi,\chi,\chi). \end{aligned}$$

D'autre part, on peut exprimer $S'_Q(\chi)$ en fonction de la somme que nous voulons expliciter :

$$\begin{aligned} S'_Q(\chi) &= \sum_{u\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\left(1+\mu\left(u+w^2\right)\right) \\ &= \sum_{u\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3) + \sum_{u\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\mu\left(u+w^2\right) \\ &= \left(\sum_{u\in\mathbb{F}_Q}\chi(u)\right)\left(\sum_{w\in\mathbb{F}_Q}\chi(w-3)\right) + \sum_{u\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\mu\left(u+w^2\right) \\ &= \left(\sum_{v\in\mathbb{F}_Q}\chi(v)\right)^2 + \sum_{u\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\mu\left(u+w^2\right). \end{aligned}$$

L'examen de la somme auxiliaire $S'_Q(\chi)$ nous a ainsi permis de démontrer l'identité :

$$\sum_{u\in\mathbb{F}_Q}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\mu\left(u+w^2\right) = \chi(4\cdot 27)\cdot\mathbf{j}_Q(\chi,\chi,\chi) - \left(\sum_{v\in\mathbb{F}_Q}\chi(v)\right)^2.$$

Réutilisons donc celle-ci dans le calcul de $M_Q(\chi)$. Supposons d'abord que χ n'est pas le caractère trivial (auquel cas $\sum_{v\neq 0}\chi(v)=0$). On a

$$\begin{aligned}M_Q(\chi) &= \overline{\chi}(4)\sum_{u\in\mathbb{F}_Q}\sum_{v\in\mathbb{F}_Q}\chi\left(v-3u\right)\mu\left(u^3+v^2\right)\\ &= \overline{\chi}(4)\sum_{v\neq 0}\chi\left(v\right)+\overline{\chi}(4)\sum_{u\neq 0}\sum_{w\in\mathbb{F}_Q}\chi(u)\chi(w-3)\mu\left(u+w^2\right)\\ &= 0+\overline{\chi}(4)\cdot\chi(4\cdot 27)\cdot\mathbf{j}_Q(\chi,\chi,\chi)-\overline{\chi}(4)\left(\sum_{v\in\mathbb{F}_Q}\chi(v)\right)^2\\ &= \chi(27)\cdot\mathbf{j}_Q(\chi,\chi,\chi)+0,\end{aligned}$$

ce qu'il fallait démontrer dans ce cas. Si à présent χ est le caractère trivial, on trouve que

$$M_Q(\mathbf{1}) = \overline{\mathbf{1}}(4)\sum_{u\in\mathbb{F}_Q}\sum_{v\in\mathbb{F}_Q}\mathbf{1}\left(v-3u\right)\mu\left(u^3+v^2\right) = (Q-1)+1\cdot\sum_{u\neq 0}\sum_{w\in\mathbb{F}_Q}\mathbf{1}(u)\mathbf{1}(w-3)\mu\left(u+w^2\right)$$

$$= (Q-1)+\sum_{u\neq 0}\left(\sum_{w\in\mathbb{F}_Q}\mu\left(w^2+u\right)\right) = (Q-1)+(Q-1)\cdot(-1) = 0.$$

Ce qui termine la preuve du Lemme 5.2.5. □

5.2.3 Réindexation des caractères

Pour toute extension finie $\mathbb{F}_{q^n}/\mathbb{F}_q$, la Proposition 5.2.4 nous permet d'écrire

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})}A(\tau,q^n) = -\sum_{\chi\in Z(3d,q^n)}\chi(27)\cdot\mathbf{j}_{q^n}(\chi,\chi,\chi),$$

la somme portant sur l'ensemble de caractères suivants :

$$Z(3d,q^n) := \left\{\chi:\mathbb{F}_{q^n}^\times\to\overline{\mathbb{Q}}^\times\;\middle|\;\chi^{3d}=\mathbf{1},\ \chi^3\neq\mathbf{1}\right\}.$$

Nous sommes à présent en mesure d'exprimer la fonction L de la courbe H_d sous la forme d'un produit. Par définition de la fonction L comme produit eulérien (*cf.* Lemme 1.3.15), on a l'identité formelle :

$$\log L\big(H_d/\mathbb{F}_q(t),T\big) = \sum_{n=1}^{\infty}\left(\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})}A(\tau,q^n)\right)\frac{T^n}{n}.$$

Ce que l'on peut réécrire ici sous la forme :

$$\log L\big(H_d/\mathbb{F}_q(t),T\big) = -\sum_{n=1}^{\infty}\left(\sum_{\chi\in Z(3d,q^n)}\chi(27)\cdot\mathbf{j}_{q^n}(\chi,\chi,\chi)\right)\frac{T^n}{n}.$$

Au membre de droite, on reconnaît une somme du type étudié à la Section 2.1.4 (et plus particulièrement à la Proposition 2.1.15 avec $\ell=3$). Plus précisément, pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$ et tout caractère non trivial $\chi:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times$, on pose

$$\sigma(\chi,Q) = \chi(27)\cdot\mathbf{j}_Q(\chi,\chi,\chi).$$

On peut montrer que cette donnée satisfait aux hypothèses de la Proposition 2.1.15 (avec $\ell=3$ et $K=1$). En effet, si $\mathbb{F}_{Q^s}/\mathbb{F}_Q$ est une extension finie supplémentaire et que $\chi^{(s)}:\mathbb{F}_{Q^s}^\times\to\overline{\mathbb{Q}}^\times$ désigne l'extension de $\chi:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times$ via la norme $\mathbf{N}_{\mathbb{F}_{Q^s}/\mathbb{F}_Q}$, comme les sommes de Jacobi vérifient une relation de Hasse-Davenport à l'ordre $K=1$ (Théorème 2.2.20) et que $27\in\mathbb{F}_q\subset\mathbb{F}_Q$, on a

$$\sigma(\chi^{(s)},Q^s) = \chi^{(s)}(27)\cdot\mathbf{j}_{Q^s}(\chi^{(s)},\chi^{(s)},\chi^{(s)}) = \chi(27)^s\cdot\left(\mathbf{j}_Q(\chi,\chi,\chi)\right)^s = \left(\sigma(\chi,Q)\right)^s.$$

D'autre part, $\sigma(\chi,Q)$ est, à multiplication par $\chi(27)$ près, une somme portant sur des éléments de $\mathbb{F}_Q\times\mathbb{F}_Q$ (par définition des sommes de Jacobi). Or, cet ensemble $\mathbb{F}_Q\times\mathbb{F}_Q$ est permuté par l'application

$x \mapsto x^q$: on a donc $\sigma(\chi^q, Q) = \sigma(\chi, Q)$. Les deux hypothèses de la Proposition 2.1.15 sus-mentionnée sont donc vérifiées (avec $\ell = 3$ et $K = 1$) et l'on en déduit que

$$\sum_{n=1}^{\infty} \left(\sum_{\chi \in Z(3d, q^n)} \chi(27) \cdot \mathbf{j}_{q^n}(\chi, \chi, \chi) \right) \frac{T^n}{n} = \sum_{m \in \mathcal{O}_q^{(3)}(3d)} -\log\left(1 - \sigma(\mathbf{t}_m, q^{u(m)}) \cdot T^{u(m)}\right).$$

Dans cette dernière identité, $\mathcal{O}_q^{(3)}(3d)$ désigne l'ensemble des orbites m de $\mathbb{Z}/3d\mathbb{Z}\smallsetminus\{0\}$ sous l'action de q par multiplication, duquel on a retiré les orbites $\{d\}$ et $\{2d\}$. Par suite, on a

$$\log L\big(H_d/\mathbb{F}_q(t), T\big) = \log \left(\prod_{m \in \mathcal{O}_q^{(3)}(3d)} \left(1 - \sigma(\mathbf{t}_m, q^{u(m)}) \cdot T^{u(m)}\right) \right).$$

D'où l'on tire que

$$L\big(H_d/\mathbb{F}_q(t), T\big) = \prod_{m \in \mathcal{O}_q^{(3)}(3d)} \left(1 - \sigma(\mathbf{t}_m, q^{u(m)}) \cdot T^{u(m)}\right).$$

Et ceci termine la preuve du Théorème 5.2.1 car $\sigma(\mathbf{t}_m, q^{u(m)}) = \mathbf{t}_m(27) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m)$ pour toute orbite $m \in \mathcal{O}_q^{(3)}(3d)$.

Remarque 5.2.7. La fonction L obtenue est bien un polynôme à coefficients entiers, de degré cohérent avec (5.6). On peut l'expliciter encore plus lorsque $3d$ divise $q - 1 = \#\mathbb{F}_q$: en effet, il existe dans ce cas un caractère $\chi_0 : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ d'ordre exactement $3d$ et l'action de q par multiplication sur $\mathbb{Z}/3d\mathbb{Z}$ est triviale ; la fonction L de H_d s'écrit donc

$$L\big(H_d/\mathbb{F}_q(t), T\big) = \prod_{\substack{j=1 \\ j \neq d, 2d}}^{3d} \left(1 - \mathbf{j}_q(\chi_0^j, \chi_0^j, \chi_0^j) \cdot T\right).$$

5.3 Rang et valeur spéciale de H_d

5.3.1 Conjecture de Birch et Swinnerton-Dyer pour H_d

Pour démontrer que H_d vérifie les conjectures de Birch et Swinnerton-Dyer, nous appliquons le résultat de Shioda (Théorème 1.4.15) que nous avons rappelé à la Section 1.4.4.

Théorème 5.3.1 (Shioda)**.** *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$. Pour tout entier $d \geqslant 2$, premier à p, on considère à nouveau la courbe elliptique Hessienne H_d sur $K = \mathbb{F}_q(t)$, dont un modèle affine est :*

$$H_d : \quad Y^2 + 3t^d XY + Y = X^3.$$

La courbe H_d/K vérifie la conjecture de Birch et Swinnerton-Dyer (Conjecture 1.4.1). En particulier, son groupe de Tate-Shafarevich $Ш(H_d/K)$ est fini et le ratio de Brauer-Siegel $\mathfrak{Bs}(H_d/K)$ également.

Démonstration. Soit d un entier premier à la caractéristique $p \geqslant 5$ de $K = \mathbb{F}_q(t)$, on définit $f \in \mathbb{F}_q[t, X, Y]$ par

$$f(t, X, Y) := Y^2 + 3t^d XY + Y - X^3 = 1 \cdot t^0 XY^2 + 3 \cdot t^d XY + 1 \cdot t^0 X^0 Y - 1 \cdot t^0 X^3 Y^0.$$

Le polynôme f est une somme de quatres monômes non nuls. Montrons qu'il satisfait la condition de Shioda : on associe à f la matrice de ses exposants

$$A_f = \begin{bmatrix} 0 & 0 & 2 & -1 \\ d & 1 & 1 & -1-d \\ 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & -2 \end{bmatrix},$$

dont le déterminant est $\det A_f = -3d$, de sorte que $d(f) \equiv 3d \bmod p$. En particulier $d(f) \not\equiv 0 \bmod p$ (car $p \geqslant 5$ et d est premier à p) et f satisfait effectivement la condition de Shioda.

Or, la (partie affine de la) courbe H_d/K est définie comme l'ensemble des zéros de f dans $\mathbb{A}^2/K$. Donc H_d/K vérifie la conjecture de Birch et Swinnerton-Dyer (Théorème 1.4.15). □

5.3.2 Rang et valeur spéciale

En combinant l'expression explicite de la fonction L avec la conjecture de Birch et Swinnerton-Dyer, il est dorénavant possible d'obtenir une expression « combinatoire » du rang du groupe de Mordell-Weil $H_d(K)$ d'une part et une formule fermée pour la valeur spéciale $L^*(H_d/K,1)$ d'autre part. Soit $d \geqslant 2$ un entier premier à la caractéristique de $K = \mathbb{F}_q(t)$. On a démontré (Théorème 5.2.1) que la fonction L de la courbe Hessienne H_d s'écrivait sous la forme d'un produit :

$$L\big(H_d/\mathbb{F}_q(t),T\big) = \prod_{m\in\mathcal{O}_q^{(3)}(3d)} \Big(1 - \mathbf{t}_m(27)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m)\cdot T^{u(m)}\Big).$$

Nous sommes donc naturellement conduits à poser la définition suivante :

Définition 5.3.2. Pour tout entier $d \geqslant 2$, premier à q, on pose :

$$\mathcal{Z}_q(3d) := \Big\{ m \in \mathcal{O}_q^{(3)}(d) \;\Big|\; \mathbf{t}_m(27)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m) = q^{u(m)} \Big\},$$

ainsi que $\mathcal{V}_q^*(3d) := \mathcal{O}_q^{(3)}(d) \smallsetminus \mathcal{Z}_q(3d)$.

Utilisons alors les techniques développées à la Section 3.1 : on obtient directement les deux propositions ci-dessous.

Proposition 5.3.3. *Soit $d \geqslant 2$ un entier premier à q et $K = \mathbb{F}_q(t)$. Le rang du groupe de Mordell-Weil $H_d(K)$ de la courbe Hessienne s'exprime sous la forme :*

$$\operatorname{rang} H_d(K) = \#\mathcal{Z}_q(3d) = \Big\{ m \in \mathcal{O}_q^{(3)}(d) \;\Big|\; \mathbf{t}_m(27)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m) = q^{u(m)} \Big\}.$$

Démonstration. D'après la conjecture de Birch et Swinnerton-Dyer (Théorème 5.3.1), expliciter le rang du groupe de Mordell-Weil $H_d(K)$ revient à calculer l'ordre d'annulation de $L\big(H_d/K,T\big)$ en $T = q^{-1}$. Pour simplifier, notons $L(T) = L\big(H_d/K,T\big) \in \mathbb{Z}[T]$ et pour toute orbite $m \in \mathcal{O}_q^{(3)}(3d)$, posons $\Omega(m) := \mathbf{t}_m(27)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m)$. D'après le Lemme 3.1.4 (voir aussi l'Exemple 3.1.9), on a

$$\operatorname{ord}_{T=q^{-1}} L(T) = \#\Big\{ m \in \mathcal{O}_q^{(3)}(3d) \;\Big|\; \Omega(m) = q^{u(m)} \Big\} = \#\mathcal{Z}_q(3d).$$

Comme annoncé, $\operatorname{rang} H_d(K) = \operatorname{ord}_{T=q^{-1}} L(T) = \#\mathcal{Z}_q(3d)$. □

Proposition 5.3.4. *Avec les mêmes hypothèses et notations, la valeur spéciale $L^*\big(H_d/K,1\big)$ de la fonction L de la courbe Hessienne H_d s'écrit*

$$L^*\big(H_d/K,1\big) = \prod_{m\in\mathcal{Z}_q(3d)} u(m)\cdot \prod_{m\in\mathcal{V}_q^*(3d)} \left(1 - \frac{\mathbf{t}_m(27)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m)}{q^{u(m)}}\right).$$

Démonstration. Une partie de ce calcul a été faite à la Section 3.1.3. Notons (*cf.* Proposition 5.3.3) :

$$r = \operatorname{ord}_{T=q^{-1}} L\big(H_d/K,T\big) = \#\mathcal{Z}_q(3d).$$

Si, pour toute orbite $m \in \mathcal{O}_q^{(3)}(3d)$, on pose

$$\Omega(m) = \mathbf{t}_m(27)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m) \quad \text{et} \quad g_m(T) = 1 - \Omega(m)\cdot T^{u(m)},$$

on a $L\big(H_d/K,T\big) = \prod_{m\in\mathcal{O}_q^{(3)}(3d)} g_m(T)$. Par construction, $g_m(q^{-1}) = 0$ si et seulement si $m \in \mathcal{Z}_q(3d)$. De ceci et de la Proposition 5.3.3 ci-dessus, on déduit que

$$\frac{L\big(H_d/K,T\big)}{(1-qT)^r} = \frac{L\big(H_d/K,T\big)}{(1-qT)^{\#\mathcal{Z}_q(3d)}} = \prod_{m\in\mathcal{Z}_q(3d)} \frac{g_m(T)}{1-qT}\cdot \prod_{m\notin\mathcal{Z}_q(3d)} g_m(T).$$

Pour expliciter la valeur spéciale $L^*\big(H_d/K,1\big)$, il s'agit d'évaluer cette expression en $T = q^{-1}$ (*cf.* Définition 1.3.12). On arrive immédiatement à l'égalité donnée dans l'énoncé de la Proposition. □

Comme la courbe H_d/K satisfait à la conjecture de Birch et Swinnerton-Dyer (Théorème 5.3.1), on a par ailleurs,

$$L^*\big(H_d/K,1\big) = \frac{\#Ш\big(H_d/K\big)\cdot \operatorname{Reg}\big(H_d/K\big)}{\big(\#H_d(K)_{\mathrm{tors}}\big)^2}\cdot \mathcal{T}am\big(H_d/K\big)\cdot \frac{q}{H\big(H_d/K\big)}.$$

Tous les termes du membre de droite sont des nombres rationnels strictement positifs, il en est donc de même de $L^*(H_d/K,1)$.

5.3.3 Un résultat de rang non borné

Nous pouvons démontrer, au passage, un résultat de « rang non borné » pour la famille des courbes Hessiennes sur $K = \mathbb{F}_q(t)$.

Proposition 5.3.5. *Supposons que $\mathbb{F}_q$ est un corps fini de caractéristique $p \geqslant 5$ tel que $q \equiv 2 \bmod 3$. Lorsque d parcourt l'ensemble des entiers premier à p, le rang des courbes Hessiennes H_d définies par le modèle (5.5) sur $K = \mathbb{F}_q(t)$ n'est pas borné :*

$$\limsup_{\mathrm{pgcd}(d,q)=1} \operatorname{rang} H_d\big(\mathbb{F}_q(t)\big) = +\infty.$$

Donnons une preuve élémentaire de ce fait : c'est un corollaire rapide de la Proposition 5.3.3 et du Théorème de Shafarevich-Tate (Théorème 2.4.4). Pour le moment, nous ne savons pas comment traiter le cas où $q \equiv 1 \bmod 3$ par cette approche. Toutefois, remarquons que cette proposition est en fait un cas particulier de [Ulm07b, Theorem 4.7] et ce, indépendamment de la congruence de q modulo 3 (on peut également consulter [Ulm11, Lecture 4, Theorem 3.1.1] et [Ber08, Theorem 4.2]).

Démonstration. Il s'agit de trouver une famille infinie d'entiers d premiers à q tels que la fonction $L\big(H_d/K, T\big)$ s'annule avec une multiplicité non bornée en $T = q^{-1}$ (car la conjecture de Birch et Swinnerton-Dyer est vraie pour H_d). Reprenons les notations introduites ci-dessus. Pour tout entier $N \in \mathbb{N}^*$, on pose $e_N = q^{3N} + 1$ (un entier pair et premier à q). Comme 3 divise $q-2$, on a $e_N \equiv 2^{3N} + 1 \equiv 0 \bmod 3$. Soit alors $d_N = e_N/3 = (q^{3N}+1)/3$, d_N est un entier premier à q tel que $3d_N$ divise $q^{3N}+1$. Le Lemme 2.4.1 montre que l'ordre de q modulo d_N vérifie $o_q(d_N) \leqslant o_q(3d_N) \leqslant 6N$.

Comme $3d_N$ divise $q^{3N}+1$, on peut alors utiliser le Corollaire 2.4.6 du Théorème de Shafarevich-Tate (Théorème 2.4.4) : pour toute orbite $m \in \mathcal{O}_q^{(3)}(3d_N)$, on a

$$\mathbf{t}_m(27) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) = q^{u(m)}.$$

Par suite, comme le rang de $H_d/\mathbb{F}_q(t)$ est donné par $\#\mathcal{Z}_q(3d)$ (*cf.* Proposition 5.3.3), on a

$$\forall N \in \mathbb{N}^*, \quad \operatorname{rang} H_{d_N}(\mathbb{F}_q(t)) = \#\mathcal{Z}_q(3d_N) = \#\mathcal{O}_q^{(3)}(3d_N) = \#\mathcal{O}_q^{(3)}(e_N).$$

On peut maintenant donner une minoration de $\#\mathcal{O}_q^{(3)}(e_N)$: comme, pour tout diviseur $d' > 3$ de e_N, on a $o_q(d') \leqslant o_q(e_N) \leqslant 6N$, on obtient :

$$\#\mathcal{O}_q^{(3)}(e_N) = \sum_{\substack{d' \mid e_N \\ d'>3}} \frac{\phi(d')}{o_q(d')} \geqslant \frac{1}{o_q(e_N)} \cdot \sum_{\substack{d' \mid e_N \\ d'>3}} \phi(d') = \frac{e_N - \phi(2) - \phi(3)}{o_q(e_N)} \geqslant \frac{e_N - 3}{6N}.$$

Or, pour $N \geqslant 1$, on a

$$\log d_N = \log(e_N/3) \geqslant 3N \cdot \log q - \log 3 \geqslant (3N-1) \cdot \log q \geqslant 2N \cdot \log q.$$

D'où l'on tire que

$$\operatorname{rang} H_{d_N}(\mathbb{F}_q(t)) \geqslant \frac{e_N - 3}{6N} \geqslant \frac{3d_N - 3}{\frac{3}{\log q} \cdot \log d_N} \gg_q \frac{d_N}{\log d_N},$$

la constante implicite ne dépendant que de q. La quantité à droite de cette inégalité tend vers $+\infty$ lorsque $N \to \infty$. Donc le rang de $H_{d_N}(K)$ n'est pas borné lorsque $q \equiv 2 \bmod 3$. □

Dans la situation décrite dans la preuve ci-dessus, la Proposition 5.3.4 implique que la valeur spéciale $L^*(H_{d_N}/K, 1)$ est un entier car $\mathcal{Z}_q(3d_N) = \mathcal{O}_q^{(3)}(3d_N)$:

$$L^*(H_{d_N}/K, 1) = \prod_{m \in \mathcal{O}_q^{(3)}(3d_N)} u(m) \in \mathbb{N}^*.$$

Par suite, on a $\log L^*(H_{d_N}/K, 1) \geqslant 0$. Auquel cas, toujours sous les hypothèses de la Proposition 5.3.5, on a

$$\mathfrak{Bs}(H_{d_N}/K, 1) \geqslant 1 + o(1) \qquad (N \to \infty).$$

Dans le cas général, nous estimerons le ratio de Brauer-Siegel des courbes Hessiennes H_d à la Section suivante.

5.4 Ratio de Brauer-Siegel des courbes Hessiennes

Dans cette dernière section, nous utilisons les résultats démontrés ci-avant pour étudier le ratio de Brauer-Siegel des courbes H_d. Le résultat principal de ce chapitre est le suivant :

Théorème 5.4.1. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \geqslant 2$, premier à q, on considère la courbe elliptique Hessienne H_d sur K, dont un modèle affine est donné par :*

$$H_d : \quad Y^2 + 3t^d XY + Y = X^3.$$

Lorsque $H\big(H_d/K\big) \to \infty$ (i.e. lorsque $d \to \infty$), le ratio de Brauer-Siegel $\mathfrak{Bs}\big(H_d/K\big)$ admet une limite et celle-ci est 1 :

$$\mathfrak{Bs}\big(H_d/K\big) \xrightarrow[\substack{\mathrm{pgcd}(d,q)=1 \\ d\to+\infty}]{} 1.$$

Notons que ce résultat est inconditionnel car la conjecture de Birch et Swinnerton-Dyer est vraie pour H_d (Théorème 5.3.1). Le raisonnement est de même nature que celui effectué à la Section 4.4 du Chapitre 4 pour les courbes de Legendre.

5.4.1 Plan de l'argument

Plaçons-nous sous les hypothèses du Théorème 5.4.1. Comme la courbe H_d vérifie la conjecture de Birch et Swinnerton-Dyer (*cf.* Théorème 5.3.1), on peut utiliser la relation entre ratio de Brauer-Siegel et valeur spéciale (démontrée à la Proposition 1.6.4 de la Section 1.6.3) : lorsque $d \to \infty$,

$$\mathfrak{Bs}\big(H_d/K\big) = 1 + \frac{\log L^*\big(H_d/K, 1\big)}{\log H\big(H_d/K\big)} + o(1). \tag{5.9}$$

Pour obtenir la limite de $\mathfrak{Bs}\big(H_d/K\big)$ promise au Théorème 5.4.1, il reste donc à encadrer la valeur spéciale $L^*\big(H_d/K, 1\big)$. Plus précisément, il s'agit de démontrer :

- une majoration :
$$\frac{\log L^*\big(H_d/K, 1\big)}{\log H\big(H_d/K\big)} \leqslant 0 + o(1) \qquad (d \to \infty).$$
Celle-ci est relativement aisée à prouver (Proposition 5.4.2).
- ainsi qu'une minoration :
$$\frac{\log L^*\big(H_d/K, 1\big)}{\log H\big(H_d/K\big)} \geqslant 0 - o(1) \qquad (d \to \infty),$$
qui est plus délicate à obtenir (*cf.* Proposition 5.4.3).

La preuve de ces deux inégalités occupe le reste de cette section. Notons dès à présent que la conjonction de celles-ci et de (5.9) donne bien le Théorème 5.4.1 pour la famille des courbes H_d :

$$1 - o(1) \leqslant \mathfrak{Bs}\big(H_d/K\big) \leqslant 1 + o(1) \qquad (d \to \infty).$$

5.4.2 Majoration de la valeur spéciale

Proposition 5.4.2. *Soit $d \geqslant 2$ un entier premier à q. Lorsque $d \to \infty$, la valeur spéciale $L^*\big(H_d/K, 1\big)$ de la fonction L associée à la courbe hessienne H_d/K admet la majoration suivante*

$$\frac{\log L^*\big(H_d/K, 1\big)}{\log H\big(H_d/K\big)} \leqslant 0 + o(1) \qquad (d \to \infty).$$

Cette majoration est une conséquence directe du théorème plus général [HP16, Theorem 7.5] qui donne une telle majoration pour la valeur spéciale de la fonction L de toute variété abélienne A/K (en termes du degré du conducteur de A/K plutôt que de la hauteur de A/K). Malgré tout, les outils développés à la Section 3.1 permettent d'obtenir de façon élémentaire une version explicite de la Proposition 5.4.2 :

$$\frac{\log L^*\big(H_d/K, 1\big)}{\log H\big(H_d/K\big)} \leqslant c' \cdot \frac{\log\log(3d)}{\log(3d)} \quad (d \to \infty),$$

où $c' > 0$ est une constante explicite et absolue, que l'on peut choisir $\leqslant 45$. Il nous semble donc que la preuve ci-dessous a son intérêt.

Démonstration. D'après la Proposition 5.3.4, la quantité à étudier est

$$L^*\big(H_d/K,1\big) = \prod_{m\in\mathcal{Z}_q(3d)} u(m)\cdot \prod_{m\in\mathcal{V}_q^*(3d)} \left(1-\frac{\mathbf{t}_m(27)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m)}{q^{u(m)}}\right),$$

où les ensembles $\mathcal{Z}_q(3d)$ et $\mathcal{V}_q^*(3d)$ ont été définis à la Section 5.3.2. La Proposition 3.1.8 (avec $K=1$) implique immédiatement qu'il existe une constante absolue $C>0$ (qu'on peut prendre $\leqslant 5$) telle que

$$\log L^*\big(H_d/K,1\big) \leqslant 3C\cdot\log q\cdot\frac{3d\cdot\log\log(3d)}{\log(3d)}.$$

Ce qui donne ici, en rappelant que $H\big(H_d/K\big)=q^d$,

$$\frac{\log L^*\big(H_d/K,1\big)}{\log H\big(H_d/K\big)} \leqslant 3C\cdot\log q\cdot\frac{3d\cdot\log\log(3d)}{\log(3d)}\cdot\frac{1}{d\cdot\log q} \leqslant 9C\cdot\frac{\log\log(3d)}{\log(3d)} = o(1).$$

Ceci termine la preuve de la Proposition et de sa version plus fine mentionnée sous l'énoncé. □

5.4.3 Minoration de la valeur spéciale

Passons à présent à la preuve de la minoration de $L^*\big(H_d/K,1\big)$ dont on a besoin pour achever la preuve du Théorème 5.4.1. Nous utilisons les outils de la Section 3.2 et obtenons :

Proposition 5.4.3. *Soit $d\geqslant 2$ un entier premier à q. Pour $d\to\infty$, la valeur spéciale $L^*\big(H_d/K,1\big)$ de la fonction L associée à la courbe hessienne H_d/K admet la minoration suivante :*

$$\frac{\log L^*\big(H_d/K,1\big)}{\log H\big(H_d/K\big)} \geqslant 0+o(1) \qquad (d\to\infty).$$

Autrement dit, la valeur spéciale $L^*\big(H_d/K,1\big)$ est « asymptotiquement presque entière » au sens suivant : comme $L^*\big(H_d/K,1\big)$ est la valeur en $T=q^{-1}$ d'un polynôme $L^*(T)$ à coefficients entiers et que cette valeur est non nulle, il existe certainement des entiers $B_d\in\mathbb{N}^*$ et $w_d\in\mathbb{N}$ tels que

$$L^*\big(H_d/K,1\big) = \frac{B_d}{q^{w_d}}.$$

L'énoncé de la Proposition affirme alors que $w_d=o\big(d\big)$; en mots, l'exposant de q dans le dénominateur de $L^*\big(H_d/K,1\big)$ devient petit (devant d) lorsque d est grand. Rappelons également que nous avons donné des exemples de valeurs explicites de $d\in\mathbb{N}^*$ pour lesquels $L^*(H_d/K,1)$ est un entier (voir Section 5.3.3).

Démonstration. En premier lieu, remarquons que dans l'expression de $L^*\big(H_d/K,1\big)$ obtenue à la Proposition 5.3.4, le terme $\prod_{m\in\mathcal{Z}_q(3d)} u(m)$ est un entier positif. On peut donc écrire :

$$\begin{aligned}
\log L^*\big(H_d/K,1\big) &= \log \prod_{m\in\mathcal{Z}_q(3d)} u(m) + \log \prod_{m\in\mathcal{V}_q^*(3d)} \left(1-\frac{\mathbf{t}_m(27)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m)}{q^{u(m)}}\right)\\
&\geqslant \log 1 + \log \prod_{m\in\mathcal{V}_q^*(3d)} \left(1-\frac{\mathbf{t}_m(27)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m)}{q^{u(m)}}\right)\\
&\geqslant \log \prod_{m\in\mathcal{V}_q^*(3d)} \left(1-\frac{\mathbf{t}_m(27)\cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m)}{q^{u(m)}}\right). \qquad (5.10)
\end{aligned}$$

Pour minorer $\log L^*\big(H_d/K,1\big)$, il s'agit donc d'estimer le produit apparaissant dans (5.10) : à cette fin, nous utilisons les résultats de la Section 3.2. Pour toute orbite $m\in\mathcal{O}_q^{(3)}(3d)$, on pose à nouveau

$$\Omega(m) = \mathbf{t}_m(27)\cdot\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m).$$

On dispose d'un ensemble d'orbites $\mathcal{V}_q^*(3d)\subset\mathcal{O}_q^{(3)}(3d)$ telles que $\Omega(m)\neq q^{u(m)}$. Vérifions que cette donnée satisfait les hypothèses (i), (ii) et (iii) de la Section 3.2.1 :

(i) Pour toute orbite $m \in \mathcal{V}_q^*(3d)$, on a $\Omega(m) \in \mathbb{Q}(\zeta_{d'}) \subset \mathbb{Q}(\zeta_d)$, où $d' = d/\operatorname{pgcd}(d,m)$. C'est immédiat car le caractère $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ est d'ordre d'. Comme $m \neq 0, d, 2d$, on a $d' > 3$.

En outre, notons que $|\Omega(m)| = q^{u(m)}$ dans tout plongement complexe de $\mathbb{Q}(\zeta_{d'})$ (*cf.* Proposition 2.2.7).

(ii) Pour toute orbite $m \in \mathcal{V}_q^*(3d)$ et tout $a \in (\mathbb{Z}/d\mathbb{Z})^\times$, notant $\sigma_a \in \operatorname{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ l'automorphisme correspondant à a, on a

$$\sigma_a(\Omega(m)) = \Omega(a \cdot m).$$

C'est une conséquence directe de l'action galoisienne sur les sommes de Jacobi (Lemme 3.3.8).

(iii) Enfin, par construction de $\mathcal{V}_q^*(3d)$, le produit

$$\prod_{m \in \mathcal{V}_q^*(3d)} \left(1 - \frac{\Omega(m)}{q^{u(m)}}\right)$$

est rationnel strictement positif. En effet, la valeur spéciale $L^*\big(H_d/K, 1\big)$ est rationnelle et strictement positive et l'on a

$$\prod_{m \in \mathcal{V}_q^*(3d)} \left(1 - \frac{\Omega(m)}{q^{u(m)}}\right) = \frac{L^*\big(H_d/K, 1\big)}{\prod_{m \in \mathcal{Z}_q(3d)} u(m)}.$$

Nous sommes donc en mesure d'appliquer le Théorème 3.2.2. Avant d'en donner le résultat, rappelons quelques notations. Pour tout diviseur $d' > 3$ de $3d$, on note $K_{d'} = \mathbb{Q}(\zeta_{d'})$ le d'-ième corps cyclotomique et $\mathfrak{p}'$ l'idéal premier de $K_{d'}$ sous $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$. On identifiera encore $\operatorname{Gal}(K_{d'}/\mathbb{Q})$ à $(\mathbb{Z}/d'\mathbb{Z})^\times$ comme ci-dessus et l'on notera $G_{d'} = (\mathbb{Z}/d'\mathbb{Z})^\times$, $\langle p \rangle_{d'}$ et $\langle q \rangle_{d'}$ les sous-groupes de $G_{d'}$ engendrés respectivement par p et q. Définissons alors

$$w'(d') := o_q(d') \cdot \sum_{m' \in G_{d'}/\langle q \rangle_{d'}} \max\left\{0, 1 - \frac{\operatorname{ord}_{\mathfrak{p}'} \Omega\left(\frac{3d}{d'} m'\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\}.$$

Le Théorème 3.2.2 donne que

$$\log \prod_{m \in \mathcal{V}_q^*(3d)} \left(1 - \frac{\mathbf{t}_m(27) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m)}{q^{u(m)}}\right) \geqslant -\log q \cdot \sum_{\substack{d' \mid 3d \\ d' > 3}} w'(d'). \tag{5.11}$$

Il nous faut majorer les quantités $w'(d')$ pour tous les diviseurs $d' > 3$ de $3d$. Pour ce faire, il faut d'abord expliciter les valuations $\mathfrak{p}'$-adiques $\operatorname{ord}_{\mathfrak{p}'} \Omega\left(\frac{3d}{d'} m'\right)$. À cet effet, définissons une fonction en escaliers $F : [0,1] \to \mathbb{R}$ par

$$F(y) = \begin{cases} 2 & \text{si } y \in \left[0, \frac{1}{3}\right] \\ 1 & \text{si } y \in \left]\frac{1}{3}, \frac{2}{3}\right] \\ 0 & \text{si } y \in \left]\frac{2}{3}, 1\right]. \end{cases}$$

Lemme 5.4.4. *Pour tout diviseur $d' > 3$ de $3d$, la quantité $w'(d')$ s'écrit*

$$w'(d') = o_q(d') \cdot \sum_{m' \in G_{d'}/\langle q \rangle_{d'}} \max\left\{0, \int_0^1 F(t)\mathrm{d}t - \frac{1}{\#\langle p \rangle_{d'}} \sum_{\pi \in \langle p \rangle_{d'}} F\left(\left\{\frac{m'\pi}{d'}\right\}\right)\right\}.$$

Démonstration. Pour la durée de la preuve, on note $\theta = o_q(d') = \#\langle q \rangle_{d'}$ et $Q = q^\theta$. Pout tout $m' \in (\mathbb{Z}/d'\mathbb{Z})^\times/\langle q \rangle_{d'}$, on pose $m = 3dm'/d' \in \mathcal{O}_q^{(3)}(3d)$ et l'on a

$$\begin{aligned} \Omega\left(\tfrac{3d}{d'} m'\right) = \Omega(m) &= \mathbf{t}_m(27) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) \\ &= \mathbf{t}(27)^{(Q-1)m'/d'} \cdot \mathbf{j}_Q\left(\mathbf{t}^{(Q-1)m'/d'}, \mathbf{t}^{(Q-1)m'/d'}, \mathbf{t}^{(Q-1)m'/d'}\right), \end{aligned}$$

où $\mathbf{t}(27)^{(Q-1)m'/d'}$ est une racine de l'unité. En particulier, c'est une unité en $\mathfrak{p}'$. On utilise alors le calcul des valuations $\mathfrak{p}'$-adiques des sommes de Jacobi (Théorème 3.3.9 et Proposition 3.3.10) : le

nombre $\Omega\left(\frac{3d}{d'}m'\right)$ est, à une racine de l'unité près, la somme de Jacobi $\mathbf{J}_Q(m',m',m',-3m')$ dans les notations de la Section 3.3. On obtient :

$$\begin{aligned}\operatorname{ord}_{\mathfrak{p}'}\Omega\left(\tfrac{3d}{d'}m'\right) &= \operatorname{ord}_{\mathfrak{p}'}\mathbf{j}_Q\left(\mathbf{t}^{(Q-1)m'/d'},\mathbf{t}^{(Q-1)m'/d'},\mathbf{t}^{(Q-1)m'/d'}\right)\\ &= \frac{[\mathbb{F}_Q:\mathbb{F}_p]}{\#\langle p\rangle_{d'}}\cdot\sum_{\pi\in\langle p\rangle_{d'}}\left\lfloor\left\{\frac{-m'\pi}{d'}\right\}+\left\{\frac{-m'\pi}{d'}\right\}+\left\{\frac{-m'\pi}{d'}\right\}\right\rfloor\\ &= \frac{[\mathbb{F}_Q:\mathbb{F}_p]}{\#\langle p\rangle_{d'}}\cdot\sum_{\pi\in\langle p\rangle_{d'}}\left\lfloor 3-3\left\{\frac{m'\pi}{d'}\right\}\right\rfloor.\end{aligned}$$

En effet, pour tout réel $y\notin\mathbb{Z}$, on a la relation : $\{-y\}=1-\{y\}$. Relation que l'on peut appliquer ici car, pour tout $\pi\in\langle p\rangle_{d'}$ et tout $m'\in(\mathbb{Z}/d'\mathbb{Z})^\times$, comme d' et p sont premiers entre eux, $m'\pi/d'$ n'est pas un entier. Observons à présent que, pour tout $y\in]0,1[$, on a

$$\lfloor 3-3\{y\}\rfloor=\begin{cases}2 & \text{si } y\in\left]0,\frac{1}{3}\right]\\ 1 & \text{si } y\in\left]\frac{1}{3},\frac{2}{3}\right]\\ 0 & \text{si } y\in\left]\frac{2}{3},1\right[\end{cases}=F(y).$$

On peut donc reformuler l'expression de $\operatorname{ord}_{\mathfrak{p}'}\Omega\left(\frac{3d}{d'}m'\right)$ à l'aide de la fonction $F:[0,1]\to\mathbb{R}$ définie avant l'énoncé du Lemme :

$$\operatorname{ord}_{\mathfrak{p}'}\Omega\left(\tfrac{3d}{d'}m'\right)=\frac{[\mathbb{F}_Q:\mathbb{F}_p]}{\#\langle p\rangle_{d'}}\cdot\sum_{\pi\in\langle p\rangle_{d'}}F\left(\left\{\tfrac{m'\pi}{d'}\right\}\right).$$

Par ailleurs, on a $\int_0^1F(t)\mathrm{d}t=1$. On en déduit immédiatement l'expression annoncée de $w'(d')$:

$$w'(d')=\theta\cdot\sum_{m'\in G_{d'}/\langle q\rangle_{d'}}\max\left\{0,\int_0^1F(t)\mathrm{d}t-\frac{1}{\#\langle p\rangle_{d'}}\sum_{\pi\in\langle p\rangle_{d'}}F\left(\left\{\tfrac{m'\pi}{d'}\right\}\right)\right\}.$$

□

Lemme 5.4.5. *Pour tout diviseur $d'>3$ de $3d$, on a*

$$\frac{w'(d')}{\phi(d')}\xrightarrow[d'\to\infty]{}0.$$

Démonstration. D'après l'expression de $w'(d')$ obtenue au Lemme ci-dessus, on a

$$0\leqslant\frac{w'(d')}{\phi(d')}\leqslant\frac{o_q(d')}{\phi(d')}\cdot\sum_{m'\in G_{d'}/\langle q\rangle_{d'}}\left|\int_0^1F(t)\mathrm{d}t-\frac{1}{\#\langle p\rangle_{d'}}\sum_{\pi\in\langle p\rangle_{d'}}F\left(\left\{\tfrac{m'\pi}{d'}\right\}\right)\right|$$

puisque $\max\{0,y\}\leqslant|y|$ pour tout $y\in\mathbb{R}$. De plus, remarquons que $\frac{o_q(d')}{\phi(d')}=\frac{\#\langle q\rangle_{d'}}{\#G_{d'}}=\frac{1}{\#(G_{d'}/\langle q\rangle_{d'})}$.

On peut alors employer les résultats d'équidistribution de la Section 3.4. D'après la Proposition 3.4.14 (corollaire du Théorème 3.4.1), lorsque $d'\to\infty$, on a

$$\frac{1}{\#(G_{d'}/\langle q\rangle_{d'})}\cdot\sum_{m'\in G_{d'}/\langle q\rangle_{d'}}\left|\int_0^1F(t)\mathrm{d}t-\frac{1}{\#\langle p\rangle_{d'}}\sum_{\pi\in\langle p\rangle_{d'}}F\left(\left\{\tfrac{m'\pi}{d'}\right\}\right)\right|=o(1).$$

La constante implicite ne dépendant que de q. Ceci termine la preuve du fait que $w'(d')/\phi(d')\to0$. □

On peut alors finaliser la démonstration de la Proposition 5.4.3. Rappelons que la hauteur de H_d/K vaut $H\big(H_d/K\big)=q^d$ (Proposition 5.1.5) et donc, en combinant (5.10) et (5.11), on obtient

$$\frac{\log L^*\big(H_d/K\big)}{\log H\big(H_d/K\big)}\geqslant-\frac{1}{d}\cdot\sum_{\substack{d'\mid3d\\d'>3}}w'(d')=-3\cdot\frac{1}{3d}\cdot\sum_{\substack{d'\mid3d\\d'>3}}w'(d').$$

Or, on vient de montrer que $w'(d')=o\big(\phi(d')\big)$ pour tout diviseur $d'>3$ de $3d$. Il en découle immédiatement (Lemme 3.4.16) que

$$\frac{1}{3d}\cdot\sum_{\substack{d'\mid3d\\d'>3}}w'(d')\xrightarrow[d\to\infty]{}0.$$

D'où finalement

$$\frac{\log L^*\big(H_d/K\big)}{\log H\big(H_d/K\big)} \geqslant o(1).$$

Ce qu'il fallait démontrer. □

6

Courbes elliptiques munies d'un point de 4-torsion

Soit $K = \mathbb{F}_q(t)$ le corps des fractions rationnelles sur un corps fini $\mathbb{F}_q$ de caractéristique $p \geqslant 3$. Ce chapitre est dédié à l'étude des courbes elliptiques suivantes : pour tout entier $d \in \mathbb{N}^*$ premier à p, on considère la courbe elliptique E_d/K, dont un modèle de Weierstrass affine est :

$$E_d : \quad Y^2 + XY + t^d Y = X^3 + t^d X^2.$$

Pour tout entier d premier à q, la courbe E_d/K est munie d'un point K-rationnel de 4-torsion. Ceci fait écho aux Chapitres 4 et 5 où l'on a étudié des courbes elliptiques munies de points de 2-torsion et d'un point de 3-torsion (respectivement). La courbe E_d est étudiée dans [Ulm13, §7-§8] et [Ulm11, Lecture 5, §3] pour illustrer les résultats de [Ber08]. De plus, D. Ulmer a construit (pour certaines valeurs de d) des points explicites sur E_d (voir [Ulm13, Theorem 8.1] et [Ulm11, Lecture 5, Theorem 4.1]) et montré que le rang de E_d peut être « grand ».

Concernant les courbes E_d/K ci-dessus, nous démontrons (entre autres) les résultats suivants :

Théorème. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \geqslant 2$ premier à p, on considère la courbe elliptique E_d définie sur K par le modèle de Weierstrass suivant, donné en coordonnées affines,*

$$E_d : \qquad Y^2 + XY + t^d Y = X^3 + t^d X^2.$$

La hauteur différentielle de E_d vaut $H\big(E_d/\mathbb{F}_q(t)\big) = q^{\lfloor \frac{d+1}{2} \rfloor + 1}$. Les conjectures de Birch et Swinnerton-Dyer sont vraies pour la courbe E_d/K. En particulier, le groupe de Tate-Shafarevich $Ш(E_d/K)$ est fini et le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ a, inconditionnellement, un sens.

De plus, lorsque $H(E_d/K) \to +\infty$ (c'est-à-dire lorsque $d \to \infty$), on a

$$\mathfrak{Bs}(E_d/K) \xrightarrow[\substack{\mathrm{pgcd}(d,q)=1 \\ d\to\infty}]{} 1.$$

Ou, de façon équivalente,

$$\log\left(\#Ш(E_d/K) \cdot \mathrm{Reg}(E_d/K)\right) \sim \log H(E_d/K) \sim \frac{d}{2} \log q \quad (d \to \infty).$$

Nous entamons ce chapitre par le calcul des invariants classiques associés à E_d : invariant j, discriminant minimal, conducteur et hauteur (Proposition 6.1.6). En passant, nous faisons une étude détaillée de la réduction de E_d en les places de K (Proposition 6.1.5). Ce qui nous permet d'étudier en détail le sous-groupe de torsion $E_d(K)_{\mathrm{tors}}$ (Proposition 6.1.7) et d'encadrer le nombre de Tamagawa $\mathcal{T}am(E_d/K)$ (Proposition 6.1.8). La seconde section est consacrée au calcul de la fonction L de E_d (Théorème 6.2.1) : nous utilisons une méthode « élémentaire » à base de sommes de caractères avec les notations et résultats du Chapitre 2. Ce calcul n'avait, à notre connaissance, pas été effectué (bien qu'il ressemble beaucoup à celui de [CHU14, §3.2]). Nous expliquons ensuite pourquoi la courbe E_d satisfait à la conjecture de Birch et Swinnerton-Dyer (Théorème 6.2.1). Ceci donne un sens à l'étude du ratio de Brauer-Siegel. Des calculs précédents, nous déduisons à la troisième section une expression

pour le rang de $E_d(K)$ (Proposition 6.3.2) et nous décomposons la valeur spéciale $L^*(E_d/K,1)$ en un produit de nombres algébriques explicites (Proposition 6.3.3). C'est à la quatrième et dernière section que nous prouvons le résultat principal du chapitre : le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ tend vers 1 lorsque $d \to \infty$. Vue la relation entre $\mathfrak{Bs}(E_d/K)$ et $L^*(E_d/K,1)$, il s'agit d'encadrer la taille de la valeur spéciale $L^*(E_d/K,1)$.

6.1 Les courbes E_d

6.1.1 Modèles, propriétés

Suivons à nouveau [Hus04, Chap. 4, §4]. Soit E une courbe elliptique sur $K=\mathbb{F}_q(t)$ avec un point rationnel P (en sus du point à l'infini $\mathcal{O}$). Quitte à effectuer un changement de coordonnées, on peut supposer que $P=(0,0)$ et que la tangente en P à E est horizontale (voir Section 5.1.1). Le modèle de Weierstrass (affine) de E est alors de la forme

$$E: \quad y^2+a_1xy+a_3y=x^3+a_2x^2,$$

avec $a_i \in K$. Si l'on suppose que P n'est ni d'ordre 2 ni d'ordre 3, on peut effectuer un changement de coordonnées supplémentaires pour assurer que $a_3=a_2\neq 0$: on pose $b=-a_2$ et $c=1-a_1$. Le modèle de Weierstrass est alors sous « forme normale de Tate » :

$$E: \quad y^2+(1-c)xy-by=x^3-bx^2,$$

avec $(b,c)\in K^\times\times K$. La *forme normale de Tate*, pour $b,c\in K$ donne une description en termes de modèles de Weierstrass des paires (E,P) formées d'une courbe elliptique E et d'un point rationnel P sur E tel que $P,2P,3P\neq\mathcal{O}$. Si $P=(0,0)$, il est facile de voir que $2P=(b,bc)$ et $-2P=(b,0)$. Ainsi, $P=(0,0)$ est de 4-torsion si et seulement si $2P=-2P$, ce qui équivaut à imposer $c=0$. La forme normale de Tate du modèle de E est alors

$$y^2+xy-by=x^3-bx^2$$

et le discriminant de ce modèle vaut $\Delta=b^4(1+16b)$ (voir [SS10, §7.10]). Nous avons ici construit une courbe E/K canoniquement munie d'un point rationnel d'ordre (exactement) 4.

Dans ce chapitre, nous étudions le cas où le paramètre $b\in K=\mathbb{F}_q(t)$ est de la forme $b=t^d$, avec $d\in\mathbb{N}^*$ un entier premier à q.

Définition 6.1.1. Soit $\mathbb{F}_q$ un corps fini de caractéristique $p\geqslant 3$ et $K=\mathbb{F}_q(t)$. Pour tout entier $n\in\mathbb{N}^*$, on considère la courbe elliptique E_d définie sur K par le modèle affine :

$$E_d: \quad Y^2+XY+t^dY=X^3+t^dX^2. \tag{6.1}$$

Remarque 6.1.2. On pourrait, avec les méthodes développées dans ce chapitre, traiter le cas où le paramètre b est de la forme $b=a\cdot t^d$ ($a\in\mathbb{F}_q^\times$). Notons $E_{d,a}$ la courbe elliptique définie sur $K=\mathbb{F}_q(t)$ par le modèle affine :

$$E_{d,a}: \quad Y^2+XY+at^dY=X^3+at^dX^2.$$

Il n'est pas très difficile de voir que les courbes $E_{d,a}$ et $E_{d,1}=E_d$ sont isomorphes sur $\overline{\mathbb{F}_q}(t)$.

Soit $d\geqslant 2$ un entier premier à q et $K=\mathbb{F}_q(t)$. On note E_d la courbe elliptique donnée par (6.1) sur K et E'_d la courbe elliptique de Legendre donnée par (4.1), définie elle aussi sur K (*cf.* Chapitre 4). Alors

Lemme 6.1.3 (Ulmer)**.** *Les courbes E_d et E'_d sont 2-isogènes sur $\overline{\mathbb{F}_q}(t)$.*

Démonstration. Nous renvoyons à [Ulm14a, Lemma 11.1] pour le détail de la preuve. Notons toutefois que E_d et E'_d ne sont pas nécessairement 2-isogènes sur $\mathbb{F}_q(t)$. De fait, si k désigne la plus petite extension de $\mathbb{F}_q$ contenant les racines d-ièmes de $1/16$, alors E_d et E'_d sont isogènes sur $k(t)$. Or, le degré de l'extension $k/\mathbb{F}_q$ tend vers $+\infty$ lorsque $d\to\infty$. Rappelons que nous travaillons sur $K=\mathbb{F}_q(t)$ fixé. □

Remarque 6.1.4. L'existence de cette isogénie entre E_d et la courbe de Legendre E'_d est peut-être suffisante pour déduire des résultats du Chapitre 4 ceux du présent chapitre. En particulier, nous allons montrer que les racines (inverses) de leurs fonctions L ne diffèrent que par des racines de l'unité. Pour l'instant, nous ne voyons pas clairement comment expliciter ce lien entre les fonctions L et ne pouvons que le constater *a posteriori* (*cf.* Théorèmes 4.2.1 et 6.2.1).

6.1.2 Analyse de la mauvaise réduction

Soit $d \in \mathbb{N}^*$ un entier premier à q. Nous considérons la courbe E_d définie sur $K = \mathbb{F}_q(t)$ comme ci-dessus. D'après le formulaire de la Section 1.1.2, le discriminant du modèle (6.1) vaut

$$\Delta = t^{4d}(16t^d - 1)$$

et les places de mauvaise réduction de la courbe $E_d/\mathbb{F}_q(t)$ sont celles qui divisent Δ. Par conséquent, la courbe E_d a mauvaise réduction en $v = 0$, $v = \infty$ et en les places $v = \zeta$ où $\zeta \in \overline{\mathbb{F}_q}$ vérifie $\zeta^d = 16^{-1}$. De plus, un calcul rapide montre que l'invariant « c_4 » s'écrit $16t^{2d} - 16t^d + 1$ et donc que

$$j(E_d/K) = -\frac{(16t^{2d} - 16t^d + 1)^3}{t^{4d}(16t^d - 1)} \in \mathbb{F}_q(t).$$

Cette fraction rationnelle en t est de degré $d > 0$ en t. Ceci assure que la courbe $E_d/\mathbb{F}_q(t)$ n'est pas isotriviale (puisque $j(E_d/K) \notin \overline{\mathbb{F}_q}$). D'autre part, il est clair que $j(E_d/K)$ n'est pas un élément de K^p, *i.e.* l'application rationnelle $j : \mathbb{P}^1 \to \mathbb{P}^1$ correspondant à $j(E_d/K)$ est séparable. Nous pouvons dès à présent donner plus d'informations sur la mauvaise réduction de E_d.

Proposition 6.1.5. *Soit d un entier premier à q, on note $\pi : \mathcal{E}_d \to \mathbb{P}^1$ le modèle régulier minimal de la courbe E_d/K. Le morphisme π a $d+2$ fibres singulières comme suit :*

- *La fibre au-dessus de $t = 0$ a $4d$ composantes irréductibles arrangées en une configuration $\mathbf{I}_{4d}$ déployée,*
- *La fibre au-dessus de $t = \zeta$ (où $\zeta \in \overline{\mathbb{F}_q}$ vérifie $\zeta^d = 16^{-1}$) est irréductible singulière (de type $\mathbf{I}_1$),*
- *Le type de la fibre au-dessus de $t = \infty$ dépend de la parité de d :*
  - *si d est pair, elle est formée de d composantes irréductibles arrangées en une configuration $\mathbf{I}_d$ déployée.*
  - *si d est impair, elle est formée de $d+6$ composantes irréductibles arrangées en une configuration $\mathbf{I}_d^*$.*

Démonstration. Les points $t \in \mathbb{P}^1$ au-dessus desquels la fibre de π est singulière correspondent aux places v de K qui divisent le discriminant d'un modèle de E_d. Comme annoncé, il n'y a que les points 0, ∞ et ζ (où $\zeta \in \overline{\mathbb{F}_q}$ parcourt les racines d-ièmes de 16^{-1}). On applique l'algorithme de Tate en chacune de ces places (*cf.* [Sil94, Chap. IV, §9] ou [Tat75] par exemple).

- En $v = 0$, on constate que $\mathrm{ord}_{v=0}\,\Delta = 4d$ et que $\mathrm{ord}_{v=0}\,j(E_d) = -4d$, ce qui est caractéristique d'une réduction de type $\mathbf{I}_{4d}$: l'algorithme de Tate s'arrête à l'étape 1. Il est par ailleurs aisé de constater que la réduction de E_d en 0 est déployée.
- Soit $\zeta \in \overline{\mathbb{F}_q}$ tel que $\zeta^d = 1/16$. En $v = \zeta$, on a $\mathrm{ord}_{v=\zeta}\,\Delta = 1$ et $\mathrm{ord}_{v=\zeta}\,j(E_d) = -1$. La réduction de E_d est donc de type $\mathbf{I}_1$: le morphisme $\pi : \mathcal{E}_d \to \mathbb{P}^1$ a, au-dessus de $t = \zeta \in \mathbb{P}^1$, une fibre singulière irréductible.
- En $v = \infty$, on commence par effectuer le changement de carte $t = 1/u$ sur $\mathbb{P}^1$: après élimination des dénominateurs, le modèle (6.1) devient

$$Y^2 + u^d XY + u^{2d}Y = X^3 + u^d X^2, \tag{6.2}$$

  le discriminant de ce modèle vaut $\Delta = u^{7d}(u^d - 16)$ et l'invariant j de la courbe E_d s'exprime en fonction de u comme $j(E_d) = \frac{(u^{2d}-16u^d+16)^3}{u^d(u^d-16)}$. On a $\mathrm{ord}_{u=0}\,j(E_d) = -d$. On distingue alors deux cas suivant la parité de d :
  - Si d est pair, on pose $c = d/2$. Le changement de variables $(x, y) = (u^{-2c}X, u^{-3c}Y)$ transforme le modèle (6.2) en
$$y^2 + u^{d/2}xy + u^{d/2}y = x^3 + x^2$$
dont le discriminant est $\Delta' = u^d(u^d - 16)$. On a $\mathrm{ord}_{u=0}\,\Delta' = d$. La réduction de E_d en $u = 0$ est donc de type $\mathbf{I}_d$. Une fois réduite modulo u, l'équation ci-dessus s'écrit : $y^2 = x^3 + x^2 = x^2(x+1)$. La tangente à cette courbe en le point singulier $(x, y) = (0, 0)$ est à coefficients $\mathbb{F}_q$-rationnels. La réduction est donc déployée.
  - Si d est impair, on pose $c = (d-1)/2$. Le changement de variables $(x, y) = (u^{-2c}X, u^{-3c}Y)$ transforme le modèle (6.2) en
$$y^2 + u^{(d+1)/2}xy + u^{(d+3)/2}y = x^3 + ux^2$$
dont le discriminant est $\Delta' = u^{d+6}(u^d - 16)$. On a $\mathrm{ord}_{u=0}\,\Delta' = d + 6$. Et la réduction de E_d en $u = 0$ est donc de type $\mathbf{I}_d^*$. Il reste à calculer le nombre de Tamagawa local $c_\infty(E_d/K)$: une « sous-procédure » de l'algorithme de Tate permet de le faire. On trouve que $c_\infty(E_d/K) = 4$.

Ceci termine l'analyse des fibres singulières de $\pi : \mathcal{E}_d \to \mathbb{P}^1$. □

On peut résumer la Proposition précédente à l'aide d'un tableau contenant, pour toute place v de mauvaise réduction pour E_d/K, la contribution $\operatorname{ord}_v \Delta_{\min}(E_d/K)$ de v au discriminant minimal, la contribution $\operatorname{ord}_v \mathcal{N}(E_d/K)$ de v au conducteur de E_d et le nombre de Tamagawa local $c_v(E_d/K)$.

Place	Type de réduction	$\operatorname{ord}_v \Delta_{\min}(E_d/K)$	$\operatorname{ord}_v \mathcal{N}(E_d/K)$	$c_v(E_d/K)$
$v = 0$	$\mathbf{I}_{4d}$ déployée	$4d$	1	$4d$
$v = \zeta$ ($\zeta^d = 16^{-1}$)	$\mathbf{I}_1$	1	1	1
$v = \infty$	$\mathbf{I}_d$ déployée si d pair	d	1	d
	$\mathbf{I}_d^*$ si d impair	$d+6$	2	4

6.1.3 Calcul des invariants

L'analyse menée au paragraphe précédent (Proposition 6.1.5) permet d'exprimer les invariants de E_d/K en termes du paramètre entier $d \in \mathbb{N}^*$. On obtient

Proposition 6.1.6. *Soit $d \geqslant 2$ un entier premier à q, $K = \mathbb{F}_q(t)$ et E_d/K la courbe elliptique donnée par le modèle de Weierstrass affine* (6.1)*. Alors sa hauteur différentielle (exponentielle) vaut*

$$H\big(E_d/K\big) = q^{\lceil \frac{d}{2} \rceil} = q^{\lfloor \frac{d+1}{2} \rfloor + 1}.$$

De plus, on a

$$\deg \mathcal{N}\big(E_d/K\big) = \begin{cases} d+2 & \text{si } d \text{ est pair} \\ d+3 & \text{si } d \text{ est impair.} \end{cases}$$

Démonstration. Il suffit de reprendre les informations compilées dans le tableau ci-avant. Pour toute place v de $K = \mathbb{F}_q(t)$, on note $d_v = [\mathbb{F}_v : \mathbb{F}_q]$ le degré de v. On a alors

$$\begin{aligned} \deg \Delta_{\min}\big(E_d/K\big) &= \operatorname{ord}_{v=0} \Delta_{\min} \cdot d_0 + \sum_{\substack{\zeta \in \overline{\mathbb{F}_q} \text{tq.} \\ \zeta^d = 16^{-1}}} \operatorname{ord}_{v=\zeta} \Delta_{\min} \cdot d_\zeta + \operatorname{ord}_{v=\infty} \Delta_{\min} \cdot d_\infty \\ &= 4d \cdot 1 + \sum_{\substack{\zeta \in \overline{\mathbb{F}_q} \text{tq.} \\ \zeta^d = 16^{-1}}} \operatorname{ord}_{v=\zeta} 1 \cdot d_\zeta + \operatorname{ord}_{v=\infty} \Delta_{\min} \cdot 1 \\ &= 4d + d + \operatorname{ord}_{v=\infty} \Delta_{\min}. \end{aligned}$$

En effet, $\sum_{\zeta^d = 16^{-1}} d_\zeta = \deg(X^d - 16^{-1}) = d$. Il suit que

$$\deg \Delta_{\min}\big(E_d/K\big) = 4d + d + \begin{cases} d & \text{si } d \text{ est pair} \\ d+6 & \text{si } d \text{ est impair} \end{cases} = \begin{cases} 6d & \text{si } d \text{ est pair} \\ 6(d+1) & \text{si } d \text{ est impair.} \end{cases}$$

Par définition, on a $H(E_d/K) = q^{(\deg \Delta_{\min}(E_d/K))/12}$ et un calcul rapide montre que l'expression annoncée dans la Proposition est juste. Un raisonnement très similaire donne $\deg \mathcal{N}\big(E_d/K\big)$. □

D'après la formule de Grothendieck-Ogg-Raynaud (*cf.* Théorème 1.3.11), puisque E_d/K n'est pas isotriviale, on déduit de $\deg \mathcal{N}\big(E_d/K\big)$ le degré de la fonction L de E_d en tant que polynôme de $\mathbb{Z}[T]$:

$$\deg L\big(E_d/K, T\big) = \deg \mathcal{N}\big(E_d/K\big) + 4g(\mathbb{P}^1) - 4 = \begin{cases} d-2 & \text{si } d \text{ est pair} \\ d-1 & \text{si } d \text{ est impair.} \end{cases}$$

6.1.4 Torsion et nombre de Tamagawa

Proposition 6.1.7 (Ulmer). *Pour tout entier d premier à p, le sous-groupe de torsion de $E_d(K)$ est comme suit :*

$$E_d(K) = E_d\big(\overline{\mathbb{F}_q}(t)\big)_{\mathrm{tors}} \simeq \mathbb{Z}/4\mathbb{Z}.$$

Nous invitons le lecteur à consulter [Ulm13, Theorem 8.1] pour la preuve (qui est similaire à celle des Propositions 4.1.6 et 5.1.6).

On peut également donner un bon encadrement du nombre de Tamagawa de E_d et retrouver le Théorème 1.5.4 (voir également [HP16, Theorem 6.5]) dans le cas particulier des courbes elliptiques E_d/K. Plus précisément :

Proposition 6.1.8. *Soit $d \geqslant 2$ un entier premier à q et E_d la courbe définie sur $K = \mathbb{F}_q(t)$ par le modèle* (6.1)*. On a*

$$16d \leqslant \mathcal{T}am\big(E_d/\mathbb{F}_q(t)\big) \leqslant (4d)^2.$$

En particulier, il existe des constantes ne dépendant que de q telles que

$$\frac{\log d}{d} \ll_q \frac{\log \mathcal{T}am(E_d/K)}{\log H(E_d/K)} \ll_q \frac{\log d}{d}.$$

Démonstration. À l'aide de la Proposition 6.1.5, on peut écrire que

$$\mathcal{T}am(E_d/K) = \prod_{v|\Delta_{\min}(E_d/K)} c_v(E_d/K) = c_0(E_d/K)\cdot 1 \cdot c_\infty(E_d/K) = 4d\cdot c_\infty(E_d/K),$$

où $c_\infty(E_d/K)$ vaut d si d est pair et vaut 4 si d est impair (voir le tableau sous la Proposition 6.1.5). Puisque $H(E_d/K) = q^{\lfloor \frac{d+1}{2} \rfloor + 1}$, l'encadrement annoncé est obtenu facilement. □

6.2 Fonction L des courbes E_d

Dans cette section, nous détaillons le calcul de la fonction L de la courbe $E_d/\mathbb{F}_q(t)$ pour tout entier $d \geqslant 2$ premier à q. Donnons le résultat de ce calcul sous la forme d'un Théorème après avoir rappelé quelques notations de la Section 2.1.3. On fixe un idéal premier $\overline{\mathfrak{P}}$ de $\overline{\mathbb{Z}}$ au-dessus de p et l'on note $\mathbf{t} : \overline{\mathbb{F}_q}^\times \to \overline{\mathbb{Q}}^\times$ le caractère de Teichmüller associé. En outre, pour tout entier $d \geqslant 2$ premier à q, nous avons défini une famille de caractères $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ $(m \in [\![1, d-1]\!])$ dont l'ordre divise d. Nous obtenons

Théorème 6.2.1. *Soit $d \geqslant 2$ un entier premier à q. La fonction L de la courbe elliptique E_d sur $K = \mathbb{F}_q(t)$, dont un modèle affine est*

$$Y^2 + XY + t^d Y = X^3 + t^d X^2$$

s'écrit sous la forme d'un produit :

$$L(E_d/\mathbb{F}_q(t), T) = \prod_{m \in \mathcal{O}_q^{(2)}(d)} \left(1 - \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 \cdot T^{u(m)}\right) \in \mathbb{Z}[T],$$

où, $\mathcal{O}_q^{(2)}(d)$ désigne l'ensemble d'orbites

$$\mathcal{O}_q^{(2)}(d) = \begin{cases} \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/2\}\big)/\langle q \bmod d\rangle & \text{si } d \text{ est pair,} \\ \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\big)/\langle q \bmod d\rangle & \text{si } d \text{ est impair,} \end{cases}$$

l'entier $u(m)$ est le cardinal de l'orbite $m \in \mathcal{O}_q^{(2)}(d)$ et $\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)$ est une somme de Jacobi.

Pour la démonstration, nous utilisons des sommes de caractères. La preuve se déroule en trois parties : nous commençons par expliciter les termes de la série génératrice définissant $L(E_d/K, T)$ sous la forme de sommes de caractères, le deuxième temps consiste à relier ces sommes à des sommes de Jacobi, enfin, dans la dernière étape, nous utilisons la technique de « réindexation des caractères » pour conclure. Le coeur de la preuve est la Proposition 6.2.3 où nous écrivons les sommes qui apparaissent naturellement sous la forme de sommes de Jacobi.

Le reste de la section est consacrée à la preuve du Théorème 6.2.1. Insistons sur le fait que la seule hypothèse sur l'entier $d \geqslant 2$ paramétrant la famille $\{E_d\}_{d\in\mathbb{N}^*}$ est que d soit premier à q. On ne suppose pas, en particulier, que d divise $q-1$.

Remarque 6.2.2. À nouveau, l'apparition de sommes de Jacobi dans la fonction L de la courbe E_d s'explique par voie « cohomologique ». En effet, notons C_d la courbe hyperelliptique définie sur $\mathbb{F}_q$ par l'équation affine $y^2+y=x^d$ et $S_d=C_d\times C_d$. Nous avons explicité la fonction zeta de $C_d/\mathbb{F}_q$ à la Section 2.3.1 : celle-ci fait intervenir des sommes de Jacobi. De plus, il y a une action antidiagonale de μ_d sur $C_d\times C_d$. Notons par ailleurs $\pi:\mathcal{E}_d\to\mathbb{P}^1$ le modèle régulier minimal de E_d/K. Alors, [Ulm13, §6.2] montre qu'il existe une application rationnelle dominante

$$(C_d\times C_d)/\mu_d \dashrightarrow \mathcal{E}_d.$$

Celle-ci permet d'expliciter le groupe de cohomologie étale $\mathrm{H}^2_{\text{ét}}(\mathcal{E}_d,\mathbb{Q}_\ell)$ en fonction de $\mathrm{H}^1_{\text{ét}}(C_d,\mathbb{Q}_\ell)$. En particulier, la fonction L de E_d peut s'exprimer à l'aide (de facteurs) du numérateur de la fonction zeta $Z(C_d/\mathbb{F}_q,T)$. Une analyse plus fine de $(C_d\times C_d)/\mu_d \dashrightarrow \mathcal{E}_d$, inspirée par exemple de [Occ12, §3], devrait permettre de retrouver le Théorème 6.2.1 par des moyens « géométriques ».

6.2.1 Comptage de points

Dans tout ce paragraphe, on fixe un entier $d\geqslant 2$ premier à q et on note E_d/K la courbe elliptique donnée par (6.1). Soit $n\geqslant 1$ et $\mathbb{F}_Q=\mathbb{F}_{q^n}$ l'extension de degré n de $\mathbb{F}_q$. Pour tout $\tau\in\mathbb{P}^1(\mathbb{F}_Q)$, on pose

$$A(\tau,Q)=Q+1-\#\overline{(E_d)}_\tau(\mathbb{F}_Q),$$

où $\overline{(E_d)}_\tau$ désigne la réduction en la place v de K correspondant à τ d'un modèle minimal entier de E_d en v (la courbe $\overline{(E_d)}_\tau$ est donc définie sur le corps résiduel $\mathbb{F}_v\subset\mathbb{F}_Q$). Comme on l'a vu à la Section 6.1.2, le modèle de Weierstrass affine (6.1) de E_d, donné par $Y^2+XY+t^dY+X^3+t^dX^2$, est minimal et entier en toutes les places v de K, sauf en ∞. Celui-ci peut aussi se mettre sous la forme « courte » :

$$y^2=x^3+(4t^d+1)x^2+8t^dx+16t^{2d} \tag{6.3}$$

après le changement de variables $(x,y)=(4X,8Y+4X+4t^d)$. Le discriminant de ce nouveau modèle de E_d ne diffère de celui de (6.1) que par une puissance de 2 (2^{12} pour être exact). Mais 2 est une unité dans tous les corps résiduels $\mathbb{F}_v$ des places v de K. Par suite, le modèle (6.3) est minimal et entier en toute place $v\neq\infty$ de K. Nous pouvons donc utiliser ce dernier modèle (6.3) pour calculer les nombres $A(\tau,Q)$ lorsque $\tau\neq\infty$. On remarque par ailleurs que

$$\forall x\in\mathbb{F}_Q,\qquad x^3+(4t^d+1)x^2+8t^dx+16t^{2d}=(x+4t^d)(x^2+x+4t^d).$$

Dans la suite de ce paragraphe, on démontre

Proposition 6.2.3. *Pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$, on a*

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)}A(\tau,Q)=-\sum_{\chi\in Y(d,q)}\mathbf{j}_Q(\chi,\chi)^2,$$

où $Y(d,Q)$ est l'ensemble des caractères χ de $\mathbb{F}_Q^\times$ tels que $\chi\notin\{\mathbf{1},\mu\}$ et dont l'ordre divise d :

$$Y(d,Q)=\left\{\chi:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times \;\middle|\; \chi^d=\mathbf{1} \text{ et } \chi\neq\mathbf{1},\mu\right\}.$$

Démonstration. Par construction du modèle (6.3), pour tout point $\tau\in\mathbb{P}^1(\mathbb{F}_Q)\smallsetminus\{\infty\}$, on a

$$\begin{aligned}A(\tau,Q)&=Q+1-\#\overline{(E_d)}_\tau(\mathbb{F}_Q)\\&=Q+1-\left(1+\#\left\{(x,y)\in\mathbb{F}_Q^2 \;\middle|\; y^2=x^3+(4\tau^d+1)x^2+8\tau^dx+16\tau^{2d}\right\}\right)\\&=Q-\sum_{x\in\mathbb{F}_Q}\#\left\{y\in\mathbb{F}_Q \;\middle|\; y^2=x^3+(4\tau^d+1)x^2+8\tau^dx+16\tau^{2d}\right\}.\end{aligned}$$

Invoquons alors le Lemme 2.2.1 pour exprimer le nombre de solutions d'une équation quadratique en fonction du caractère « de Legendre » $\mu:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times$:

$$\begin{aligned}A(\tau,Q)&=Q-\sum_{x\in\mathbb{F}_Q}\left(1+\mu(x^3+(4\tau^d+1)x^2+8\tau^dx+16\tau^{2d})\right)\\&=-\sum_{x\in\mathbb{F}_Q}\mu(x^3+(4\tau^d+1)x^2+8\tau^dx+16\tau^{2d})\\&=-\sum_{x\in\mathbb{F}_Q}\mu\big((x+4\tau^d)(x^2+x+4\tau^d)\big).\end{aligned}$$

Lorsque l'on reporte cette identité dans la somme à calculer, en utilisant le Lemme 2.2.2, on obtient

$$\begin{aligned}\sum_{\tau\in\mathbb{F}_Q} A(\tau,Q) &= -\sum_{\tau\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\mu\big((x+4\tau^d)(x^2+x+4\tau^d)\big)\\ &= -\sum_{\chi^d=\mathbf{1}}\left(\sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z)\mu\big((x+4z)(x^2+x+4z)\big)\right).\end{aligned}$$

La somme extérieure portant sur tous les caractères de $\mathbb{F}_Q^\times$ dont l'ordre divise d (y compris le caractère trivial). Nous sommes ainsi conduits à considérer, pour tout caractère $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ (d'ordre quelconque pour le moment), la double somme :

$$T_Q(\chi) := \sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z)\mu\big((x+4z)(x^2+x+4z)\big)$$

qu'il s'agit d'écrire sous la forme (du carré) d'une somme de Jacobi. Commençons par traiter le cas où χ est le caractère trivial :

Lemme 6.2.4. *Si $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ est le caractère trivial, on a $T_Q(\mathbf{1}) = 0$.*

Démonstration. En permutant les deux sommes constituant $T_Q(\chi)$, on obtient que

$$T_Q(\mathbf{1}) = \sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\mu\big((x+4z)(x^2+x+4z)\big) = \sum_{x\in\mathbb{F}_Q}\sum_{z\in\mathbb{F}_Q}\mu\big(16z^2+4x(x+2)z+x^2(x+1)\big).$$

Pour chaque $x\in\mathbb{F}_Q$, on pose maintenant $q_x(Z) = 16Z^2+4x(x+2)Z+x^2(x+1)\in\mathbb{F}_Q[X]$. Le discriminant de cette forme quadratique vaut $\delta_x = 16x^4$. Ceci nous permet d'utiliser le Lemme 2.2.3 :

$$\sum_{z\in\mathbb{F}_Q}\mu(q_x(z)) = \begin{cases}-\mu(16) & \text{si } \delta_x\neq 0\\ (Q-1)\mu(16) & \text{si } \delta_x = 0\end{cases} = \begin{cases}-1 & \text{si } x\neq 0\\ Q-1 & \text{si } x=0.\end{cases}$$

En reportant dans $T_Q(\mathbf{1})$, on déduit le résultat souhaité :

$$T_Q(\mathbf{1}) = \sum_{x\in\mathbb{F}_Q}\left(\sum_{z\in\mathbb{F}_Q}\mu\big(q_x(z)\big)\right) = (Q-1)+\sum_{x\neq 0}(-1) = Q-1+(-1)(Q-1) = 0.$$

□

Supposons désormais que $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ est un caractère *non trivial*.

Lemme 6.2.5. *Soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère non trivial. On a $T_Q(\chi) = \mathbf{j}_q(\chi,\chi)^2$.*

Démonstration. D'après la définition de $T_Q(\chi)$, en posant « $z' = 4z$ », on a

$$\begin{aligned}T_Q(\chi) &= \sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z)\mu\big((x+4z)(x^2+x+4z)\big) = \sum_{z'\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z'/4)\mu\big((x+z')(x^2+x+z')\big)\\ &= \overline{\chi}(4)\cdot\sum_{z'\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z')\mu\big((x+z')(x^2+x+z')\big) = \overline{\chi}(4)\cdot\sum_{x\in\mathbb{F}_Q}\sum_{z'\in\mathbb{F}_Q}\chi(z')\mu\big((x+z')(x^2+x+z')\big).\end{aligned}$$

Séparons alors les termes avec $x=0$ des autres afin de faire un changement de variables « $z = xy$ » dans les sommes internes :

$$\begin{aligned}T_Q(\chi) &= \overline{\chi}(4)\cdot\left(\sum_{x\neq 0}\sum_{z'\in\mathbb{F}_Q}\chi(z')\mu\big((x+z')(x^2+x+z')\big)+\sum_{z\in\mathbb{F}_Q}\chi(z)\mu(z^2)\right)\\ &= \overline{\chi}(4)\cdot\sum_{x\neq 0}\sum_{z\in\mathbb{F}_Q}\chi(z)\mu\big((x+z)(x^2+x+z)\big)+\overline{\chi}(4)\cdot\sum_{z\neq 0}\chi(z)\\ &= \overline{\chi}(4)\cdot\sum_{x\neq 0}\sum_{y\in\mathbb{F}_Q}\chi(xy)\mu\big((x+xy)(x^2+x+xy)\big)+0\\ &= \overline{\chi}(4)\cdot\sum_{x\neq 0}\chi(x)\sum_{y\in\mathbb{F}_Q}\chi(y)\mu(x)^2\mu\big((1+y)(x+1+y)\big)\\ &= \overline{\chi}(4)\cdot\sum_{x\neq 0}\chi(x)\sum_{y\in\mathbb{F}_Q}\chi(y)\mu\big((1+y)(x+1+y)\big)\end{aligned}$$

car, x étant non nul, on a $\mu(x)^2 = 1$. De plus, χ étant non trivial, on a $\sum_{z\neq 0}\chi(z) = 0$. Effectuons alors une translation « $y' = y+1$ » sur la variable de sommation interne, comme $\chi(0) = 0$ et $\mu(0) = 0$, on obtient que

$$\begin{aligned} T_Q(\chi) &= \overline{\chi}(4)\cdot\sum_{x\neq 0}\chi(x)\sum_{y'\in\mathbb{F}_Q}\chi(y'-1)\mu\big(y'(x+y')\big) = \overline{\chi}(4)\cdot\sum_{x\in\mathbb{F}_Q}\chi(x)\sum_{y'\in\mathbb{F}_Q}\chi(y'-1)\mu\big(y'(x+y')\big)\\ &= \overline{\chi}(4)\cdot\sum_{y'\in\mathbb{F}_Q}\chi(y'-1)\mu(y')\left(\sum_{x\in\mathbb{F}_Q}\chi(x)\mu(x+y')\right)\\ &= \overline{\chi}(4)\cdot\sum_{y'\neq 0}\chi(y'-1)\mu(y')\left(\sum_{x\in\mathbb{F}_Q}\chi(x)\mu(x+y')\right). \end{aligned}$$

Mais, pour tout $y\in\mathbb{F}_Q^\times$, en posant successivement « $x' = y/x$ » et « $x'' = x'+1$ », on observe que

$$\begin{aligned} \sum_{x\in\mathbb{F}_Q}\chi(x)\mu(x+y) &= \sum_{x'\in\mathbb{F}_Q}\chi(yx')\mu(yx'+y) = \chi(y)\mu(y)\sum_{x'\in\mathbb{F}_Q}\chi(x')\mu(x'+1)\\ &= \chi(y)\mu(y)\sum_{x''\in\mathbb{F}_Q}\chi(x''-1)\mu(x'') = \chi(y)\mu(y)\chi(-1)\sum_{x''\in\mathbb{F}_Q}\chi(1-x'')\mu(x")\\ &= -\chi(-y)\mu(y)\cdot\mathbf{j}_Q(\chi,\mu) = -\chi(-y)\mu(y)\cdot\chi(4)\mathbf{j}_Q(\chi,\chi). \end{aligned}$$

Dans la dernière égalité, on a utilisé le Lemme 2.2.9 pour écrire que $\mathbf{j}_Q(\chi,\mu) = \chi(4)\mathbf{j}_Q(\chi,\chi)$. On a donc

$$\begin{aligned} T_Q(\chi) &= \overline{\chi}(4)\cdot\sum_{y'\neq 0}\chi(y'-1)\mu(y')\left(\sum_{x\in\mathbb{F}_Q}\chi(x)\mu(x+y')\right)\\ &= -\mathbf{j}_Q(\chi,\chi)\cdot\sum_{y'\neq 0}\chi(y'-1)\mu(y')^2\chi(-y') = -\mathbf{j}_Q(\chi,\chi)\cdot\sum_{y'\neq 0}\chi(y'-1)\chi(-1)\chi(y')\\ &= -\mathbf{j}_Q(\chi,\chi)\cdot\sum_{y'\neq 0}\chi(1-y')\chi(y') = \mathbf{j}_Q(\chi,\chi)\cdot\mathbf{j}_Q(\chi,\chi) = \mathbf{j}_Q(\chi,\chi)^2. \end{aligned}$$

Ce qui termine la preuve du Lemme. □

Notons en particulier que, lorsque $\chi = \mu$ est le caractère d'ordre 2, on a $T_Q(\mu) = \mathbf{j}_Q(\mu,\mu)^2 = 1$ (*cf.* Proposition 2.2.7). Jusqu'ici, nous avons montré que

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) = A(\infty,Q) - \sum_{\chi^d=\mathbf{1}} T_Q(\chi),$$

où l'on vient de calculer les quantités $T_Q(\chi)$. Définissons à présent $X(d,Q)$, l'ensemble des caractères non triviaux $\chi:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times$ dont l'ordre divise d. Alors la discussion précédente mène à

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) = A(\infty,Q) - \sum_{\chi\in X(d,Q)}\mathbf{j}_Q(\chi,\chi)^2.$$

On peut expliciter facilement le terme $A(\infty,Q)$: d'après la Proposition 6.1.5, la réduction de E_d en ∞ est multiplicative déployée (resp. additive) si d est pair (resp. si d est impair). D'où

$$A(\infty,Q) = \begin{cases} 1 & \text{si } d \text{ est pair}\\ 0 & \text{si } d \text{ est impair.}\end{cases}$$

Par ailleurs, comme dans l'énoncé de la Proposition, on pose

$$Y(d,Q) = \left\{\chi:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times \;\middle|\; \chi^d = \mathbf{1} \text{ et } \chi\neq\mathbf{1},\mu\right\}.$$

Pour conclure la preuve de la Proposition, distinguons deux cas :

- Si d est impair, on a $A(\infty,Q) = 0$ et $Y(d,Q) = X(d,Q)$ car $\mu\notin X(d,Q)$ (le caractère $\mu^d = \mu$ n'est pas trivial). On a donc fini la preuve dans ce cas.

– Si d est pair, on a $A(\infty, Q) = 1$ et, cette fois, $\mu \in X(d,Q)$ et $Y(d,Q) = X(d,Q) \smallsetminus \{\mu\}$. Par suite, en utilisant le fait que $T_Q(\mu) = \mathbf{j}_Q(\mu,\mu)^2 = 1 = A(\infty, Q)$, on a

$$\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_Q)} A(\tau, Q) = A(\infty, Q) - \sum_{\chi \in X(d,Q)} \mathbf{j}_Q(\chi,\chi)^2 = 1 - \mathbf{j}_Q(\mu,\mu)^2 - \sum_{\chi \in Y(d,Q)} \mathbf{j}_Q(\chi,\chi)^2$$
$$= 1 - 1 - \sum_{\chi \in Y(d,Q)} \mathbf{j}_Q(\chi,\chi)^2 = - \sum_{\chi \in Y(d,Q)} \mathbf{j}_Q(\chi,\chi)^2.$$

Ce qui termine la démonstration de l'identité recherchée.

□

6.2.2 Réindexation des caractères

Aux paragraphes précédents, nous avons explicité $\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau, q^n)$ pour toute extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. Or, le Lemme 1.3.15 donne l'expression suivante de la fonction L de $E_d/\mathbb{F}_q(t)$:

$$\log L\big(E_d/\mathbb{F}_q(t), T\big) = \sum_{n=1}^{\infty} \left(\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau, q^n) \right) \frac{T^n}{n}.$$

Utilisons alors les outils de la Section 2.1.4 pour terminer la démonstration du Théorème 6.2.1. Pour cela, pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$ et tout caractère non trivial $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$, on pose $\sigma(\chi, Q) = \mathbf{j}_Q(\chi,\chi)^2$. La preuve que cette donnée satisfait aux hypothèses de la Proposition 2.1.15 avec $K = 1$ et $\ell = 2$ est très similaire à la vérification effectuée à la Section 4.2.2, nous l'omettons donc : il s'agit de vérifier que $\sigma(\chi^q, Q) = \sigma(\chi, Q)$ et que $\sigma(\chi, Q)$ vérifie une relation de Hasse-Davenport à l'ordre 1 (Théorème 2.2.20). On déduit alors de la Proposition 2.1.15 que

$$\log L\big(E_d/\mathbb{F}_q(t), T\big) = \sum_{m \in \mathcal{O}_q^{(2)}(d)} \log\left(1 - \sigma(\mathbf{t}_m, q^{u(m)}) \cdot T^{u(m)}\right).$$

Et il ne reste qu'à écrire la définition de $\sigma(\mathbf{t}_m, q^{u(m)}) = \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2$ pour conclure la preuve du Théorème 6.2.1.

6.2.3 Conjecture de Birch et Swinnerton-Dyer

Dans cette section, nous expliquons pourquoi les courbes elliptiques E_d/K vérifient la conjecture de Birch et Swinnerton-Dyer. Pour cela, nous commençons par démontrer le Lemme ci-dessous.

Lemme 6.2.6. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et d un entier premier à q. On note à nouveau E_d la courbe elliptique définie sur $K = \mathbb{F}_q(t)$ par le modèle* (6.1)*. De plus, soit $X_d \subset \mathbb{P}^1 \times \mathbb{P}^1$ la courbe définie sur K par l'équation*

$$X_d : \quad x_0(x_0 - x_1)(y_1 - y_0)y_1 = t^d \cdot x_1^2 y_0^2$$

donnée dans les coordonées $([x_0 : x_1], [y_0 : y_1])$ sur $\mathbb{P}^1 \times \mathbb{P}^1$. Alors E_d est birationnelle à X_d (sur K).

Démonstration. Partons de l'équation de $X_d \subset \mathbb{P}^1 \times \mathbb{P}^1$ et posons $(X_1, Y_1) = \left(\frac{x_0}{x_1}, \frac{y_0}{y_1}\right)$. On obtient

$$X_1(X_1 - 1)(1 - Y_1) = t^d \cdot Y_1^2.$$

On pose alors $(X_2, Y_2) = (-t^d Y_1, t^d X_1(Y_1 - 1))$. Après multiplication par $(X_2 + t^d)^2$, ceci nous conduit à la relation

$$Y_2^2 + X_2 Y_2 + t^d Y_2 = X_2^3 + t^d X_2^2,$$

une équation affine de E_d. Autrement dit, l'application rationnelle $X_d \dashrightarrow E_d$ donnée par

$$([x_0 : x_1], [y_0 : y_1]) \in X_d \mapsto \left(-t^d \cdot \frac{y_0}{y_1}, t^d \cdot \frac{x_0}{x_1}\left(\frac{y_0}{y_1} - 1\right)\right) = (X_2, Y_2) \in E_d$$

est birationnelle. On pourra également consulter [Ulm13, §7.3]. □

Ce Lemme montre que E_d est birationnelle à une courbe affine de la forme

$$X'_d : \quad f(x) - t^d g(y) = 0,$$

où $f, g : \mathbb{P}^1 \to \mathbb{P}^1$ sont les applications rationnelles données par $f(x) = x(x-1)$ et $g(y) = y^2/(1-y)$ (pour tous $x, y \in \mathbb{P}^1$). Nous sommes donc en mesure d'appliquer le théorème de Berger (Théorème 1.4.17).

Théorème 6.2.7 (Berger)**.** *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. Pour tout entier $d \geqslant 2$ premier à q, la courbe E_d définie sur $K = \mathbb{F}_q(t)$, dont un modèle affine est*

$$E_d : \quad Y^2 + XY + t^d Y = X^3 + t^d X^2$$

vérifie les conjectures de Birch et Swinnerton-Dyer. En particulier, son groupe de Tate-Shafarevich $Ш(E_d/K)$ est fini et son ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ a un sens.

Nous renvoyons la lectrice à [Ber08, Theorem 2.3], [Ulm13, §1-§8] et [Ulm11, Lecture 5, §3] pour plus de détails sur la démonstration.

6.3 Rang et valeur spéciale de E_d

En combinant l'expression explicite de la fonction L de E_d/K (Théorème 6.2.1) avec le fait que E_d vérifie la conjecture de Birch et Swinnerton-Dyer (Théorème 6.2.7), il est dorénavant possible d'obtenir une expression « combinatoire » du rang de $E_d(K)$ d'une part et une formule fermée pour la valeur spéciale $L^*(E_d/K, 1)$ d'autre part.

6.3.1 Expressions du rang et de la valeur spéciale

Soit $d \geqslant 2$ un entier premier à q. On a écrit au Théorème 6.2.1 la fonction L de la courbe E_d comme un produit :

$$L(E_d/\mathbb{F}_q(t), T) = \prod_{m \in \mathcal{O}_q^{(2)}(d)} (1 - \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 \cdot T^{u(m)}) \in \mathbb{Z}[T].$$

Ce produit porte sur un ensemble d'orbites $\mathcal{O}_q^{(2)}(d) \subset \mathcal{O}'_q(d)$ de la multiplication par q sur $\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$:

$$\mathcal{O}_q^{(2)}(d) = \begin{cases} \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/2\}\big)/\langle q \bmod d\rangle & \text{si } d \text{ est pair,} \\ \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\big)/\langle q \bmod d\rangle & \text{si } d \text{ est impair.} \end{cases}$$

De plus, pour tout $m \in \mathcal{O}_q^{(2)}(d)$, on a $|\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2| = q^{u(m)}$ (*cf.* (2.1) sous la Proposition 2.2.7). Ceci nous incite à définir les deux ensembles suivants :

Définition 6.3.1. Pour tout entier $d \geqslant 2$ premier à q, on pose

$$\mathcal{Z}_q(d) := \left\{ m \in \mathcal{O}_q^{(2)}(d) \;\middle|\; \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 = q^{u(m)} \right\}$$

et son complémentaire $\mathcal{N}_q^*(d) := \mathcal{O}_q^{(2)}(d) \smallsetminus \mathcal{Z}_q(d)$.

On peut alors exprimer l'ordre d'annulation de $L(E_d/K, T)$ en $T = q^{-1}$ à l'aide des résultats de la Section 3.1.

Proposition 6.3.2. *Soit $d \geqslant 2$ un entier premier à q. On considère la courbe E_d définie sur $K = \mathbb{F}_q(t)$ par* (6.1)*. Le rang du groupe de Mordell-Weil $E_d(K)$ s'écrit*

$$\operatorname{rang} E_d(K) = \#\mathcal{Z}_q(d) = \# \left\{ m \in \mathcal{O}_q^{(2)}(d) \;\middle|\; \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 = q^{u(m)} \right\}.$$

Démonstration. Commençons par exprimer le rang analytique $\operatorname{rang}_{an}(E_d/K) = \operatorname{ord}_{T=q^{-1}} L(E_d/K, T)$. Pour simplifier les notations, nous posons $L_d(T) = L(E_d/K, T) \in \mathbb{Z}[T]$ et, pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$, $\omega(m) := \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2$. Alors $L_d(T) = \prod_{m \in \mathcal{O}_q^{(2)}(d)} \big(1 - \omega(m) \cdot T^{u(m)}\big)$ est un polynôme de la forme considérée à la Section 3.1 et le Lemme 3.1.4 permet d'écrire que

$$\operatorname{ord}_{T=q^{-1}} L_d(T) = \# \left\{ m \in \mathcal{O}_q^{(2)}(d) \;\middle|\; \omega(m) = q^{u(m)} \right\} = \#\mathcal{Z}_q(d).$$

Voir également l'Exemple 3.1.9. Ceci démontre que le rang analytique de E_d/K est $\#\mathcal{Z}_q(d)$. Or la courbe E_d/K vérifie l'intégralité des conjectures de Birch et Swinnerton-Dyer (Théorème 6.2.7). En particulier, les rangs algébrique et analytique de E_d sont égaux, *i.e.* $\operatorname{rang} E_d(K) = \operatorname{ord}_{T=q^{-1}} L(E_d/K, T)$. □

Une fois obtenu le rang analytique de E_d/K, il est aisé d'exprimer la valeur spéciale de sa fonction L en « $s = 1$ ».

Proposition 6.3.3. *Avec les hypothèses et notations de la Proposition 6.3.2 ci-dessus, la valeur spéciale $L^*(E_d/K, 1)$ de la fonction L de la courbe E_d/K s'exprime sous la forme :*

$$L^*(E_d/K,1) = \prod_{m\in\mathcal{Z}_q(d)} u(m)\cdot \prod_{m\in\mathcal{N}_q^*(d)} \left(1-\frac{\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m)^2}{q^{u(m)}}\right).$$

Démonstration. Reprenons également les notations introduites dans la preuve de la Proposition 6.3.2. En outre, pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$, on pose $g_m(T) = 1 - \omega(m)\cdot T^{u(m)}$. On pose $r = \#\mathcal{Z}_q(d) = \mathrm{ord}_{T=q^{-1}} L_d(T)$. Par construction, $g_m(T)$ s'annule en $T = q^{-1}$ si et seulement si $m \in \mathcal{Z}_q(d)$. D'après les résultats de la Section 3.1.3, on a

$$\frac{L_d(T)}{(1-qT)^r} = \frac{\prod_{m\in\mathcal{O}_q^2(d)} g_m(T)}{(1-qT)^{\#\mathcal{Z}_q(d)}} = \prod_{m\in\mathcal{Z}_q(d)} \frac{g_m(T)}{1-qT}\cdot \prod_{m\notin\mathcal{Z}_q(d)} g_m(T).$$

Par construction, le polynôme $\frac{L_d(T)}{(1-qT)^r}$ ne s'annule pas en $T = q^{-1}$ et sa valeur en $T = q^{-1}$ est la valeur spéciale $L^*(E_d/K, 1)$ de la fonction L de E_d (Définition 1.3.12). Si $m \in \mathcal{Z}_q(d)$, le polynôme $\frac{g_m(T)}{1-qT}$ vaut $u(m)$ en $T = q^{-1}$ et si $m \notin \mathcal{Z}_q(d)$, le polynôme $g_m(T)$ vaut $1 - \frac{\omega(m)}{q^{u(m)}} \neq 0$ en $T = q^{-1}$. Ce qu'il fallait démontrer. □

Remarquons que $L^*(E_d/K, 1)$ est un nombre rationnel strictement positif. Par construction même, $L^*(E_d/K, 1)$ est la valeur en $T = q^{-1}$ d'un polynôme à coefficients entiers donc $L^*(E_d/K, 1) \in \mathbb{Z}[q^{-1}] \subset \mathbb{Q}$. Pour démontrer la positivité, on peut utiliser le fait que $s \mapsto L(E_d/K, s)$ vérifie l'hypothèse de Riemman : la fonction L ne s'annule donc pas sur $\{\mathrm{Re}(s) > 1\}$ et est positive pour $\mathrm{Re}(s) > 3/2$ (voir Remarque 1.3.13).

6.3.2 Rang non borné

Nous pouvons maintenant prouver un résultat de « rang non borné » pour la famille des courbes E_d. C'est une conséquence assez immédiate de la Proposition 6.3.2 et du théorème de Shafarevich-Tate (Théorème 2.4.4). Il convient de remarquer que, lorsqu'on se restreint à considérer seulement les valeurs impaires de d, la Proposition ci-dessous est un cas particulier de [Ulm07b, Theorem 4.7].

Proposition 6.3.4. *Supposons que $\mathbb{F}_q$ est un corps fini de caractéristique $p \geqslant 3$. Lorsque d parcourt l'ensemble des entiers premier à p, le rang des courbes E_d définies par* (6.1) *sur $K = \mathbb{F}_q(t)$ n'est pas borné :*

$$\limsup_{\mathrm{pgcd}(d,q)=1} \mathrm{rang}\, E_d\big(\mathbb{F}_q(t)\big) = +\infty.$$

Démonstration. Pour prouver la Proposition, il suffit de produire une suite infinie d'entiers d premiers à q et tels que la fonction $L(E_d/K, T)$ s'annule avec une multiplicité non bornée. Pour tout entier $N \in \mathbb{N}^*$, on pose $d_N = q^N + 1$: c'est un entier pair et premier à q. D'après le Lemme 2.4.1, l'ordre de q modulo d_N vérifie : $o_q(d_N) = 2N$. Nous utilisons alors le Corollaire 2.4.5 du théorème de Shafarevich-Tate (Théorème 2.4.4) : pour toute orbite $m \in \mathcal{O}_q^{(2)}(d_N)$, on a $\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m) = -q^{u(m)/2}$, d'où $\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2 = q^{u(m)}$. Par conséquent, avec les notations introduites plus haut, on a $\mathcal{Z}_q(d_N) = \mathcal{O}_q^{(2)}(d_N)$ et la suite d'égalités :

$$\mathrm{rang}\, E_{d_N}(K) = \mathrm{ord}_{T=q^{-1}} L(E_{d_N}/K, T) = \#\mathcal{Z}_q(d_N) = \#\mathcal{O}_q^{(2)}(d_N) = \#\mathcal{O}'_q(d_N) - 1.$$

La Proposition sera démontrée si l'on peut minorer $\#\mathcal{O}'_q(d_N)$ par une quantité non bornée lorsque $N \to \infty$. D'après la Proposition 3.1.3, on a

$$\#\mathcal{O}'_q(d_N) = \sum_{\substack{d'\mid d_N\\ d'\geqslant 2}} \frac{\phi(d')}{o_q(d')} \geqslant \frac{1}{o_q(d_N)}\cdot \sum_{\substack{d'\mid d_N\\ d'\geqslant 2}} \phi(d') = \frac{d_N-1}{o_q(d_N)} = \frac{d_N-1}{2N}.$$

En effet, pour tout diviseur $d' \geqslant 2$ de d_N, l'ordre de q modulo d' divise $o_q(d_N)$. Par construction, on a $\log d_N = \log(q^N + 1) \geqslant N \cdot \log q$. On déduit finalement la minoration souhaitée :

$$\mathrm{rang}\, E_{d_N}(K) = \#\mathcal{O}'_q(d_N) - 1 \geqslant \frac{d_N-1}{2N} - 1 \geqslant \frac{\log q}{2}\cdot\frac{d_N-1}{\log d_N} - 1 \geqslant \frac{\log q}{8}\cdot\frac{d_N}{\log d_N} \gg_q \frac{d_N}{\log d_N},$$

la constante implicite ne dépendant que de q. Lorsque $N \to \infty$, on a $d_N \to \infty$ et $\frac{d_N}{\log d_N} \to \infty$. Par suite, le rang des courbes E_{d_N} sur $K = \mathbb{F}_q(t)$ ($N \in \mathbb{N}^*$) n'est pas borné. Remarquons en passant que la minoration de rang $E_{d_N}(K)$ ci-dessus est du même ordre de grandeur que la majoration de A. Brumer (*cf.* Théorème 1.5.5) : il existe deux constantes ne dépendant que de q telle que

$$\frac{d_N}{\log d_N} \ll_q \operatorname{rang} E_{d_N}(K) \ll_q \frac{d_N}{\log d_N}.$$

□

6.4 Ratio de Brauer-Siegel

Dans cette dernière section, nous utilisons les résultats démontrés précédemment pour prouver le Théorème principal de ce chapitre.

Théorème 6.4.1. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$. Pour tout entier $d \geqslant 2$ premier à p, on considère la courbe elliptique E_d définie sur $K = \mathbb{F}_q(t)$ par le modèle de Weierstrass, donné en coordonnées affines,*

$$Y^2 + XY + t^d Y = X^3 + t^d X^2.$$

Lorsque $d \to \infty$, on a $H(E_d/K) \to \infty$ et le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ admet 1 pour limite :

$$\mathfrak{Bs}(E_d/K) \xrightarrow[\substack{\operatorname{pgcd}(d,q)=1 \\ d\to\infty}]{} 1.$$

Ce résultat est inconditionnel car la conjecture de Birch et Swinnerton-Dyer est vraie pour les courbes E_d/K (Théorème 6.2.7). Comme cette conjecture est vraie, on peut utiliser la relation entre $\mathfrak{Bs}(E_d/K)$ et la valeur spéciale $L^*(E_d/K, 1)$ de la Proposition 1.6.4 :

$$\mathfrak{Bs}(E_d/K) = 1 + \frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} + o(1) \qquad (H(E_d/K) \to \infty).$$

Pour démontrer le Théorème 6.4.1, il s'agit donc de démontrer que

$$\frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} \xrightarrow[d\to\infty]{} 0.$$

Nous procédons en deux temps : d'abord nous cherchons une majoration de $L^*(E_d/K, 1)$ (Proposition 6.4.2), puis une minoration (Proposition 6.4.3). Ces deux inégalités se combinent pour démontrer que, lorsque $d \to \infty$,

$$0 - o(1) \leqslant \frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} \leqslant 0 + o(1).$$

Ce qui prouvera le Théorème 6.4.1.

6.4.1 Majoration de la valeur spéciale

Soit $d \geqslant 2$ un entier premier à q. La valeur spéciale $L^*(E_d/K, 1)$ admet l'expression sous forme de produit (*cf.* Proposition 6.3.3) :

$$L^*(E_d/K, 1) = \prod_{m \in \mathcal{Z}_q(d)} u(m) \cdot \prod_{m \in \mathcal{N}_q^*(d)} \left(1 - \frac{\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2}{q^{u(m)}}\right),$$

où $\mathcal{Z}_q(d)$ et $\mathcal{N}_q^*(d)$ sont les deux sous-ensembles de $\mathcal{O}_q^{(2)}(d)$ définis à la Section 6.3.

Proposition 6.4.2. *Soit $d \geqslant 2$ un entier premier à q. La valeur spéciale $L^*(E_d/K, 1)$ de la fonction L associée à la courbe E_d vérifie, lorsque $d \to \infty$,*

$$\frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} \leqslant 0 + o(1).$$

Démonstration. Il est assez clair que la fonction L de la courbe E_d vérifie les hypothèses de la Section 3.1 (avec $K = 1$). On peut alors appliquer la Proposition 3.1.8 : il existe une constante absolue $C > 0$ (qu'on peut choisir $\leqslant 5$) telle que

$$\log L^*(E_d/K, 1) \leqslant 3C \log q \cdot \frac{d \cdot \log\log d}{\log d}.$$

Rappelons par ailleurs que $\log H(E_d/K) = \left(\left\lfloor \frac{d+1}{2} \right\rfloor + 1\right) \log q$ (Proposition 6.1.6). D'où l'on tire que $\log H(E_d/K) \geqslant \frac{\log q}{2} d$ et que

$$\frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} \leqslant 3C \log q \cdot \frac{d \cdot \log\log d}{\log d} \cdot \frac{1}{\frac{\log q}{2} \cdot d} \leqslant 6C \cdot \frac{\log\log d}{\log d}.$$

La quantité à droite tend vers 0 lorsque $d \to \infty$. □

Nous notons que cette majoration est un cas particulier de [HP16, Theorem 7 ?5]. Nous avons tout de même obtenu une version effective de ce résultat dans le cas des courbes E_d. En effet, la preuve ci-dessus prouve l'existence d'une constante $c'' > 0$ (absolue) telle que

$$\frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} \leqslant c'' \frac{\log\log d}{\log d}.$$

Mieux, on peut choisir $c'' \leqslant 30$.

6.4.2 Minoration de la valeur spéciale

Pour conclure la preuve du Théorème 6.4.1, il faut à présent obtenir une minoration de $L^*(E_d/K, 1)$. Nous utiliserons pour cela les outils de la Section 3.2.

Proposition 6.4.3. *Soit $d \geqslant 2$ un entier premier à q. La valeur spéciale de la fonction L associée à la courbe E_d/K vérifie, lorsque $d \to \infty$, la minoration :*

$$\frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} \geqslant 0 + o(1).$$

La preuve de cette Proposition est très similaire à la preuve de la Proposition 4.4.3 où l'on a démontré la minoration de la valeur spéciale de la fonction L associée à la courbe de Legendre. Nous nous permettrons donc de ne pas donner tous les détails.

Démonstration. Rappelons que l'on a écrit la valeur spéciale $L^*(E_d/K, 1)$ sous la forme d'un produit indexé par l'ensemble d'orbites $\mathcal{O}_q^{(2)}(d)$ (Proposition 6.3.3). Dans ce produit, les termes correspondant aux orbites $m \in \mathcal{Z}_q(d)$ sont des entiers strictement positifs. Ainsi, on peut minorer $\log L^*(E_d/K, 1)$ comme suit :

$$\log L^*(E_d/K, 1) \geqslant \log \prod_{m \in \mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2}{q^{u(m)}}\right). \tag{6.4}$$

Afin d'obtenir la minoration « forte » des termes restants, nous appliquons le Théorème 3.2.2. Pour ce faire, il faut vérifier les hypothèses (i), (ii) et (iii) de la Section 3.2.1. Pour toute orbite $m \in \mathcal{V}_q^*(d)$, on pose $y(m) = \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2$. On choisit $\mathcal{M} = \mathcal{V}_q^*(d)$. Le fait que cette donnée satisfait les hypothèses (i), (ii) et (iii) a déjà été vérifié à la preuve de la Proposition 4.4.3 (à un facteur « $\mathbf{t}_m(16)$ » près, qui n'a pas d'influence ici). on peut appliquer le Théorème 3.2.2.

Pour tout diviseur $d' > 2$ de d, soit $K_{d'} = \mathbb{Q}(\zeta_{d'})$ et $\mathfrak{p}'$ l'idéal premier de $K_{d'}$ qui est en-dessous de $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$. On identifie $\mathrm{Gal}(K_{d'}/\mathbb{Q})$ et $(\mathbb{Z}/d'\mathbb{Z})^\times$ de la façon usuelle. De plus, on notera $G_{d'} = (\mathbb{Z}/d'\mathbb{Z})^\times$ et $\langle p \rangle_{d'}$ (resp. $\langle q \rangle_{d'}$) le sous-groupe de $G_{d'}$ engendré par p (resp. par q). On pose maintenant :

$$w'(d') := o_q(d') \cdot \sum_{m' \in G_{d'}/\langle q \rangle_{d'}} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{d}{d'} m'\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\}.$$

Notons que $o_q(d') = \#\langle q \rangle_{d'}$ est un diviseur de $\phi(d') = \#G_{d'}$. Puisque les hypothèses adéquates sont satisfaites, on peut appliquer le Théorème 3.2.2 : celui-ci donne que

$$\log \prod_{m \in \mathcal{V}_q^*(d)} \left(1 - \frac{y(m)}{q^{u(m)}}\right) \geqslant -\log q \cdot \sum_{\substack{d' \mid d \\ d' > 2}} w'(d'). \tag{6.5}$$

La minoration annoncée de la valeur spéciale suivra d'une *majoration* des exposants $w'(d')$ pour tous les diviseurs $d' \geqslant 2$ de d. Comme précédemment, on explicite d'abord les $w'(d')$. À cet effet, soit $F : [0,1] \to \mathbb{R}$ la fonction en escaliers suivante :

$$F(x) := \begin{cases} 1 & \text{si } x \in \left[0, \frac{1}{2}\right], \\ 0 & \text{si } x \in \left]\frac{1}{2}, 1\right]. \end{cases}$$

On montrerait, de façon tout à fait similaire au Lemme 4.4.4, que l'on a :

Lemme 6.4.4. *Pour tout diviseur $d' > 2$ de d, $w'(d')$ admet l'expression suivante :*

$$w'(d') = o_q(d') \cdot \sum_{m' \in G_{d'}/\langle q \rangle_{d'}} \max\left\{0, \int_0^1 F(t)\mathrm{d}t - \frac{1}{\#\langle p \rangle_{d'}} \cdot \sum_{\pi \in \langle p \rangle_{d'}} F\left(\left\{\tfrac{m'd'}{\pi}\right\}\right)\right\}.$$

Maintenant, les résultats d'équidistribution de la Section 3.4 impliquent :

Lemme 6.4.5. *Pour tout diviseur $d' > 2$ de d, la quantité $w'(d')$ ci-dessus vérifie :*

$$\frac{w'(d')}{\phi(d')} \xrightarrow[d' \to \infty]{} 0.$$

De plus, on a

$$\frac{1}{d} \cdot \sum_{\substack{d' \mid d \\ d' > 2}} w'(d') \xrightarrow[d \to \infty]{} 0. \tag{6.6}$$

Ceci a déjà été prouvé au Lemme 4.4.5 : la première assertion découle de l'application de la Proposition 3.4.14 (corollaire du Théorème 3.4.1), la seconde majoration (6.6) découle de la première par le Lemme 3.4.16.

On combine alors les inégalités (6.4), (6.5) et (6.6) et l'on obtient que

$$\frac{\log L^*(E_d/K, 1)}{d} \geqslant \frac{1}{d} \cdot \log \prod_{m \in \mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)^2}{q^{u(m)}}\right) \geqslant -\log q \cdot \frac{1}{d} \cdot \sum_{\substack{d' \mid d \\ d' > 2}} w'(d') = o(1).$$

Enfin, d'après le calcul de la hauteur de E_d (Proposition 6.1.6), on constate que

$$\frac{\log H(E_d/K)}{d} = \log q \cdot \frac{1}{d} \cdot \left(\left\lfloor \frac{d+1}{2} \right\rfloor + 1\right) \leqslant \log q \cdot \frac{1}{d} \cdot \left(\frac{d}{2} + 1\right) \leqslant \log q.$$

De sorte que l'on a

$$\frac{\log L^*\big(E_d/K, 1\big)}{\log H\big(E_d/K\big)} = \frac{d}{\log H\big(E_d/K\big)} \cdot \frac{\log L^*\big(E_d/K, 1\big)}{d} \geqslant -\frac{1}{d} \cdot \sum_{\substack{d' \mid d \\ d' > 2}} w'(d') = o\big(1\big).$$

Ce qu'il fallait démontrer. □

7

Courbes elliptiques
$Y^2 + XY - t^d \cdot Y = X^3$

Dans ce chapitre, nous étudions la famille des courbes elliptiques suivantes : soit $K = \mathbb{F}_q(t)$ le corps des fractions rationnelles sur un corps fini de caractéristique $p \geqslant 3$, pour tout entier $d \in \mathbb{N}^*$, premier à p, on considère la courbe elliptique E_d définie sur K et donnée en coordonnées affines par

$$E_d : \quad Y^2 + XY - t^d Y = X^3.$$

Cette courbe est étudiée dans [DO14] sur $\mathbb{F}_{q^2}$ dans le cas où $d = q+1$. Davis et Occhipinti produisent des points rationnels explicites sur E_d et en déduisent plusieurs résultats sur des sommes de caractères. Récapitulons en un seul théorème les principaux résultats que nous obtenons pour les courbes E_d.

Théorème. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \geqslant 2$, premier à p, on considère la courbe elliptique E_d définie sur K dont un modèle affine est :*

$$E_d : \quad Y^2 + XY - t^d Y = X^3.$$

La hauteur différentielle de E_d/K vaut $H(E_d/K) = q^{\left\lfloor \frac{d+2}{3} \right\rfloor}$. Les conjectures de Birch et Swinnerton-Dyer sont vraies pour la courbe E_d/K. En particulier, son groupe de Tate-Shafarevich $Ш(E_d/K)$ est fini et son ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ a un sens. De plus, lorsque $H(E_d/K) \to +\infty$ (i.e. lorsque $d \to +\infty$ en étant premier à p), on a

$$\mathfrak{Bs}(E_d/K) \xrightarrow[\substack{\operatorname{pgcd}(d,q)=1 \\ d\to\infty}]{} 1.$$

Autrement dit, on a

$$\log\left(\#Ш(E_d/K) \cdot \operatorname{Reg}(E_d/K)\right) \sim \log H(E_d/K) \sim \frac{d}{3}\log q \quad (d \to \infty).$$

Le résultat principal de cet énoncé est l'analogue du Théorème de Brauer-Siegel pour les courbes E_d/K. On peut en effet réécrire l'équivalent ci-dessus sous la forme :

$$\forall \varepsilon > 0, \quad H(E_d/K)^{1-\varepsilon} \ll_\varepsilon \#Ш(E_d/K) \cdot \operatorname{Reg}(E_d/K) \ll_\varepsilon H(E_d/K)^{1+\varepsilon}.$$

Pour arriver à ce résultat, nous suivons un plan assez similaire à ceux des chapitres précédents. Dans la première section, nous décrivons la « mauvaise réduction » des courbes E_d (Proposition 7.1.3) et calculons leur hauteur (Proposition 7.1.4). La seconde section est dévolue au calcul de la fonction L de la courbe E_d (Théorème 7.2.1). Il semble que l'expression que nous obtenons soit un résultat nouveau. Comme dans les chapitres précédents, nous utilisons des sommes de caractères pour expliciter la série génératrice définissant $L(E_d/K, T)$. Les sommes mentionnées sont en fait des sommes de Jacobi (Lemme 7.2.4) et nous utilisons ce fait de façon cruciale pour encadrer le ratio de Brauer-Siegel. Dans la troisième section, nous tirons profit du caractère explicite de la fonction $L(E_d/K, T)$ pour en donner l'ordre d'annulation en $T = q^{-1}$ (Proposition 7.3.3) et pour écrire sa valeur spéciale sous une forme agréable (Proposition 7.3.4). Nous expliquons également pourquoi les courbes E_d vérifient les conjectures de Birch et Swinnerton-Dyer (Théorème 7.3.1). C'est à la quatrième et dernière section qu'est démontré l'analogue du Théorème de Brauer-Siegel (Théorème 7.4.4), nous y exploitons les résultats des sections antérieures.

7.1 Les courbes E_d

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$. Pour tout entier $d \geqslant 2$ premier à q, on considère la courbe elliptique E_d définie sur $K = \mathbb{F}_q(t)$ et dont un modèle affine de Weierstrass est

$$Y^2 + XY - t^d Y = X^3. \tag{7.1}$$

Le discriminant de ce modèle, calculé à l'aide du formulaire de la Section 1.1.2 (voir aussi [Sil09, Chapter III.1, p. 42]), vaut

$$\Delta = -t^{3d}(27t^d + 1).$$

D'autre part, l'invariant $j(E_d/K)$ s'écrit :

$$j(E_d/K) = -\frac{(24t^d + 1)^3}{t^{3d}(27t^d + 1)}.$$

En particulier, on constate que $j(E_d/K) \in \mathbb{F}_q(t)$ est une fraction rationnelle de degré $-d \neq 0$ en t et donc que la courbe $E_d/\mathbb{F}_q(t)$ n'est pas isotriviale. Par ailleurs, $j(E_d/K)$ n'est pas une puissance p-ième dans K. En particulier, l'application rationnelle $j : \mathbb{P}^1 \to \mathbb{P}^1$ donnée par $t \mapsto j(E_d/K)(t)$ est non constante et séparable.

Remarque 7.1.1. Avec des notations classiques, on a $a_1 = 1$ et $a_3 = -t^d$ (*cf.* Section 1.1.2). En particulier la courbe E_d satisfait les conditions pour avoir un point de 3-torsion rationnel (*cf.* [Hus04, Chapter 4, §2] ou le Chapitre 5 ci-avant). Ce point de torsion est donné, dans le modèle (7.1), par $P = (0, 0)$. On a alors $2P = (0, t^d) = -P$.

Remarque 7.1.2. Notons que la courbe $E_{3d}/\mathbb{F}_q(t)$ est isomorphe, sur $\overline{\mathbb{F}_q}(t)$, à la courbe hessienne $H_d/\mathbb{F}_q(t)$ du Chapitre 5. Plus précisément, si $k/\mathbb{F}_q$ désigne la plus petite extension de $\mathbb{F}_q$ contenant les racines $3d$-ièmes de -27, les courbes E_{3d} et H_d sont isomorphes sur $k(t)$. En effet, si l'on pose $t' = (-27)^{1/3d} t^{-1}$, on a

$$j(E_{3d}/K)(t) = -\frac{(24t^{3d} + 1)^3}{t^{9d}(27t^{3d} + 1)} = -\frac{t'^{9d}\left(1 - \frac{24}{27t'^{3d}}\right)^3}{-27\left(-t'^{-3d} + 1\right)} = \frac{t'^{3d}\left(9t'^{3d} - 8\right)^3}{\left(t'^{3d} - 1\right)} = j(H_d/K)(t').$$

Cependant, lorsque $d \to \infty$ à q fixé, on a $[k : \mathbb{F}_q] \to \infty$. Du point de vue de notre étude où le corps de base $K = \mathbb{F}_q(t)$ est fixé, les familles $\{E_{3d}\}$ et $\{H_d\}$ sont donc distinctes. *A fortiori*, $\{E_{3d}\}$ et $\{H_d\}$ le sont.

7.1.1 Mauvaise réduction et invariants

Les places de mauvaise réduction de E_d/K sont exactement les places v de K qui divisent le discriminant d'un modèle de E_d. On constate sur le discriminant $\Delta = -t^{3d}(27t^d + 1)$ du modèle (7.1) que E_d/K a bonne réduction partout, sauf éventuellement en $v = 0$, $v = \infty$ et les places v de K correspondant aux $\zeta \in \overline{\mathbb{F}_q}$ tels que $\zeta^d = -27^{-1}$. Plus précisément, on a :

Proposition 7.1.3. *Soit $d \geqslant 2$ premier à q, on note $\pi : \mathcal{E}_d \to \mathbb{P}^1$ le modèle régulier minimal de E_d/K. Le morphisme π a les fibres singulières suivantes :*

- *la fibre $\pi^{-1}(0)$ a $3d$ composantes arrangées en une configuration $\mathbf{I}_{3d}$ déployée.*
- *la fibre $\pi^{-1}(\zeta)$, où $\zeta \in \overline{\mathbb{F}_q}$ vérifie $\zeta^d = -27^{-1}$, est irréductible (type $\mathbf{I}_1$).*
- *la fibre $\pi^{-1}(\infty)$ est*
  - *une courbe elliptique si $d \equiv 0 \bmod 3$ (type $\mathbf{I}_0$),*
  - *de type $\mathbf{IV}$ déployée si $d \equiv -1 \bmod 3$,*
  - *de type $\mathbf{IV}^*$ déployée tsi $d \equiv -2 \bmod 3$.*

Démonstration. Nous recourons à nouveau à l'algorithme de Tate [Tat75], tel qu'il est décrit dans [Sil94, Chap. IV, §9], pour déterminer le type de la fibre $\pi^{-1}(v)$ au-dessus de chacune des places de mauvaise réduction pour E_d. Rappelons que le discriminant du modèle 7.1 vaut $\Delta = -t^{3d}(27t^d + 1)$.

- En la place $v = 0$ de K, on a $\operatorname{ord}_{v=0} \Delta = 3d$ et $\operatorname{ord}_{v=0} j(E_d/K) = -3d$. La fibre de π au-dessus de 0 est donc de type $\mathbf{I}_{3d}$ (autrement dit, la courbe E_d a réduction multiplicative en 0). De plus, le modèle (7.1) est entier et minimal en $v = 0$ et sa réduction a des tangentes rationnelles en le point singulier ; la réduction est donc déployée.

  La place $v = 0$ donne donc une contribution $\operatorname{ord}_{v=0} \Delta_{\min}(E_d/K) = 3d$ au discriminant minimal de E_d, une contribution $\operatorname{ord}_{v=0} \mathcal{N}(E_d/K) = 1$ au conducteur et le nombre de Tamagawa local en 0 est $c_0(E_d/K) = 9d$.

- Au-dessus de $v = \zeta \in \overline{\mathbb{F}_q}$ (où ζ vérifie $\zeta^d = -27^{-1}$), la fibre de π est singulière (car ζ annule Δ) et irréductible. En effet, on a $\mathrm{ord}_{v=\zeta} \Delta = 1$ et $\mathrm{ord}_{v=\zeta} j(E_d/K) = -1$.

  Chacune des places ζ (où $27\zeta^d = -1$) contribue donc pour $\mathrm{ord}_{v=\zeta} \Delta_{\min}(E_d/K) = 1$ au discriminant minimal de E_d et pour $\mathrm{ord}_{v=\zeta} \mathcal{N}(E_d/K) = 1$ au conducteur. D'autre part, le nombre de Tamagawa local en ζ est nécessairement $c_\zeta(E_d/K) = 1$.

- Pour étudier la fibre en $v = \infty$, on commence par effectuer un changement de cartes $t = 1/u$ sur $\mathbb{P}^1$. On obtient, après un changement de coordonnées du type $(X, Y) = (u^{2c}X', u^{3c}Y')$, le modèle affine suivant pour $E_d/\mathbb{F}_q(u)$:

$$Y^2 + u^c XY - u^{3c-d}Y = X^3, \tag{7.2}$$

  où $c \in \mathbb{N}^*$ reste à choisir pour minimiser l'ordre $\mathrm{ord}_{u=0}$ du discriminant $\Delta' = -u^{12c-4d}(27 + u^d)$ de ce modèle. On distingue alors trois cas :
  - Si d est divisible par 3, on choisit $c = d/3$ et le modèle (7.2) devient

$$Y^2 + u^{d/3}XY - Y = X^3,$$

    l'équation d'une cubique lisse (autrement dit $\mathrm{ord}_{u=0} \Delta' = 0$). La réduction de $E_d/\mathbb{F}_q(u)$ en $u = 0$ (donc de $E_d/\mathbb{F}_q(t)$ en ∞) est donc de type $\mathbf{I}_0$ (bonne réduction).
  - Si $d \equiv 2 \bmod 3$, on choisit $c = (d+1)/3$. Le modèle 7.2 devient

$$Y^2 + u^{(d+1)/3}XY - uY = X^3$$

    et on constate que $\mathrm{ord}_{u=0} \Delta' = 4$ et, avec des notations classiques, $\mathrm{ord}_{u=0} b_6 = 2 < 3$. La fibre de π au-dessus de ∞ est donc de type **IV**. Par suite, la place $v = \infty$ de K donne une contribution $\mathrm{ord}_\infty \Delta_{\min}(E_d/K) = 4$ au diviseur discriminant minimal de E_d et une contribution $\mathrm{ord}_\infty \mathcal{N}(E_d/K) = 2$ au conducteur. Enfin, on peut voir (*cf.* [Sil94, Chap. IV, §9]) qu'ici $c_\infty(E_d/K) = 3$.
  - Si $d \equiv 1 \bmod 3$, on choisit $c = (d+2)/3$ et le modèle 7.2 se réécrit

$$Y^2 + u^{(d+2)/3}XY - u^2Y = X^3$$

    et on constate que $\mathrm{ord}_{u=0} \Delta' = 8$ et l'algorithme de Tate s'arrête à l'étape 8 : la fibre de π au-dessus de ∞ est de type $\mathbf{IV}^*$. Dans ce cas, la place $v = \infty$ de K contribue donc pour $\mathrm{ord}_\infty \Delta_{\min}(E_d/K) = 8$ au discriminant minimal de E_d et pour $\mathrm{ord}_\infty \mathcal{N}(E_d/K) = 2$ au conducteur. De même que ci-dessus, il y a une procédure simple pour calculer $c_\infty(E_d/K)$ [Sil94, Chap. IV, §9]. Ici, on trouve que $c_\infty(E_d/K) = 3$.

Ce qui achève l'analyse des fibres singulières du morphisme π. □

On peut former un tableau récapitulatif des informations locales démontrées ci-avant :

Place	Type de réduction	$\mathrm{ord}_v \Delta_{\min}(E_d/K)$	$\mathrm{ord}_v \mathcal{N}(E_d/K)$	$c_v(E_d/K)$
$v = 0$	$\mathbf{I}_{3d}$ déployée	$3d$	1	$3d$
$v = \zeta$ $(27\zeta^d = -1)$	$\mathbf{I}_1$	1	1	1
$v = \infty$	$\mathbf{I}_0$ si $d \equiv 0 \bmod 3$	0	0	1
	IV déployée si $d \equiv -1 \bmod 3$	4	2	3
	$\mathbf{IV}^*$ si $d \equiv -2 \bmod 3$	8	2	3

Dans ce tableau, pour toute place v de K, on a noté $\mathrm{ord}_v \Delta_{\min}(E_d/K)$ la valuation en v du discriminant minimal de E_d, $\mathrm{ord}_v \mathcal{N}(E_d/K)$ la valuation du conducteur de E_d et $c_v(E_d/K)$ le nombre de Tamagawa local.

7.1.2 Hauteur et conducteur

À l'aide de l'analyse de la mauvaise réduction ci-avant, on déduit la valeur de la hauteur de E_d/K en fonction de d :

Proposition 7.1.4. *Soit d un entier premier à q et E_d la courbe définie sur $K = \mathbb{F}_q(t)$ par (7.1). Sa hauteur différentielle s'écrit*

$$H\big(E_d/K\big) = q^{\lfloor \frac{d+2}{3} \rfloor}$$

et son conducteur est de degré

$$\deg \mathcal{N}(E_d/K) = \begin{cases} d+1 & \text{si } 3 \mid d \\ d+3 & \text{sinon .} \end{cases}$$

Démonstration. Ceci suit de la preuve de la Proposition précédente et des informations collectées dans le tableau ci-dessus. En effet, si l'on note d_v le degré de toute place v de K et simplement $\Delta_{\min} = \Delta_{\min}\big(E_d/K\big)$, on a

$$\begin{aligned} \deg \Delta_{\min}(E_d/K) &= d_0 \cdot \operatorname{ord}_{v=0} \Delta_{\min} + \sum_{\substack{\zeta \in \overline{\mathbb{F}_q} \text{ tq.} \\ 27\zeta^d = -1}} d_\zeta \cdot \operatorname{ord}_{v=\zeta} \Delta_{\min} + d_\infty \cdot \operatorname{ord}_{v=\infty} \Delta_{\min} \\ &= 3d + d + \operatorname{ord}_{v=\infty} \Delta_{\min} = \begin{cases} 4d & \text{si } d \equiv 0 \bmod 3 \\ 4(d+1) & \text{si } d \equiv -1 \bmod 3 \\ 4(d+2) & \text{si } d \equiv -2 \bmod 3. \end{cases} \end{aligned}$$

On en déduit que

$$H\big(E_d/K\big) = q^{(\deg \Delta_{\min})/12} = \begin{cases} q^{d/3} & \text{si } d \equiv 0 \bmod 3 \\ q^{(d+1)/3} & \text{si } d \equiv -1 \bmod 3 \\ q^{(d+2)/3} & \text{si } d \equiv -2 \bmod 3 \end{cases} = q^{\lfloor \frac{d+2}{3} \rfloor}.$$

De même, on trouve le degré du conducteur $\mathcal{N}(E_d/K)$ en sommant les contributions locales regroupées dans le tableau ci-dessus. □

On peut alors anticiper la forme de la fonction L de E_d/K comme suit. Comme E_d n'est pas isotriviale, le Théorème 1.3.11 affirme que $L(E_d/K, s)$ est un polynôme à coefficients entiers en $T = q^{-s}$, de degré donné par :

$$\deg L(E_d/K, T) = \deg \mathcal{N}(E_d/K) + 4g(\mathbb{P}^1) - 4 = \begin{cases} d-3 & \text{si } 3 \mid d \\ d-1 & \text{sinon .} \end{cases} \tag{7.3}$$

7.1.3 Sous-groupe de torsion

Nous pouvons à présent expliciter le groupe de torsion de $E_d(K)$.

Proposition 7.1.5. *Soit d un entier premier à la caractéristique p de $K = \mathbb{F}_q(t)$. Soit également E_d la courbe elliptique définie sur $K = \mathbb{F}_q(t)$ par (7.1). Le sous-groupe de torsion du groupe de Mordell-Weil de E_d vérifie*

$$E_d(\mathbb{F}_q(t)) \simeq \mathbb{Z}/3\mathbb{Z}$$

et il est engendré par $P_0 = (0, 0)$ (donné en coordonnées affines sur (7.1)).

Démonstration. Notons $T = E_d(K)_{\text{tors}}$. Il est clair que $P_0 \in E_d(K)$ et que $2P_0 = (0, t^d) = -P_0$ (dans le modèle (7.1)). En particulier, P_0 est bien un point de 3-torsion et T contient au moins un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Il s'agit maintenant de démontrer que l'on a ainsi énuméré tous les points de torsion de $E_d(K)$.

Tout d'abord, comme le j-invariant $j(E_d/K) \in K$ n'est pas une puissance p-ième dans K, la partie p-primaire de T est triviale (voir [Ulm11, Lecture 1, Proposition 7.3]). Autrement dit, il n'y a pas de points de torsion d'ordre une puissance de p dans le groupe de Mordell-Weil $E_d(K)$.

Pour toute place v de K, qui est de mauvaise réduction pour E_d, on note G_v le groupe des composantes de la fibre en v du modèle de Néron de E_d (voir [SS10, §7] ou [Sil94, Chapter IV, §9]). Le formulaire [SS10, Lemma 7.3] (ou le tableau [Sil94, p.365]) donne :

$$G_v \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{si la fibre en } v \text{ est de type } \mathbf{I}_n, \\ \mathbb{Z}/3\mathbb{Z} & \text{si la fibre en } v \text{ est de type } \mathbf{IV}, \\ \mathbb{Z}/3\mathbb{Z} & \text{si la fibre en } v \text{ est de type } \mathbf{IV}^*. \end{cases}$$

Distinguons maintenant deux cas. Premièrement, si d n'est pas divisible par 3, d'après l'analyse de la mauvaise réduction de E_d (Proposition 7.1.3), la courbe E_d a mauvaise réduction additive en la place ∞ de K (de type **IV** ou **IV***). On peut alors invoquer [SS10, Lemma 7.8] : le groupe T s'injecte dans le groupe des composantes G_v d'une fibre additive de E_d. Noter qu'*a priori* seul le sous-groupe des points d'ordre premier à p admet une telle injection, mais ici il s'agit de T entier d'après ce que l'on a démontré plus haut. Ce qui prouve l'existence d'un morphisme injectif $T \hookrightarrow G_\infty \simeq \mathbb{Z}/3\mathbb{Z}$ et, avec le premier paragraphe de cette preuve, achève la démonstration dans ce cas.

Reste à traiter le cas où d est divisible par 3 : dans ce cas, la courbe E_d est semi-stable (Proposition 7.1.3) et la place ∞ est de bonne réduction. Utilisons alors le [SS10, Corollary 7.5] : le groupe de torsion T s'injecte dans le produit $\prod_{v|\Delta} G_v$ des groupes des composantes G_v. Si d est divisible par 3, on a $\prod_{v|\Delta} G_v \simeq \mathbb{Z}/3d\mathbb{Z}$. Ainsi, T est isomorphe à un sous-groupe de $\mathbb{Z}/3d\mathbb{Z}$ (et contient au moins un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z}$). En particulier, T est cyclique et son ordre $M \in \mathbb{N}^*$ vérifie : $3 \mid M \mid 3d$. Fixons maintenant $Q \in T \subset E_d(K)$ un point d'ordre exactement M de sorte que $\langle Q \rangle = T \simeq \mathbb{Z}/M\mathbb{Z}$. On note $X_1(M)$ la (projectivisée de la) courbe modulaire définie sur $\overline{\mathbb{F}_p}$ qui classifie les paires (E, P) formées d'une courbe elliptique E et d'un point rationnel P d'ordre exactement M. La paire (E_d, Q) est donc un point K-rationnel de $X_1(M)$ avec $K = \mathbb{F}_q(\mathbb{P}^1)$; on en déduit un morphisme $j' : \mathbb{P}^1 \to X_1(M)$. Comme E_d n'est pas isotriviale, son j-invariant $j(E_d/K) : \mathbb{P}^1 \to \mathbb{P}^1$ n'est pas constant et le morphisme j' qui s'en déduit n'est pas constant non plus. Par suite, $j' : \mathbb{P}^1 \to X_1(M)$ est surjectif et la formule de Riemann-Hurwitz implique que les genres $g(\mathbb{P}^1)$ et $g(X_1(M))$ de $\mathbb{P}^1$ et de $X_1(M)$ sont reliés par : $0 = g(\mathbb{P}^1) \geqslant g(X_1(M)) \geqslant 0$. Donc le genre de $X_1(M)$ est nul, ce qui n'arrive que pour $M \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ (voir [Ser97, §5.4], [HS00, Theorem F.4.1.1]). Comme M est par ailleurs divisible par 3, il ne reste que 4 valeurs possibles : $M \in \{3, 6, 9, 12\}$. Pour terminer la preuve de la proposition dans le cas où $3 \mid d$, il s'agit de montrer que $M = 3$: il suffit de montrer que T ne contient pas de point de 2-torsion (auquel cas M sera impair) et que T ne contient pas de 9-torsion.

Supposons qu'il existe un point de 2-torsion $P = (x, y) \in E_d(K)$. Alors $P = -P$ et ceci impose que la coordonnée x de P vérifie $4x^3 - 2x^2 - 2t^d \cdot x + t^{2d} = 0$. Comme d est un mutiple de 3, posant $u = 1/t$ et $x_1 = u^{2d/3} \cdot x$, on obtient que $4x_1^3 - 2u^{2d/3} \cdot x_1^2 - 2u^{d/3} \cdot x_1 + 1 = 0$. Cette dernière équation n'a pas de solution $x_1 \in \mathbb{F}_q(u)$ car elle se réécrit sous la forme

$$(4x_1^2 - 2u^{2d/3} \cdot x_1 - 2u^{d/3}) \cdot x_1 = -1.$$

Il n'y a donc pas de point K-rationnel de 2-torsion sur E_d et $M = \#T$ est impair.

Admettons maintenant qu'il existe un point K-rationnel $Q = (x, y)$ d'ordre 9 sur E_d. Quitte à prendre un multiple de Q, on peut supposer que Q vérifie $3 \cdot Q = P_0 = (0, 0)$. À l'aide de la formule de triplication (voir [Sil09, Chapter III, Exercice 3.7 (d)]), on peut exprimer $x(3Q)$, la coordonnée en x de $3Q = P_0$, en fonction de x. À l'aide d'un logiciel de calcul formel (ou à la main), on en déduit que x doit vérifier :

$$x^9 + 6t^d \cdot x^7 + t^d(1 - 24t^d) \cdot x^6 - 6t^{2d} \cdot x^5 + 3t^{3d} \cdot x^4 + t^{3d}(3t^d - 1) \cdot x^3 + 3t^{4d} \cdot x^2 - 3t^{5d} \cdot x + t^{6d} = 0.$$

Ici encore, on peut poser $u = 1/t$, $v = u^{d/3}$ et $x_2 = u^{2d/3} \cdot x = v^2 \cdot x$: la relation ci-dessus donne que $x_2 \in \mathbb{F}_q(u)$ est solution de

$$\begin{aligned} 0 &= x_2^3 + v \cdot x_2^2 - 3x_2^2 - v \cdot x_2 + 1 \\ \text{ou } 0 &= x_2^6 + (3 - v) \cdot x_2^5 + (v^2 + v + 9) \cdot x_2^4 + (v^2 - 3v + 2) \cdot x_2^3 + (v^2 - v + 3) \cdot x_2^2 - 2v^2 \cdot x_2 + 1. \end{aligned}$$

Aucune de ces deux équations n'a de solution $x_2 \in \mathbb{F}_q(u)$. C'est donc que le point $Q = (x, y)$ ne peut pas exister. Ainsi, $E_d(K)$ ne contient aucun point de 9-torsion et $M = 3$. Ce qu'il fallait démontrer. □

7.2 Fonctions L des courbes E_d

Pour estimer le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$, nous aurons besoin d'une expression suffisamment explicite de la fonction L de E_d/K. Nous démontrons donc dans cette section le Théorème ci-dessous. Pour ce faire, nous utilisons les définitions et les notations introduites aux Sections 2.1.2 et 2.1.3. En particulier, nous fixons un idéal premier $\mathfrak{P} \subset \overline{\mathbb{Z}}$ au-dessus de p afin de disposer du caractère de Teichmüller $\mathbf{t} : \overline{\mathbb{F}_q}^\times \to \overline{\mathbb{Q}}^\times$. Pour tout entier $d \geqslant 2$, on note à nouveau $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ les caractères (où $m \in \mathcal{O}'_q(d)$) dont l'ordre divise d construits à la Section 2.1.3. Avec ces notations :

Théorème 7.2.1. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \geqslant 2$ premier à q, nous notons à nouveau E_d la courbe elliptique sur K dont un modèle est* (7.1)*. La*

fonction L de E_d admet alors l'expression suivante :

$$L\big(E_d/K, T\big) = \prod_{m \in \mathcal{O}_q^{(3)}(d)} \Big(1 - \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) \cdot T^{u(m)}\Big).$$

où, $\mathcal{O}_q^{(3)}(d)$ désigne l'ensemble d'orbites suivant :

$$\mathcal{O}_q^{(3)}(d) = \begin{cases} \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/3, 2d/3\}\big)\big/\langle q \bmod d\rangle & \text{si } 3 \mid d \\ \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\big)\big/\langle q \bmod d\rangle & \text{si } 3 \nmid d, \end{cases}$$

et pour toute orbite $m \in \mathcal{O}_q^{(3)}(d)$, l'entier $u(m)$ est le cardinal de l'orbite m et $\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m)$ est une somme de Jacobi.

La démonstration de ce Théorème occupe le reste de la présente section. Nous utilisons à nouveau des calculs élémentaires sur les sommes de caractères.

7.2.1 Dénombrement de points rationnels

Dans tout le reste de la section, on fixe un entier $d \geqslant 2$ premier à q. Nous débutons le calcul de la fonction L de la courbe E_d par un dénombrement de points rationnels sur les réductions de E_d en différentes places de K. Pour tout $\tau \in \mathbb{P}^1(\overline{\mathbb{F}_q})$, on notera $\overline{(E_d)}_\tau$ la réduction en τ d'un modèle entier et minimal (en la place v_τ de K correspondant à τ) de E_d. Ainsi, $\overline{(E_d)}_\tau$ est une courbe cubique plane (éventuellement singulière), sur le corps résiduel $\mathbb{F}_q(\tau)$ de K en τ. Commençons par expliciter un « bon » modèle de E_d :

Lemme 7.2.2. *L'équation affine*

$$E'_d : \quad Y^2 = X^3 + X^2 - 8t^d X + 16t^{2d} \tag{7.4}$$

est un modèle entier de (la partie affine de) la courbe E_d/K. Celui-ci est de plus minimal en toute place $v \neq \infty$ de K.

Démonstration. Le changement de variables $(x, y) = (4X, 8Y + 4X - 4t^d)$ transforme (7.1) en

$$y^2 = x^3 + x^2 - 8t^d x + 16t^{2d},$$

dont le discriminant est $\Delta' = -2^{12}t^{3d}(27t^d + 1)$ (*cf.* le formulaire de la Section 1.1.2). L'équation écrite est clairement à coefficients dans $\mathbb{F}_q[t]$, les entiers de K. En outre, comme 2 est une unité dans tous les corps résiduels des places de K (la caractéristique de K est $p \geqslant 5$), ce modèle est minimal en toute place v de K, sauf en $v = \infty$. □

Pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$ et tout $\tau \in \mathbb{P}^1(\mathbb{F}_Q)$, on pose

$$A(\tau, Q) := Q + 1 - \#\overline{(E_d)}_\tau(\mathbb{F}_Q).$$

À l'aide du Lemme ci-dessus, on peut donner une expression pratique de $A(\tau, Q)$ pour tout $\tau \neq \infty$. Soit en effet $\tau \in \mathbb{P}^1(\mathbb{F}_q) \smallsetminus \{\infty\}$: le modèle (7.4) étant entier et minimal en τ, on peut utiliser sa réduction en τ pour calculer $A(\tau, Q)$. Le Lemme 2.2.1 donne :

$$\begin{aligned} \#\overline{(E_d)}_\tau(\mathbb{F}_Q) &= 1 + \#\left\{(x, y) \in \mathbb{F}_Q^2 \;\middle|\; y^2 = x^3 + x^2 - 8\tau^d x + 16\tau^{2d}\right\} \\ &= 1 + \sum_{x \in \mathbb{F}_Q} \big(1 + \mu(x^3 + x^2 - 8\tau^d x + 16\tau^{2d})\big) \\ &= Q + 1 + \sum_{x \in \mathbb{F}_Q} \mu(x^3 + x^2 - 8\tau^d x + 16\tau^{2d}). \end{aligned}$$

De sorte que, pour tout $\tau \in \mathbb{F}_Q$, on a

$$A(\tau, Q) = Q + 1 - \#\overline{(E_d)}_\tau(\mathbb{F}_Q) = -\sum_{x \in \mathbb{F}_Q} \mu(x^3 + x^2 - 8\tau^d x + 16\tau^{2d}).$$

On peut alors démontrer l'identité :

Proposition 7.2.3. *Soit $\mathbb{F}_Q/\mathbb{F}_q$ une extension finie. Alors*

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) = -\sum_{\chi\in Z(d,Q)} \mathbf{j}_Q(\chi,\chi,\chi),$$

où la somme porte sur l'ensemble de caractères $Z(d,Q)$ défini ainsi :

$$Z(d,Q) := \left\{\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times \;\middle|\; \chi^d = \mathbf{1}, \chi^3 \neq \mathbf{1}\right\}.$$

Démonstration. Avant toute chose, rappelons que le type de réduction de la courbe E_d en $\tau=\infty$ (*cf.* Proposition 7.1.3) : si $3 \mid d$, la courbe a bonne réduction en $\tau=\infty$ et la courbe réduite $\overline{(E_d)}_\infty$ a pour équation (affine) $y^2-y=x^3$; si d n'est pas divisible par 3, la courbe E_d a mauvaise réduction de type additive en ∞, d'où $A(\infty,Q) = Q+1-\#\overline{(E_d)}_\infty(\mathbb{F}_Q) = 0$. Nous reviendrons plus loin sur ce fait.

Pour commencer, nous séparons la somme à expliciter en deux parties :

$$\begin{aligned}\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) &= A(\infty,Q) + \sum_{\tau\in\mathbb{F}_Q} A(\tau,Q)\\ &= A(\infty,Q) - \sum_{\tau\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q} \mu(x^3+x^2-8\tau^d x+16\tau^{2d}).\end{aligned}$$

On peut alors utiliser le Lemme 2.2.2 pour « réindexer » la somme sur $\tau\in\mathbb{F}_Q$:

$$\begin{aligned}\sum_{\tau\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q} \mu(x^3+x^2-8\tau^d x+16\tau^{2d}) &= \sum_{\chi^d=\mathbf{1}}\sum_{z\in\mathbb{F}_Q}\chi(z)\left(\sum_{x\in\mathbb{F}_Q}\mu(x^3+x^2-8zx+16z^2)\right)\\ &= \sum_{\chi^d=\mathbf{1}}\left(\sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z)\mu(x^3+x^2-8zx+16z^2)\right),\end{aligned}$$

la somme portant sur l'ensemble des caractères $\chi:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times$ dont la puissance d-ième est triviale. Pour démontrer la Proposition, il s'agit d'écrire les doubles sommes sur (x,z) sous la forme de sommes de Jacobi. Pour un caractère quelconque $\chi:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times$, on pose donc

$$E_Q(\chi) := \sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z)\mu(x^3+x^2-8zx+16z^2).$$

Alors on a

Lemme 7.2.4. *Soit $\chi:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times$ un caractère quelconque. Alors*

$$E_Q(\chi) = \begin{cases} 0 & \text{si } \chi \text{ est trivial}\\ \mathbf{j}_Q(\chi,\chi,\chi) & \text{sinon,}\end{cases}$$

où $\mathbf{j}_Q(\chi,\chi,\chi)$ est une somme de Jacobi (cf. Section 2.2.2).

Afin de ne pas interrompre le calcul de $\sum_\tau A(\tau,Q)$, nous différons la preuve de ce Lemme à la Section 7.2.2 ci-après. Pour l'heure admettons celui-ci. On peut appliquer l'identité du Lemme 7.2.4 à tous les caractères χ dont l'ordre divise d. On obtient alors

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) = A(\infty,Q) - 0 - \sum_{\substack{\chi^d=\mathbf{1}\\ \chi\neq\mathbf{1}}} \mathbf{j}_Q(\chi,\chi,\chi).$$

Définissons alors l'ensemble de caractères suivant :

$$Z(d,Q) := \left\{\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times \;\middle|\; \chi^d = \mathbf{1}, \chi^3 \neq \mathbf{1}\right\}.$$

On distingue deux cas :

– Si d n'est pas divisible par 3, aucun caractère $\chi:\mathbb{F}_Q^\times\to\overline{\mathbb{Q}}^\times$ dont l'ordre divise d ne vérifie $\chi^3=\mathbf{1}$. Ainsi, dans ce cas, $Z(d,Q)$ consiste en les caractères non triviaux dont l'ordre divise d. D'autre part, on a déjà remarqué que $A(\infty,Q)=0$ si $3\nmid d$. Il suit alors que

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) = A(\infty,Q) - \sum_{\substack{\chi^d=\mathbf{1}\\ \chi\neq\mathbf{1}}} \mathbf{j}_Q(\chi,\chi,\chi) = 0 - \sum_{\chi\in Z(d,Q)} \mathbf{j}_Q(\chi,\chi,\chi).$$

C'est l'identité recherchée.

– Si maintenant d est divisible par 3, un décompte de points sur la réduction de E_d en ∞ donne facilement :

$$A(\infty, Q) = -\sum_{x \in \mathbb{F}_Q} \mu(x^3 + 1/4).$$

Comme au Lemme 5.2.6, dégageons deux sous-cas :

– Ou bien $3 \mid q-1$, auquel cas il existe deux caractères non triviaux d'ordre 3 sur $\mathbb{F}_Q^\times$, notons-les ξ et ξ^2. Alors (*cf.* Proposition 2.2.7)

$$\mathbf{j}_Q(\xi, \xi, \xi) = \xi(-1) \cdot \mathbf{j}_Q(\xi, \xi) \quad \text{et} \quad \mathbf{j}_Q(\xi^2, \xi^2, \xi^2) = \xi^2(-1) \cdot \mathbf{j}_Q(\xi^2, \xi^2).$$

De plus, d'après le Lemme 2.2.2 et la relation du Lemme 2.2.9, on a

$$\begin{aligned}
-A(\infty, Q) &= \sum_{x \in \mathbb{F}_Q} \mu(x^3 + 1/4) = \sum_{z \in \mathbb{F}_Q} \big(1 + \xi(z) + \xi^2(z)\big)\, \mu(z + 1/4) \\
&= \sum_{z \in \mathbb{F}_Q} \mu(z + 1/4) + \sum_{z \in \mathbb{F}_Q} \xi(z)\mu(z + 1/4) + \sum_{z \in \mathbb{F}_Q} \xi^2(z)\mu(z + 1/4) \\
&= 0 + \overline{\xi}(-4)\mu(4) \cdot \sum_{z' \in \mathbb{F}_Q} \xi(z')\mu(1 - z') + \overline{\xi}^2(-4)\mu(4) \cdot \sum_{z' \in \mathbb{F}_Q} \xi^2(z')\mu(1 - z') \\
&= -\overline{\xi}(-4) \cdot 1 \cdot \mathbf{j}_Q(\xi, \mu) - \overline{\xi}^2(-4) \cdot 1 \cdot \mathbf{j}_Q(\xi^2, \mu) \\
&= -\overline{\xi}(-4)\xi(4) \cdot \mathbf{j}_Q(\xi, \xi) - \overline{\xi}^2(-4)\xi^2(4) \cdot \mathbf{j}_Q(\xi^2, \xi^2) \\
&= -\xi(-1) \cdot \mathbf{j}_Q(\xi, \xi) - \xi^2(-1) \cdot \mathbf{j}_Q(\xi^2, \xi^2).
\end{aligned}$$

Autrement dit, on vient de montrer que $A(\infty, Q) = \mathbf{j}_Q(\xi, \xi, \xi) + \mathbf{j}_Q(\xi^2, \xi^2, \xi^2)$. Par suite, on obtient

$$\begin{aligned}
\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_Q)} A(\tau, Q) &= A(\infty, Q) - \sum_{\substack{\chi^d = \mathbf{1} \\ \chi \neq \mathbf{1}}} \mathbf{j}_Q(\chi, \chi, \chi) \\
&= A(\infty, Q) - \mathbf{j}_Q(\xi, \xi, \xi) - \mathbf{j}_Q(\xi^2, \xi^2, \xi^2) - \sum_{\substack{\chi^d = \mathbf{1} \\ \chi \neq \mathbf{1}, \xi, \xi^2}} \mathbf{j}_Q(\chi, \chi, \chi) \\
&= 0 - \sum_{\substack{\chi^d = \mathbf{1} \\ \chi \neq \mathbf{1}, \xi, \xi^2}} \mathbf{j}_Q(\chi, \chi, \chi) = -\sum_{\chi \in Z(d, Q)} \mathbf{j}_Q(\chi, \chi, \chi).
\end{aligned}$$

– Ou bien $3 \nmid q - 1$ et l'application $x \mapsto x^3$ est une bijection $\mathbb{F}_Q^\times \to \mathbb{F}_Q^\times$ qui se prolonge en une bijection $\psi : \mathbb{F}_Q \to \mathbb{F}_Q$. On peut donc « réindexer » la somme donnant $A(\infty, Q)$:

$$-A(\infty, Q) = \sum_{x \in \mathbb{F}_Q} \mu(x^3 + 1/4) = \sum_{x \in \mathbb{F}_Q} \mu(\psi(x) + 1/4) = \sum_{z \in \mathbb{F}_Q} \mu(z + 1/4) = 0,$$

car μ n'est pas le caractère trivial. D'autre part, lorsque $3 \nmid q - 1$ aucun caractère non trivial χ de $\mathbb{F}_Q^\times$ ne vérifie $\chi^3 = \mathbf{1}$. Ainsi, $Z(d, Q)$ est formé dans ce cas des caractères non triviaux dont la puissance d-ième est triviale. On a donc

$$\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_Q)} A(\tau, Q) = A(\infty, Q) - \sum_{\substack{\chi^d = \mathbf{1} \\ \chi \neq \mathbf{1}}} \mathbf{j}_Q(\chi, \chi, \chi) = 0 - \sum_{\chi \in Z(d, Q)} \mathbf{j}_Q(\chi, \chi, \chi).$$

Nous avons démontré l'identité recherchée dans tous les cas. Ce qui conclut la preuve de la Proposition. □

Remarque 7.2.5. Si d divise $Q - 1$, cette Proposition conclut la preuve du Théorème 7.2.1. En effet, dans cette situation $\mathcal{O}_q^{(3)}(d) = \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ si d n'est pas divisible par 3 (resp. $\mathcal{O}_q^{(3)}(d) = \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/3, 2d/3\}$ si d est divisible par 3). On peut fixer un caractère $\chi_0 : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ d'ordre exactement d et on a

$$L(E_d/K, T) = \prod_j \Big(1 - \mathbf{j}_q(\chi_0^j, \chi_0^j, \chi_0^j) \cdot T\Big),$$

où j parcourt $[\![1, d-1]\!]$ en évitant (le cas échéant) $d/3$ et $2d/3$.

7.2.2 Preuve du Lemme 7.2.4

Donnons à présent la preuve du Lemme 7.2.4. Rappelons que, pour tout caractère $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$, on a posé

$$E_Q(\chi) = \sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q} \chi(z)\mu(x^3+x^2-8zx+16z^2)$$

et que l'on souhaite écrire $E_Q(\chi)$ comme une somme de Jacobi si χ n'est pas trivial.

Démonstration. Commençons par effectuer le changement de variables « $z = 4z'$ » dans la somme extérieure puis séparons le terme « $x = 0$ » des autres :

$$\begin{aligned}
E_Q(\chi) &= \sum_{z\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q} \chi(z)\mu(x^3+x^2-8zx+16z^2) = \overline{\chi}(4)\cdot\sum_{z'\in\mathbb{F}_Q}\sum_{x\in\mathbb{F}_Q}\chi(z')\mu(x^3+x^2-2z'x+z'^2)\\
&= \overline{\chi}(4)\cdot\sum_{z'\in\mathbb{F}_Q}\chi(z')\mu(z')^2 + \overline{\chi}(4)\cdot\sum_{x\neq 0}\sum_{z'\in\mathbb{F}_Q}\chi(z')\mu(x^3+x^2-2z'x+z'^2)\\
&= \overline{\chi}(4)\cdot\sum_{z'\neq 0}\chi(z') + \overline{\chi}(4)\cdot\sum_{x\neq 0}\sum_{z'\in\mathbb{F}_Q}\chi(z')\mu(x^3+x^2-2z'x+z'^2).
\end{aligned}$$

Pour $x \neq 0$ donné, on peut « réindexer » la somme sur $z' \in \mathbb{F}_Q$ en posant $y = z'/x - 1$ (c'est-à-dire $z' = x(y+1)$) :

$$\begin{aligned}
\sum_{z'\in\mathbb{F}_Q}\chi(z')\mu(x^3+x^2-2z'x+z'^2) &= \sum_{y\in\mathbb{F}_Q}\chi(x(y+1))\mu(x^3+x^2-2x^2(y+1)+x^2(y+1)^2)\\
&= \chi(x)\sum_{y\in\mathbb{F}_Q}\chi(y+1)\mu(x)^2\mu(x+1-2(y+1)+(y+1)^2)\\
&= \chi(x)\sum_{y\in\mathbb{F}_Q}\chi(y+1)\mu(x+y^2).
\end{aligned}$$

Ainsi, en sommant la dernière identité sur les $x \neq 0$, on tire que

$$\begin{aligned}
E_Q(\chi) &= \overline{\chi}(4)\cdot\sum_{z'\neq 0}\chi(z') + \overline{\chi}(4)\cdot\sum_{x\neq 0}\chi(x)\sum_{y\in\mathbb{F}_Q}\chi(y+1)\mu(x+y^2)\\
&= \overline{\chi}(4)\cdot\sum_{z'\neq 0}\chi(z') + \overline{\chi}(4)\cdot\sum_{y\in\mathbb{F}_Q}\chi(y+1)\left(\sum_{x\neq 0}\chi(x)\mu(x+y^2)\right).
\end{aligned}$$

Si χ est le caractère trivial, on a donc

$$\begin{aligned}
E_Q(\mathbf{1}) &= \sum_{z'\neq 0}1 + \sum_{y\in\mathbb{F}_Q}\left(\sum_{x\neq 0}\mu(x+y^2)\right) = Q-1+\sum_{y\in\mathbb{F}_Q}\left(\sum_{x\in\mathbb{F}_Q}\mu(x+y^2)-\mu(y^2)\right)\\
&= Q-1+\sum_{y\in\mathbb{F}_Q}\big(0-\mu(y^2)\big) = Q-1-\sum_{y\in\mathbb{F}_Q}\mu(y^2)\\
&= Q-1-\sum_{y\neq 0}1 = Q-1-(Q-1) = 0.
\end{aligned}$$

On suppose à présent que χ n'est pas trivial. Alors $\sum_{z\neq 0}\chi(z) = 0$ et $\chi(0) = 0$. Ce qui nous permet d'écrire

$$E_Q(\chi) = 0 + \overline{\chi}(4)\cdot\sum_{y\in\mathbb{F}_Q}\chi(y+1)\left(\sum_{x\in\mathbb{F}_Q}\chi(x)\mu(x+y^2)\right).$$

Mais, pour tout $y \in \mathbb{F}_Q$, en utilisant à nouveau le Lemme 2.2.1, on obtient que

$$\begin{aligned}
\sum_{x\in\mathbb{F}_Q}\chi(x)\mu(x+y^2) &= \sum_{x\in\mathbb{F}_Q}\chi(x)\big(1+\mu(x+y^2)\big) = \sum_{x\in\mathbb{F}_Q}\chi(x)\cdot\#\left\{t\in\mathbb{F}_Q \;\middle|\; t^2 = x+y^2\right\}\\
&= \sum_{x\in\mathbb{F}_Q}\chi(x)\cdot\#\left\{t\in\mathbb{F}_Q \;\middle|\; x = t^2-y^2\right\} = \sum_{t\in\mathbb{F}_Q}\chi(t^2-y^2)\\
&= \sum_{t\in\mathbb{F}_Q}\chi(t-y)\chi(t+y).
\end{aligned}$$

Ce qui nous permet de transformer la somme $E_Q(\chi)$ en

$$E_Q(\chi) = \overline{\chi}(4) \cdot \sum_{y \in \mathbb{F}_Q} \chi(y+1) \left(\sum_{x \neq 0} \chi(x) \mu(x + y^2) \right) = \overline{\chi}(4) \cdot \sum_{y \in \mathbb{F}_Q} \chi(y+1) \sum_{t \in \mathbb{F}_Q} \chi(t-y)\chi(t+y)$$
$$= \overline{\chi}(4) \cdot \sum_{y \in \mathbb{F}_Q} \sum_{t \in \mathbb{F}_Q} \chi(t-y)\chi(t+y)\chi(y+1).$$

Réindexons enfin la double somme en posant $(x_1, x_2, x_3) = \left(\frac{t-y}{-2}, \frac{t+y}{-2}, y+1 \right)$ de sorte que

$$x_1 + x_2 + x_3 = 1, \quad t - y = -2x_1, \quad t + y = -2x_2, \quad y + 1 = x_3.$$

On trouve que

$$\sum_{y \in \mathbb{F}_Q} \sum_{t \in \mathbb{F}_Q} \chi(t-y)\chi(t+y)\chi(y+1) = \sum_{x_1+x_2+x_3=1} \chi(-2x_1)\chi(-2x_2)\chi(x_3)$$
$$= \chi(4) \cdot \sum_{x_1+x_2+x_3} \chi(x_1)\chi(x_2)\chi(x_3)$$
$$= \chi(4) \cdot \mathbf{j}_Q(\chi, \chi, \chi).$$

Ce qui prouve que $E_Q(\chi) = \mathbf{j}_Q(\chi, \chi, \chi)$ si χ n'est pas trivial. □

7.2.3 Réindexation des caractères

Par définition de la fonction L de E_d/K (voir Lemme 1.3.15), on a

$$\log L\big(E_d/K, T\big) = \sum_{n=1}^{\infty} \left(\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau, q^n) \right) \frac{T^n}{n}.$$

À l'aide de la Proposition 7.2.3, on peut maintenant exprimer la somme interne : pour toute extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, on a

$$\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau, q^n) = - \sum_{\chi \in Z(d, q^n)} \mathbf{j}_q(\chi, \chi, \chi),$$

où l'ensemble de caractères $Z(d, q^n)$ est défini dans l'énoncé de la Proposition. Nous avons donc démontré que

$$-\log L\big(E_d/K, T\big) = \sum_{n=1}^{\infty} \left(\sum_{\chi \in Z(d, q^n)} \mathbf{j}_q(\chi, \chi, \chi) \right) \frac{T^n}{n}.$$

On reconnaît une fois de plus la situation étudiée à la Section 2.1.4. Pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$ et tout caractère χ de $\mathbb{F}_Q$, on pose donc

$$\sigma(\chi, Q) = \mathbf{j}_Q(\chi, \chi, \chi).$$

Des vérifications assez similaires à celles que l'on a effectuées à la Section 5.2.3 montrent que la donnée des $\sigma(\chi, Q)$ vérifie les hypothèses de la Proposition 2.1.15 (avec $K = 1$ et $\ell = 3$). On en déduit que

$$\log L\big(E_d/K, T\big) = \sum_{m \in \mathcal{O}_q^{(3)}(d)} \log \left(1 - \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) \cdot T^{u(m)} \right),$$

où $\mathcal{O}_q^{(3)}(d)$ désigne l'ensemble des orbites de m de $\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ sous l'action de q par multiplication, duquel on a retiré les orbites $\{d/3\}$ et $\{2d/3\}$ si 3 divise d :

$$\mathcal{O}_q^{(3)}(d) = \begin{cases} \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/3, 2d/3\}\big) \big/ \langle q \bmod d \rangle & \text{si } 3 \mid d \\ \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\big) \big/ \langle q \bmod d \rangle & \text{si } 3 \nmid d. \end{cases}$$

On en conclut que

$$L\big(E_d/K, T\big) = \prod_{m \in \mathcal{O}_q^{(3)}(d)} \left(1 - \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) \cdot T^{u(m)} \right).$$

Nous avons donc terminé la preuve du Théorème 7.2.1. On constate au passage que l'expression de $L\big(E_d/K, T\big)$ obtenue est bien un polynôme en T, de bon degré (*cf.* (7.3)).

7.3 Rang et valeur spéciale

Maintenant que nous disposons d'une expression assez explicite de la fonction L des courbes E_d/K, nous pouvons étudier leur rang (analytique) et la valeur spéciale de leur fonction L en $s = 1$.

7.3.1 Conjecture de Birch et Swinnerton-Dyer

La courbe E_d/K est donnée (en coordonnées affines) comme l'ensemble des zéros d'un polynôme qui est somme de quatre monômes. Pour démontrer que E_d vérifie les conjectures de Birch et Swinnerton-Dyer, nous appliquons donc le résultat de Shioda (Théorème 1.4.15 à la Section 1.4.4).

Théorème 7.3.1 (Shioda)**.** *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $K = \mathbb{F}_q(t)$. Pour tout entier $d \geqslant 2$, premier à p, on considère la courbe E_d sur K, dont un modèle affine est*

$$Y^2 + XY - t^d Y = X^3.$$

La courbe elliptique E_d/K vérifie les conjectures de Birch et Swinnerton-Dyer (Conjecture 1.4.1). En particulier, son groupe de Tate-Shafarevich $Ш(E_d/K)$ est fini et le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ a un sens.

Démonstration. Soit d un entier premier à p et $K = \mathbb{F}_q(t)$. On définit $g \in \mathbb{F}_q[t, X, Y]$ par

$$g(t, X, Y) := Y^2 + XY - t^d Y - X^3 = 1 \cdot t^0 XY^2 + 1 \cdot t^0 XY - 1 \cdot t^d X^0 Y - 1 \cdot t^0 X^3 Y^0.$$

Le polynôme g est une somme de quatre monômes non nuls. Montrons qu'il satisfait la condition de Shioda : on associe à g la matrice de ses exposants

$$A_g = \begin{bmatrix} 0 & 0 & 2 & -1 \\ 0 & 1 & 1 & -1 \\ d & 0 & 1 & -1-d \\ 0 & 3 & 0 & -2 \end{bmatrix},$$

dont le déterminant est $\det A_g = d$. En particulier, on a $d(g) = |\det A_g| \not\equiv 0 \bmod p$ (car d est premier à p) et g satisfait la condition de Shioda. Comme la (partie affine de la) courbe E_d/K est définie par l'annulation de g dans $\mathbb{A}^2/K$, elle vérifie la conjecture de Birch et Swinnerton-Dyer (Théorème 1.4.15). □

7.3.2 Expressions du rang et de la valeur spéciale

En combinant l'expression explicite de la fonction L avec la conjecture de Birch et Swinnerton-Dyer, nous pouvons exprimer le rang de $E_d(K)$ et la valeur spéciale $L^*(E_d/K, 1)$.

Pour tout entier $d \geqslant 2$, premier à la caractéristique de $K = \mathbb{F}_q(t)$, nous avons démontré (Théorème 7.2.1) que la fonction L de la courbe E_d (donnée par (7.1)) s'écrit sous la forme d'un produit :

$$L\big(E_d/K, T\big) = \prod_{m \in \mathcal{O}_q^{(3)}(d)} \Big(1 - \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) \cdot T^{u(m)}\Big).$$

Comme nous sommes intéressés par l'ordre d'annulation de ce produit en $T = q^{-1}$, nous posons la définition suivante :

Définition 7.3.2. Pour tout entier $d \geqslant 2$, premier à q, on pose

$$\mathcal{Z}_q(d) := \Big\{ m \in \mathcal{O}_q^{(3)}(d) \;\Big|\; \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) = q^{u(m)} \Big\},$$

ainsi que son complémentaire $\mathcal{V}_q^*(d) := \mathcal{O}_q^{(3)}(d) \smallsetminus \mathcal{Z}_q(d)$.

Démontrons alors la

Proposition 7.3.3. *Soit $d \geqslant 2$ un entier premier à q et $K = \mathbb{F}_q(t)$. Le rang du groupe de Mordell-Weil $E_d(K)$ de la courbe E_d donnée par (7.1) s'écrit*

$$\operatorname{rang} E_d(L) = \#\mathcal{Z}_q(d) = \# \Big\{ m \in \mathcal{O}_q^{(3)}(d) \;\Big|\; \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) = q^{u(m)} \Big\}.$$

Démonstration. Comme la conjecture « faible » de Birch et Swinnerton-Dyer est vraie pour E_d (*cf.* Théorème 7.3.1), les rangs algébrique et analytique de E_d sont égaux, *i.e.*

$$\operatorname{rang} E_d(K) = \operatorname{ord}_{T=q^{-1}} L\big(E_d/K, T\big).$$

On peut invoquer les outils de la Section 3.1 pour trouver l'expression annoncée du rang car la fonction $L(E_d/K, T)$ est un polynôme de forme convenable (avec $K = 1$). Plus précisément, si pour toute orbite $m \in \mathcal{O}_q^{(3)}(d)$ on pose $\omega(m) = \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m)$, le Lemme 3.1.4 (*cf.* Exemple 3.1.9) donne directement que

$$\operatorname{ord}_{T=q^{-1}} L\big(E_d/K, T\big) = \#\left\{m \in \mathcal{O}_q^{(3)}(d) \;\middle|\; \omega(m) = q^{u(m)}\right\} = \#\mathcal{Z}_q(d).$$

□

Proposition 7.3.4. *Avec les mêmes hypothèses et notations, la valeur spéciale $L^*\big(E_d/K, 1\big)$ de la fonction L associée à E_d/K s'écrit*

$$L^*\big(E_d/K, 1\big) = \prod_{m \in \mathcal{Z}_q(d)} u(m) \cdot \prod_{m \in \mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m)}{q^{u(m)}}\right). \tag{7.5}$$

Démonstration. Une bonne partie du calcul a été faite à la Section 3.1. Pour la durée de la preuve, notons $r = \operatorname{ord}_{T=q^{-1}} L(E_d/K, T) = \#\mathcal{Z}_q(d)$. Pour toute orbite $m \in \mathcal{O}_q^{(3)}(d)$, on pose $g_m(T) = 1 - \omega(m)T^{u(m)}$. Alors $L(E_d/K, T) = \prod_m g_m(T)$; et la Proposition précédente donne :

$$\frac{L\big(E_d/K, T\big)}{(1-qT)^r} = \frac{L\big(E_d/K, T\big)}{(1-qT)^{\#\mathcal{Z}_q(d)}} = \prod_{m \in \mathcal{Z}_q(d)} \frac{g_m(T)}{1-qT} \cdot \prod_{m \in \mathcal{V}_q^*(d)} g_m(T).$$

Mais alors, pour toute $m \in \mathcal{Z}_q(d)$ l'évaluation de $\frac{g_m(T)}{1-qT}$ en $T = q^{-1}$ donne $u(m)$ et pour toute $m \notin \mathcal{Z}_q(d)$, l'évaluation de $g_m(T)$ en $T = q^{-1}$ donne $1 - \omega(m) \cdot q^{-u(m)}$. Le produit de ces évaluations donne la valeur spéciale $L^*(E_d/K, 1)$ et on trouve l'expression annoncée de celle-ci. □

D'autre part, comme la conjecture « forte » de Birch et Swinnerton-Dyer est vraie pour la courbe E_d/K, on a

$$L^*\big(E_d/K, 1\big) = \frac{\#Ш\big(E_d/K\big) \cdot \operatorname{Reg}\big(E_d/K\big)}{\big(\#E_d(K)_{\mathrm{tors}}\big)^2} \cdot \mathcal{T}am\big(E_d/K\big) \cdot \frac{q}{H\big(E_d/K\big)}.$$

Cette dernière égalité montre que le produit (7.5) de nombres algébriques est en fait rationnel et strictement positif.

7.3.3 Rang non borné

Dans cette section, nous démontrons rapidement un résultat de « rang non borné » sur $K = \mathbb{F}_q(t)$ pour la famille des courbes E_d. Il s'agit d'un cas particulier du théorème général de Ulmer [Ulm07b, Theorem 4.7] (voir également [Ulm11, Lecture 4, Theorem 3.1.1] et [Ber08, Theorem 4.2]) mais nous pouvons le prouver ici rapidement comme corollaire de la Proposition 7.3.3 et du Théorème de Shafarevich-Tate sur les sommes de Jacobi (Théorème 2.4.4).

Proposition 7.3.5. *Supposons que $\mathbb{F}_q$ est un corps fini de caractéristique $p \geqslant 5$. Lorsque d parcourt l'ensemble des entiers premier à p, le rang des groupes de Mordell-Weil $E_d(K)$ n'est pas borné :*

$$\limsup_{\operatorname{pgcd}(d,q)=1} \operatorname{rang} E_d\big(\mathbb{F}_q(t)\big) = +\infty.$$

Démonstration. Pour démontrer la Proposition, comme la conjecture de Birch et Swinnerton-Dyer est vraie pour toutes les courbes E_d/K (Théorème 7.3.1), il suffit de démontrer que

$$\limsup_{\operatorname{pgcd}(d,q)=1} \operatorname{ord}_{T=q^{-1}} L(E_d/K, T) = +\infty.$$

Pour tout entier $N \in \mathbb{N}^*$, posons $d_N = q^N + 1$. Le Lemme 2.4.1 montre que l'ordre de q modulo d_N vaut exactement $o_q(d_N) = 2N$.

Par ailleurs, comme par construction d_N divise q^N+1, on peut utiliser le Corollaire 2.4.6 du Théorème de Shafarevich-Tate (Théorème 2.4.4). On en déduit que, pour toute orbite $m \in \mathcal{O}_q^{(3)}(d_N)$, on a

$$\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) = q^{u(m)}.$$

Aves les notations introduites précédemment, on a donc $\mathcal{Z}_{d_N} = \mathcal{O}_q^{(3)}(d_N)$. Par conséquent, le rang de $E_{d_N}(K)$ vaut $\operatorname{ord}_{T=q^{-1}} L(E_d/K,T) = \#\mathcal{Z}_{d_N} = \#\mathcal{O}^{(3)}(d_N)$ (*cf.* Proposition 7.3.3). Il faut maintenant prouver une minoration de $\#\mathcal{O}_q^{(3)}(d_N)$: pour tout diviseur $d' > 3$ de d_N, on a $o_q(d') \leqslant o_q(d_N) = 2N$ et l'on en tire que

$$\#\mathcal{O}_q^{(3)}(d_N) = \sum_{\substack{d'\mid d_N \\ d'>3}} \frac{\phi(d')}{o_q(d')} \geqslant \frac{1}{o_q(d_N)} \cdot \sum_{\substack{d'\mid d_N \\ d'>3}} \phi(d') \geqslant \frac{d_N - \phi(2) - \phi(3)}{o_q(d_N)} = \frac{d_N-3}{2N}.$$

Mais, pour tout $N \geqslant 1$, on a $\log d_N = \log(q^N+1) \geqslant N \cdot \log q$. Il s'ensuit que

$$\operatorname{rang} E_{d_N}(K) \geqslant \frac{d_N-3}{2N} \geqslant \frac{\log q}{2}\frac{d_N-3}{\log d_N} \gg_q \frac{d_N}{\log d_N},$$

la constante implicite ne dépendant que de q. Il est alors clair que la quantité minorante tend vers $+\infty$ lorsque $N \to \infty$. C'est précisément ce qu'il fallait démontrer : le rang de $E_{d_N}(K)$ ne saurait être borné. □

7.4 Ratio de Brauer-Siegel des courbes E_d

Dans toute la suite de cette section, on fixe un corps fini $\mathbb{F}_q$ de caractéristique $p \geqslant 5$, on notera $K = \mathbb{F}_q(t)$ et, pour tout entier $d \geqslant 2$ premier à q, on considère la courbe elliptique E_d/K donnée par le modèle (7.1). Nous démontrons ici le résultat principal de ce Chapitre, à savoir que le ratio de Brauer-Siegel des courbes E_d admet une limite et que celle-ci vaut 1.

7.4.1 Majoration de la valeur spéciale

À partir de l'expression (7.5), nous prouvons d'abord une majoration de la valeur spéciale $L^*(E_d/K,1)$ en termes de la hauteur $H\big(E_d/K\big)$ de E_d. Précisément :

Proposition 7.4.1. *Pour tout entier $d \geqslant 2$ premier à q, la valeur spéciale $L^*(E_d/K,1)$ de la fonction L associée à la courbe E_d définie sur K par* (7.1) *admet la majoration asymptotique suivante :*

$$\frac{\log L^*\big(E_d/K,1\big)}{\log H\big(E_d/K\big)} \leqslant 0 + o(1) \qquad (d \to \infty).$$

Cette majoration est en fait une conséquence immédiate de [HP16, Theorem 7.5], qui donne une telle majoration pour toute variété abélienne A/K. Cependant, notre preuve est élémentaire et explicite : nous prouvons en fait que

$$\frac{\log L^*\big(E_d/K,1\big)}{\log H\big(E_d/K\big)} \leqslant c' \cdot \frac{\log\log d}{\log d}, \qquad (d \to \infty)$$

où $c' > 0$ est une constante explicite et absolue, que l'on peut choisir $c' \leqslant 90$.

Démonstration. Il s'agit d'appliquer les résultats de la Section 3.1 à $L\big(E_d/K,T\big)$, ce qu'il est loisible de faire. Plus précisément, d'après la Proposition 7.3.4, la valeur spéciale à étudier est le produit :

$$L^*\big(E_d/K,1\big) = \prod_{m\in\mathcal{Z}_q(d)} u(m) \cdot \prod_{m\in\mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m,\mathbf{t}_m)}{q^{u(m)}}\right),$$

les produits portant sur les ensembles $\mathcal{Z}_q(d)$ et $\mathcal{V}_q^*(d)$ définis à la Section 7.3.2. On note pour simplifier $L(T) = L\big(E_d/K,T\big)$ la fonction L de la courbe E_d/K : c'est un polynôme de la forme étudiée à la Section 3.1. La Proposition 3.1.8 donne alors l'existence d'une constante absolue $C > 0$ (qu'on peut choisir $\leqslant 5$) telle que

$$L^*\big(E_d/K,1\big) \leqslant 3C \cdot \log q \cdot \frac{d \cdot \log\log d}{\log d}.$$

Se rappelant que $H\big(E_d/K\big) = q^{\lfloor \frac{d+2}{3} \rfloor}$, nous en déduisons que

$$\begin{aligned}\frac{\log L^*\big(E_d/K,1\big)}{\log H\big(E_d/K\big)} &\leqslant 3C \cdot \log q \cdot \frac{1}{\lfloor \frac{d+2}{3} \rfloor \cdot \log q} \cdot \frac{d \cdot \log\log d}{\log d} \leqslant 3C \cdot \frac{3}{d-1} \cdot \frac{d \cdot \log\log d}{\log d} \\ &\leqslant 18C \cdot \frac{\log\log d}{\log d} = o(1).\end{aligned}$$

Ce qui termine la preuve de la Proposition et de sa version explicite mentionnée ci-dessus. □

7.4.2 Minoration de la valeur spéciale

Démontrons à présent une minoration de la valeur spéciale $L^*(E_d/K,1)$.

Proposition 7.4.2. *Pour un entier $d \geqslant 2$ premier à q, la valeur spéciale $L^*(E_d/K,1)$ de la fonction L associée à la courbe elliptique E_d définie sur K par le modèle*(7.1) *admet la minoration suivante :*

$$\frac{\log L^*\big(E_d/K,1\big)}{\log H\big(E_d/K\big)} \geqslant 0 + o(1) \qquad (d \to \infty).$$

Comme dans les chapitres précédents, la minoration de la valeur spéciale est plus délicate que sa majoration. Ici, nous obtenons des résultats comparables aux précédents : à savoir que la valeur spéciale $L^*\big(E_d/K,1\big)$ est « asymptotiquement presque entière ».

Démonstration. La preuve de cette Proposition est très proche de la démonstration de la Proposition 5.4.3. Contentons-nous de détailler les points principaux de celle-ci. Dans un premier temps, on remarque que l'expression (7.5) fait intervenir un produit d'entiers $\prod_{m \in \mathcal{Z}_q(d)} u(m)$, dont le logarithme est positif. On a donc

$$\log L^*\big(E_d/K,1\big) \geqslant \log \prod_{m \in \mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m)}{q^{u(m)}}\right). \tag{7.6}$$

La quantité apparaissant dans le membre de droite est du type étudié à la Section 3.2. Si l'on pose $y(m) = \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m)$ pour toute orbite $m \in \mathcal{O}_q^{(3)}(d)$ et $\mathcal{M} = \mathcal{V}_q^*(d)$, cette donnée satisfait aux hypothèses (i), (ii) et (iii) de la Section 3.2 : les arguments sont strictement similaires à ceux de la Proposition 5.4.3.

Pour tout diviseur $d' > 3$ de d, on note $\mathfrak{p}'$ l'idéal premier de $\mathbb{Q}(\zeta_{d'})$ qui est en dessous de $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$ et on identifie le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_{d'})/\mathbb{Q})$ à $(\mathbb{Z}/d'\mathbb{Z})^\times$. Pour des raisons de compacité, on notera $G'_d = (\mathbb{Z}/d'\mathbb{Z})^\times$, $\langle p \rangle_{d'}$ et $\langle q \rangle_{d'}$ les sous-groupes de $G_{d'}$ engendrés par p et q respectivement. On peut alors définir

$$w'(d') := o_q(d') \cdot \sum_{m' \in G_{d'}/\langle q \rangle_{d'}} \max\left\{0, 1 - \frac{\mathrm{ord}_{\mathfrak{p}'}\, y\left(\frac{d}{d'}m'\right)}{o_q(d') \cdot [\mathbb{F}_q : \mathbb{F}_p]}\right\}.$$

Lorsque l'on applique le Théorème 3.2.2, on obtient la minoration

$$\log \prod_{m \in \mathcal{V}_q^*(d)} \left(1 - \frac{\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m)}{q^{u(m)}}\right) \geqslant -\log q \cdot \sum_{\substack{d' \mid d \\ d' > 3}} w'(d'). \tag{7.7}$$

On cherche alors à exprimer $w'(d')$ de façon explicite afin de le majorer. Définissons à cet effet une fonction en escaliers $F : [0,1] \to \mathbb{R}$ par

$$F(x) := \begin{cases} 2 & \text{si } x \in \left[0, \frac{1}{3}\right] \\ 1 & \text{si } x \in \left]\frac{1}{3}, \frac{2}{3}\right] \\ 0 & \text{si } x \in \left]\frac{2}{3}, 1\right]. \end{cases}$$

Un calcul presque identique à celui mené au Lemme 5.4.4 (lors de la preuve de la Proposition 5.4.3) conduit à

$$w'(d') = o_q(d') \cdot \sum_{m' \in G_{d'}/\langle q \rangle_{d'}} \max\left\{0, \int_0^1 F(t)\mathrm{d}t - \frac{1}{\#\langle p \rangle_{d'}} \sum_{\pi \in \langle p \rangle_{d'}} F\left(\left\{\frac{m'\pi}{d'}\right\}\right)\right\},$$

et ce, pour tout diviseur $d' > 3$ de d. On peut alors appliquer le Théorème 3.4.1 d'équidistribution comme au Lemme 5.4.5 et obtenir la majoration « forte »

$$\frac{w'(d')}{\phi(d')} \xrightarrow[d'\to\infty]{} 0, \tag{7.8}$$

qui implique (*cf.* Lemme 3.4.16) à son tour que

$$\frac{1}{d} \cdot \sum_{\substack{d'\mid d\\ d'>3}} w'(d') \xrightarrow[d\to\infty]{} 0. \tag{7.9}$$

On combine alors les minorations (7.6), (7.7) et (7.9), on trouve que

$$\frac{\log L^*\big(E_d/K,1\big)}{d} \geqslant -\log q \cdot o\big(1\big) \qquad (d\to\infty).$$

Il ne reste finalement qu'à remarquer que $\log H\big(E_d/K\big) \sim \frac{d}{3}\cdot\log q$ pour conclure la preuve. □

7.4.3 Lien entre valeur spéciale et ratio de Brauer-Siegel

Soit $d \geqslant 2$ un entier premier à q. Comme la courbe E_d vérifie la conjecture de Birch et Swinnerton-Dyer (Théorème 7.3.1), on peut utiliser la Proposition 1.6.4 pour relier le ratio de Brauer-Siegel $\mathfrak{Bs}(E_d/K)$ à la valeur spéciale de la fonction L de E_d : lorsque $H(E_d/K)\to\infty$, on a

$$\mathfrak{Bs}(E_d/K) = 1 + \frac{\log L^*\big(E_d/K,1\big)}{\log H\big(E_d/K\big)} + o(1). \tag{7.10}$$

Le terme « d'erreur » dans cette relation vient des bornes générales sur la torsion (Théorème 1.5.2) et sur le nombre de Tamagawa (Théorème 1.5.4).

Remarque 7.4.3. Ici, on connaît explicitement le nombre de Tamagawa $\mathcal{T}am(E_d/K)$ de la courbe E_d. On a en effet démontré (Proposition 7.1.3) que, pour tout entier $d\geqslant 2$ premier à q,

$$3d \leqslant \mathcal{T}am(E_d/K) \leqslant 9d$$

et que $H(E_d/K) = q^{\lfloor\frac{d+2}{3}\rfloor}$. Il existe donc deux constantes $c_1, c_2 > 0$ (ne dépendant que de q) telles que

$$c_1\cdot\frac{\log d}{d} \leqslant \frac{\log \mathcal{T}am(E_d/K)}{\log H\big(E_d/K\big)} \leqslant c_2\cdot\frac{\log d}{d}.$$

Nous retrouvons en particulier [HP16, Theorem 6.5] sous une forme explicite : on peut choisir $c_1 = 3/2\log q$ et $c_2 = 12/\log q$.

7.4.4 Analogue du théorème de Brauer-Siegel

Nous pouvons déduire des résultats précédents le théorème principal de ce chapitre :

Théorème 7.4.4. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p\geqslant 5$ et $K=\mathbb{F}_q(t)$. Pour tout entier $d\geqslant 2$, premier à q, on considère la courbe elliptique E_d définie sur K par le modèle affine :*

$$Y^2 + XY - t^dY = X^3.$$

Lorsque $H\big(E_d/K\big)\to+\infty$ (i.e. lorsque $d\to\infty$), le ratio de Brauer-Siegel $\mathfrak{Bs}\big(E_d/K\big)$ admet une limite et celle-ci vaut 1 :

$$\mathfrak{Bs}\big(E_d/K\big) \xrightarrow[\substack{\operatorname{pgcd}(d,q)=1\\ d\to+\infty}]{} 1.$$

En d'autres termes, on a

$$\log\big(\#Ш(E_d/K)\cdot\operatorname{Reg}(E_d/K)\big) \sim \log H(E_d/K) \quad (d\to\infty).$$

Démonstration. Partons de la relation (7.10) entre ratio de Brauer-Siegel et valeur spéciale :

$$\mathfrak{Bs}(E_d/K) = 1 + \frac{\log L^*\big(E_d/K, 1\big)}{\log H\big(E_d/K\big)} + o(1).$$

Nous avons démontré successivement que

$$\frac{\log L^*\big(E_d/K, 1\big)}{\log H\big(E_d/K\big)} \leqslant 0 + o(1) \qquad (d \to \infty)$$

à la Proposition 7.4.1, puis que

$$\frac{\log L^*\big(E_d/K, 1\big)}{\log H\big(E_d/K\big)} \geqslant 0 + o(1) \qquad (d \to \infty)$$

à la Proposition 7.4.2. On en déduit donc que

$$1 - o(1) \leqslant \mathfrak{Bs}(E_d/K) \leqslant 1 + o(1) \qquad (d \to \infty).$$

Ce qu'il fallait démontrer. □

8

Une famille issue des travaux de Berger

Dans ce chapitre, nous étudions la famille des courbes elliptiques $B_{a,d}$ définies sur $K = \mathbb{F}_q(t)$ par le modèle affine

$$B_{a,d} : \quad Y^2 + t^d XY - at^{2d}Y = X^3 - (a+1)t^d X^2 + at^{2d}X,$$

où $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et d est un entier premier à la caractéristique de K. Cette famille est l'un des exemples donnés par L. Berger dans [Ber08] pour illustrer sa construction de courbes elliptiques satisfaisant à la conjecture de Birch et Swinnerton-Dyer (*cf.* [Ber08, § 4.3, Example 6]).

Résumons les résultats que nous obtenons quant au ratio de Brauer-Siegel des courbes $B_{a,d}$ dans un théorème.

Théorème. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Pour tout $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et tout entier $d \geqslant 2$ premier à p, on considère la courbe elliptique $B_{a,d}$ définie sur K dont un modèle affine est*

$$Y^2 + t^d XY - at^{2d}Y = X^3 - (a+1)t^d X^2 + at^{2d}X.$$

Alors les conjectures de Birch et Swinnerton-Dyer sont vraies pour la courbe $B_{a,d}/K$. En particulier le groupe de Tate-Shafarevich $Ш(B_{a,d}/K)$ est fini et le ratio de Brauer-Siegel $\mathfrak{Bs}(B_{a,d}/K)$ a un sens. Pour tout $a \neq 0, 1$, lorsque $d \to \infty$, on a $H\big(B_{a,d}/K\big) \to \infty$ et

$$0 + o(1) \leqslant \mathfrak{Bs}(B_{a,d}/K) \leqslant 1 + o(1) \quad (d \to \infty).$$

En outre, dans le cas où $a = 1/2 \in \mathbb{F}_q \smallsetminus \{0,1\}$, lorsque d est impair et $d \to \infty$, on a

$$\mathfrak{Bs}\big(B_{1/2,d}/K\big) \xrightarrow[\substack{\mathrm{pgcd}(d,q)=1 \\ d \text{ impair},\ d\to\infty}]{} 1.$$

Autrement dit, pour d impair,

$$\log\big(\#Ш(B_{1/2,d}/K) \cdot \mathrm{Reg}(B_{1/2,d}/K)\big) \sim \log H\big(B_{1/2,d}/K\big) \sim \frac{d}{2}\log q \quad (d \to \infty).$$

Nous démontrons en outre un résultat nouveau quant aux rangs des groupes de Mordell-Weil $B_{a,d}(K)$ (voir Théorème 8.3.10 et Corollaire 8.3.13).

Théorème. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Dans la famille des courbes elliptiques $B_{a,d}/K$ (où $d \geqslant 2$ est premier à q et $a \in \mathbb{F}_q \smallsetminus \{0,1\}$), le rang $r_{a,d} = \mathrm{rang}\, B_{a,d}(K)$ n'est pas borné*

$$\limsup_{\substack{\mathrm{pgcd}(d,q)=1 \\ a \in \mathbb{F}_q \smallsetminus \{0,1\}}} \mathrm{rang}\, B_{a,d}(K) = +\infty.$$

Nous prouvons en fait le résultat plus précis suivant : le rang des courbes $B_{1/2,d}/K$ n'est pas borné lorsque d est un entier impair et premier à q. Ce théorème n'est pas une conséquence directe des résultats de D. Ulmer sur les courbes elliptiques de rangs non bornés (Voir [Ulm07b, Theorem 4.7]

cité dans [Ber08, Theorem 4.2]). Pour toute autre valeur de $a \in \mathbb{F}_q \smallsetminus \{0,1\}$, nous ne savons pas si le rang des courbes $B_{a,d}/K$ est borné ou non.

Les preuves de ces différentes assertions sont réparties dans ce chapitre comme suit. Dans la première section, nous définissons les courbes $B_{a,d}$ et calculons leur hauteur et conducteur (Proposition 8.1.5). Au passage, nous menons une analyse détaillée de la réduction de celles-ci (Proposition 8.1.4). Dans la deuxième section, nous explicitons la fonction L, notée $L\big(B_{a,d}/K, T\big) \in \mathbb{Z}[T]$, de la courbe $B_{a,d}$ par un calcul de sommes de caractères (Théorème 8.2.1). Le polynôme obtenu s'écrit en termes de sommes de Jacobi et de sommes de Legendre. C'est un résultat nouveau. Nous rappelons également pourquoi la conjecture de Birch et Swinnerton-Dyer est vérifiée par ces courbes elliptiques. La troisième section est dédiée à l'étude du rang de $B_{a,d}$ et à l'expression de la valeur spéciale $L^*\big(B_{a,d}/K, 1\big)$. Nous y démontrons entre autres l'assertion de « rang non borné » (Théorème 8.3.10 et Corollaire 8.3.13). Malheureusement, notre connaissance des sommes de Legendre $\boldsymbol{S}_q(\chi; b)$ est trop incomplète pour un paramètre $b \in \mathbb{F}_q$ quelconque. C'est pourquoi, à partir de la quatrième section, nous supposons que $b = 0$ (*i.e.* que $a = 1/2$) et que d est impair. Nous prouvons alors l'encadrement du ratio de Brauer-Siegel annoncé (Théorème 8.4.1).

8.1 Les courbes $B_{a,d}$, premières propriétés

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Soit aussi $a \in \mathbb{F}_q$, un paramètre qu'on suppose différent de 0 et 1. Pour tout entier d premier à p, on considère la courbe elliptique $B_{a,d}$ définie sur K par le modèle de Weierstrass affine suivant :

$$B_{a,d} : \quad Y^2 + t^d XY - at^{2d}Y = X^3 - (a+1)t^d X^2 + at^{2d}X. \tag{8.1}$$

Les coefficients de (8.1) permettent de calculer, à l'aide du formulaire [Sil09, III.1, p. 42] rappelé à la section 1.1.2, le discriminant de ce modèle :

$$\Delta = a^2(a-1)^2 t^{6d}(t^{2d} + 8(2a-1)t^d + 16).$$

Avec le même formulaire, on peut également calculer l'invariant j de $B_{a,d}/K$:

$$j(B_{a,d}/K) = \frac{(t^{2d} + 8(2a-1)t^d + 16(a^2-a+1))^3}{a^2(a-1)^2(t^{2d} + 8(2a-1)t^d + 16)}.$$

En particulier, comme $a \neq 0, 1$, le discriminant $\Delta \in K$ n'est pas nul, donc la courbe $B_{a,d}$ est lisse. De plus, l'examen du discriminant Δ de (8.1) montre que ce modèle est entier et minimal en toute place v de $\mathbb{P}^1$, sauf éventuellement en $v = 0$ et $v = \infty$.

Par ailleurs, on constate que l'invariant $j(B_{a,d}/K) \in K = \mathbb{F}_q(t)$ est une fraction rationnelle de degré $4d > 0$ en t : la courbe $B_{a,d}/K$ n'est donc pas isotriviale. D'autre part, il est assez clair que $j(B_{a,d}/K)$ n'est pas une puissance p-ième dans K, donc $j(B_{a,d}/K)$ est séparable.

Remarque 8.1.1. Noter une petite faute de frappe dans [Ber08, Section 4.4, Example 2] : le modèle de Weierstrass y est écrit « $y^2 + t^d xy - at^{2d}y = x^3 - (a+1)x^2 + at^{2d}x$ », ce qui n'est pas cohérent avec la construction de $B_{a,d}$. Voir la Section 8.2.4

Remarque 8.1.2. Comme la caractéristique p de $\mathbb{F}_q$ est $\geqslant 5$, l'élément $1/2 \in \mathbb{F}_q$ est différent de 0 et 1. Dans le cas particulier où $a = 1/2 \in \mathbb{F}_q$, le discriminant du modèle (8.1) de $B_{1/2,d}$ s'écrit simplement

$$\Delta = 2^{-4} t^{6d}(t^{2d} + 16),$$

et son invariant j vaut

$$j(B_{1/2,d}/K) = \frac{2^4(t^{2d} + 12)^3}{t^{2d} + 16}.$$

Le lecteur pourra facilement se convaincre que celui-ci est différent des invariants j des autres courbes étudiées dans cette thèse. En d'autres termes, la courbe $B_{1/2,d}/K$ n'est pas isomorphe (sur K) à l'une des courbes elliptiques étudiées dans les chapitres précédents.

8.1.1 Analyse de la mauvaise réduction

Avant d'entamer l'analyse de la mauvaise réduction, démontrons un Lemme à propos d'un des facteurs du discriminant Δ de $B_{a,d}$.

Lemme 8.1.3. *Soit $a \in \mathbb{F}_q$, qu'on suppose différent de 0 ou 1, et d un entier premier à q. On note*

$$Q_{a,d}(T) = T^{2d} + 8(2a-1)T^d + 16 \in \mathbb{F}_q[T].$$

Le polynôme $Q_{a,d}(T)$ admet $2d$ racines distinctes (nécessairement simples) et non nulles dans $\overline{\mathbb{F}_q}$.

Démonstration. Le discriminant δ_a du polynôme quadratique $q_a(U) = U^2 + 8(2a-1)U + 16 \in \mathbb{F}_q[T]$ vaut

$$\delta_a = 8^2(2a-1)^2 - 8^2 = 16^2 a(a-1).$$

Comme on a supposé $a \neq 0, 1$, ce discriminant δ_a est non nul et l'équation $q_a(u) = 0$ admet deux racines distinctes u_1, u_2 dans $\overline{\mathbb{F}_q}$. Ni u_1 ni u_2 ne peut être nulle car $q_a(0) = 16 \neq 0$. Chaque u_i admet donc d racines d-ièmes distinctes dans $\overline{\mathbb{F}_q}$ (car d est premier à q), on les note $t_{i,j}$ ($j = 0, \dots, d-1$). Pour tout $i \in \{1, 2\}$ et tout $j \in [\![0, d-1]\!]$, on a $Q_{a,d}(t_{i,j}) = q_a(u_i) = 0$. Ceci fournit $2d$ racines distinctes de $Q_{a,d}$, qui est de degré $2d$. □

Rappelons que le discriminant du modèle (8.1) de la courbe $B_{a,d}$ vaut

$$\Delta = a^2(a-1)^2 t^{6d}(t^{2d} + 8(2a-1)t^d + 16) = a^2(a-1)^2 t^{6d} Q_{a,d}(t).$$

Les places v de K en lesquelles $B_{a,d}$ a mauvaise réduction sont exactement celles qui divisent Δ. C'est-à-dire que $B_{a,d}$ a mauvaise réduction en $v = 0$, en $v = \infty$ et en les places v correspondant aux racines de $Q_{a,d}(T)$ dans $\overline{\mathbb{F}_q}$. Comme dans les chapitres précédents, nous appliquons l'algorithme de Tate pour avoir des informations plus précises sur ces réductions :

Proposition 8.1.4. *Soit $a \in \mathbb{F}_q \smallsetminus \{0, 1\}$ et $d \geqslant 2$ un entier premier à q. Notons $\pi : \mathcal{B}_{a,d} \to \mathbb{P}^1$ le modèle régulier minimal de $B_{a,d}/\mathbb{F}_q(t)$. Le morphisme π a les fibres singulières suivantes :*

- *au-dessus du point ∞, la fibre $\pi^{-1}(\infty)$ est de type $\mathbf{I}_{4d}$ déployée.*
- *au-dessus des points $\alpha \in \overline{\mathbb{F}_q}$ où $Q_{a,d}(\alpha) = 0$, la fibre $\pi^{-1}(\alpha)$ est de type $\mathbf{I}_1$.*
- *au-dessus du point $0 \in \mathbb{P}^1$, la fibre $\pi^{-1}(0)$ est de type $\begin{cases} \mathbf{I}_0 & \text{si } d \text{ est pair,} \\ \mathbf{I}_0^* & \text{si } d \text{ est impair.} \end{cases}$*

Démonstration. Les places v de K en lesquelles $B_{a,d}$ a mauvaise réduction sont celles qui divisent le discriminant Δ. En chacune de ces places, on applique l'algorithme de Tate [Tat75] tel qu'il est décrit dans [Sil94, Chap. 4, §9].

- En $v = \alpha$ où $\alpha \in \overline{\mathbb{F}_q}$ est une racine de $Q_{a,d}$, on a

  $$\operatorname{ord}_{v=\alpha} \Delta(B_{a,d}/K) = 1 \quad \text{et} \quad \operatorname{ord}_{v=\alpha} j(B_{a,d}/K) = -1.$$

  La réduction de $B_{a,d}$ en v est donc de type de Kodaira $\mathbf{I}_1$. La contribution locale au discriminant minimal est donc $\operatorname{ord}_{v=\alpha} \Delta_{\min}(B_{a,d}/K) = 1$, le conducteur de $B_{a,d}$ a un coefficient $\operatorname{ord}_{v=\alpha} \mathcal{N}(B_{a,d}/K) = 1$ et le nombre de Tamagawa local vaut $c_\alpha(B_{a,d}/K) = 1$.
- Pour étudier la fibre en $v = 0$, distinguons deux cas :
  - Si d est pair, on pose $c = d/2 \in \mathbb{N}^*$. Le changement de variables $(X, Y) = (t^{2c}x, t^{3c}y)$ dans le modèle (8.1) de $B_{a,d}$ conduit à l'équation

    $$y^2 + t^c xy - at^c y = x^3 - (a+1)x^2 + ax,$$

    dont le discriminant est $\Delta' = a^2(a-1)^2(t^{2d} + 8(2a-1)t^d + 16) \in \mathbb{F}_q[t]$. On a $\operatorname{ord}_{v=0} \Delta = 0$, donc la courbe $B_{a,d}$ a en fait bonne réduction en $t = 0$. La réduction de ce modèle en $t = 0$ s'écrit :

    $$y^2 = x^3 - (a+1)x^2 + ax = x(x-1)(x-a).$$

  - Si d est impair, on pose $c = (d-1)/2 \in \mathbb{N}^*$. Le changement de variables $(X, Y) = (t^{2c}x, t^{3c}y)$ dans le modèle (8.1) de $B_{a,d}$ conduit à l'équation

    $$y^2 + t^{(d+1)/2}xy - at^{(d+3)/2}y = x^3 - (a+1)tx^2 + at^2x$$

    dont le discriminant est $\Delta' = a^2(a-1)^2 t^6(t^{2d} + 8(2a-1)t^d + 16) \in \mathbb{F}_q[t]$. On a $\operatorname{ord}_{v=0} \Delta' = 6$ et $\operatorname{ord}_{v=0} j(E_d(a)/K) = 0$. L'algorithme de Tate s'arrête à l'Étape 6 : la réduction est de type $\mathbf{I}_0^*$. Cette fibre donne donc une contribution $\operatorname{ord}_{v=0} \Delta_{\min}(B_{a,d}/K) = 6$ au discriminant minimal, une contribution $\operatorname{ord}_{v=0} \mathcal{N}(B_{a,d}/K) = 2$ au conducteur. Il reste à calculer le nombre de Tamagawa local en 0 : avec les notations de [Sil94, Chap. 4, §9, p. 367],

    $$c_v(B_{a,d}/K) = 1 + \#\left\{\beta \in \mathbb{F}_v \;\middle|\; \beta^3 - (a+1)\beta^2 + a\beta = 0\right\} = 4.$$

    Le modèle ci-dessus se réduit modulo $t = 0$ en $y^2 = x^3$.

- Enfin, pour étudier la fibre en $v = \infty$, on effectue le changement $u = 1/t$ dans le modèle (8.1) de $B_{a,d}$. Ceci nous conduit à

$$Y^2 + XY - au^dY = X^3 - (a+1)u^dX^2 + au^{2d}X, \tag{8.2}$$

dont le discriminant est $\Delta' = a^2(a-1)^2u^{4d}(16u^2 + 8(2a-1)u + 1)$ et l'invariant j s'écrit

$$j(B_{a,d}/K) = \frac{(16(a^2-a+1)u^{2d} + 8(2a-1)u^d + 1)^3}{a^2(a-1)^2u^{4d}(16u^{2d} + 8(2a-1)u^d + 1)}.$$

En particulier $\operatorname{ord}_{v=\infty} \Delta(B_{a,d}/K) = \operatorname{ord}_{u=0} \Delta' = 4d$ et $\operatorname{ord}_{u=0} j(B_{a,d}/K) = -4d$. L'algorithme de Tate s'arrête à l'Étape 1 : la courbe $B_{a,d}/K$ a réduction de type $\mathbf{I}_{4d}$ en $t = \infty$. La place $v = \infty$ contribue pour $\operatorname{ord}_{v=\infty} \Delta_{\min}(B_{a,d}/K) = 4d$ au discriminant minimal et pour $\operatorname{ord}_{v=\infty} \mathcal{N}(B_{a,d}/K) = 1$ au conducteur de $B_{a,d}$. Par ailleurs, les tangentes à la courbe réduite en $u = 0$ (dans le modèle (8.2)), donnée par

$$Y^2 + XY = X^3,$$

en le point singulier $(0,0)$ sont définies sur $\mathbb{F}_q$: la réduction est donc déployée et $c_v(B_{a,d}/K) = 4d$.

□

Résumons cette analyse dans un tableau :

Place	Type de réduction	$\operatorname{ord}_v \Delta_{\min}(B_{a,d}/K)$	$\operatorname{ord}_v \mathcal{N}(B_{a,d}/K)$	$c_v(B_{a,d}/K)$
$v = 0$	$\mathbf{I}_0$ si d pair	0	0	1
	$\mathbf{I}_0^*$ si d impair	6	2	4
$v = \alpha$ $(Q_a(\alpha) = 0)$	$\mathbf{I}_1$	1	1	1
$v = \infty$	$\mathbf{I}_{4d}$ déployée	$4d$	1	$4d$

Dans ce tableau, pour toute place v de $\mathbb{P}^1$, on a noté $\operatorname{ord}_v \Delta_{\min}(B_{a,d}/K)$ la valuation en v du discriminant minimal de $B_{a,d}$, $\operatorname{ord}_v \mathcal{N}(B_{a,d}/K)$ la valuation du conducteur de $B_{a,d}$ et $c_v(B_{a,d}/K)$ le nombre de Tamagawa local en v.

8.1.2 Hauteur et conducteur

Grâce à l'analyse des fibres de mauvaise réduction de $B_{a,d}/K$ effectuée ci-dessus, on peut calculer sa hauteur et son conducteur.

Proposition 8.1.5. *Soit $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et un entier $d \geqslant 2$ premier à q. Soit alors $B_{a,d}$ la courbe elliptique sur $K = \mathbb{F}_q(t)$ donnée par le modèle* (8.1)*. Alors sa hauteur différentielle vaut*

$$H\big(B_{a,d}/K\big) = q^{\lfloor \frac{d+1}{2} \rfloor}.$$

De plus, on a

$$\deg \mathcal{N}\big(B_{a,d}/K\big) = \begin{cases} 2d+1 & \text{si } d \text{ pair} \\ 2d+3 & \text{si } d \text{ impair.} \end{cases}$$

Démonstration. On reprend les informations obtenues à la Proposition précédente et rappelées dans le tableau ci-dessus. Pour toute place v de K, on note $\mathbb{F}_v$ son corps résiduel et $d_v = [\mathbb{F}_v : \mathbb{F}_q]$ son degré. On obtient, en notant simplement $\Delta_{\min} = \Delta_{\min}(B_{a,d}/K)$,

$$\begin{aligned} \deg \Delta_{\min} &= \operatorname{ord}_0 \Delta_{\min} \cdot d_0 + \sum_{\substack{\alpha \in \overline{\mathbb{F}_q} \\ Q_{a,d}(\alpha)=0}} \operatorname{ord}_\alpha \Delta_{\min} \cdot d_\alpha + \operatorname{ord}_\infty \Delta_{\min} \cdot d_\infty \\ &= \operatorname{ord}_0 \Delta_{\min} \cdot 1 + \sum_{\substack{\alpha \in \overline{\mathbb{F}_q} \\ Q_{a,d}(\alpha)=0}} d_\alpha + 4d \cdot 1 \\ &= \operatorname{ord}_{v=0} \Delta_{\min} + \deg Q_{a,d} + 4d = \begin{cases} 6d & \text{si } d \text{ est pair} \\ 6(d+1) & \text{si } d \text{ est impair.} \end{cases} \end{aligned}$$

La valeur de la hauteur différentielle $H\big(B_{a,d}/K\big)$ suit alors immédiatement, par définition de celle-ci. Un calcul très similaire conduit à l'expression voulue de $\deg \mathcal{N}\big(B_{a,d}/K\big)$. □

Remarque 8.1.6. Comme la courbe $B_{a,d}$ n'est pas isotriviale, sa fonction L est un polynôme à coefficients entiers. A partir du degré du conducteur, grâce à la formule de Grothendieck-Ogg-Raynaud (Theorème 1.3.11), on peut calculer le degré de celui-ci :

$$\deg L\big(B_{a,d}/K,T\big) = \deg \mathcal{N}\big(B_{a,d}/K\big) + 4g(\mathbb{P}^1) - 4 = \begin{cases} 2d-3 & \text{si } d \text{ pair} \\ 2d-1 & \text{si } d \text{ impair.} \end{cases}$$

Remarque 8.1.7. Il est remarquable que ces invariants sont indépendants de la valeur du paramètre $a \in \mathbb{F}_q \smallsetminus \{0,1\}$.

8.1.3 Nombre de Tamagawa

De la Proposition 8.1.4, on déduit également le nombre de Tamagawa de la courbe $B_{a,d}$.

Proposition 8.1.8. *Soit $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et un entier $d \geqslant 2$ premier à q. La courbe $B_{a,d}/K$ a pour nombre de Tamagawa « global »*

$$\mathcal{T}am\big(B_{a,d}/K\big) = 4^{\varepsilon(d)} \cdot 4d,$$

où $\varepsilon(d) = 0$ ou 1 est donné par $d \equiv \varepsilon(d) \bmod 2$.

Démonstration. On reprend à nouveau les informations obtenues durant la preuve de la Proposition 8.1.4 et compilées dans le tableau qui la suit : on a

$$\mathcal{T}am(B_{a,d}/K) = \prod_{v|\Delta_{\min}} c_v(B_{a,d}/K) = 4^{\varepsilon(d)} \cdot 1 \cdot 4d,$$

avec $\varepsilon(d)$ valant 0 (resp. $\varepsilon(d) = 1$) si d est pair (resp. impair). □

Remarque 8.1.9. En particulier, on remarque que

$$\frac{\log \mathcal{T}am\big(B_{a,d}/K\big)}{\log H\big(B_{a,d}/K\big)} = \frac{(1+\varepsilon(d))\log 4}{\log H\big(B_{a,d}/K\big)} + \frac{\log d}{\log H\big(B_{a,d}/K\big)},$$

avec $\log H\big(B_{a,d}/K\big) = \left\lfloor \frac{d+1}{2} \right\rfloor \cdot \log q \geqslant \frac{\log q}{2} \cdot d$. D'où, pour $d \geqslant 16$,

$$\frac{\log \mathcal{T}am\big(B_{a,d}/K\big)}{\log H\big(B_{a,d}/K\big)} \leqslant \frac{4}{\log q} \cdot \frac{\log d}{d} \xrightarrow[d\to\infty]{} 0.$$

On retrouve donc le Théorème 1.5.4 dans notre cas particulier.

8.2 Fonctions L des courbes $B_{a,d}$

Dans cette section, on calcule la fonction L des courbes $B_{a,d}$ sous une forme explicite. Pour ce faire, rappelons les notations introduites aux Sections 2.1.2 et 2.1.3 : on fixe un idéal premier $\overline{\mathfrak{P}} \subset \overline{\mathbb{Z}}$ au-dessus de p et on note $\mathbf{t} : \overline{\mathbb{F}_q}^\times \to \overline{\mathbb{Q}}^\times$ le caractère de Teichmüller associé. Pour tout entier $d \geqslant 2$, premier à q, on dispose alors d'une famille de caractères $\mathbf{t}_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ dont l'ordre divise d ($m \in [\![1, d-1]\!]$). Rappelons également (Théorème 2.2.21) que, pour tout $b \in \mathbb{F}_q \smallsetminus \{1,-1\}$ et tout caractère $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ sur une extension finie $\mathbb{F}_Q/\mathbb{F}_q$, il existe deux entiers algébriques $\alpha_b(\chi)$ et $\beta_b(\chi)$ (de module $\sqrt{Q}$) tels que

$$\boldsymbol{S}_Q(\chi; b) = -\sum_{x \in \mathbb{F}_Q} \chi(x)\mu_Q(x^2+2bx+1) = \alpha_b(\chi) + \beta_b(\chi).$$

Avec ces notations, nous démontrons :

Théorème 8.2.1. *Soit $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et $d \geqslant 2$, un entier premier à q. On pose $b = 1-2a \in \mathbb{F}_q \smallsetminus \{1,-1\}$. On considère à nouveau la courbe elliptique $B_{a,d}$ définie sur $K = \mathbb{F}_q(t)$ par l'équation* (8.1). *La fonction L de $B_{a,d}$ s'exprime sous la forme suivante :*

$$L\big(B_{a,d}/\mathbb{F}_q(t), T\big) = (1-qT) \cdot \prod_{m \in \mathcal{O}_q^{(2)}(d)} \Big(1 - \mathbf{J}'_m \cdot \alpha_b(\mathbf{t}_m) \cdot T^{u(m)}\Big)\Big(1 - \mathbf{J}'_m \cdot \beta_b(\mathbf{t}_m) \cdot T^{u(m)}\Big),$$

où, comme précédemment, $\mathcal{O}_q^{(2)}(d)$ désigne l'ensemble des orbites

$$\mathcal{O}_q^{(2)}(d) = \begin{cases} \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/2\}\big)/\langle q \bmod d\rangle & \text{si } d \text{ est pair,} \\ \big(\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}\big)/\langle q \bmod d\rangle & \text{si } d \text{ est impair,} \end{cases}$$

$u(m)$ est le cardinal de l'orbite $m \in \mathcal{O}_q^{(2)}(d)$ et, pour tout $m \in \mathcal{O}_q^{(2)}(d)$, on a posé

$$\mathbf{J}'_m = \mathbf{t}_m(-1) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)$$

et $\alpha_b(\mathbf{t}_m)$ et $\beta_b(\mathbf{t}_m)$ ont la même signification que ci-dessus.

Pour démontrer ce théorème, nous utilisons la définition de la fonction L comme produit eulérien et explicitons ses coefficients à l'aide de calculs élémentaires sur les sommes de caractères. Le point clé est l'identification de certaines sommes de caractères sous la forme d'un produit d'une somme de Jacobi et d'une somme de Legendre (Lemme 8.2.4). Le reste de la section est consacrée à la preuve du Théorème 8.2.1.

Remarque 8.2.2. Le degré de la fonction L de $B_{a,d}$ comme polynôme en T est cohérent avec le degré du conducteur (*cf.* Proposition 8.1.4) et la formule (1.8). Notons également que, pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$, on a

$$\begin{aligned}\Big(1 - \mathbf{J}'_m \cdot \alpha_b(\mathbf{t}_m) \cdot T^{u(m)}\Big)\Big(1 - \mathbf{J}'_m \cdot \beta_b(\mathbf{t}_m) \cdot T^{u(m)}\Big) \\ = 1 - \mathbf{J}'_m \cdot \boldsymbol{S}_{q^{u(m)}}(\mathbf{t}_m; b) \cdot T^{u(m)} + {\mathbf{J}'_m}^2 q^{u(m)} \cdot T^{2u(m)}.\end{aligned}$$

8.2.1 Comptage de points

On fixe pour toute la durée du calcul un élément $a \in \mathbb{F}_q \smallsetminus \{0, 1\}$ et un entier $d \geqslant 2$ premier à q, on écrit à nouveau $b = 1 - 2a \neq 1, -1$. Pour tout point $\tau \in \mathbb{P}^1(\overline{\mathbb{F}_q})$, on note v_τ la place de K lui correspondant et $\overline{(B_{a,d})}_\tau$ la réduction en v_τ d'un modèle minimal et entier en v_τ de $B_{a,d}$. La courbe $\overline{(B_{a,d})}_\tau$ est donc une cubique plane irréductible (et parfois singulière) sur le corps résiduel $\mathbb{F}_{v_\tau} = \mathbb{F}_q(\tau)$.

Pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$, on pose

$$A(\tau, Q) := Q + 1 - \#\overline{(B_{a,d})}_\tau(\mathbb{F}_Q).$$

Pour expliciter $L\big(B_{a,d}/K, T\big)$, il s'agit de « calculer » ces quantités (Lemme 1.3.15). Pour cela, il sera commode de disposer d'un modèle de Weierstrass « court » de $B_{a,d}$: à partir du modèle (8.1)

$$Y^2 + t^d XY - at^{2d}Y = X^3 - (a+1)t^d X^2 + at^{2d}X,$$

le changement de variable $(x, y) = \big(4X, 8Y + 4t^d(X - at^d)\big)$ donne l'équation (affine)

$$E_d : \quad y^2 = x^3 + t^d\big(t^d - 4(a+1)\big)x^2 + 8at^{2d}(2 - t^d)x + 16a^2t^{4d} \tag{8.3}$$

dont le discriminant vaut $\Delta = 2^{12}a^2(a-1)^2t^{6d}(t^{2d} + 2(2a-1)t^d + 16)$. Ce dernier ne diffère du discriminant calculé à la Section 8.1 que par une puissance de 2, qui est inversible dans K. Autrement dit, le modèle (8.3) est entier et minimal en toute place $v \neq 0, \infty$. D'autre part, on remarque que pour tout $x \in \mathbb{F}_Q$,

$$x^3 + t^d\big(t^d - 4(a+1)\big)x^2 + 8at^{2d}(2 - t^d)x + 16a^2t^{4d} = (x - 4at^d)(x^2 + t^d(t^d - 4)x - 4at^{3d}). \tag{8.4}$$

Dans cette section, on démontre que

Proposition 8.2.3. *Pour toute extension finie $\mathbb{F}_Q/\mathbb{F}_q$, on a*

$$\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_Q)} A(\tau, Q) = -Q - \sum_{\chi \in Y(d,Q)} \chi(-1) \cdot \mathbf{j}_Q(\chi, \chi) \cdot \boldsymbol{S}_Q(\chi; b),$$

où $Y(d, Q)$ est l'ensemble suivant de caractères :

$$Y(d, Q) = \Big\{\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times \;\Big|\; \chi^d = \mathbf{1},\ \chi \neq \mathbf{1}, \mu\Big\}.$$

Démonstration. Soit $\tau \in \mathbb{P}^1(\mathbb{F}_Q)$, on suppose dans un premier temps que $\tau \neq 0, \infty$ et on note $\overline{(B_{a,d})}_\tau$ la réduction de $B_{a,d}/K$ en τ. C'est une courbe projective, dont un modèle affine est (8.3). Commençons par dénombrer les points $\mathbb{F}_Q$-rationnels sur cette courbe. Une fois pris en compte l'unique point à l'infini de $\overline{(B_{a,d})}_\tau$, on peut utiliser le Lemme 2.2.1 pour compter les points affines sur $\overline{(B_{a,d})}_\tau$:

$$\begin{aligned}
\#\overline{(B_{a,d})}_\tau(\mathbb{F}_Q) &= 1 + \#\left\{(x,y) \in \mathbb{F}_Q^2 \;\middle|\; y^2 = (x - 4a\tau^d)(x^2 + \tau^d(\tau^d - 4)x - 4a\tau^{3d})\right\} \\
&= 1 + \sum_{x \in \mathbb{F}_Q} \#\left\{y \in \mathbb{F}_Q \;\middle|\; y^2 = (x - 4a\tau^d)(x^2 + \tau^d(\tau^d - 4)x - 4a\tau^{3d})\right\} \\
&= 1 + \sum_{x \in \mathbb{F}_Q} \left(1 + \mu\left((x - 4a\tau^d)(x^2 + \tau^d(\tau^d - 4)x - 4a\tau^{3d})\right)\right) \\
&= Q + 1 + \sum_{x \in \mathbb{F}_Q} \mu\left((x - 4a\tau^d)(x^2 + \tau^d(\tau^d - 4)x - 4a\tau^{3d})\right).
\end{aligned}$$

Il suit de cette égalité que, pour tout $\tau \in \mathbb{P}^1(\mathbb{F}_Q) \smallsetminus \{0, \infty\}$,

$$A(\tau, Q) = -\sum_{x \in \mathbb{F}_Q} \mu\left((x - 4a\tau^d)(x^2 + \tau^d(\tau^d - 4)x - 4a\tau^{3d})\right).$$

En la place $\tau = \infty$, la courbe $B_{a,d}$ a réduction multiplicative déployée (*cf.* Proposition 8.1.4) donc on a $A(\infty, Q) = 1$. Enfin, en $v = 0$, la courbe $B_{a,d}$ a bonne réduction si d est pair et mauvaise réduction additive si d est impair. Nous avons vu pendant la preuve de la Proposition 8.1.4 que, dans le cas où d est pair, un modèle affine de $\overline{(B_{a,d})}_0$ est

$$y^2 = x(x-1)(x-a).$$

Un calcul similaire à celui qu'on vient d'effectuer pour $\tau \neq 0, \infty$ conduit alors à

$$A(0, Q) = \begin{cases} -\sum_{x \in \mathbb{F}_Q} \mu(x(x-1)(x-a)) & \text{si } d \text{ est pair} \\ 0 & \text{si } d \text{ est impair.} \end{cases}$$

On peut alors sommer les quantités $A(\tau, Q)$ sur $\tau \in \mathbb{P}^1(\mathbb{F}_Q)$ et mettre à part les termes $\tau = 0$ et $\tau = \infty$:

$$\begin{aligned}
\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_Q)} A(\tau, Q) &= A(\infty, Q) + A(0, Q) + \sum_{\tau \in \mathbb{F}_Q^\times} A(\tau, Q) \\
&= A(\infty, Q) + A(0, Q) - \sum_{\tau \in \mathbb{F}_Q^\times} \sum_{x \in \mathbb{F}_Q} \mu\left((x - 4a\tau^d)(x^2 + \tau^d(\tau^d - 4)x - 4a\tau^{3d})\right).
\end{aligned}$$

En utilisant le Lemme 2.2.2, on peut « réindexer » la somme :

$$\begin{aligned}
-\sum_{\tau \in \mathbb{F}_Q^\times} A(\tau, Q) &= \sum_{\tau \in \mathbb{F}_Q^\times} \sum_{x \in \mathbb{F}_Q} \mu\left((x - 4a\tau^d)(x^2 + \tau^d(\tau^d - 4)x - 4a\tau^{3d})\right) \\
&= \sum_{z \in \mathbb{F}_Q^\times} \left(\sum_{\chi^d = \mathbf{1}} \chi(z) \sum_{x \in \mathbb{F}_Q} \mu\left((x - 4az)(x^2 + z(z-4)x - 4az^3)\right) \right) \\
&= \sum_{\chi^d = \mathbf{1}} \left(\sum_{z \in \mathbb{F}_Q^\times} \sum_{x \in \mathbb{F}_Q} \chi(z) \mu\left((x - 4az)(x^2 + z(z-4)x - 4az^3)\right) \right),
\end{aligned}$$

la somme externe portant sur l'ensemble des caractères $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ dont la puissance d-ième est triviale. Il s'agit à présent d'expliciter les doubles sommes internes en termes de sommes de Jacobi et de sommes de Legendre. Pour un caractère quelconque $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$, on pose

$$M_Q(\chi) := \sum_{z \in \mathbb{F}_Q^\times} \sum_{x \in \mathbb{F}_Q} \chi(z) \mu\left((x - 4az)(x^2 + z(z-4)x - 4az^3)\right).$$

Nous démontrerons à la Section 8.2.2 ci-dessous le

Lemme 8.2.4. *Pour tout caractère $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$, on a*

$$M_Q(\chi) = \begin{cases} Q+1 & \text{si } \chi \text{ est trivial,} \\ \overline{\chi}(-1)\cdot \mathbf{j}_Q(\overline{\chi},\overline{\chi})\cdot \boldsymbol{S}_Q(\overline{\chi};b) & \text{sinon.} \end{cases}$$

Admettons cette identité pour le moment et utilisons-la pour expliciter $\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q)$. On a

$$\begin{aligned}\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) &= A(0,Q)+A(\infty,Q)-\sum_{\chi^d=\mathbf{1}} M_Q(\chi)\\ &= A(0,Q)+1-M_Q(\mathbf{1})+\sum_{\substack{\chi^d=\mathbf{1}\\ \chi\neq\mathbf{1}}} M_Q(\chi)\\ &= -Q+A(0,Q)-\sum_{\substack{\chi^d=\mathbf{1}\\ \chi\neq\mathbf{1}}} \overline{\chi}(-1)\cdot\mathbf{j}_Q(\overline{\chi},\overline{\chi})\cdot\boldsymbol{S}_Q(\overline{\chi};b)\\ &= -Q+A(0,Q)-\sum_{\substack{\chi^d=\mathbf{1}\\ \chi\neq\mathbf{1}}} \chi(-1)\cdot\mathbf{j}_Q(\chi,\chi)\cdot\boldsymbol{S}_Q(\chi;b). \qquad (8.5)\end{aligned}$$

La dernière égalité vient du fait que l'ensemble des caractères non triviaux dont l'ordre divise d est stable par $\chi\mapsto\overline{\chi}$. Pour conclure la preuve de la Proposition 8.2.3, posons $Y(d,Q)$ l'ensemble de caractères défini dans l'énoncé de celle-ci et distinguons deux cas :

– Si d est impair, on a $A(0,Q)=0$ et le caractère μ n'est pas un caractère dont l'ordre divise d. Donc $Y(d,Q)$ est formé des caractères non triviaux de $\mathbb{F}_Q^\times$ dont la puissance d-ième est triviale (*i.e.* la condition $\chi\neq\mu$ dans la définition de $Y(d,Q)$ est superflue). D'après (8.5), on a

$$\begin{aligned}\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) &= -Q+A(0,Q)-\sum_{\substack{\chi^d=\mathbf{1}\\ \chi\neq\mathbf{1}}}\chi(-1)\cdot\mathbf{j}_Q(\chi,\chi)\cdot\boldsymbol{S}_Q(\chi;b)\\ &= -Q-\sum_{\chi\in Y(d,Q)}\chi(-1)\cdot\mathbf{j}_Q(\chi,\chi)\cdot\boldsymbol{S}_Q(\chi;b).\end{aligned}$$

C'est ce qu'il fallait démontrer.

– Si maintenant d est pair, on a vu plus haut que $A(0,Q)$ s'exprimait sous la forme

$$A(0,Q) = -\sum_{x\in\mathbb{F}_Q}\mu\left(x(x-1)(x-a)\right).$$

Remarquons d'autre part que, si $\chi=\mu$ est le caractère d'ordre 2, on a $\mathbf{j}_Q(\mu,\mu)=\mu(-1)$ (Proposition 2.2.7) et donc, d'après le Lemme 8.2.4 et la Proposition 2.2.14,

$$M_Q(\mu) = \mu(-1)^2\boldsymbol{S}_Q(\mu;b) = -\sum_{x\in\mathbb{F}_Q}\mu(x(x-1)(x-a)) = A(0,Q).$$

Comme d est pair, le caractère d'ordre 2 intervient dans l'expression (8.5). On obtient

$$\begin{aligned}\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_Q)} A(\tau,Q) &= -Q+A(0,Q)-\sum_{\substack{\chi^d=\mathbf{1}\\ \chi\neq\mathbf{1}}}\chi(-1)\cdot\mathbf{j}_Q(\chi,\chi)\cdot\boldsymbol{S}_Q(\chi;b)\\ &= -Q+A(0,Q)-A(0,Q)-\sum_{\substack{\chi^d=\mathbf{1}\\ \chi\neq\mathbf{1},\mu}}\chi(-1)\cdot\mathbf{j}_Q(\chi,\chi)\cdot\boldsymbol{S}_Q(\chi;b)\\ &= -Q-\sum_{\chi\in Y(d,Q)}\chi(-1)\cdot\mathbf{j}_Q(\chi,\chi)\cdot\boldsymbol{S}_Q(\chi;b).\end{aligned}$$

Ce qui termine la preuve de la Proposition 8.2.3.

□

8.2.2 Preuve du Lemme 8.2.4

Dans cette section, nous démontrons le Lemme 8.2.4. Pour tout caractère $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ (dont l'ordre ne divise pas nécessairement d), nous avons posé :

$$M_Q(\chi) := \sum_{z\in\mathbb{F}_Q^\times}\sum_{x\in\mathbb{F}_Q}\chi(z)\mu\left((x-4az)(x^2+z(z-4)x-4az^3)\right).$$

Et il s'agit d'expliciter $M_Q(\chi)$ en fonction de sommes de Jacobi et de sommes de Legendre.

Démonstration. Soit donc $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$ un caractère quelconque. Découpons la preuve du Lemme 8.2.4 en trois parties : premièremenent, nous écrivons $M_Q(\chi)$ sous une forme plus pratique, ensuite nous concluons le calcul dans le cas où $\chi = \mathbf{1}$ et enfin, nous traitons le cas où $\chi \neq \mathbf{1}$.

Mise en forme de $M_Q(\chi)$. Partons de la définition

$$M_Q(\chi) = \sum_{z\in\mathbb{F}_Q^\times} \chi(z) \left(\sum_{x\in\mathbb{F}_Q} \mu\left((x-4az)(x^2+z(z-4)x-4az^3)\right)\right).$$

On amorce le calcul en réindexant la somme intérieure par « $x = zy$ » (ce qui est licite car la sommation sur z porte seulement sur $z \neq 0$) : pour tout $z \neq 0$, on a

$$\begin{aligned}\sum_{x\in\mathbb{F}_Q} \mu\left((x-4az)(x^2+z(z-4)x-4az^3)\right) &= \sum_{y\in\mathbb{F}_Q} \mu(zy-4az)\mu(z^2y^2+z^2y(z-4)-4az^3)\\ &= \sum_{y\in\mathbb{F}_Q} \mu(z)\cdot\mu(y-4a)\mu(z^2)\mu(y^2+y(z-4)-4az)\\ &= \mu(z)\sum_{y\in\mathbb{F}_Q} \mu(y-4a)\mu(y^2+y(z-4)-4az)\\ &= \mu(z)\sum_{y\in\mathbb{F}_Q} \mu(y-4a)\mu((y-4a)z+y^2-4y).\end{aligned}$$

Dans cette somme, le terme « $y = 4a$ » ne contribue pas car $\mu(0) = 0$, on peut donc réécrire celle-ci sous la forme

$$\begin{aligned}\sum_{y\in\mathbb{F}_Q} \mu(y-4a)\mu((y-4a)z+y^2-4y) &= \sum_{y\neq 4a} \mu(y-4a)\mu((y-4a)z+y(y-4))\\ &= \sum_{y\neq 4a} \mu(y-4a)^2\mu\left(z+\frac{y(y-4)}{y-4a}\right)\\ &= \sum_{y\neq 4a} \mu\left(z+\frac{y(y-4)}{y-4a}\right).\end{aligned}$$

car $\mu(y-4a)^2 = 1$. Ainsi, pour tout $z \neq 0$, on a

$$\sum_{x\in\mathbb{F}_Q} \mu\left((x-4az)(x^2+z(z-4)x-4az^3)\right) = \mu(z)\cdot\sum_{y\neq 4a} \mu\left(z+\frac{y(y-4)}{y-4a}\right).$$

Exploitons cette identité dans la somme $M_Q(\chi)$: après intervertion des sommes, il vient

$$\begin{aligned}M_Q(\chi) &= \sum_{z\in\mathbb{F}_Q^\times} \chi(z)\mu(z)\cdot\sum_{y\neq 4a} \mu\left(z+\frac{y(y-4)}{y-4a}\right)\\ &= \sum_{y\neq 4a}\left(\sum_{z\in\mathbb{F}_Q^\times} \chi(z)\mu(z)\mu\left(z+\frac{y(y-4)}{y-4a}\right)\right).\end{aligned}$$

Examinons à présent les sommes internes. Pour tout $Y \in \mathbb{F}_Q$, on a

$$\sum_{z\in\mathbb{F}_Q^\times} \chi(z)\mu(z)\mu(z+Y) = \sum_{z\in\mathbb{F}_Q^\times} \chi(z)\mu(z)^2\mu\left(1+Yz^{-1}\right) = \sum_{z\in\mathbb{F}_Q^\times} \chi(z)\mu\left(1+Yz^{-1}\right).$$

Si $Y = 0$, on a donc

$$\sum_{z\in\mathbb{F}_Q^\times} \chi(z)\mu(z)\mu(z+Y) = \sum_{z\neq 0}\chi(z).$$

Si maintenant $Y \neq 0$, on peut poser « $u = -Yz^{-1}$ » et on obtient que

$$\begin{aligned}\sum_{z\in\mathbb{F}_Q^\times} \chi(z)\mu\left(1+Yz^{-1}\right) &= \sum_{u\in\mathbb{F}_Q^\times} \chi(-Yu^{-1})\mu\left(1-u\right) \ = \chi(-Y)\cdot \sum_{u\in\mathbb{F}_Q^\times} \overline{\chi}(u)\mu\left(1-u\right)\\ &= \chi(-Y)\cdot\left(\sum_{u\in\mathbb{F}_Q} \overline{\chi}(u)\mu\left(1-u\right) \ -\overline{\chi}(0)\right)\\ &= -\chi(-Y)\cdot\left(\mathbf{j}_Q(\overline{\chi},\mu) \ +\overline{\chi}(0)\right).\end{aligned}$$

Ce qui permet (en posant $Y = y(y-4)/(y-4a)$) d'exprimer $M_Q(\chi)$ sous la forme :

$$\begin{aligned}M_Q(\chi) &= \sum_{y\neq 4a}\left(\sum_{z\in\mathbb{F}_Q^\times}\chi(z)\mu(z)\mu\left(z+\frac{y(y-4)}{y-4a}\right)\right)\\ &= 2\sum_{z\neq 0}\chi(z) - \left(\mathbf{j}_Q(\overline{\chi},\mu) \ +\overline{\chi}(0)\right)\cdot\sum_{y\neq 0,4,4a}\chi\left(-\frac{y(y-4)}{y-4a}\right)\\ &= 2\sum_{z\neq 0}\chi(z) - \chi(-1)\cdot\mathbf{j}_Q(\overline{\chi},\mu) \ \cdot\sum_{y\neq 0,4,4a}\chi\left(\frac{y(y-4)}{y-4a}\right) - \overline{\chi}(0)\cdot\chi(-1)\cdot\sum_{y\neq 0,4,4a}\chi\left(\frac{y(y-4)}{y-4a}\right).\end{aligned} \tag{8.6}$$

Il convient alors de distinguer deux cas :

Calcul de $M_Q(\mathbf{1})$. Supposons d'abord que χ est le caractère trivial $\mathbf{1}$. D'après l'identité (8.6) démontrée ci-dessus, se rappelant que $\mathbf{j}_Q(\mathbf{1},\mu) = 0$ (*cf.* Proposition 2.2.7), on a

$$M_Q(\mathbf{1}) = 2(Q-1) - 1\cdot\sum_{y\neq 0,4,4a}\mathbf{1}\left(\frac{y(y-4)}{y-4a}\right) + 0.$$

D'où finalement,

$$M_Q(\mathbf{1}) = 2(Q-1) - (Q-3) - 0 = Q+1.$$

Calcul de $M_Q(\chi)$ ($\chi \neq \mathbf{1}$). Supposons maintenant que χ n'est pas trivial. Alors $\chi(0) = 0$ et $\sum_{z\neq 0}\chi(z) = 0$. Lorsque l'on reporte ceci dans (8.6), on obtient que

$$M_Q(\chi) = -\chi(-1)\cdot\mathbf{j}_Q(\overline{\chi},\mu)\cdot\sum_{y\neq 0,4,4a}\chi\left(\frac{y(y-4)}{y-4a}\right).$$

Dans cette somme, les termes « $y = 0$ » et « $y = 4$ » ne contribuent pas si on les rajoute (car $\chi(0) = 0$). Ce qui nous permet d'écrire, en posant $y = 4x$:

$$\begin{aligned}M_Q(\chi) &= -\chi(-1)\cdot\mathbf{j}_Q(\overline{\chi},\mu)\cdot\sum_{y\neq 4a}\chi\left(\frac{y(y-4)}{y-4a}\right)\\ &= -\chi(-1)\cdot\mathbf{j}_Q(\overline{\chi},\mu)\cdot\sum_{x\neq a}\chi\left(\frac{4x(4x-4)}{4x-4a}\right)\\ &= -\chi(-4)\cdot\mathbf{j}_Q(\overline{\chi},\mu)\cdot\sum_{x\neq a}\chi\left(\frac{x(x-1)}{x-a}\right).\end{aligned}$$

On peut alors appliquer la Proposition 2.2.14 : pour χ non trivial et $b = 1-2a$, on a

$$-\sum_{x\neq a}\chi\left(\frac{x(x-1)}{x-a}\right) = -\sum_{z\in\mathbb{F}_Q}\chi(z)\cdot\mu_Q(x^2+2bx+1) = \boldsymbol{S}_Q(\chi;b).$$

De plus, on a $\mathbf{j}_Q(\overline{\chi},\mu) = \overline{\chi}(4)\cdot\mathbf{j}_Q(\overline{\chi},\overline{\chi})$ (*cf.* Lemme 2.2.9). Nous avons donc démontré que

$$M_Q(\chi) = \chi(-1)\cdot\mathbf{j}_Q(\overline{\chi},\overline{\chi})\cdot\boldsymbol{S}_Q(\chi;b).$$

En outre, il est clair que $\chi(-1) = \overline{\chi}(-1)$ et que $\boldsymbol{S}_Q(\chi;b) = \boldsymbol{S}(\overline{\chi};b)$ (Proposition 2.2.12). Nous obtenons finalement l'identité annoncée : $M_Q(\chi) = \overline{\chi}(-1)\cdot\mathbf{j}_Q(\overline{\chi},\overline{\chi})\cdot\boldsymbol{S}_Q(\overline{\chi};b)$. □

8.2.3 Réindexation de caractères

On procède à présent comme dans les chapitres précédents : une fois que l'on a obtenu, pour tout $n \geqslant 1$, une « bonne expression » pour $\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau, q^n)$ sous la forme d'une somme, on peut utiliser les méthodes de la Section 2.1.4 pour obtenir l'expression de $L(B_{a,d}/K, T)$. Pour toute extension finie $\mathbb{F}_{q^n}/\mathbb{F}_q$, la Proposition 8.2.3 donne

$$\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau, q^n) = -q^n - \sum_{\chi \in Y(d,q^n)} \chi(-1) \cdot \mathbf{j}_{q^n}(\chi, \chi) \cdot \boldsymbol{S}_{q^n}(\chi; 1-2a),$$

la somme portant sur l'ensemble suivant de caractères :

$$Y(d, q^n) = \left\{ \chi : \mathbb{F}_{q^n}^\times \to \overline{\mathbb{Q}}^\times \;\middle|\; \chi^d = \mathbf{1},\ \chi \neq \mathbf{1}, \mu \right\}.$$

Par construction de la fonction L de la courbe $B_{a,d}/K$ (voir Lemme 1.3.15), on a

$$\log L(B_{a,d}/K, T) = \sum_{n=1}^{\infty} \left(\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau, q^n) \right) \frac{T^n}{n}.$$

Ainsi, vu l'identité ci-dessus (où l'on a posé $b = 1 - 2a$), on a

$$\begin{aligned} \log L(B_{a,d}/K, T) &= \sum_{n=1}^{\infty} \frac{T^n}{n} \left(-q^n - \sum_{\chi \in Y(d,q^n)} \chi(-1) \cdot \mathbf{j}_{q^n}(\chi, \chi) \cdot \boldsymbol{S}_{q^n}(\chi, b) \right) \\ &= -\sum_{n=1}^{\infty} \frac{(qT)^n}{n} - \sum_{n=1}^{\infty} \left(\sum_{\chi \in Y(d,q^n)} \chi(-1) \cdot \mathbf{j}_{q^n}(\chi, \chi) \cdot \boldsymbol{S}_{q^n}(\chi, b) \right) \frac{T^n}{n}. \end{aligned}$$

La première de ces deux sommes est aisée à calculer :

$$-\sum_{n=1}^{\infty} \frac{(qT)^n}{n} = \log(1 - qT).$$

Pour expliciter la seconde somme, on fait appel à la Proposition 2.1.15. Pour toute extension $\mathbb{F}_Q/\mathbb{F}_q$ et tout caractère non trivial $\chi : \mathbb{F}_Q^\times \to \overline{\mathbb{Q}}^\times$, posons à cet effet

$$\sigma(\chi, Q) := \chi(-1) \cdot \mathbf{j}_Q(\chi, \chi) \cdot \boldsymbol{S}_Q(\chi, b)$$

et vérifions que cette donnée satisfait aux hypothèses de la Proposition 2.1.15 (avec $K = 2$ et $\ell = 2$). D'une part, il est clair que $\sigma(\chi, Q) = \sigma(\chi^q, Q)$ car $\sigma(\chi, Q)$ est défini comme un produit de sommes portant sur $\mathbb{F}_Q$. D'autre part, pour toute extension supplémentaire $\mathbb{F}_{Q^s}/\mathbb{F}_Q$, on note $\chi^{(s)} = \chi \circ \mathbf{N}_{\mathbb{F}_{Q^s}/\mathbb{F}_Q}$ le caractère de $\mathbb{F}_{Q^s}^\times$ déduit de χ. Les sommes de Jacobi vérifient une relation de Hasse-Davenport à l'ordre 1 (Théorème 2.2.20) donc

$$\mathbf{j}_{Q^s}(\chi^{(s)}, \chi^{(s)}) = \mathbf{j}_Q(\chi, \chi)^s.$$

En outre, les sommes de Legendre $\boldsymbol{S}_Q(\chi; b)$ vérifient une relation de Hasse-Davenport à l'ordre 2 (Théorème 2.2.21) : il existe deux entiers algébriques $\alpha_b(\chi)$ et $\beta_b(\chi)$ tels que

$$\boldsymbol{S}_{Q^s}(\chi^{(s)}; b) = \alpha_b(\chi)^s + \beta_b(\chi)^s.$$

Dans la suite de ce chapitre, $\alpha_b(\chi)$ et $\beta_b(\chi)$ auront toujours cette signification. On en conclut que

$$\begin{aligned} \sigma(\chi^{(s)}, Q^s) &= \chi^{(s)}(-1) \cdot \mathbf{j}_{Q^s}(\chi^{(s)}, \chi^{(s)}) \cdot \boldsymbol{S}_{Q^s}(\chi^{(s)}, b) \\ &= \chi(-1)^s \cdot \mathbf{j}_Q(\chi, \chi)^s \cdot (\alpha_b(\chi)^s + \beta_b(\chi)^s) \\ &= (\chi(-1) \cdot \mathbf{j}_Q(\chi, \chi) \cdot \alpha_b(\chi))^s + (\chi(-1) \cdot \mathbf{j}_Q(\chi, \chi) \cdot \beta_b(\chi))^s. \end{aligned}$$

Autrement dit, nous avons vérifié que $\sigma(\chi, Q)$ satisfait une relation de Hasse-Davenport à l'ordre $K = 2$ (au sens de la Proposition 2.1.14). Posons temporairement

$$\omega_1(\chi) = \chi(-1) \cdot \mathbf{j}_Q(\chi, \chi) \cdot \alpha_b(\chi) \quad \text{et} \quad \omega_2(\chi) = \chi(-1) \cdot \mathbf{j}_Q(\chi, \chi) \cdot \beta_b(\chi).$$

Le raisonnement ci-dessus montre que les $\sigma(\chi, Q)$ satisfont les deux hypothèses de la Proposition 2.1.15 (avec $K = 2$ et $\ell = 2$). On a donc

$$-\sum_{n=1}^{\infty}\left(\sum_{\chi\in Y(d,q^n)}\sigma(\chi,Q)\right)\frac{T^n}{n} = \sum_{m\in\mathcal{O}_q^{(2)}(d)}\log\left(\left(1-\omega_1(\mathbf{t}_m)\cdot T^{u(m)}\right)\left(1-\omega_2(\mathbf{t}_m)\cdot T^{u(m)}\right)\right).$$

Nous avons donc prouvé que

$$\log L(B_{a,d}/K,T) = \log(1-qT) + \sum_{m\in\mathcal{O}_q^{(2)}(d)}\log\left(\left(1-\omega_1(\mathbf{t}_m)\cdot T^{u(m)}\right)\left(1-\omega_2(\mathbf{t}_m)\cdot T^{u(m)}\right)\right).$$

En revenant à la définition de $\omega_1(\mathbf{t}_m)$ et $\omega_2(\mathbf{t}_m)$, on en déduit facilement que $L(B_{a,d}/K,T)$ s'écrit

$$L\big(B_{a,d}/K,T\big) = (1-qT)\cdot\prod_{m\in\mathcal{O}_q^{(2)}(d)}\left(1-\mathbf{J}'_m\cdot\alpha_b(\mathbf{t}_m)\cdot T^{u(m)}\right)\left(1-\mathbf{J}'_m\cdot\beta_b(\mathbf{t}_m)\cdot T^{u(m)}\right),$$

où $\mathbf{J}'_m = \mathbf{t}_m(-1)\mathbf{j}_{q^{u(m)}}(\mathbf{t}_m,\mathbf{t}_m)$. Ceci termine la preuve du Théorème 8.2.1.

8.2.4 Conjecture de Birch et Swinnerton-Dyer

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Soit $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et d un entier premier à q. Considérons la courbe $Y_{a,d} \subset \mathbb{P}^1\times\mathbb{P}^1$ définie sur K par l'équation

$$Y_{a,d}: \quad t^d\cdot x_0(x_0-x_1)y_0(y_0-y_1) = x_1y_1^2(x_0-ax_1), \tag{8.7}$$

dans les coordonnées $([x_0:x_1],[y_0:y_1])$ sur $\mathbb{P}^1\times\mathbb{P}^1$. Cette courbe admet au moins un point rationnel (par exemple $([0:1],[1:0])$) et, d'après [Ber08, Section 3], elle est lisse de genre 1 (si $a \neq 0,1$ et si d est premier à p). Un ouvert affine de celle-ci est donné (dans les coordonnées x, y sur $\mathbb{A}^1\times\mathbb{A}^1$) par :

$$\frac{x-a}{x(x-1)} - t^d\cdot y(y-1) = 0.$$

Autrement dit, $Y_{a,d}$ est une courbe du type considéré au Théorème 1.4.17. Relions maintenant la courbe $Y_{a,d}$ à $B_{a,d}$ (définie par le modèle (8.1)).

Proposition 8.2.5. *Soit d un entier premier à q et $a \in \mathbb{F}_q \smallsetminus \{0,1\}$. Soit $B_{a,d}$ la courbe définie sur $K = \mathbb{F}_q(t)$ par* (8.1) *et $Y_{a,d}$ la courbe définie sur K comme ci-dessus.*

Les courbes $B_{a,d}/K$ et $Y_{a,d}/K$ sont birationnelles.

Démonstration. Partons de l'équation (8.7) donnant $Y_{a,d}$ comme une courbe dans $\mathbb{P}^1\times\mathbb{P}^1$. Multiplions (8.7) par $x_0^{-2}y_1^{-2}$, on obtient :

$$t^d\left(1-\frac{x_1}{x_0}\right)\frac{y_0}{y_1}\left(\frac{y_0}{y_1}-1\right) = \frac{x_1}{x_0}\left(1-a\frac{x_1}{x_0}\right).$$

Soit alors

$$X_1 = \frac{x_1}{x_0} \quad\text{et}\quad Y_1 = \frac{y_0}{y_1}\left(\frac{x_1}{x_0}-1\right),$$

l'équation précédente se réécrit

$$t^dY_1\,(Y_1 - X_1 + 1) = X_1(1-aX_1)(1-X_1),$$

ce qui, une fois développé, donne

$$t^dY_1^2 - t^dX_1Y_1 + t^dY_1 = aX_1^3 - (a+1)X_1^2 + X_1.$$

On multiplie maintenant cette relation par a^2t^{3d} :

$$(at^{2d}Y_1)^2 - t^d(at^dX_1)(at^{2d}Y_1) + at^{2d}(at^{2d}Y_1) = (at^dX_1)^3 - (a+1)t^d(at^dX_1)^2 + at^{2d}(at^dX_1)$$

et on effectue le changement de variables $(X_2,Y_2) = \big(at^dX_1, -at^{2d}Y_1\big)$; ce qui nous amène à l'équation :

$$Y_2^2 + t^dX_2Y_2 - at^{2d}Y_2 = X_2^3 - (a+1)t^dX_2^2 + at^{2d}X_2.$$

On reconnaît ici le modèle de Weierstrass affine de $B_{a,d}/K$ donné en (8.1). En résumé, il y a une application rationnelle $Y_{a,d} \dashrightarrow B_{a,d}$, donnée par :

$$\big([x_0:x_1],[y_0:y_1]\big) \in Y_{a,d} \mapsto \left(at^d\frac{x_1}{x_0}, -at^{2d}\frac{y_0}{y_1}\left(\frac{x_1}{x_0}-1\right)\right) = (X_2,Y_2) \in B_{a,d}.$$

Et celle-ci est dominante. Les courbes $Y_{a,d}$ et $B_{a,d}$ sont donc birationnelles (sur K). □

En d'autres termes, d'après la Proposition ci-dessus, la courbe $Y_{a,d}$ (définie a priori comme une courbe $\subset \mathbb{P}^1 \times \mathbb{P}^1$), admet en fait une description comme une cubique plane munie d'un point rationnel. Définissons deux applications rationnelles $f, g : \mathbb{P}^1 \to \mathbb{P}^1$ par $f(x) = (x-a)/x(x-1)$ et $g(y) = y(y-1)$. Comme on l'a dit plus haut, un ouvert affine de la courbe $Y_{a,d}$ est donné (sur $K = \mathbb{F}_q(t)$) par l'équation $f(x) - t^d \cdot g(y) = 0$. Et la Proposition précédente montre que $B_{a,d}/K$ et $Y_{a,d}/K$ sont birationnelles. Le théorème [Ber08, Theorem 2.3] (voir Théorème 1.4.17) implique alors immédiatement le résultat ci-dessous :

Théorème 8.2.6 (Berger). *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Pour tout $a \in \mathbb{F}_q \smallsetminus \{0, 1\}$ et tout entier $d \geqslant 2$ premier à q, on considère la courbe elliptique $B_{a,d}$ définie sur K par* (8.1). *Les conjectures de Birch et Swinnerton-Dyer (Conjecture 1.4.1) sont vraies pour la courbe $B_{a,d}/K$. En particulier le groupe de Tate-Shafarevich $Ш(B_{a,d}/K)$ est fini et le ratio de Brauer-Siegel $\mathfrak{Bs}(B_{a,d}/K)$ également.*

8.3 Le cas où $a = 1/2$

Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 3$ et $K = \mathbb{F}_q(t)$. On fixe un entier $d \geqslant 2$ premier à q. Dans cette section, nous étudions plus particulièrement la courbe $B_{1/2,d}/K$, pour laquelle on peut expliciter plus avant sa fonction L. En particulier, nous examinons en détail le rang de $B_{1/2,d}/K$: on démontre qu'il peut être arbitrairement grand lorsque d varie.

Du point de vue de [Ulm13], le cas où $a = 1/2$ est celui où la courbe $B_{a,d}/K$ acquiert des automorphismes supplémentaires. On devrait pouvoir redémontrer le résultat de rang non borné (Théorème 8.3.10) dans le style de [Ulm13, §7].

8.3.1 Retour sur les sommes de Legendre

Pour tout caractère $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ et tout $b \in \mathbb{F}_q \smallsetminus \{-1, 1\}$, nous avons posé (Section 2.2.3) :

$$\boldsymbol{S}_q(\chi; b) = -\sum_{x \in \mathbb{F}_q} \chi(x)\mu_q(x^2 + 2bx + 1).$$

Comme nous l'avons rappelé à la Section 8.2, ces sommes vérifient une « relation de Hasse-Davenport » à l'ordre 2 : pour tout $b \neq \pm 1$ et tout caractère non trivial χ, il existe deux entiers algébriques $\alpha_b(\chi)$ et $\beta_b(\chi)$, de module $\sqrt{q}$ dans tout plongement complexe, tels que

$$\boldsymbol{S}_q(\chi; b) = \alpha_b(\chi) + \beta_b(\chi) \qquad \text{et} \qquad \alpha_b(\chi)\beta_b(\chi) = q.$$

Ces faits ont été démontrés aux Théorème 2.2.21 et Corollaire 2.3.5. Pour $b = 0$, nous pouvons expliciter complètement $\alpha_b(\chi)$ et $\beta_b(\chi)$ comme suit.

Proposition 8.3.1. *Soit $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ un caractère non trivial. On note à nouveau $\alpha_0(\chi)$ et $\beta_0(\chi)$ les entiers algébriques associés à la somme $\boldsymbol{S}_q(\chi; 0)$ comme ci-dessus. Alors, à permutation de $\alpha_0(\chi)$ et $\beta_0(\chi)$ près,*

- *si $\chi(-1) = -1$,*
$$\alpha_0(\chi) = i \cdot \sqrt{q} \qquad \text{et} \qquad \beta_0(\chi) = -i \cdot \sqrt{q},$$
- *si $\chi(-1) = 1$, il existe un caractère $\theta : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ tel que $\chi = \theta^2$ (Lemme 2.1.1) et*
$$\alpha_0(\chi) = \theta(-1) \cdot \mathbf{j}_q(\theta, \mu) \qquad \text{et} \qquad \beta_0(\chi) = \mu(-1)\theta(-1) \cdot \mathbf{j}_q(\mu \cdot \theta, \mu).$$

Démonstration. Premièrement, si $\chi(-1) = -1$, on a $\boldsymbol{S}_q(\chi; 0) = 0$ (*cf.* Proposition 2.2.13). Or, la seule paire $\{\alpha, \beta\}$ de nombres complexes conjugués de module $\sqrt{q}$ qui vérifient $\alpha + \beta = 0$ et $\alpha \cdot \beta = q$ est $\{+i\sqrt{q}, -i\sqrt{q}\}$. Quitte à permuter les rôles de $\alpha_0(\chi)$ et $\beta_0(\chi)$, on a donc bien $\alpha_0(\chi) = i \cdot \sqrt{q}$ et $\beta_0(\chi) = \overline{\alpha_0(\chi)} = -i \cdot \sqrt{q}$. Si maintenant $\chi(-1) = 1$, on peut fixer un caractère θ tel que $\chi = \theta^2$ (Lemme 2.1.1) et l'on a (d'après la Proposition 2.2.13 encore)

$$\boldsymbol{S}_q(\chi; 0) = \theta(-1) \cdot \mathbf{j}_q(\theta, \mu) + \mu(-1)\theta(-1) \cdot \mathbf{j}_q(\mu\theta, \mu).$$

Dans cette expression, θ et $\theta\mu$ ne sont pas le caractère trivial (sans quoi $\chi = \mathbf{1}$...). On peut donc utiliser la Proposition 2.2.7 à deux fins. D'une part pour constater que, dans tout plongement complexe, on

a $|\mathbf{j}_q(\theta,\mu)| = |\mathbf{j}_q(\mu\theta,\mu)| = \sqrt{q}$. D'autre part pour exprimer les sommes de Jacobi $\mathbf{j}_q(\theta,\mu)$ et $\mathbf{j}_q(\mu\theta,\mu)$ en termes de sommes de Gauss :

$$\mathbf{j}_q(\theta,\mu) = \frac{\mathbf{g}_q(\theta)\cdot\mathbf{g}_q(\mu)}{\mathbf{g}_q(\mu\theta)} \quad \text{et} \quad \mathbf{j}_q(\mu\theta,\mu) = \frac{\mathbf{g}_q(\mu\theta)\cdot\mathbf{g}_q(\mu)}{\mathbf{g}_q(\theta)}.$$

Pour démontrer les égalités recherchées, il reste donc à montrer que $\theta(-1)\mathbf{j}_q(\theta,\mu)$ et $\mu\theta(-1)\mathbf{j}_q(\mu\theta,\mu)$ sont conjugués, *i.e.* que le produit de $\theta(-1)\cdot\mathbf{j}_q(\theta,\mu)$ et de $\mu(-1)\theta(-1)\cdot\mathbf{j}_q(\mu\theta,\mu)$ vaut q. Or, la Proposition 2.2.5 fournit la relation $\mathbf{g}_q(\mu)^2 = \mu(-1)q$ et l'on en déduit que

$$\begin{aligned}(\theta(-1)\cdot\mathbf{j}_q(\theta,\mu))\cdot(\mu(-1)\theta(-1)\cdot\mathbf{j}_q(\mu\theta,\mu)) &= \mu(-1)\cdot\theta(-1)^2\cdot\frac{\mathbf{g}_q(\theta)\cdot\mathbf{g}_q(\mu)}{\mathbf{g}_q(\mu\theta)}\cdot\frac{\mathbf{g}_q(\mu\theta)\cdot\mathbf{g}_q(\mu)}{\mathbf{g}_q(\theta)}\\ &= \mu(-1)\cdot\theta((-1)^2)\cdot\mathbf{g}(\mu)^2 = \mu(-1)^2\cdot q = q.\end{aligned}$$

On a donc bien, à permutation de $\alpha_0(\chi)$ et $\beta_0(\chi)$ près, les égalités voulues. □

Remarquons que le cas « $b=0$ » (*i.e.* $a=1/2$) est le seul où l'on sait expliciter autant les sommes $\boldsymbol{S}_q(\chi;b)$. C'est l'un des facteurs limitants dans notre étude des courbes $B_{a,d}$ (et plus généralement des courbes elliptiques dont la fonction L fait intervenir ces sommes).

8.3.2 La fonction $L\big(B_{1/2,d}/K,T\big)$ dans le cas où d est impair

Supposons encore que $a=1/2$ et ajoutons l'hypothèse que l'entier d est impair. On peut alors écrire la fonction L de la courbe $B_{1/2,d}/K$ uniquement en termes de sommes de Jacobi. Pour clarifier les notations, nous noterons $\boldsymbol{\theta}_n : \mathbb{F}_{q^{u(n)}}^\times \to \overline{\mathbb{Q}}^\times$ les caractères associés à l'entier $2d$ ($n \in [\![1, 2d-1]\!]$), *cf.* Section 2.1.3.

Théorème 8.3.2. *On note $a=1/2\in\mathbb{F}_q$ et $b=1-2a=0$. Soit $d\geqslant 3$ un entier* impair *et premier à q. On considère ici la courbe elliptique $B_{1/2,d}$ définie sur $K=\mathbb{F}_q(t)$ par l'équation* (8.1)*. La fonction L de $B_{1/2,d}$ s'exprime sous la forme suivante :*

$$L\big(B_{1/2,d}/\mathbb{F}_q(t),T\big) = (1-qT)\cdot\prod_{n\in\mathcal{O}_q^{(2)}(2d)}\Big(1-\boldsymbol{\theta}_n(-1)\cdot\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2)\cdot T^{u(n)}\Big),$$

où $\mathcal{O}_q^{(2)}(2d)$ désigne l'ensemble d'orbites suivant :

$$\mathcal{O}_q^{(2)}(2d) = \big(\mathbb{Z}/2d\mathbb{Z}\smallsetminus\{0,d\}\big)/\langle q \bmod 2d\rangle$$

et les caractères $\boldsymbol{\theta}_n : \mathbb{F}_{q^{u(n)}}^\times \to \overline{\mathbb{Q}}^\times$ sont ceux qui sont associés à $2d$ (et non plus d).

Remarque 8.3.3. Pour toute orbite $n\in\mathcal{O}_q^{(2)}(2d)$, l'écriture des sommes de Jacobi en termes de sommes de Gauss (Proposition 2.2.7) donne l'identité suivante :

$$\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2) = \boldsymbol{\theta}_n(4)\cdot\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\boldsymbol{\theta}_n)\cdot\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2) = \boldsymbol{\theta}_n(4)\cdot\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\boldsymbol{\theta}_n,\boldsymbol{\theta}_n^2).$$

On note en effet que, pour $n\in\mathcal{O}_q^{(2)}(2d)$, le caractère $\boldsymbol{\theta}_n$ n'est ni le caractère trivial, ni le caractère quadratique, ni un caractère d'ordre 4 (car d est impair).

Remarque 8.3.4. Lorsque d est pair, il devrait exister une identité similaire pour la fonction L de la courbe $B_{1/2,d}$.

Démonstration. Commençons par faire deux remarques. Premièrement, pour tout entier impair $D\geqslant 2$, premier à q (q est impair car la caractéristique de K est supposée être $\geqslant 5$), on a $o_q(D) = o_q(2D)$. En effet, par construction de l'ordre, D divise $q^{o_q(D)}-1$, mais d est impair et $q^{o_q(D)}-1$ est pair, c'est donc que $2D$ divise $q^{o_q(D)}-1$. À nouveau par construction de l'ordre, ceci implique que $o_q(2D) \mid o_d(D)$. D'autre part, comme D divise $2D$ qui divise à son tour $q^{o_q(2D)}-1$, on a $o_q(D)\mid o_q(2D)$. Ce qui termine la preuve que $o_q(D)=o_q(2D)$: une autre façon d'exprimer ceci est que les actions de q par multiplication sur $\mathbb{Z}/d\mathbb{Z}$ et sur $\mathbb{Z}/2d\mathbb{Z}$ sont « identiques ». Deuxièmement, pour tout $m\in[\![1,d-1]\!]$, le caractère $\mathbf{t}_m$ associé à m est d'ordre $d_m := d/\operatorname{pgcd}(d,m)$ (*cf.* Section 2.1.3). Comme $m\neq 0, d/2$, on a $d_m>2$ et d_m est un diviseur de d. C'est donc un entier impair et l'ordre de $\mathbf{t}_m$ est impair. D'après le Lemme 2.1.1, on a $\mathbf{t}_m(-1)=1$ et il existe un caractère $\theta_m : \mathbb{F}_{q^{u(m)}}^\times \to \overline{\mathbb{Q}}^\times$ tel que ${\theta_m}^2 = \mathbf{t}_m$. En outre, l'unique autre caractère θ'_m de $\mathbb{F}_{q^{u(m)}}^\times$ qui vérifie ${\theta'_m}^2 = \mathbf{t}_m$ est alors donné par $\theta'_m = \theta_m\cdot\mu_{q^{u(m)}}$.

Pour tout $m \in [\![1, d-1]\!]$, on pose

$$\boldsymbol{\theta}_m : \mathbb{F}_{q^{u(m)}}^{\times} \to \overline{\mathbb{Q}}^{\times}, \qquad \boldsymbol{\theta}_m := \mathbf{t}^{(q^{u(m)}-1)m/2d}.$$

Comme on l'a vu ci-dessus, $2d$ divise $m(q^{u(m)}-1)$ si bien que le caractère $\boldsymbol{\theta}_m$ est correctement défini. Par construction même, $\boldsymbol{\theta}_m$ vérifie ${\boldsymbol{\theta}_m}^2 = \mathbf{t}_m$ et

$$\boldsymbol{\theta}_m \cdot \mu_{q^{u(m)}} = \mathbf{t}^{(q^{u(m)}-1)m/2d} \cdot \mathbf{t}^{(q^{u(m)}-1)/2} = \mathbf{t}^{(q^{u(m)}-1)(m+d)/2d} := \boldsymbol{\theta}_{m+d}.$$

Là encore, $2d$ divise clairement $(m+d)(q^{u(m)}-1)$ et le caractère $\boldsymbol{\theta}_{m+d}$ est bien défini. Pour tout $m \in [\![1, d-1]\!]$, nous venons ainsi de produire deux caractères distincts $\boldsymbol{\theta}_m$ et $\boldsymbol{\theta}_{m+d}$ de $\mathbb{F}_{q^{u(m)}}^{\times}$ dont le carré est $\mathbf{t}_m$ (ce sont donc les deux seuls). Et, lorsque m parcourt $[\![1, d-1]\!]$, m et $m+d$ parcourent $[\![1, 2d-1]\!] \smallsetminus \{d\}$. Nous avons donc défini des caractères $\boldsymbol{\theta}_n$ pour tout $n \in [\![1, 2d-1]\!] \smallsetminus \{d\}$. Et par définition, les caractères $\boldsymbol{\theta}_n$ ainsi construits sont les mêmes que ceux que l'on a introduits à la Section 2.1.3. D'après la première remarque en début de preuve, l'action de q sur $\mathbb{Z}/2d\mathbb{Z}\smallsetminus\{0\}$ est « la même » que celle sur $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ au sens où :

$$\forall n \in \mathbb{Z}/2d\mathbb{Z}\smallsetminus\{0\}, \quad u(n) = o_q\big(2d/\operatorname{pgcd}(2d, n)\big) = o_q\big(d/\operatorname{pgcd}(d, n \bmod d)\big) = u(n \bmod d).$$

En d'autres termes, lorsque n parcourt l'ensemble d'orbites $\mathcal{O}_q^{(2)}(2d)$ tel que défini dans l'énoncé, $\boldsymbol{\theta}_n$ parcourt l'ensemble de toutes les classes d'équivalence (modulo l'action du Frobenius) des caractères sur $\overline{\mathbb{F}_q}^{\times}$ dont l'ordre divise $2d$ (*cf.* Section 2.1.3).

Revenons alors à la fonction L de la courbe $B_{1/2,d}$, on pose $b = 1-2a = 0$. Comme d est impair, on a $\mathcal{O}_q^{(2)}(d) = (\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\})/\langle q \bmod d\rangle = \mathcal{O}'_q(d)$. D'après le Théorème 8.2.1, on a

$$L\big(B_{1/2,d}/\mathbb{F}_q(t), T\big) = (1-qT) \cdot \prod_{m \in \mathcal{O}'_q(d)} \Big(1 - \mathbf{J}'_m \cdot \alpha_b(\mathbf{t}_m) \cdot T^{u(m)}\Big) \Big(1 - \mathbf{J}'_m \cdot \beta_b(\mathbf{t}_m) \cdot T^{u(m)}\Big),$$

où $\mathbf{J}'_m = \mathbf{t}_m(-1) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)$ et où $\alpha_b(\mathbf{t}_m) = \alpha_0(\mathbf{t}_m)$ et $\beta_b(\mathbf{t}_m) = \beta_0(\mathbf{t}_m)$ ont été calculés à la Proposition 8.3.1. Plus précisément, comme $\mathbf{t}_m(-1) = 1$, quitte à permuter $\alpha_0(\mathbf{t}_m)$ et $\beta_0(\mathbf{t}_m)$, comme $\mathbf{t}_m(-1) = 1$, on a

$$\alpha_0(\mathbf{t}_m) = \boldsymbol{\theta}_m(-1) \cdot \mathbf{j}_{q^{u(m)}}(\boldsymbol{\theta}_m, \mu) \quad \text{ et } \beta_0(\mathbf{t}_m) = \boldsymbol{\theta}_{m+d}(-1) \cdot \mathbf{j}_{q^{u(m)}}(\boldsymbol{\theta}_{m+d}, \mu).$$

Par suite, le facteur

$$\Big(1 - \mathbf{J}'_m \cdot \alpha_b(\mathbf{t}_m) \cdot T^{u(m)}\Big) \Big(1 - \mathbf{J}'_m \cdot \beta_b(\mathbf{t}_m) \cdot T^{u(m)}\Big)$$

correspondant à $m \in \mathcal{O}_q^{(2)}(d)$ peut se réécrire

$$\Big(1 - \boldsymbol{\theta}_m(-1) \cdot \mathbf{j}_{q^{u(m)}}(\boldsymbol{\theta}_m, \mu) \cdot \mathbf{j}_{q^{u(m)}}(\boldsymbol{\theta}_m^2, \boldsymbol{\theta}_m^2) \cdot T^{u(m)}\Big) \cdot \Big(1 - \boldsymbol{\theta}_{m+d}(-1) \cdot \mathbf{j}_{q^{u(m+d)}}(\boldsymbol{\theta}_{m+d}, \mu) \cdot \mathbf{j}_{q^{u(m+d)}}(\boldsymbol{\theta}_{m+d}^2, \boldsymbol{\theta}_{m+d}^2) \cdot T^{u(m+d)}\Big).$$

Le produit de tous ces facteurs lorsque m parcourt $\mathcal{O}_q^{(2)}(d)$ peut donc être écrit comme un produit portant sur les orbites $n \in \mathcal{O}_q^{(2)}(2d)$:

$$\prod_{n \in \mathcal{O}_q^{(2)}(2d)} \Big(1 - \boldsymbol{\theta}_n(-1) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n, \mu) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2, \boldsymbol{\theta}_n^2) \cdot T^{u(n)}\Big),$$

ceci, à nouveau grâce à la première remarque de la preuve que l'action de q sur $\mathbb{Z}/2d\mathbb{Z}\smallsetminus\{0\}$ est la même que sur $\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\}$ (en particulier, $u(m) = u(m+d) = u(n)$). Ce qui achève la preuve du Théorème 8.3.2. □

8.3.3 Le rang des courbes $B_{1/2,d}$

Plaçons-nous à nouveau dans la situation du paragraphe précédent : le paramètre $a \in \mathbb{F}_q$ est fixé égal à $a = 1/2$ et d est un entier *impair* et premier à q. Le Lemme 3.1.4 s'applique ici et l'on peut expliciter le rang de $B_{1/2,d}/K$ en termes « combinatoires ». Pour cela, posons la définition suivante :

Définition 8.3.5. Soit $d \geqslant 3$ un entier impair premier à q. On définit

$$\mathcal{Z}_q(2d) := \left\{ n \in \mathcal{O}_q^{(2)}(2d) \;\middle|\; \boldsymbol{\theta}_n(-1) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n, \mu) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2, \boldsymbol{\theta}_n^2) = q^{u(n)} \right\}$$

et $\mathcal{V}_q^*(2d) := \mathcal{O}_q^{(2)}(2d) \smallsetminus \mathcal{Z}_q(2d)$ son complémentaire.

Avec cette notation, on a

Proposition 8.3.6. *Soit d un entier impair et premier à q. On considère à nouveau la courbe elliptique $B_{1/2,d}$ définie sur $K = \mathbb{F}_q(t)$ par le modèle de Weierstrass* (8.1)*. Le rang du groupe de Mordell-Weil $B_{1/2,d}(K)$ vaut*

$$\operatorname{rang} B_{1/2,d}(K) = 1 + \#\mathcal{Z}_q(2d).$$

Démonstration. On a vu (Théorème 8.2.6) que la courbe $B_{1/2,d}$ satisfait aux conjectures de Birch et Swinnerton-Dyer. En particulier, la partie « faible » de ces conjectures est vraie : l'ordre d'annulation de la fonction $L\big(B_{1/2,d}/K, T\big)$ en $T = q^{-1}$ (le rang analytique) est égal au rang du groupe de Mordell-Weil $B_{1/2,d}(K)$ (le rang algébrique). Pour expliciter ce dernier, il suffit donc d'expliciter $\operatorname{ord}_{T=q^{-1}} L\big(B_{1/2,d}/K, T\big)$: la proposition est alors une application directe du Lemme 3.1.4. En effet, si l'on pose $L(T) := L\big(B_{1/2,d}/K, T\big)$ et

$$\forall n \in \mathcal{O}_q^{(2)}(2d), \quad \omega(n) := \boldsymbol{\theta}_n(-1) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n, \mu) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2, \boldsymbol{\theta}_n^2),$$

on peut écrire $L(T) = (1 - qT) \cdot \prod_{n \in \mathcal{O}_q^{(2)}(2d)} (1 - \omega(n) T^{u(n)})$. D'après l'Exemple 3.1.9 (illustrant le Lemme 3.1.4), on a

$$\operatorname{ord}_{T=q^{-1}} L\big(B_{1/2,d}/K, T\big) = 1 + \#\left\{ n \in \mathcal{O}_q^{(2)}(2d) \mid \omega(n) = q^{u(n)} \right\}.$$

Par définition de $\mathcal{Z}_q(2d)$, c'est ce qu'il fallait démontrer. □

On peut par ailleurs donner une expression de la valeur spéciale $L^*\big(B_{1/2,d}/K, 1\big)$ dans ce cas. Ceci nous sera utile à la Section 8.4.4.

Proposition 8.3.7. *Soit d un entier impair et premier à q. La valeur spéciale en $T = q^{-1}$ de la fonction L associée à la courbe elliptique $B_{1/2,d}/K$ admet l'expression suivante :*

$$L^*\big(B_{1/2,d}/K, 1\big) = \prod_{n \in \mathcal{Z}_q(2d)} u(n) \cdot \prod_{n \in \mathcal{V}_q^*(2d)} \left(1 - \frac{\boldsymbol{\theta}_n(-1) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n, \mu) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2, \boldsymbol{\theta}_n^2)}{q^{u(n)}} \right).$$

Démonstration. On réutilise les calculs faits à la Section 3.1. Notons $L(T) = L\big(B_{1/2,d}/K, T\big)$ et $r = \operatorname{ord}_{T=q^{-1}} L(T) = 1 + \#\mathcal{Z}_q(2d)$ (voir la Proposition précédente). Pour toute orbite $n \in \mathcal{O}_q^{(2)}(2d)$, on pose à nouveau

$$\omega(n) := \boldsymbol{\theta}_n(-1) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n, \mu) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2, \boldsymbol{\theta}_n^2) \quad \text{et} \quad g_n(T) = 1 - \omega(n) \cdot T^{u(n)}$$

et $g_0(T) = 1 - qT$ de sorte que $L(T) = g_0(T) \cdot \prod_{n \in \mathcal{O}_q^{(2)}(2d)} g_n(T)$. Par construction, on a

$$\frac{L(T)}{(1-qT)^r} = \frac{g_0(T) \cdot \prod_{n \in \mathcal{O}_q^{(2)}(2d)} g_n(T)}{(1-qT)^{1+\#\mathcal{Z}_q(2d)}} = \frac{g_0(T)}{1-qT} \cdot \prod_{n \in \mathcal{Z}_q(2d)} \frac{g_n(T)}{1-qT} \cdot \prod_{n \notin \mathcal{Z}_q(2d)} g_n(T). \tag{8.8}$$

Dans ce dernier produit, si $n \in \mathcal{Z}_q(2d)$ alors $g_n(q^{-1}) = 0$ mais

$$\left(\frac{g_n(T)}{1-qT} \right)(q^{-1}) = u(n) \neq 0;$$

et si $n \notin \mathcal{Z}_q(2d)$, on a $g_n(q^{-1}) \neq 0$. Ainsi, lorsque l'on évalue l'expression (8.8) en $T = q^{-1}$, on trouve bien l'expression annoncée de la valeur spéciale (*cf.* Définition 1.3.12). □

8.3.4 Un cas où le rang n'est pas borné

D'après la Proposition 8.3.6, pour que le rang de $B_{1/2,d}(K)$ soit « grand », il faut que $\#\mathcal{Z}_q(2d)$ soit « grand », *i.e.* il faut que « beaucoup » de $\boldsymbol{\theta}_n(-1)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2)$ soient égaux à $q^{u(n)}$ (n parcourant $\mathcal{O}_q^{(2)}(2d)$). Nous expliquons dans cette section que ce phénomène se produit effectivement pour certaines valeurs (impaires) de d.

Lemme 8.3.8. *Soit $d \geqslant 3$ un entier impair premier à q. On suppose qu'il existe un entier $N \in \mathbb{N}^*$ tel que d divise $q^N + 1$. Alors, pour toute orbite $n \in \mathcal{O}_q^{(2)}(2d)$, on a*

$$\boldsymbol{\theta}_n(-1)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2) = q^{u(n)}.$$

Autrement dit, $\mathcal{Z}_q(2d) = \mathcal{O}_q^{(2)}(2d)$ et $\mathcal{V}_q^*(2d) = \varnothing$.

Démonstration. Ce Lemme est une conséquence quasi-directe du Corollaire 2.4.5. Fixons un entier $N \in \mathbb{N}^*$ tel que d divise $q^N + 1$: on peut supposer que N est minimal pour cette propriété. D'après le Lemme 2.4.1, l'ordre de q modulo d est exactement $o_q(d) = 2N$. Comme d est impair et que $q^N + 1$ est pair, $2d$ divise également $q^N + 1$ et on peut facilement voir que $o_q(d) = o_q(2d)$ (*cf.* la remarque dans la preuve du Théorème 8.3.2). Pour toutes les orbites $n \in \mathcal{O}_q^{(2)}(2d)$, on en déduit que $u(n)$ est pair et que $2d$ divise $n(q^{u(n)/2} + 1)$ (c'est le résultat du Lemme 2.4.2). Soit $\boldsymbol{\theta}_n : \mathbb{F}_{q^{u(n)}}^\times \to \overline{\mathbb{Q}}^\times$ le caractère associé à une orbite $n \in \mathcal{O}_q^{(2)}(2d)$. Puisque $u(n)$ est pair, il existe une sous-extension $\mathbb{F}_{q^{u(n)}}/\mathbb{F}_{q^{u(n)/2}}$ quadratique de $\mathbb{F}_{q^{u(n)}}/\mathbb{F}_q$. Et comme $2d$ divise $n(q^{u(n)/2} + 1)$, la restriction de $\boldsymbol{\theta}_n$ à $\mathbb{F}_{q^{u(n)/2}}^\times$ est le caractère trivial (*cf.* la preuve du Corollaire 2.4.5). De même, la restriction du caractère quadratique $\mu : \mathbb{F}_{q^{u(n)}}^\times \to \overline{\mathbb{Q}}^\times$ à $\mathbb{F}_{q^{u(n)/2}}^\times$ est triviale. Comme n n'est pas l'orbite $\{d\}$, l'ordre de $\boldsymbol{\theta}_n$ est impair : $\boldsymbol{\theta}_n$ n'est pas le caractère quadratique et $\boldsymbol{\theta}_n^4 \neq \mathbf{1}$. Nous pouvons donc utiliser la Proposition 2.2.7 pour exprimer les sommes de Jacobi ci-dessus en termes de sommes de Gauss :

$$\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu) = \frac{\mathbf{g}_{q^{u(n)}}(\boldsymbol{\theta}_n)\cdot \mathbf{g}_{q^{u(n)}}(\mu)}{\mathbf{g}_{q^{u(n)}}(\mu\cdot\boldsymbol{\theta}_n)} \quad \text{et} \quad \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2) = \frac{\mathbf{g}_{q^{u(n)}}(\boldsymbol{\theta}_n^2)\cdot \mathbf{g}_{q^{u(n)}}(\boldsymbol{\theta}_n^2)}{\mathbf{g}_{q^{u(n)}}(\boldsymbol{\theta}_n^4)}.$$

Dans ces expressions, les caractères $\boldsymbol{\theta}_n$, μ, $\boldsymbol{\theta}_n\cdot\mu$, $\boldsymbol{\theta}_n^2$ et $\boldsymbol{\theta}_n^4$ vérifient tous la propriété suivante : ils sont non triviaux mais leur restriction à $\mathbb{F}_{q^{u(n)/2}}^\times$ est le caractère trivial. On peut donc appliquer le Théorème 2.4.4 à chacun ces 5 caractères : pour tout $c \in \mathbb{F}_{q^{u(n)}}$ tel que $\mathrm{Tr}_{\mathbb{F}_{q^{u(n)}}/\mathbb{F}_{q^{u(n)/2}}}(c) = 0$, on a

$$\frac{\mathbf{g}_{q^{u(n)}}(\boldsymbol{\theta}_n)\cdot \mathbf{g}_{q^{u(n)}}(\mu)}{\mathbf{g}_{q^{u(n)}}(\mu\cdot\boldsymbol{\theta}_n)} = \frac{\left(-\boldsymbol{\theta}_n(-c)\cdot q^{u(n)/2}\right)\cdot\left(-\mu(-c)\cdot q^{u(n)/2}\right)}{-\mu\cdot\boldsymbol{\theta}_n(-c)\cdot q^{u(n)/2}} = -q^{u(n)/2}$$

$$\text{et} \quad \frac{\mathbf{g}_{q^{u(n)}}(\boldsymbol{\theta}_n^2)\cdot \mathbf{g}_{q^{u(n)}}(\boldsymbol{\theta}_n^2)}{\mathbf{g}_{q^{u(n)}}(\boldsymbol{\theta}_n^4)} = \frac{\left(-\boldsymbol{\theta}_n^2(-c)\cdot q^{u(n)/2}\right)^2}{-\boldsymbol{\theta}_n^4(-c)\cdot q^{u(n)/2}} = -q^{u(n)/2}.$$

Par suite,

$$\boldsymbol{\theta}_n(-1)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2) = \boldsymbol{\theta}_n(-1)\cdot q^{u(n)}.$$

Mais la restriction de $\boldsymbol{\theta}_n$ à $\mathbb{F}_{q^{u(n)/2}}^\times$ est triviale et $-1 \in \mathbb{F}_q^\times \subset \mathbb{F}_{q^{u(n)/2}}^\times$, donc on a $\boldsymbol{\theta}_n(-1) = 1$. □

Lemme 8.3.9. *Pour tout entier $\nu \in \mathbb{N}$, on pose*

$$d_\nu := q^{2\nu} - q^{2\nu-1} + \cdots - q + 1 = \sum_{i=0}^{2\nu}(-q)^i.$$

Alors d_ν est un entier impair et premier à q, d_ν divise $q^{2\nu+1} + 1$ et l'ordre de q modulo $2d_\nu$ vérifie $o_q(2d_\nu) \leqslant 2(2\nu + 1)$. Dans cette situation, on a

$$\#\mathcal{O}'_q(2d_\nu) \gg_q \frac{d_\nu}{\log d_\nu},$$

où la constante implicite ne dépend que de q.

Démonstration. Soit $\nu \in \mathbb{N}$ et d_ν comme ci-dessus. En tant que somme d'un nombre impair d'entiers impairs, d_ν est un entier impair. De plus, il n'est pas divisible par q ($d_\nu \equiv 1 \bmod q$) : il est donc premier à q (car q est une puissance d'un nombre premier p). Par construction, d_ν divise $q^{2\nu+1} + 1$ grâce à l'identité

$$q^{2\nu+1} + 1 = q^{2\nu+1} - (-1)^{2\nu+1} = (q+1)\cdot(q^{2\nu} - q^{2\nu-1} + \cdots - q + 1) = (q+1)\cdot d_\nu.$$

D'après le Lemme 2.4.1, l'ordre de q modulo $2d_\nu$ vaut $2N_0$ où N_0 est le plus petit entier N tel que $2d_\nu$ divise q^N+1. Comme $2d_\nu$ divise $q^{2\nu+1}+1$, on a $N_0 \leqslant 2\nu+1$ et $o_q(2d_\nu) = 2N_0 \leqslant 2(2\nu+1)$. Enfin, démontrons la minoration de $\#\mathcal{O}'_q(2d_\nu)$ annoncée. D'après la Proposition 3.1.3, on a

$$\#\mathcal{O}'_q(2d_\nu) = \sum_{\substack{d'\mid 2d_\nu \\ d'\geqslant 2}} \frac{\phi(d')}{o_q(d')}.$$

Or, pour tout diviseur $d' \geqslant 2$ de $2d$, l'ordre de q modulo d' divise $o_q(2d_\nu)$: en particulier, $o_q(d') \leqslant o_q(2d_\nu)$. D'où

$$\#\mathcal{O}'_q(2d_\nu) \geqslant \sum_{\substack{d'\mid 2d_\nu \\ d'\geqslant 2}} \frac{\phi(d')}{o_q(2d_\nu)} = \frac{1}{o_q(2d_\nu)} \cdot \sum_{\substack{d'\mid 2d_\nu \\ d'\geqslant 2}} \phi(d') = \frac{2d_\nu - 1}{o_q(2d_\nu)}.$$

De plus, on a vu que $o_q(2d_\nu) = o_q(d_\nu) \leqslant 2(2\nu+1)$, on obtient donc :

$$\#\mathcal{O}'_q(2d_\nu) \geqslant \frac{2d_\nu - 1}{2(2\nu+1)}.$$

De la définition de $d_\nu = (q^{2\nu+1}+1)/(q+1)$, on tire que

$$(2\nu+1) \leqslant \frac{\log d_\nu + \log(q+1)}{\log q}.$$

D'où les minorations successives (et peu optimales) :

$$\begin{aligned}\frac{2d_\nu - 1}{22\nu+1} &\geqslant \log q \cdot \frac{2d_\nu - 1}{\log d_\nu + \log(q+1)} \geqslant \log q \cdot \frac{2d_\nu - 1}{2\log d_\nu} \geqslant \log q \cdot \frac{d_\nu - 1/2}{\log d_\nu} \\ &\geqslant \frac{\log q}{2} \cdot \frac{d_\nu}{\log d_\nu} = \log\sqrt{q} \cdot \frac{d_\nu}{\log d_\nu}.\end{aligned}$$

Ce qui donne finalement la minoration annoncée. □

Les deux Lemmes précédents se combinent aux résultats antérieurs pour donner :

Théorème 8.3.10. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$, on fixe $a = 1/2 \in \mathbb{F}_q \smallsetminus \{0,1\}$. Pour tout entier $\nu \in \mathbb{N}$, on pose $d_\nu = q^{2\nu} - q^{2\nu-1} + \cdots - q + 1$ comme ci-dessus. Alors*

$$\operatorname{rang} B_{1/2,d_\nu}(K) \gg_q \frac{d_\nu}{\log d_\nu},$$

la constante implicite ne dépendant que de q (et peut être choisie $\geqslant \log\sqrt{q}$).

Démonstration. Comme d_ν est un entier impair (voir le Lemme 8.3.9), la Proposition 8.3.6 donne que

$$\operatorname{rang} B_{1/2,d_\nu}(K) = 1 + \#\mathcal{Z}_q(2d_\nu),$$

où $\mathcal{Z}_q(2d_\nu) \subset \mathcal{O}_q^{(2)}(2d_\nu)$ est l'ensemble des orbites $n \in \mathcal{O}_q^{(2)}(2d_\nu)$ telles que

$$\boldsymbol{\theta}_n(-1) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n, \mu) \cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2, \boldsymbol{\theta}_n^2) = q^{u(n)}.$$

Mais par construction, d_ν divise $q^{2\nu+1}+1$. On peut donc appliquer le résultat du Lemme 8.3.8 : *toutes* les orbites $n \in \mathcal{O}_q^{(2)}(2d_\nu)$ vérifient l'égalité ci-dessus. Autrement dit, on a $\mathcal{Z}_q(2d_\nu) = \mathcal{O}_q^{(2)}(2d_\nu)$. Par conséquent,

$$\operatorname{rang} B_{1/2,d_\nu}(K) = 1 + \#\mathcal{O}_q^{(2)}(2d_\nu) = \#\mathcal{O}'_q(2d_\nu).$$

La minoration de $\#\mathcal{O}'_q(2d_\nu)$ donnée au Lemme 8.3.9 permet alors de conclure. □

Remarque 8.3.11. Sous les hypothèses du Théorème ci-dessus, la valeur spéciale $L^*\big(B_{1/2,d_\nu}/K, 1\big)$ est un entier. En effet, avec la Proposition 8.3.7, on trouve que :

$$L^*\big(B_{1/2,d_\nu}/K, 1\big) = \prod_{n\in\mathcal{O}_q^{(2)}(2d_\nu)} u(n) \in \mathbb{N}^*.$$

En particulier, on en déduit que $\log L^*\big(B_{1/2,d_\nu}/K, 1\big) \geqslant 0$ (comparer à la Proposition 8.4.8).

Remarque 8.3.12. On peut également comparer la minoration du rang obtenue dans ce Théorème à la majoration du rang que donne la Proposition 3.1.5 : il existe deux constantes ne dépendant que de q telles que, pour tout $\nu \in \mathbb{N}$,

$$\frac{d_\nu}{\log d_\nu} \ll_q \operatorname{rang} B_{1/2,d_\nu}(K) \ll_q \frac{d_\nu}{\log d_\nu}.$$

Le Théorème 8.3.10 est un résultat de « rang non borné », on peut en effet en déduire le corollaire ci-dessous.

Corollaire 8.3.13. *Soit $\mathbb{F}_q$ un corps fini de caractéristique $p \geqslant 5$ et $K = \mathbb{F}_q(t)$. Dans la famille des courbes elliptiques $B_{a,d}/K$ (où $d \geqslant 2$ est premier à q et $a \in \mathbb{F}_q \smallsetminus \{0,1\}$), le rang $r_{a,d} = \operatorname{rang} B_{a,d}(K)$ n'est pas borné :*

$$\limsup_{\substack{\operatorname{pgcd}(d,q)=1 \\ a\in\mathbb{F}_q\smallsetminus\{0,1\}}} \operatorname{rang} B_{a,d}(K) = \limsup_{\operatorname{pgcd}(d,q)=1} \operatorname{rang} B_{1/2,d}(K) = +\infty.$$

Remarque 8.3.14. Il convient de mentionner que ce résultat de « rang non borné » n'est pas une conséquence de [Ulm07b, Theorem 4.7] (voir aussi [Ber08, Theorem 4.2]). En effet, si $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et d est un entier premier à q, on note $\mathcal{N}'(B_{a,d}/K) \in \operatorname{Div}(\mathbb{P}^1)$ la partie première à $0, \infty \in \mathbb{P}^1$ du conducteur $\mathcal{N}(B_{a,d}/K)$ de $B_{a,d}$. On a $\deg \mathcal{N}'(B_{a,d}/K) = 2d$ d'après la Proposition 8.1.5. Pour appliquer [Ulm07b, Theorem 4.7], il faudrait que $\deg \mathcal{N}'(B_{a,d}/K)$ soit impair.

8.4 Ratio de Brauer-Siegel

Dans cette section, nous étudions le ratio de Brauer-Siegel des courbes elliptiques $B_{a,d}$ sur $K = \mathbb{F}_q(t)$. Dans un premier temps, nous nous plaçons dans le cas général (où $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et d est un entier premier à q) : nous démontrons une majoration de $\mathfrak{Bs}(B_{a,d}/K)$ et une minoration « faible », ces inégalités nous permettent de retrouver l'encadrement « trivial » de $\mathfrak{Bs}(B_{a,d}/K)$. Ensuite, nous nous restreignons au cas où $a = 1/2$ et d est impair : dans cette situation, nous démontrons que le ratio de Brauer-Siegel tend vers 1 lorsque $d \to \infty$.

8.4.1 Résultats obtenus

Soit $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et d un entier premier à q. Comme la courbe elliptique $B_{a,d}$ vérifie la conjecture de Birch et Swinnerton-Dyer (Théorème 8.2.6), il y a une relation inconditionnelle entre la valeur spéciale de sa fonction L et son ratio de Brauer-Siegel. Plus précisément, la Proposition 1.6.4 donne que

$$\mathfrak{Bs}\big(B_{a,d}/K\big) = 1 + \frac{\log L^*\big(B_{a,d}/K, 1\big)}{\log H\big(B_{a,d}/K\big)} + o(1) \qquad (d \to \infty). \tag{8.9}$$

Pour obtenir un encadrement du ratio de Brauer-Siegel $\mathfrak{Bs}\big(B_{a,d}/K\big)$, nous allons donc encadrer la valeur spéciale $\log L^*\big(B_{a,d}/K, 1\big)$. Comme annoncé ci-dessus, nous obtenons deux types de résultats. Tout d'abord, dans le cas général, on a :

Théorème 8.4.1. *Soit $a \in \mathbb{F}_q \smallsetminus \{0,1\}$, pour tout entier $d \geqslant 2$ premier à q, on considère la courbe $B_{a,d}$ définie sur $K = \mathbb{F}_q(t)$ par le modèle* (8.1). *Lorsque $H\big(B_{a,d}/K\big) \to \infty$ (i.e. lorsque $d \to \infty$), le ratio de Brauer-Siegel $\mathfrak{Bs}\big(B_{a,d}/K\big)$ admet l'encadrement suivant :*

$$0 + o(1) \leqslant \mathfrak{Bs}\big(B_{a,d}/K\big) \leqslant 1 + o(1).$$

C'est un cas particulier inconditionnel de [HP16, Corollary 1.13]. Dans un second temps, nous nous plaçons dans la situation de la Section 8.3.

Théorème 8.4.2. *Soit $a = 1/2$, pour tout entier* impair *$d \geqslant 2$ premier à q, on considère la courbe $B_{1/2,d}$ définie sur K par le modèle* (8.1). *Lorsque $d \to \infty$ (en étant impair et premier à q), le ratio de Brauer-Siegel $\mathfrak{Bs}\big(B_{1/2,d}/K\big)$ admet une limite et celle-ci vaut 1 :*

$$\mathfrak{Bs}\big(B_{1/2,d}/K\big) \xrightarrow[\substack{\operatorname{pgcd}(d,q)=1 \\ d \text{ impair} \\ d\to\infty}]{} 1.$$

Remarque 8.4.3. Il est sûrement possible d'étendre ce Théorème au cas où d est pair (toujours en supposant $a = 1/2$). Pour ce faire, il faudrait disposer d'une expression explicite de la fonction $L\big(B_{1/2,d}/K, T\big)$ dans ce cas (voir Théorème 8.3.2).

Cependant, il semble beaucoup plus difficile de traiter le cas où $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ est quelconque. Pour minorer $L^*\big(B_{a,d}/K, 1\big)$ dans le cas général, il faudrait en effet pouvoir étudier la répartition des sommes $\boldsymbol{S}_{q^{u(m)}}(\mathbf{t}_m; 1-2a)$ (*cf.* Théorème 8.2.1) : ceci paraît hors de portée des techniques développées ici.

8.4.2 Majoration de la valeur spéciale

Pour majorer la valeur spéciale de la fonction L associée à $B_{a,d}$, nous utilisons les techniques développées à la Section 3.1. On obtient :

Proposition 8.4.4. *Soit $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et $d \geqslant 2$ un entier premier à q. Lorsque $d \to \infty$, la valeur spéciale $L^*\big(B_{a,d}/K, 1\big)$ admet la majoration*

$$\frac{\log L^*\big(B_{a,d}/K, 1\big)}{\log H\big(B_{a,d}/K\big)} \leqslant 0 + o\big(1\big) \quad (d \to \infty).$$

Là encore, cette majoration est un cas particulier du Théorème plus général [HP16, Theorem 7.5] qui donne une telle majoration pour les valeurs spéciales de toutes les fonctions L des variétés abéliennes $A/\mathbb{F}_q(t)$. Toutefois, nous démontrons une version plus précise de façon élémentaire : il existe une constante absolue $c' > 0$ telle que

$$\frac{\log L^*\big(B_{a,d}/K, 1\big)}{\log H\big(B_{a,d}/K\big)} \leqslant c' \cdot \frac{\log\log d}{\log d} \quad (d \to \infty).$$

On peut même expliciter $c' \leqslant 40$ qui convient.

Démonstration. D'après le Théorème 8.2.1, la fonction L de la courbe $B_{a,d}$ s'écrit sous la forme d'un produit :

$$L\big(B_{a,d}/\mathbb{F}_q(t), T\big) = (1 - qT) \cdot \prod_{m \in \mathcal{O}_q^{(2)}(d)} \Big(1 - \mathbf{J}'_m \cdot \alpha_b(\mathbf{t}_m) \cdot T^{u(m)}\Big) \Big(1 - \mathbf{J}'_m \cdot \beta_b(\mathbf{t}_m) \cdot T^{u(m)}\Big),$$

où, pour tout $m \in \mathcal{O}_q^{(2)}(d)$, $\mathbf{J}'_m = \mathbf{t}_m(-1) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)$ est une somme de Jacobi et $\{\alpha_b(\mathbf{t}_m), \beta_b(\mathbf{t}_m)\}$ est la paire de nombres algébriques associés à la somme de Legendre $\boldsymbol{S}_{q^{u(m)}}(\mathbf{t}_m; b)$. Pour alléger les écritures, définissons quelques notations : on désignera $L\big(B_{a,d}/\mathbb{F}_q(t), T\big)$ par $L(T)$. Pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$, on pose

$$\omega_1(m) := \mathbf{t}_m(-1) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m) \cdot \alpha_b(\mathbf{t}_m) \quad \text{et} \quad \omega_2(m) := \mathbf{t}_m(-1) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m) \cdot \beta_b(\mathbf{t}_m)$$

et $g_m(T) := (1 - \omega_1(m) \cdot T^{u(m)}) \cdot (1 - \omega_2(m) \cdot T^{u(m)})$; enfin, soit $g_0(T) := 1 - qT$. Ainsi, on a $L(T) = g_0(T) \cdot \prod_{m \in \mathcal{O}_q^{(2)}(d)} g_m(T)$. Au facteur $g_0(T)$ près, le polynôme $L(T)$ est donc de la forme de ceux étudiés à la Section 3.1 (*cf.* l'équation (3.1) avec $K = 2$). Mais, si l'on pose $L_1(T) = L(T)/g_0(T) \in \mathbb{Z}[T]$, il n'est pas difficile de voir que les valeurs spéciales $L_1^*(q^{-1})$ et $L^*(q^{-1})$ des polynômes $L_1(T)$ et $L(T)$ sont égales. Appliquons donc la Proposition 3.1.8 (avec $K = 2$) au polynôme $L_1(T)$: on obtient que

$$\log L^*\big(B_{a,d}/K, 1\big) = \log |L_1^*(q^{-1})| \leqslant 6C \log q \cdot \frac{d \log\log d}{\log d},$$

où C est une constante absolue. Or, on a vu à la Proposition 8.1.5 que la hauteur de $B_{a,d}$ vaut $H\big(B_{a,d}/K\big) = q^{\lfloor \frac{d+1}{2} \rfloor}$. Donc on a bien la majoration :

$$\frac{\log L^*\big(B_{a,d}/K, 1\big)}{\log H\big(B_{a,d}/K\big)} \leqslant 6C \cdot \frac{d}{\lfloor \frac{d+1}{2} \rfloor} \cdot \frac{\log\log d}{\log d} \leqslant 6C \cdot \frac{2d}{d-1} \cdot \frac{\log\log d}{\log d} \leqslant 8C \cdot \frac{\log\log d}{\log d}.$$

Ce qui termine la preuve. □

Lorsque l'on utilise la majoration de la Proposition 8.4.4 dans la relation (8.9), on obtient la majoration ci-dessous du ratio de Brauer-Siegel :

Corollaire 8.4.5. *Soit $a \in \mathbb{F}_q \smallsetminus \{0,1\}$, pour tout entier $d \geqslant 2$ premier à q, le ratio de Brauer-Siegel $\mathfrak{Bs}\big(B_{a,d}/K\big)$ vérifie*

$$\mathfrak{Bs}\big(B_{a,d}/K\big) \leqslant 1 + o(1) \qquad (d \to \infty).$$

8.4.3 Minoration « faible » de la valeur spéciale

Commençons par donner une minoration de $L^*\big(B_{a,d}/K,1\big)$ valable pour tout $a \in \mathbb{F}_q \smallsetminus \{0,1\}$. Nous faisons pour cela appel aux outils mis en place à la Section 3.2.

Proposition 8.4.6. *Soit $a \in \mathbb{F}_q \smallsetminus \{0,1\}$ et $d \geqslant 2$ un entier premier à q. Lorsque $d \to \infty$, la valeur spéciale $L^*\big(B_{a,d}/K,1\big)$ admet la minoration*

$$\frac{\log L^*\big(B_{a,d}/K,1\big)}{\log H\big(B_{a,d}/K\big)} \geqslant -1 + o\big(1\big) \quad (d \to \infty).$$

Démonstration. Dans un premier temps, nous allons nous ramener à la situation étudiée à la Section 3.2. Pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$, nous notons $\mathbf{J}'_m = \mathbf{t}_m(-1) \cdot \mathbf{j}_{q^{u(m)}}(\mathbf{t}_m, \mathbf{t}_m)$ et $\alpha_m = \alpha_b(\mathbf{t}_m)$, $\beta_m = \beta_b(\mathbf{t}_m)$ les nombres algébriques apparaissant dans l'énoncé du Théorème 8.2.1. Nous avons vu que

$$L\big(B_{a,d}/K,T\big) = (1-qT) \cdot \prod_{m \in \mathcal{O}_q^{(2)}(d)} \Big(1 - \alpha_m \mathbf{J}'_m \cdot T^{u(m)}\Big)\Big(1 - \beta_m \mathbf{J}'_m \cdot T^{u(m)}\Big).$$

On pose $g_m(T) = \big(1 - \alpha_m \mathbf{J}'_m \cdot T^{u(m)}\big)\big(1 - \beta_m \mathbf{J}'_m \cdot T^{u(m)}\big)$ pour toute $m \in \mathcal{O}_q^{(2)}(d)$, où $|\alpha_m \mathbf{J}'_m| = |\beta_m \mathbf{J}'_m| = q^{u(m)}$ (*cf.* Proposition 2.2.7 et Théorème 2.2.21). Trois cas de figures se présentent alors :

- ou bien $g_m(q^{-1}) \neq 0$. Appelons $\mathcal{M}_0 = \Big\{m \in \mathcal{O}_q^{(2)}(d) \;\Big|\; g_m(q^{-1}) = 0\Big\}$.
- ou bien g_m s'annule à l'ordre 1 en $T = q^{-1}$. On note $\mathcal{M}_1 = \Big\{m \in \mathcal{O}_q^{(2)}(d) \;\Big|\; \mathrm{ord}_{T=q^{-1}}\, g_m = 1\Big\}$.
- ou bien g_m s'annule à l'ordre 2 en $T = q^{-1}$. Soit $\mathcal{M}_2 = \Big\{m \in \mathcal{O}_q^{(2)}(d) \;\Big|\; \mathrm{ord}_{T=q^{-1}}\, g_m = 2\Big\}$.

Afin d'expliciter la valeur spéciale $L^*\big(B_{a,d}/K,1\big)$ (voir Définition 1.3.12), nous devons évaluer en $T = q^{-1}$ le polynôme

$$L^*(T) := \frac{L\big(B_{a,d}/K,T\big)}{(1-qT)^r},$$

où l'on a noté $r = \mathrm{ord}_{T=q^{-1}}\, L\big(B_{a,d}/K,T\big)$. Par construction de $\mathcal{M}_0$, $\mathcal{M}_1$ et $\mathcal{M}_2$, on a

$$L^*(T) = 1 \cdot \prod_{m \in \mathcal{M}_0} g_m(T) \cdot \prod_{m \in \mathcal{M}_1} \frac{g_m(T)}{1-qT} \cdot \prod_{m \in \mathcal{M}_2} \frac{g_m(T)}{(1-qT)^2}.$$

Pour toute orbite $m \in \mathcal{O}_q^{(2)}(d)$, posons maintenant $g_m^*(T) = g_m(T)/(1-qT)^i$ si $m \in \mathcal{M}_i$ et

$$y(m) = \mathbf{J}'_m \cdot (\alpha_m + \beta_m - \mathbf{J}'_m).$$

Distinguons à nouveau trois cas :

- Si $m \in \mathcal{M}_0$ d'abord, alors $g_m = g_m^*$ et, comme $\alpha_m \cdot \beta_m = q^{u(m)}$,

$$\begin{aligned} g_m^*(q^{-1}) = g_m(q^{-1}) &= \left(1 - \frac{\alpha_m \mathbf{J}'_m}{q^{u(m)}}\right)\left(1 - \frac{\beta_m \mathbf{J}'_m}{q^{u(m)}}\right) \\ &= 1 - \frac{(\mathbf{J}'_m \alpha_m + \mathbf{J}'_m \beta_m - {\mathbf{J}'_m}^2)}{q^{u(m)}} = 1 - \frac{y(m)}{q^{u(m)}}. \end{aligned}$$

- Si $m \in \mathcal{M}_1$, alors g_m s'annule à l'ordre 1 en $T = q^{-1}$ et $g_m^*(T) = g_m(T)/(1-qT)$. Dans ce cas, ou bien $\alpha_m \mathbf{J}'_m = q^{u(m)}$ ou bien $\beta_m \mathbf{J}'_m = q^{u(m)}$. Quitte à échanger les rôles de α_m et β_m, on peut supposer que $\alpha_m \mathbf{J}'_m = q^{u(m)}$ et $\beta_m \mathbf{J}'_m \neq q^{u(m)}$. Alors

$$g_m^*(q^{-1}) = \left(\frac{g_m}{1-qT}\right)(q^{-1}) = u(m) \cdot \left(1 - \frac{\beta_m \mathbf{J}'_m}{q^{u(m)}}\right).$$

  Mais, si $\alpha_m \mathbf{J}'_m = q^{u(m)}$ c'est que $\alpha_m \mathbf{J}'_m = \alpha_m \beta_m$ et donc que $\beta_m = \mathbf{J}'_m$. Ainsi,

$$g_m^*(q^{-1}) = u(m) \cdot \left(1 - \frac{{\mathbf{J}'_m}^2}{q^{u(m)}}\right) \neq 0.$$

- Enfin, si $m \in \mathcal{M}_2$ alors g_m s'annule à l'ordre 2 en $T = q^{-1}$ et $g_m^*(T) = g_m(T)/(1-qT)^2$. Dans ce cas, on a

$$g_m^*(q^{-1}) = u(m)^2 \in \mathbb{N}^*.$$

À l'issue de ce calcul, nous avons donc

$$L^*\big(B_{a,d}/K,1\big) = \prod_{m\in\mathcal{M}_0}\left(1-\frac{y(m)}{q^{u(m)}}\right)\cdot\prod_{m\in\mathcal{M}_1}u(m)\cdot\prod_{m\in\mathcal{M}_1}\left(1-\frac{{\mathbf{J}'_m}^2}{q^{u(m)}}\right)\cdot\prod_{m\in\mathcal{M}_2}u(m)^2.$$

Puisque $u(m)\in\mathbb{N}^*$, on a $\log\prod_{m\in\mathcal{M}_2}u(m)^2\geqslant 0$ et $\log\prod_{m\in\mathcal{M}_1}u(m)\geqslant 0$. D'où

$$\log L^*\big(B_{a,d}/K,1\big)\geqslant\log\prod_{m\in\mathcal{M}_0}\left(1-\frac{y(m)}{q^{u(m)}}\right)+\log\prod_{m\in\mathcal{M}_1}\left(1-\frac{{\mathbf{J}'_m}^2}{q^{u(m)}}\right). \tag{8.10}$$

Nous avons déjà minoré le second produit de cette inégalité. En effet, la preuve de la Proposition 6.4.3 permet d'écrire que

$$\frac{1}{d\cdot\log q}\cdot\log\prod_{m\in\mathcal{M}_1}\left(1-\frac{{\mathbf{J}'_m}^2}{q^{u(m)}}\right)\geqslant 0+o(1)\qquad(d\to\infty).$$

Il reste donc à minorer le premier produit dans (8.10). Pour cela, on applique la minoration « naïve » de la Proposition 3.2.1 :

$$\log\prod_{m\in\mathcal{M}_0}\left(1-\frac{y(m)}{q^{u(m)}}\right)\geqslant-\log q\cdot d.$$

En effet, la donnée des $y(m)$ (avec $m\in\mathcal{M}_0$) vérifie les hypothèses (i), (ii) et (iii) de la Section 3.2.1. □

Cette minoration n'est pas meilleure que la minoration « naïve » de $L^*\big(B_{a,d}/K,1\big)$. Autrement dit, elle est insuffisante pour donner une minoration de $\mathfrak{Bs}\big(B_{a,d}/K\big)$ du même ordre de grandeur que la majoration du Corollaire 8.4.5.

Corollaire 8.4.7. *Soit $a\in\mathbb{F}_q\smallsetminus\{0,1\}$, pour tout entier $d\geqslant 2$ premier à q, le ratio de Brauer-Siegel $\mathfrak{Bs}\big(B_{a,d}/K\big)$ vérifie*

$$\mathfrak{Bs}\big(B_{a,d}/K\big)\geqslant 0+o(1)\qquad(d\to\infty).$$

8.4.4 Minoration « forte » de la valeur spéciale dans le cas où $a=1/2$ et d est impair

Supposons maintenant que le paramètre $a\in\mathbb{F}_q\smallsetminus\{0,1\}$ est fixé égal à $1/2$ et que d est un entier impair (et encore premier à q). À la Section 8.3, nous avons explicité la fonction $L\big(B_{1/2,d}/K,T\big)$ en termes de sommes de Jacobi. Dans cette situation, on peut donner une minoration bien meilleure de la valeur spéciale $L^*\big(B_{1/2,d}/K,1\big)$:

Proposition 8.4.8. *Soit $a=1/2\in\mathbb{F}_q$ et $d\geqslant 3$ un entier « impair » premier à q. Lorsque $d\to\infty$, la valeur spéciale $L^*\big(B_{1/2,d}/K,1\big)$ de la fonction L associée à la courbe elliptique $B_{a,d}$ admet la minoration suivante :*

$$\frac{\log L^*\big(B_{1/2,d}/K,1\big)}{\log H\big(B_{1/2,d}/K\big)}\geqslant 0+o\big(1\big)\qquad(d\text{ impair, }d\to\infty).$$

Démonstration. Pour démontrer cette minoration, nous faisons appel aux résultats de la Section 3.2 et nous suivons le plan suivant : dans un premier temps, nous minorons trivialement les termes qui peuvent l'être ; ensuite, nous vérifions que la fonction $L\big(B_{1/2,d}/K,T\big)$ vérifie les hypothèses de la Section 3.2.1 ; puis nous utilisons le Théorème 3.2.2 pour donner un minorant de $L^*\big(B_{1/2,d}/K,1\big)$; enfin, il reste à montrer que ce minorant est « bon » en utilisant le Théorème 3.4.1.

Soit d un entier impair et premier à q. Tout d'abord, rappelons que nous avons donné (Proposition 8.3.7) l'expression suivante de $L^*\big(B_{1/2,d}/K,1\big)$:

$$L^*\big(B_{1/2,d}/K,1\big)=\prod_{n\in\mathcal{Z}_q(2d)}u(n)\cdot\prod_{n\in\mathcal{V}_q^*(2d)}\left(1-\frac{\boldsymbol{\theta}_n(-1)\cdot\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2)}{q^{u(n)}}\right),$$

où $\mathcal{V}_q^*(2d)=\mathcal{O}_q^{(2)}(2d)\smallsetminus\mathcal{Z}_q(2d)$ avec

$$\mathcal{Z}_q(2d)=\left\{n\in\mathcal{O}_q^{(2)}(2d)\;\middle|\;\boldsymbol{\theta}_n(-1)\cdot\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot\mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2)=q^{u(n)}\right\}.$$

Dans le produit, le terme $\prod_{n\in\mathcal{Z}_q(2d)} u(n)$ est un entier strictement positif. On en déduit la première minoration de $L^*\big(B_{1/2,d}/K,1\big)$:

$$\begin{aligned}\log L^*\big(B_{1/2,d}/K,1\big) &= \log \prod_{n\in\mathcal{Z}_q(2d)} u(n) + \log \prod_{n\in\mathcal{V}_q^*(2d)} \left(1-\frac{\boldsymbol{\theta}_n(-1)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2)}{q^{u(n)}}\right)\\ &\geqslant \log 1 + \log \prod_{n\in\mathcal{V}_q^*(2d)} \left(1-\frac{\boldsymbol{\theta}_n(-1)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2)}{q^{u(n)}}\right)\\ &\geqslant \log \prod_{n\in\mathcal{V}_q^*(2d)} \left(1-\frac{\boldsymbol{\theta}_n(-1)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2)}{q^{u(n)}}\right). \end{aligned} \tag{8.11}$$

Pour minorer ce dernier produit, nous faisons à nouveau appel aux résultats de la Section 3.2. Pour cela, pour toute orbite $n\in\mathcal{O}_q^{(2)}(2d)$, on pose

$$\omega(n) := \boldsymbol{\theta}_n(-1)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n,\mu)\cdot \mathbf{j}_{q^{u(n)}}(\boldsymbol{\theta}_n^2,\boldsymbol{\theta}_n^2).$$

D'autre part, par construction de $\mathcal{V}_q^*(2d)$, ce nombre algébrique $\omega(n)$ est différent de $q^{u(n)}$ pour toute $n\in\mathcal{V}_q^*(2d)$. Vérifions que la donnée de $\omega(n)$ et de $\mathcal{V}_q^*(2d)$ satisfait aux hypothèses (i), (ii) et (iii) de la Section 3.2.1 :

(i) Pour toute orbite $n\in\mathcal{O}_q^{(2)}(2d)$, on a $\omega(n)\in\mathbb{Q}(\zeta_{d'})\subset\mathbb{Q}(\zeta_{2d})$, où $d'=2d/\operatorname{pgcd}(2d,n)$. C'est clair car, pour tout choix de représentant de n, le caractère $\boldsymbol{\theta}_n : \mathbb{F}_{q^{u(n)}}^\times \to \overline{\mathbb{Q}}^\times$ est d'ordre d'. De plus, comme $n\neq\{0\},\{d\}$, on a $d'>2$. D'où l'on tire, au vu du module des sommes de Jacobi (Proposition 2.2.7), que $|\omega(n)|=q^{u(n)}$ dans tout plongement complexe de $\mathbb{Q}(\zeta_{d'})$.

(ii) Pour toute orbite $n\in\mathcal{O}_q^{(2)}(2d)$ et tout $a\in(\mathbb{Z}/d\mathbb{Z})^\times$, on note encore $\sigma_a\in\operatorname{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ l'automorphisme galoisien correspondant à a. Alors, vu l'action du groupe de Galois $\operatorname{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ sur les sommes de Jacobi (Lemme 3.3.8), on a $\sigma_a(\omega(n))=\omega(a\cdot n)$.

(iii) Finalement, comme

$$\prod_{n\in\mathcal{V}_q^*(2d)}\left(1-\frac{\omega(n)}{q^{u(n)}}\right)=\frac{L^*\big(B_{1/2,d}/K,1\big)}{\prod_{n\in\mathcal{Z}_q(2d)}u(n)},$$

le produit du membre de gauche est un nombre rationnel strictement positif (car la valeur spéciale $L^*\big(B_{1/2,d}/K,1\big)$ l'est).

La donnée des $\omega(n)$ vérifie donc les hypothèses de la Section 3.2.1 et l'on peut appliquer le Théorème 3.2.2. Rappelons d'abord quelques notations. Pour définir les caractères $\boldsymbol{\theta}_n$, nous avons fixé un idéal premier $\overline{\mathfrak{P}}$ de $\overline{\mathbb{Z}}$ au-dessus de p. Pour tout diviseur $d'>2$ de $2d$, on note $\mathfrak{p}'$ l'idéal premier de $\mathbb{Q}(\zeta_{d'})$ qui est au-dessous de $\overline{\mathfrak{P}}$. On conserve l'identification de $\operatorname{Gal}(\mathbb{Q}(\zeta_{d'})/\mathbb{Q})$ avec $(\mathbb{Z}/d'\mathbb{Z})^\times$ et l'on note $G_{d'}=(\mathbb{Z}/d'\mathbb{Z})^\times$, $\langle p\rangle_{d'}$ et $\langle q\rangle_{d'}$ les sous-groupes de G'_d engendrés respectivement par $p \bmod d'$ et $q \bmod d'$. On définit alors

$$w'(d') := o_q(d')\cdot \sum_{n'\in G_{d'}/\langle q\rangle_{d'}} \max\left\{0, 1-\frac{\operatorname{ord}_{\mathfrak{p}'}\omega\left(\frac{2d}{d'}n'\right)}{o_q(d')\cdot[\mathbb{F}_q:\mathbb{F}_p]}\right\}.$$

L'application du Théorème 3.2.2 donne la minoration :

$$\prod_{n\in\mathcal{V}_q^*(2d)}\left(1-\frac{\omega(n)}{q^{u(n)}}\right)\geqslant -\log q\cdot\sum_{\substack{d'\mid 2d\\ d'>2}} w'(d'). \tag{8.12}$$

Pour obtenir la minoration souhaitée de $L^*\big(B_{1/2,d}/K,1\big)$, il reste à majorer $w'(d')$ pour tout diviseur $d'>2$ de $2d$. Plus précisément, il suffit de montrer que $w'(d')/\phi(d')\to\ 0$ lorsque $d'\to\infty$. Séparons la preuve de ce fait en deux Lemmes.

Définissons une fonction en escaliers $G:[0,1]\to\mathbb{R}$ par

$$G(x)=\begin{cases}2 & \text{si } x\in\left[0,\frac14\right]\\ 1 & \text{si } x\in\left]\frac14,\frac34\right]\\ 0 & \text{si } x\in\left]\frac34,1\right].\end{cases}$$

On constate que $\int_0^1 G(t)\mathrm{d}t=1$ et qu'à l'aide de G, on peut expliciter la quantité $w'(d')$:

Lemme 8.4.9. *Soit $d' > 2$ un diviseur de $2d$. On a*

$$w'(d') = o_q(d') \cdot \sum_{n' \in G_{d'}/\langle q \rangle_{d'}} \max\left\{0, \int_0^1 G(t)\mathrm{d}t - \frac{1}{\#\langle p \rangle_{d'}} \sum_{\pi \in \langle p \rangle_{d'}} G\left(\left\{\tfrac{n'\pi}{d'}\right\}\right)\right\}.$$

Démonstration. Il s'agit essentiellement d'expliciter les valuations $\mathfrak{p}'$-adiques de $\omega\left(\frac{2d}{d'}n'\right)$. Notons $\theta = o_q(d') = \#\langle q \rangle_{d'}$ et $Q = q^\theta$. Pour toute orbite $n' \in G_{d'}/\langle q \rangle_{d'}$, on choisit un représentant de celle-ci dans $\mathbb{Z}/d'\mathbb{Z}$ (encore noté n') et l'on note $n = 2dn'/d' \in \mathbb{Z}/2d\mathbb{Z}$. On peut écrire

$$\begin{aligned}\omega\left(\tfrac{2d}{d'}n'\right) &= \boldsymbol{\theta}_n(-1) \cdot \mathbf{j}_Q(\boldsymbol{\theta}_n, \mu) \cdot \mathbf{j}_Q(\boldsymbol{\theta}_n^2, \boldsymbol{\theta}_n^2) = \boldsymbol{\theta}_n(-4) \cdot \mathbf{j}_Q(\boldsymbol{\theta}_n, \boldsymbol{\theta}_n) \cdot \mathbf{j}_Q(\boldsymbol{\theta}_n^2, \boldsymbol{\theta}_n^2) \\ &= \mathbf{t}(-4)^{(Q-1)n'/d'} \cdot \mathbf{j}_Q\left(\mathbf{t}^{(Q-1)n'/d'}, \mathbf{t}^{(Q-1)n'/d'}\right) \cdot \mathbf{j}_Q\left(\mathbf{t}^{(Q-1)2n'/d'}, \mathbf{t}^{(Q-1)2n'/d'}\right),\end{aligned}$$

où $\mathbf{t}(-1)^{(Q-1)n'/d'}$ est une racine (d'-ième) de l'unité. En particulier, on a $\mathrm{ord}_{\mathfrak{p}'}\, \mathbf{t}(-4)^{(Q-1)n'/d'} = 0$. On peut alors invoquer le calcul des valuations $\mathfrak{p}'$-adiques des sommes de Jacobi que l'on a rappelé au Théorème 3.3.9 et à la Proposition 3.3.10 : on trouve

$$\mathrm{ord}_{\mathfrak{p}'}\, \mathbf{j}_Q\left(\mathbf{t}^{(Q-1)n'/d'}, \mathbf{t}^{(Q-1)n'/d'}\right) = \frac{[\mathbb{F}_Q : \mathbb{F}_p]}{\#\langle p \rangle_{d'}} \cdot \sum_{\pi \in \langle p \rangle_{d'}} \left\lfloor \left\{\tfrac{-n'}{d'}\right\} + \left\{\tfrac{-n'}{d'}\right\} \right\rfloor$$

$$\text{et } \mathrm{ord}_{\mathfrak{p}'}\, \mathbf{j}_Q\left(\mathbf{t}^{(Q-1)2n'/d'}, \mathbf{t}^{(Q-1)2n'/d'}\right) = \frac{[\mathbb{F}_Q : \mathbb{F}_p]}{\#\langle p \rangle_{d'}} \cdot \sum_{\pi \in \langle p \rangle_{d'}} \left\lfloor \left\{\tfrac{-2n'}{d'}\right\} + \left\{\tfrac{-2n'}{d'}\right\} \right\rfloor.$$

Sommant ces deux égalités, on obtient l'expression suivante de $\mathrm{ord}_{\mathfrak{p}'}\, \omega\left(\frac{2d}{d'}n'\right)$:

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}'}\, \omega\left(\tfrac{2d}{d'}n'\right) &= \mathrm{ord}_{\mathfrak{p}'}\, \mathbf{j}_Q\left(\mathbf{t}^{(Q-1)n'/d'}, \mathbf{t}^{(Q-1)n'/d'}\right) + \mathrm{ord}_{\mathfrak{p}'}\, \mathbf{j}_Q\left(\mathbf{t}^{(Q-1)2n'/d'}, \mathbf{t}^{(Q-1)2n'/d'}\right) \\ &= \frac{[\mathbb{F}_Q : \mathbb{F}_p]}{\#\langle p \rangle_{d'}} \cdot \sum_{\pi \in \langle p \rangle_{d'}} \left(\left\lfloor 2\left\{\tfrac{-n'}{d'}\right\}\right\rfloor + \left\lfloor 2\left\{\tfrac{-2n'}{d'}\right\}\right\rfloor\right).\end{aligned}$$

Une rapide étude montre que, pour tout $y \in]0,1[$, on a

$$\lfloor 2\{-y\}\rfloor + \lfloor 2\{-2y\}\rfloor = \begin{cases} 2 & \text{si } y \in \left]0, \frac{1}{4}\right] \\ 1 & \text{si } y \in \left]\frac{1}{4}, \frac{3}{4}\right] \\ 0 & \text{si } y \in \left]\frac{3}{4}, 1\right[\end{cases} = G(y).$$

Si bien que l'on peut reformuler l'expression de $\mathrm{ord}_{\mathfrak{p}'}\, \omega\left(\frac{2d}{d'}n'\right)$ à l'aide de la fonction $G : [0,1] \to \mathbb{R}$ définie avant l'énoncé du Lemme :

$$\mathrm{ord}_{\mathfrak{p}'}\, \omega\left(\tfrac{2d}{d'}n'\right) = \frac{[\mathbb{F}_Q : \mathbb{F}_p]}{\#\langle p \rangle_{d'}} \cdot \sum_{\pi \in \langle p \rangle_{d'}} G\left(\left\{\tfrac{n'\pi}{d'}\right\}\right).$$

Il ne reste qu'à reporter cette identité dans la définition de $w'(d')$ pour terminer la preuve. □

Maintenant que $w'(d')$ est assez explicite, nous pouvons démontrer la majoration annoncée :

Lemme 8.4.10. *Pour tout diviseur $d' > 2$ de d, on a*

$$\frac{w'(d')}{\phi(d')} \xrightarrow[d' \to \infty]{} 0.$$

Démonstration. Avec l'expression de $w'(d')$ obtenue au Lemme ci-dessus, on peut écrire

$$0 \leqslant \frac{w'(d')}{\phi(d')} \leqslant \frac{o_q(d')}{\phi(d')} \cdot \sum_{n' \in G_{d'}/\langle q \rangle_{d'}} \left| \int_0^1 G(t)\mathrm{d}t - \frac{1}{\#\langle p \rangle_{d'}} \sum_{\pi \in \langle p \rangle_{d'}} G\left(\left\{\tfrac{n'\pi}{d'}\right\}\right)\right|$$

puisque $\max\{0, y\} \leqslant |y|$ pour tout $y \in \mathbb{R}$. Avec les notations introduites ci-avant, on a de plus $\frac{o_q(d')}{\phi(d')} = \frac{\#\langle q \rangle_{d'}}{\#G_{d'}} = \frac{1}{\#(G_{d'}/\langle q \rangle_{d'})}$. On utilise alors le théorème d'équidistribution de la Section 3.4. Plus précisément, d'après le Corollaire 3.4.14 (et les remarques qui suivent la Proposition 3.4.13), lorsque $d' \to \infty$, on a

$$\frac{1}{\#(G_{d'}/\langle q \rangle_{d'})} \cdot \sum_{n' \in G_{d'}/\langle q \rangle_{d'}} \left| \int_0^1 G(t)\mathrm{d}t - \frac{1}{\#\langle p \rangle_{d'}} \sum_{\pi \in \langle p \rangle_{d'}} G\left(\left\{\tfrac{n'\pi}{d'}\right\}\right)\right| \leqslant \kappa' \cdot (\log p)^{1/6} \cdot \left(\frac{\log\log d'}{\log d'}\right)^{1/6},$$

où $\kappa' > 0$ est une constante absolue (que l'on peut choisir $\leqslant 16$). Nous nous contenterons de la version faible suivante :

$$\frac{1}{\#(G_{d'}/\langle q\rangle_{d'})} \cdot \sum_{n' \in G_{d'}/\langle q\rangle_{d'}} \left| \int_0^1 G(t)\mathrm{d}t - \frac{1}{\#\langle p\rangle_{d'}} \sum_{\pi \in \langle p\rangle_{d'}} G\left(\left\{\tfrac{n'\pi}{d'}\right\}\right) \right| = o(1).$$

La constante implicite ne dépend alors que de p. Ce qui conclut la preuve du fait que $w'(d')/\phi(d')$ converge vers 0. □

Nous sommes à présent en mesure de terminer la preuve de la Proposition 8.4.8. Rappelons que $H\big(B_{1/2,d}/K\big) = q^{\left\lfloor \frac{d+1}{2} \right\rfloor}$ (Proposition 8.1.5). En combinant ceci avec (8.11) et (8.12), on obtient

$$\frac{\log L^*\big(B_{1/2,d}/K, 1\big)}{\log H\big(B_{1/2,d}/K\big)} \geqslant -\frac{1}{\left\lfloor \frac{d+1}{2} \right\rfloor} \cdot \sum_{\substack{d'|2d \\ d'>2}} w'(d') \geqslant -\frac{2}{d+1} \cdot \sum_{\substack{d'|2d \\ d'>2}} w'(d') = -\frac{4d}{d+1} \cdot \frac{1}{2d} \sum_{\substack{d'|2d \\ d'>2}} w'(d').$$

Or, $4d/(d+1) \to 4$ lorsque $d \to \infty$ et l'on vient de montrer que $w'(d') = o\big(\phi(d')\big)$ pour tout diviseur $d' > 2$ de $2d$. Il découle donc du Lemme 3.4.16 que

$$\frac{1}{2d} \sum_{\substack{d'|2d \\ d'>2}} w'(d') \xrightarrow[d\to\infty]{} 0.$$

Finalement, on a

$$\frac{\log L^*\big(B_{1/2,d}/K, 1\big)}{\log H\big(B_{1/2,d}/K\big)} \geqslant 0 - o(1) \quad (d \to \infty).$$

Ce qu'il fallait démontrer. □

Corollaire 8.4.11. *Soit $a = 1/2 \in \mathbb{F}_q$, pour tout entier impair $d \geqslant 2$ et premier à q, le ratio de Brauer-Siegel $\mathfrak{Bs}\big(B_{1/2,d}/K\big)$ vérifie :*

$$\mathfrak{Bs}\big(B_{1/2,d}/K\big) \geqslant 1 - o(1) \qquad (d \to \infty).$$


That's all Folks!

Bibliographie

[Art86] Michael Artin : Néron models. *In Arithmetic geometry (Storrs, Conn., 1984)*, pages 213–230. Springer, New York, 1986. ↑ 65

[Ber08] Lisa Berger : Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields. *J. Number Theory*, 128(12):3013–3030, 2008. ↑ 27, 30, 31, 33, 51, 54, 55, 56, 79, 159, 160, 178, 185, 194, 210, 215, 216, 226, 227, 233

[BK10] Enrico Bombieri et Nicholas M. Katz : A note on lower bounds for Frobenius traces. *Enseign. Math. (2)*, 56(3-4):203–227, 2010. ↑ 34, 57

[Bra47] Richard Brauer : On the zeta-functions of algebraic number fields. *Amer. J. Math.*, 69:243–250, 1947. ↑ 19, 41, 83

[Bru92] Armand Brumer : The average rank of elliptic curves. I. *Invent. Math.*, 109(3):445–472, 1992. ↑ 81, 82, 87, 90, 121, 126

[BW93] A. Baker et G. Wüstholz : Logarithmic forms and group varieties. *J. Reine Angew. Math.*, 442:19–62, 1993. ↑ 34, 57

[Cas65] John W. S. Cassels : Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965. ↑ 77

[Cas91] John W. S. Cassels : *Lectures on elliptic curves*, volume 24 de *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991. ↑ 62, 68

[CHU14] Ricardo P. Conceição, Chris Hall et Douglas Ulmer : Explicit points on the Legendre curve II. *Math. Res. Lett.*, 21(2):261–280, 2014. ↑ 27, 30, 50, 53, 75, 149, 154, 158, 185

[Coh07] Henri Cohen : *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 de *Graduate Texts in Mathematics*. Springer, New York, 2007. ↑ 102, 103, 122, 135, 137

[Con06] Brian Conrad : Chow's K/k-image and K/k-trace, and the Lang-Néron theorem. *Enseign. Math. (2)*, 52(1-2):37–108, 2006. ↑ 68, 77

[Con15] Brian Conrad : Minimal models for elliptic curves. 2015. http://math.stanford.edu/~conrad/papers/minimalmodel.pdf. ↑ 65

[Del74] Pierre Deligne : La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974. ↑ 69

[Del80] Pierre Deligne : La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980. ↑ 69

[DH35] Harold Davenport et Helmut Hasse : Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *J. Reine Angew. Math.*, 172:151–182, 1935. ↑ 108

[DO14] Christopher Davis et Thomas Occhipinti : Explicit points on $y^2 + xy - t^d y = x^3$ and related character sums. (preprint), 2014. http://www.math.uci.edu/~davis/RationalGeneration.pdf. ↑ 27, 51, 199

[Eva86] Ronald J. Evans : Hermite character sums. *Pacific J. Math.*, 122(2):357–390, 1986. ↑ 29, 52, 103

[GL78] Sudesh K. Gogia et Indar S. Luthar : The Brauer-Siegel theorem for algebraic function fields. *J. Reine Angew. Math.*, 299/300:28–37, 1978. ↑ 21, 43

[Gor79] William J. GORDON : Linking the conjectures of Artin-Tate and Birch-Swinnerton-Dyer. *Compositio Math.*, 38(2):163–199, 1979. ↑ 22, 45, 76, 77, 78, 100

[Gre87] John GREENE : Hypergeometric functions over finite fields. *Trans. Amer. Math. Soc.*, 301(1):77–101, 1987. ↑ 103

[Gro95] Alexander GROTHENDIECK : Formule de Lefschetz et rationalité des fonctions L. *In Séminaire Bourbaki, Vol. 9*, pages Exp. No. 279, 41–55. Soc. Math. France, Paris, 1995. ↑ 72

[Gro11] Benedict H. GROSS : Lectures on the conjecture of Birch and Swinnerton-Dyer. *In Arithmetic of L-functions*, volume 18 de *IAS/Park City Math. Ser.*, pages 169–209. Amer. Math. Soc., Providence, RI, 2011. ↑ 61, 63, 64, 66, 67, 72, 76, 79

[GS95] Dorian GOLDFELD et Lucien SZPIRO : Bounds for the order of the Tate-Shafarevich group. *Compositio Math.*, 97(1-2):71–87, 1995. Special issue in honour of Frans Oort. ↑ 64, 66, 69, 80, 88

[Hal06] Chris HALL : L-functions of twisted Legendre curves. *J. Number Theory*, 119(1):128–147, 2006. ↑ 73

[Har77] Robin HARTSHORNE : *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. ↑ 61, 62

[Hin07] Marc HINDRY : Why is it difficult to compute the Mordell-Weil group ? *In Diophantine geometry*, volume 4 de *CRM Series*, pages 197–219. Ed. Norm., Pisa, 2007. ↑ 15, 18, 26, 37, 40, 49, 66, 83, 84, 85

[Hin08] Marc HINDRY : *Arithmétique : primalité et codes, théorie analytique des nombres, équations diophantiennes, courbes elliptiques*. Tableau noir. Calvage & Mounet, 2008. ↑ 62, 64, 101, 102, 118, 153

[Hin10] Marc HINDRY : Introduction to zeta and L-functions from arithmetic geometry and some applications. 2010. https://webusers.imj-prg.fr/~marc.hindry/Notes_rev_Brasilia.pdf. ↑ 21, 43, 69, 70, 76, 83

[HP16] Marc HINDRY et Amìlcar PACHECO : An analogue of the Brauer–Siegel theorem for abelian varieties in positive characteristic. *Moscow Math. J.*, 16(1):45—93, January–March 2016. ↑ 15, 18, 19, 23, 25, 26, 28, 33, 35, 37, 40, 41, 46, 48, 49, 50, 51, 57, 59, 66, 76, 78, 80, 83, 84, 85, 86, 87, 88, 89, 91, 121, 122, 141, 161, 179, 189, 197, 211, 213, 233, 234

[HS88] Marc HINDRY et Joseph H. SILVERMAN : The canonical height and integral points on elliptic curves. *Invent. Math.*, 93(2):419–450, 1988. ↑ 64

[HS00] Marc HINDRY et Joseph H. SILVERMAN : *Diophantine geometry*, volume 201 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction. ↑ 62, 63, 64, 65, 67, 68, 72, 76, 169, 203

[Hus04] Dale HUSEMÖLLER : *Elliptic curves*, volume 111 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. ↑ 150, 166, 186, 200

[HW08] Godfrey H. HARDY et Edward M. WRIGHT : *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth édition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles. ↑ 144

[IR90] Kenneth IRELAND et Michael ROSEN : *A classical introduction to modern number theory*, volume 84 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 1990. ↑ 94, 101, 102, 122, 132, 135, 137, 139, 173

[Kat81] Nicholas M. KATZ : Crystalline cohomology, Dieudonné modules, and Jacobi sums. *In Automorphic forms, representation theory and arithmetic (Bombay, 1979)*, volume 10 de *Tata Inst. Fund. Res. Studies in Math.*, pages 165–246. Tata Inst. Fundamental Res., Bombay, 1981. ↑ 70, 95, 100, 102, 106

[KM85] Nicholas M. KATZ et Barry MAZUR : *Arithmetic moduli of elliptic curves*, volume 108 de *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985. ↑ 169

[KN74] Lauwrens KUIPERS et Harald NIEDERREITER : *Uniform distribution of sequences*. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1974. Pure and Applied Mathematics. ↑ 142

[KT03] Kazuya KATO et Fabien TRIHAN : On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$. *Invent. Math.*, 153(3):537–592, 2003. ↑ 22, 25, 45, 48, 78, 84

[KT08] Boris È. KUNYAVSKIĬ et Michael A. TSFASMAN : Brauer-Siegel theorem for elliptic surfaces. *Int. Math. Res. Not. IMRN*, (8):Art. ID rnn009, 9, 2008. ↑ 24, 47, 91

[KT10] Boris È. KUNYAVSKIĬ et Michael A. TSFASMAN : Erratum to : Brauer-Siegel theorem for elliptic surfaces. *Int. Math. Res. Not. IMRN*, (16):3263, 2010. ↑ 25, 47, 91

[Lan83a] Serge LANG : Conjectured Diophantine estimates on elliptic curves. *In Arithmetic and geometry, Vol. I*, volume 35 de *Progr. Math.*, pages 155–171. Birkhäuser Boston, Boston, MA, 1983. ↑ 16, 17, 38, 40, 41, 84, 85

[Lan83b] Serge LANG : *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983. ↑ 62, 67, 68, 77

[Lan94] Serge LANG : *Algebraic number theory*, volume 110 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 1994. ↑ 21, 43, 76, 83, 135, 137

[Len92] Hendrik W. LENSTRA, Jr. : Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 26(2):211–244, 1992. ↑ 16, 38

[Liu02] Qing LIU : *Algebraic geometry and arithmetic curves*. OUP Oxford, (Trad. Erné, Reinie) édition, 2002. ↑ 65

[LN59] Serge LANG et André NÉRON : Rational points of abelian varieties over function fields. *Amer. J. Math.*, 81:95–118, 1959. ↑ 67, 77

[LN97] Rudolf LIDL et Harald NIEDERREITER : *Finite fields*, volume 20 de *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second édition, 1997. With a foreword by P. M. Cohn. ↑ 94, 101, 102, 103, 105, 108, 116, 119, 120

[Man71] Yuri I. MANIN : Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971. ↑ 85

[Mes86] Jean-François MESTRE : Formules explicites et minorations de conducteurs de variétés algébriques. *Compositio Math.*, 58(2):209–232, 1986. ↑ 82

[Mic99] Philippe MICHEL : Sur les zéros de fonctions L sur les corps de fonctions. *Math. Ann.*, 313(2):359–370, 1999. ↑ 26, 49

[Mil68] James S. MILNE : The Tate-Šafarevič group of a constant abelian variety. *Invent. Math.*, 6:91–105, 1968. ↑ 22, 24, 26, 33, 45, 49, 57, 67, 79, 89

[Mil75] James S. MILNE : On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975. ↑ 22, 45, 78

[Mil80] James S. MILNE : *Étale cohomology*, volume 33 de *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980. ↑ 68, 70, 72, 74

[Mil86] James S. MILNE : Abelian varieties. *In Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986. ↑ 63

[Mon94] Hugh L. MONTGOMERY : *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84 de *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC ; by the American Mathematical Society, Providence, RI, 1994. ↑ 142

[Mum84] David MUMFORD : *Tata lectures on theta. II*, volume 43 de *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1984. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. ↑ 111

[Nat00] Melvyn B. NATHANSON : *Elementary methods in number theory*, volume 195 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. ↑ 142

[Occ12] Thomas OCCHIPINTI : A family of elliptic curves of large rank. *J. Number Theory*, 132(4): 657–665, 2012. ↑ 33, 56, 74, 190

[Oes90] Joseph OESTERLÉ : Empilements de sphères. *Astérisque*, (189-190):Exp. No. 727, 375–397, 1990. Séminaire Bourbaki, Vol. 1989/90. ↑ 61, 76, 89

[OU14] Thomas OCCHIPINTI et Douglas ULMER : Low-dimensional factors of superelliptic jacobians. *European Journal of Mathematics*, 1(2):279–285, 2014. ↑ 141

[Poo07] Bjorn POONEN : Gonality of modular curves in characteristic p. *Math. Res. Lett.*, 14(4):691–701, 2007. ↑ 16, 38, 80

[PS00] Jérôme PESENTI et Lucien SZPIRO : Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques. *Compositio Math.*, 120(1):83–117, 2000. ↑ 64

[PU14] Rachel PRIES et Douglas ULMER : Arithmetic of abelian varieties in Artin-Schreier extensions. (preprint), 2014. http://people.math.gatech.edu/~ulmer/research/preprints/AS.pdf. ↑ 79

[Ray95] Michel RAYNAUD : Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes. *In Séminaire Bourbaki, Vol. 9*, pages Exp. No. 286, 129–147. Soc. Math. France, Paris, 1995. ↑ 73

[Ros02] Michael ROSEN : *Number theory in function fields*, volume 210 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. ↑ 61, 70, 81

[RV99] Dinakar RAMAKRISHNAN et Robert J. VALENZA : *Fourier analysis on number fields*, volume 186 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999. ↑ 62, 76

[Saw92] Yoshiaki SAWABE : Legendre character sums. *Hiroshima Math. J.*, 22(1):15–22, 1992. ↑ 103

[Ser65] Jean-Pierre SERRE : Zeta and L functions. *In Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 82–92. Harper & Row, New York, 1965. ↑ 69

[Ser97] Jean-Pierre SERRE : *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third édition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. ↑ 62, 67, 169, 203

[Shi86] Tetsuji SHIODA : An explicit algorithm for computing the Picard number of certain algebraic surfaces. *Amer. J. Math.*, 108(2):415–432, 1986. ↑ 22, 45, 117

[Shi87] Tetsuji SHIODA : Some observations on Jacobi sums. *In Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986)*, volume 12 de *Adv. Stud. Pure Math.*, pages 119–135. North-Holland, Amsterdam, 1987. ↑ 32, 55, 132, 139, 140

[Shi90] Tetsuji SHIODA : On the Mordell-Weil lattices. *Comment. Math. Univ. St. Paul.*, 39(2):211–240, 1990. ↑ 65, 67, 68

[Shi92] Tetsuji SHIODA : Some remarks on elliptic curves over function fields. *Astérisque*, (209):12, 99–114, 1992. Journées Arithmétiques, 1991 (Geneva). ↑ 73, 74, 170

[Shy77] Jih Min SHYR : On some class number relations of algebraic tori. *Michigan Math. J.*, 24(3):365–377, 1977. ↑ 21, 44

[Sie35] Carl Ludwig SIEGEL : Über die Classenzahl quadratischer Zahlkörper. *Acta Arith.*, 1:83–86, 1935. ↑ 19, 41, 83

[Sie69] Carl Ludwig SIEGEL : Abschätzung von Einheiten. *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II*, 1969:71–86, 1969. ↑ 20, 42, 83

[Sil86a] Joseph H. SILVERMAN : Heights and elliptic curves. *In Arithmetic geometry (Storrs, Conn., 1984)*, pages 253–265. Springer, New York, 1986. ↑ 64, 66

[Sil86b] Joseph H. SILVERMAN : The theory of height functions. *In Arithmetic geometry (Storrs, Conn., 1984)*, pages 151–166. Springer, New York, 1986. ↑ 67

[Sil94] Joseph H. SILVERMAN : *Advanced topics in the arithmetic of elliptic curves*, volume 151 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. ↑ 61, 63, 64, 65, 66, 67, 68, 151, 187, 200, 201, 202, 217

[Sil09] Joseph H. SILVERMAN : *The arithmetic of elliptic curves*, volume 106 de *Graduate Texts in Mathematics*. Springer, Dordrecht, second édition, 2009. ↑ 61, 62, 63, 66, 67, 71, 72, 76, 167, 169, 200, 203, 216

[SK79] Tetsuji SHIODA et Toshiyuki KATSURA : On Fermat varieties. *Tôhoku Math. J. (2)*, 31(1):97–115, 1979. ↑ 23, 34, 45, 57, 77, 117, 139, 170

[SS10] Matthias SCHÜTT et Tetsuji SHIODA : Elliptic surfaces. *In Algebraic geometry in East Asia—Seoul 2008*, volume 60 de *Adv. Stud. Pure Math.*, pages 51–160. Math. Soc. Japan, Tokyo, 2010. ↑ 61, 62, 63, 64, 65, 67, 68, 77, 88, 169, 186, 202, 203

[Sta74] Harold M. STARK : Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23:135–152, 1974. ↑ 21, 43

[Sti90] Ludwig STICKELBERGER : Über eine Verallgemeinerung der Kreistheilung. *Math. Ann.*, 37(3):321–367, 1890. ↑ 135

[Szp90] Lucien SZPIRO : Discriminant et conducteur des courbes elliptiques. *Astérisque*, (183):7–18, 1990. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). ↑ 64, 66

[Tat65] John T. TATE : Algebraic cycles and poles of zeta functions. *In Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 93–110. Harper & Row, New York, 1965. ↑ 77

[Tat75] John T. TATE : Algorithm for determining the type of a singular fiber in an elliptic pencil. *In Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975. ↑ 15, 37, 65, 66, 151, 167, 187, 200, 217

[Tat94] John T. TATE : Conjectures on algebraic cycles in l-adic cohomology. *In Motives (Seattle, WA, 1991)*, volume 55 de *Proc. Sympos. Pure Math.*, pages 71–83. Amer. Math. Soc., Providence, RI, 1994. ↑ 22, 77

[Tat66] John T. TATE : On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. *In Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1965/66. ↑ 22, 45, 67, 74, 76, 77, 78

[TŠ67] John T. TATE et Igor R. ŠAFAREVIČ : The rank of elliptic curves. *Dokl. Akad. Nauk SSSR*, 175:770–773, 1967. ↑ 24, 46, 83, 117, 119

[Tsi12] Jacob TSIMERMAN : Brauer-Siegel for arithmetic tori and lower bounds for Galois orbits of special points. *J. Amer. Math. Soc.*, 25(4):1091–1117, 2012. ↑ 21, 43, 44

[TV02] Michael A. TSFASMAN et Serge G. VLĂDUŢ : Infinite global fields and the generalized Brauer-Siegel theorem. *Mosc. Math. J.*, 2(2):329–402, 2002. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. ↑ 21, 43

[Ulm02] Douglas ULMER : Elliptic curves with large rank over function fields. *Ann. of Math. (2)*, 155(1):295–315, 2002. ↑ 24, 26, 46, 49, 74, 83, 86, 95, 117, 119, 170

[Ulm07a] Douglas ULMER : Jacobi sums, Fermat Jacobians, and ranks of abelian varieties over towers of function fields. *Math. Res. Lett.*, 14(3):453–467, 2007. ↑ 141

[Ulm07b] Douglas ULMER : L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields. *Invent. Math.*, 167(2):379–408, 2007. ↑ 31, 55, 83, 100, 160, 178, 195, 210, 215, 233

[Ulm11] Douglas ULMER : Elliptic curves over function fields. *In Arithmetic of L-functions*, volume 18 de *IAS/Park City Math. Ser.*, pages 211–280. Amer. Math. Soc., Providence, RI, 2011. ↑ 61, 63, 64, 65, 68, 70, 71, 72, 73, 76, 77, 78, 79, 80, 83, 151, 159, 160, 169, 178, 185, 194, 202, 210

[Ulm13] Douglas ULMER : On Mordell-Weil groups of Jacobians over function fields. *J. Inst. Math. Jussieu*, 12(1):1–29, 2013. ↑ 27, 50, 79, 159, 185, 189, 190, 193, 194, 227

[Ulm14a] Douglas ULMER : Explicit points on the Legendre curve. *J. Number Theory*, 136:165–194, 2014. ↑ 27, 50, 83, 88, 149, 150, 153, 159, 160, 186

[Ulm14b] Douglas ULMER : Explicit points on the Legendre curve III. *Algebra Number Theory*, 8(10):2471–2522, 2014. ↑ 27, 50, 149

[UY15] Emmanuel ULLMO et Andrei YAFAEV : Nombre de classes des tores de multiplication complexe et bornes inférieures pour les orbites galoisiennes de points spéciaux. *Bull. Soc. Math. France*, 143(1):197–228, 2015. ↑ 21, 44

[vF14] Machiel van FRANKENHUIJSEN : *The Riemann hypothesis for function fields : Frobenius flow and shift operators*, volume 80. Cambridge University Press, 2014. ↑ 61

[War12] Kenneth WARD : Asymptotics of class number and genus for abelian extensions of an algebraic function field. *J. Number Theory*, 132(11):2491–2498, 2012. ↑ 21, 43

[Was97] Lawrence C. WASHINGTON : *Introduction to cyclotomic fields*, volume 83 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 1997. ↑ 102, 122, 135

[Wei49] André WEIL : Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949. ↑ 34, 57, 69, 108, 111, 170

[WM71] William C. WATERHOUSE et James S. MILNE : Abelian varieties over finite fields. *In 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 53–64. Amer. Math. Soc., Providence, R.I., 1971. ↑ 27, 50, 71, 89

[Yui94] Noriko YUI : A note on the norms of algebraic numbers associated to Jacobi sums. *J. Number Theory*, 47(1):106–129, 1994. ↑ 139, 170

[Zyk05] Alexey ZYKIN : The Brauer-Siegel and Tsfasman-Vlăduţ theorems for almost normal extensions of number fields. *Mosc. Math. J.*, 5(4):961–968, 974, 2005. ↑ 21, 43

[Zyk15] Alexey ZYKIN : Asymptotic properties of zeta functions over finite fields. *Finite Fields Appl.*, 35:247–283, 2015. ↑ 21, 25, 43, 48, 90, 91

Résumé

Dans cette thèse, nous étudions le comportement asymptotique du ratio de Brauer-Siegel des familles de courbes elliptiques sur les corps de fonctions en caractéristique positive. Si E/K est une courbe elliptique sur un corps de fonctions K, on définit son ratio de Brauer-Siegel par

$$\mathfrak{Bs}(E/K) = \log(\#Ш(E/K) \cdot \mathrm{Reg}(E/K))/\log H(E/K),$$

où $\mathrm{Reg}(E/K)$ désigne le régulateur de Néron-Tate, $Ш(E/K)$ le groupe de Tate-Shafarevich et $H(E/K)$ la hauteur différentielle exponentielle de E/K. Cette quantité est définie en analogie avec le théorème éponyme pour les corps de nombres.

Nous démontrons que $\mathfrak{Bs}(E/K) \to 1$ (inconditionellement) lorsque E/K pacrourt l'une de cinq familles de courbes elliptiques, avec $H(E/K) \to \infty$. En d'autres termes, ces familles vérifient un analogue du théorème de Brauer-Siegel.

Pour prouver une telle relation asymptotique, nous commençons par exprimer les fonctions L des courbes elliptiques concernées en termes de sommes de caractères sur les corps finis. Puis, *via* la conjecture de Birch et Swinnerton-Dyer, nous relions le ratio $\mathfrak{Bs}(E/K)$ à la valeur spéciale $L^*(E/K, 1)$ de la fonction $L(E/K, s)$ en $s = 1$ (pour les cinq familles considérées, cette conjecture a été démontrée par d'autres auteurs). Reste alors à encadrer la taille de $L^*(E/K, 1)$ en termes de $H(E/K)$: la majoration est aisée, mais la minoration requiert des estimations plus délicates. Nous développons donc quelques outils adaptés : nous exprimons sous forme combinatoire la valuation q-adique d'un produit de nombres algébriques associés aux sommes de Jacobi et démontrons un résultat d'équidistribution en moyenne des sous-groupes de $(\mathbb{Z}/d\mathbb{Z})^\times$.

Nous obtenons au passage des résultats sur le rang, la torsion et le nombre de Tamagawa des courbes étudiées.

Abstract

In this thesis, we study the asymptotic behaviour of the Brauer-Siegel ratio in families of elliptic curves over function fields in positive characteristic. If E/K is an elliptic curve over a function field K, its Brauer-Siegel ratio is defined by

$$\mathfrak{Bs}(E/K) = \log(\#Ш(E/K) \cdot \mathrm{Reg}(E/K))/\log H(E/K),$$

where $\mathrm{Reg}(E/K)$ denotes the Néron-Tate regulator, $Ш(E/K)$ the Tate-Shafarevich group and $H(E/K)$ is the exponential differential height of E/K. This invariant is introduced by analogy with the Brauer-Siegel theorem for number fields.

We prove that $\mathfrak{Bs}(E/K) \to 1$ (unconditionally) when E/K runs through one of five families of elliptic curves, with $H(E/K) \to \infty$. In other words, these families satisfy an analogue of the Brauer-Siegel theorem.

To prove such an asymptotic relation, we first write the L-functions of the relevant elliptic curves in terms of character sums over finite fields. Then, *via* the Birch and Swinnerton-Dyer conjecture, we link $\mathfrak{Bs}(E/K)$ to the special value $L^*(E/K, 1)$ of the L function $L(E/K, s)$ at $s = 1$ (for the five families we sstudy, this conjecture has been proved by other authors). It then remains to bound the size of $L^*(E/K, 1)$: a good upper bound is easily proved, but the lower bound we require is more subtle. We thus develop tools to prove it: we find a combinatorial expression of the q-adic valuation of a product of algebrac numbers associated to Jacobi sums and we prove an average equidistribution result for subgroups of $(\mathbb{Z}/d\mathbb{Z})^\times$.

We also obtain auxiliary results about the Mordell-Weil rank, the torsion and the Tamagawa number of the elliptic curves under consideration.