Université Paris.Diderot (Paris 7)
Sorbonne Paris Cité

École Doctorale de Sciences Mathématiques de Paris Centre
Institut de Mathématiques de Jussieu - Paris Rive Gauche

Thèse de doctorat

Discipline : Mathématiques

présentée par

Richard Griffon

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

---

dirigée par Marc Hindry

Exemplaire soumis aux rapporteurs

Cet exemplaire ne contient que l'introduction.
Le texte intégral est disponible sur ma page web :
`http://bit.do/Griffon_thesis`

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
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 infinies de courbes elliptiques sur $K = \mathbb{F}_q(t)$. 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 $\mathfrak{Bs}(E/K) \to 1$ lorsque $H(E/K) \to \infty$ pour les cinq familles considérées.

La preuve d'une telle relation asymptotique requiert de calculer les fonctions L des courbes E/K et, *via* la conjecture de Birch et Swinnerton-Dyer, encadrer $\mathfrak{Bs}(E/K)$ revient à encadrer les valeurs spéciales $L^*(E/K, 1)$. Nous exprimons les fonctions L des courbes $E/\mathbb{F}_q(t)$ des familles étudiées, à l'aide de sommes de caractères sur $\mathbb{F}_q$. En général, trouver une minoration adéquate de $L^*(E/K, 1)$ est très délicat. Nous développons un outil de minoration de $L^*(E/K, 1)$ adapté aux courbes elliptiques considérées. Nous obtenons au passage des résultats sur le rang, la torsion et le nombre de Tamagawa des courbes étudiées.

Mots-clefs

Courbes elliptiques, Corps de fonctions en caractéristique positive, Régulateur de Néron-Tate, Groupe de Tate-Shafarevich, Théorème de Brauer-Siegel, Conjecture de Birch et Swinnerton-Dyer, Sommes de caractères, Fonctions L, 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 $K = \mathbb{F}_q(t)$. 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 in analogy with the Brauer-Siegel theorem for number fields.

We prove that $\mathfrak{Bs}(E/K) \to 1$ when $H(E/K) \to \infty$ for five families of elliptic curves.

To prove such an asymptotic relation, we compute the L-functions of the curves E/K and, *via* the Birch and Swinnerton-Dyer conjecture, we bound $\mathfrak{Bs}(E/K)$ by bounding their special values $L^*(E/K, 1)$ from above and from below. We find expressions of the L-functions of all curves $E/\mathbb{F}_q(t)$ in the families we study, in terms of character sums over $\mathbb{F}_q$. In general, finding a good lower bound on $L^*(E/K, 1)$ is difficult. We develop a framework to prove the required lower bound on $L^*(E/K, 1)$ in the cases we study. We also obtain results about the rank, the torsion subgroup and the Tamagawa number of these elliptic curves.

Keywords

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

R. Griffon. Submitted for review 21.IV.2016

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

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

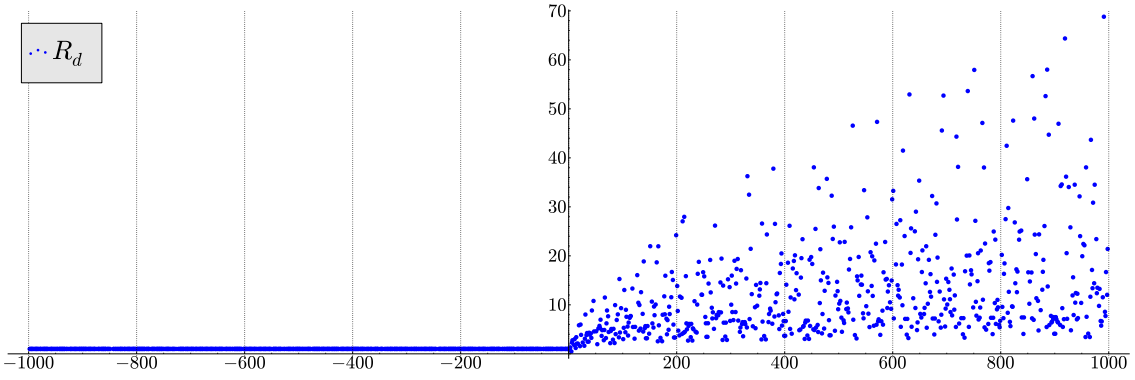
for all non-torsion $P \in E(K)$. So we turn to bounding the regulator $\text{Reg}(E/K)$ from above. In other words, we want to understand how complicated (in terms of $H(E/K)$) it is to compute generators for the Mordell-Weil group of E/K. We would also like to know how optimal the upper bound is, *i.e.*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

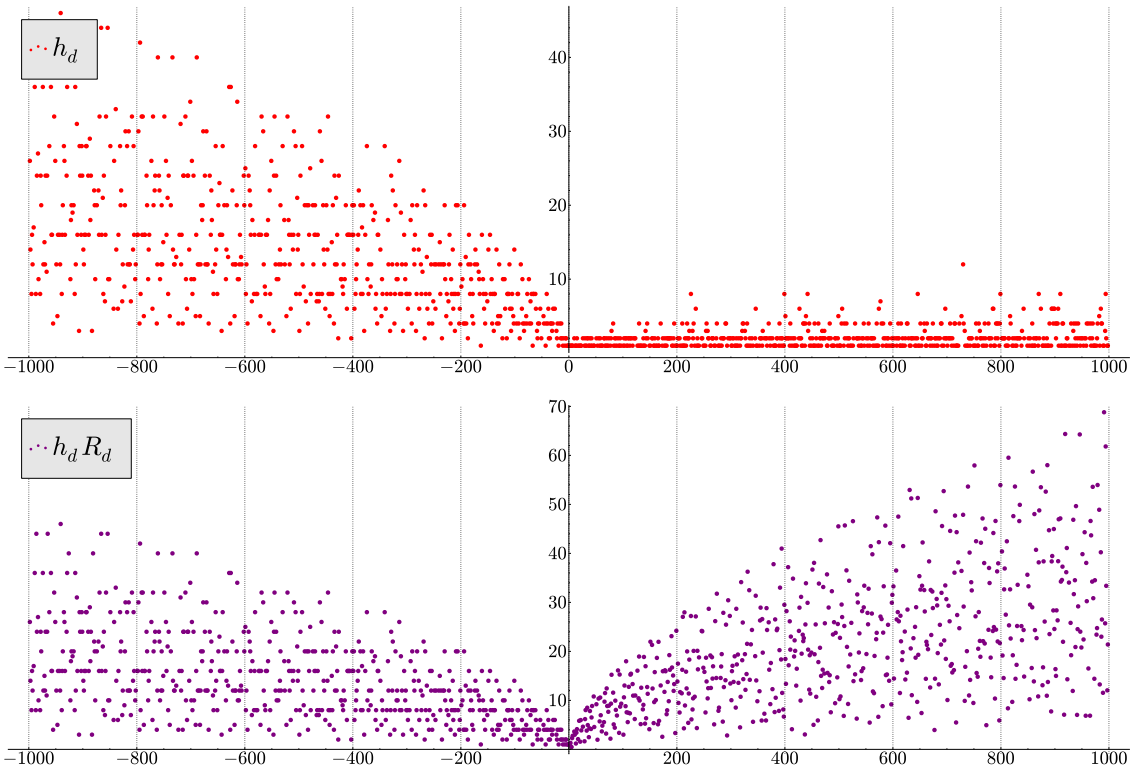
The situation at hand is reminiscent of the classical problem of giving upper bounds on the regulator of units $R_k = \text{Reg}(\mathcal{O}_k^\times)$ of a number field $k/\mathbb{Q}$ in terms of the absolute value Δ_k of its discriminant. In algorithmic terms, given a number field k, how difficult 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*

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

R. Griffon. Submitted for review 21.IV.2016

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

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

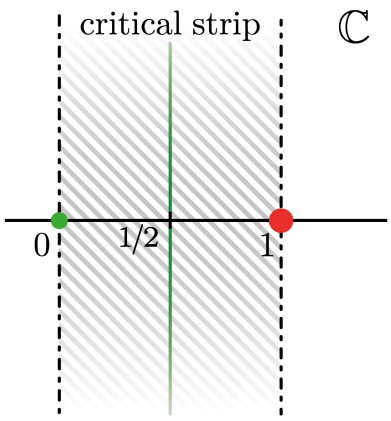
Step 2. Studying the size of ρ_k (in terms of Δ_k) is tantamount to studying the behaviour of $\zeta_k(s)$ in the neighborhood of its pole $s=1$ because

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

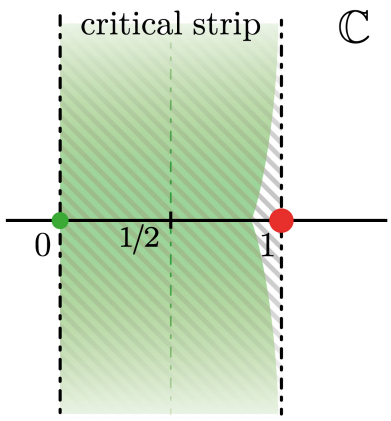
Actually, it suffices to study $x \mapsto \zeta_k(x)$ for real $x \neq 1$ near 1. The presence (or absence) of zeroes of $\zeta_k(x)$ close to $x = 1$ tends to influence the size of ρ_k. Since $\zeta_k(x)$ doesn't vanish on $]1, +\infty[$, the upper bound on ρ_k in (7) is easy to get. One can even prove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

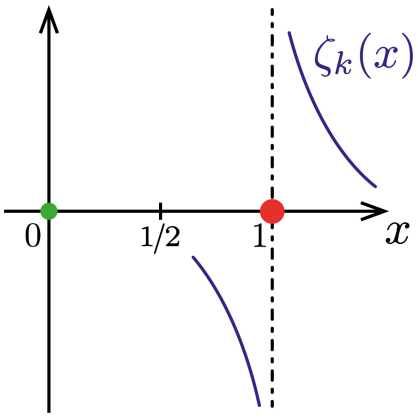


Zeroes of $\zeta_k(x)$ under GRH.

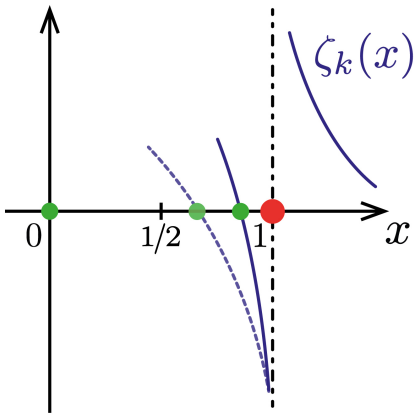


Zeroes of $\zeta_k(x)$ without GRH.

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 Tsimmerman 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, 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 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 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 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

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

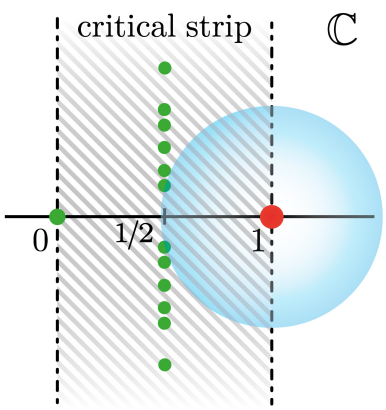
If our elliptic curve E/K satisfies the BSD conjecture, this improved upper bound on $L^*(E/K,1)$ immediately leads to

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

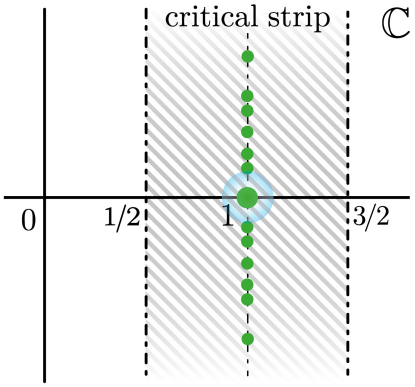
We now have completed "**Step 2.**" of the proof of an analogue of the Brauer-Siegel theorem.

The 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 $K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_i \subset \ldots$ (correponding 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]) :

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

R. Griffon. Submitted for review 21.IV.2016

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 so is $\mathfrak{Bs}(E/K)$.*
- *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 $0 \leqslant W_E \leqslant \sum u_m$.

R. Griffon. Submitted for review 21.IV.2016

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 obtained:

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:

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

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 $\mathcal{O}'_q(d) = (\mathbb{Z}/d\mathbb{Z}\smallsetminus\{0\})/\langle q \bmod d\rangle$ 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 is 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 [Ulm07, 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 $o\big(d\big)$ 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 needed 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 de 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.

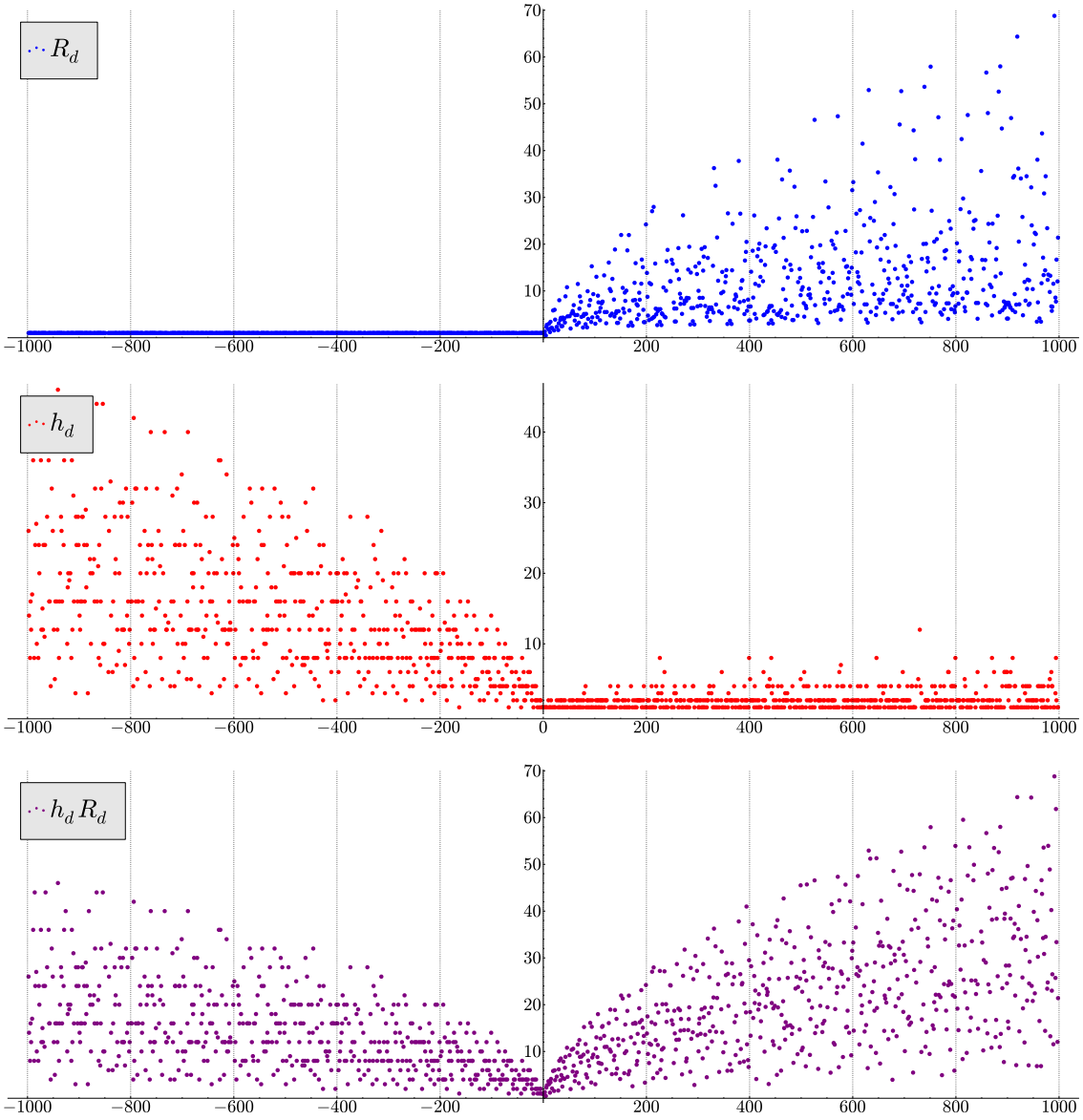
Il s'avère que calculer seulement une « base » de la partie libre du groupe des unités $\mathcal{O}_k^\times$ n'est pas beaucoup plus simple que d'expliciter à la fois une telle base *et* un ensemble de générateurs du groupe des classes $\mathcal{C}\ell(\mathcal{O}_k)$ de k (voir [Len92, §5]). On note $h_k = \#\mathcal{C}\ell(\mathcal{O}_k)$ 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 $H(E/K) \to \infty$.

R. Griffon. Submitted for review 21.IV.2016

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

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

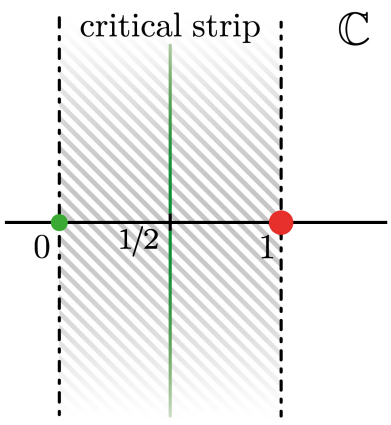
Étape 2. Étudier la taille de ρ_k (en fonction de Δ_k) est équivalent à étudier le comportement de $\zeta_k(s)$ au voisinage de son pôle $s = 1$ car

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

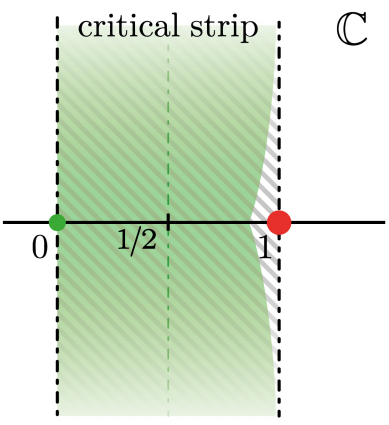
En fait, il suffit même d'étudier $x \mapsto \zeta_k(x)$ lorsque $x \neq 1$ est un réel proche de 1. La présence (ou l'absence) de zéros de $\zeta_k(x)$ voisins de $x = 1$ a une grande influence sur la taille de ρ_k. Comme $x \mapsto \zeta_k(x)$ ne s'annule pas sur $]1, +\infty[$, la majoration de ρ_k 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 $\zeta_k(s)$.

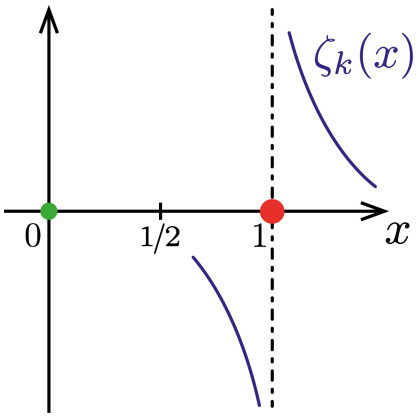


Zéros de $\zeta_k(x)$ en supposant GRH.

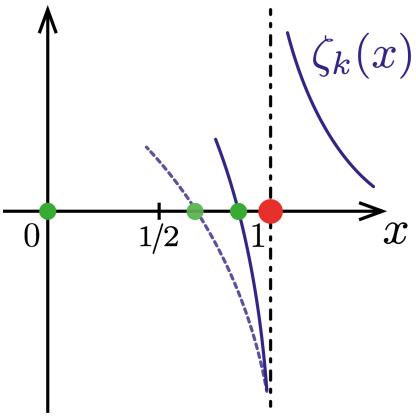


Zéros de $\zeta_k(x)$ sans supposer GRH.

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 $\mathfrak{Bs}(k/\mathbb{Q})$, 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

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

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 Tsimmerman 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 Tsimmerman 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 fonctionelle 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 $\mathfrak{Bs}(E/K)$ à celle de $L^*(E/K,1)$.

Pour ce faire, nous devons nous assurer que les deux termes « parasites » $\#E(K)_{\mathrm{tors}}$ 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 $\#E(K)_{\mathrm{tors}}$ (lorsque K est fixé) :

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

Notons qu'une majoration plus faible (de la forme $\#E(K)_{\mathrm{tors}} \ll_\varepsilon H(E/K)^\varepsilon$, 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 :

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

Par conséquent, pour encadrer $\mathfrak{Bs}(E/K)$, 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

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

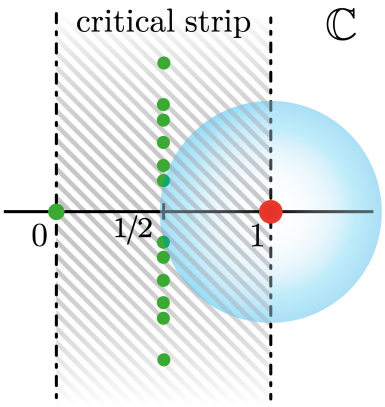
Ce qui termine l'« **Étape 2.** » de la preuve d'un analogue du théorème de Brauer-Siegel.

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 :

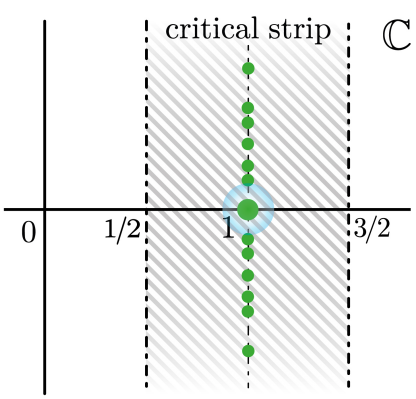
– D'abord, $\zeta_k(s)$ a un pôle simple en $s = 1$, alors que $\mathcal{L}(E/K,s)$ a vraisemblablement un zéro de grande multiplicité en $s = 1$. Nous mentionnons ici, qu'il y a des exemples explicites de courbes elliptiques sur $\mathbb{F}_q(t)$ de rang arbitrairement grand et qui satisfont à la conjecture 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 sugère 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 $G_D^*(a_E) \neq 0$, $\deg G_D^* = g_D - o(g_D)$ 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

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

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

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

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 $\mathfrak{Bs}(E/K)$ également.*
- *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 :

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

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 $d \mid q-1$. Mous 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 [Ulm07, 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 de 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 $a = 1/2$

Bibliographie

[Art86] Michael Artin : Néron models. *In Arithmetic geometry (Storrs, Conn., 1984)*, pages 213–230. Springer, New York, 1986. ↑ 59

[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. ↑ 21, 24, 25, 27, 45, 48, 49, 50, 73, 153, 154, 171, 177, 185, 202, 207, 208, 218, 219, 224

[BK10] Enrico Bombieri et Nicholas M. Katz : A note on lower bounds for Frobenius traces. *Enseign. Math. (2)*, 56(3-4):203–227, 2010. ↑ 28, 51

[Bra47] Richard Brauer : On the zeta-functions of algebraic number fields. *Amer. J. Math.*, 69:243–250, 1947. ↑ 13, 35, 77

[Bru92] Armand Brumer : The average rank of elliptic curves. I. *Invent. Math.*, 109(3):445–472, 1992. ↑ 75, 76, 81, 83, 115, 120

[BW93] A. Baker et G. Wüstholz : Logarithmic forms and group varieties. *J. Reine Angew. Math.*, 442:19–62, 1993. ↑ 28, 51

[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. ↑ 70

[Cas91] John W. S. Cassels : *Lectures on elliptic curves*, volume 24 de *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991. ↑ 56, 62

[CHU14] Ricardo P. Conceição, Chris Hall et Douglas Ulmer : Explicit points on the Legendre curve II. *Math. Res. Lett.*, 21(2):261–280, 2014. ↑ 21, 24, 44, 47, 69, 143, 148, 152

[Coh07] Henri Cohen : *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 de *Graduate Texts in Mathematics*. Springer, New York, 2007. ↑ 96, 97, 116, 129, 131

[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. ↑ 62, 71

[Con15] Brian Conrad : Minimal models for elliptic curves. 2015. http://math.stanford.edu/~conrad/papers/minimalmodel.pdf. ↑ 59

[Del74] Pierre Deligne : La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974. ↑ 63

[Del80] Pierre Deligne : La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.*, (52):137–252, 1980. ↑ 63

[DH35] Harold Davenport et Helmut Hasse : Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *J. Reine Angew. Math.*, 172:151–182, 1935. ↑ 102

[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. ↑ 21, 45, 191

[Eva86] Ronald J. Evans : Hermite character sums. *Pacific J. Math.*, 122(2):357–390, 1986. ↑ 23, 46, 97

[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. ↑ 15, 37

[Gor79] William J. GORDON : Linking the conjectures of Artin-Tate and Birch-Swinnerton-Dyer. *Compositio Math.*, 38(2):163–199, 1979. ↑ 16, 39, 70, 71, 72, 94

[Gre87] John GREENE : Hypergeometric functions over finite fields. *Trans. Amer. Math. Soc.*, 301(1):77–101, 1987. ↑ 97

[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. ↑ 66

[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. ↑ 55, 57, 58, 60, 61, 66, 70, 72

[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. ↑ 58, 60, 63, 74, 81

[Hal06] Chris HALL : *L*-functions of twisted Legendre curves. *J. Number Theory*, 119(1):128–147, 2006. ↑ 67

[Har77] Robin HARTSHORNE : *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. ↑ 55, 56

[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. ↑ 9, 12, 20, 31, 34, 43, 60, 77, 78, 79

[Hin08] Marc HINDRY : *Arithmétique : primalité et codes, théorie analytique des nombres, équations diophantiennes, courbes elliptiques*. Tableau noir. Calvage & Mounet, 2008. ↑ 56, 58, 95, 96, 112, 147

[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. ↑ 15, 37, 63, 64, 70, 77

[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 2016. ↑ 9, 12, 13, 17, 19, 20, 22, 27, 29, 31, 34, 35, 40, 42, 43, 44, 45, 51, 53, 60, 70, 72, 74, 77, 78, 79, 80, 81, 82, 83, 85, 115, 116, 135, 155, 173, 180, 189, 203, 205, 225

[HS88] Marc HINDRY et Joseph H. SILVERMAN : The canonical height and integral points on elliptic curves. *Invent. Math.*, 93(2):419–450, 1988. ↑ 58

[HS00] Marc HINDRY et Joseph H. SILVERMAN : *Diophantine geometry*, volume 201 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction. ↑ 56, 57, 58, 59, 61, 62, 66, 69, 70, 163, 195

[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. ↑ 144, 160, 178, 192

[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. ↑ 138

[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. ↑ 88, 95, 96, 116, 126, 129, 131, 133, 166

[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. ↑ 64, 89, 94, 96, 100

[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. ↑ 163

[KN74] Lauwrens KUIPERS et Harald NIEDERREITER : *Uniform distribution of sequences*. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1974. Pure and Applied Mathematics. ↑ 136

[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. ↑ 16, 19, 39, 42, 72, 77

[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. ↑ 18, 41, 84

[KT10] Boris Kunyavskiĭ et Michael Tsfasman : Erratum to : Brauer-Siegel theorem for elliptic surfaces. *Int. Math. Res. Not. IMRN*, (16):3263, 2010. ↑ 19, 41, 84

[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. ↑ 10, 11, 32, 34, 35, 78, 79

[Lan83b] Serge Lang : *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983. ↑ 56, 61, 62, 71

[Lan94] Serge Lang : *Algebraic number theory*, volume 110 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 1994. ↑ 15, 37, 70, 77, 129, 131

[Len92] Hendrik W. Lenstra, Jr. : Algorithms in algebraic number theory. *Bull. Amer. Math. Soc. (N.S.)*, 26(2):211–244, 1992. ↑ 10, 32

[Liu02] Qing Liu : *Algebraic geometry and arithmetic curves*. OUP Oxford, (Trad. Erné, Reinie) édition, 2002. ↑ 59

[LN59] Serge Lang et André Néron : Rational points of abelian varieties over function fields. *Amer. J. Math.*, 81:95–118, 1959. ↑ 61, 71

[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. ↑ 88, 95, 96, 97, 99, 102, 110, 113, 114

[Man71] Yuri I. Manin : Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971. ↑ 79

[Mes86] Jean-François Mestre : Formules explicites et minorations de conducteurs de variétés algébriques. *Compositio Math.*, 58(2):209–232, 1986. ↑ 76

[Mic99] Philippe Michel : Sur les zéros de fonctions L sur les corps de fonctions. *Math. Ann.*, 313(2):359–370, 1999. ↑ 20, 43

[Mil68] James S. Milne : The Tate-Šafarevič group of a constant abelian variety. *Invent. Math.*, 6:91–105, 1968. ↑ 16, 18, 20, 27, 39, 43, 51, 61, 72, 82

[Mil75] James S. Milne : On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975. ↑ 16, 39, 71, 72

[Mil80] James S. Milne : *Étale cohomology*, volume 33 de *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980. ↑ 62, 64, 66, 68

[Mil86] James S. Milne : Abelian varieties. *In Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986. ↑ 57

[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. ↑ 136

[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. ↑ 105

[Nat00] Melvyn B. Nathanson : *Elementary methods in number theory*, volume 195 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. ↑ 136

[Occ12] Thomas Occhipinti : A family of elliptic curves of large rank. *J. Number Theory*, 132(4): 657–665, 2012. ↑ 27, 50, 68, 181

[Oes90] Joseph Oesterlé : Empilements de sphères. *Astérisque*, (189-190):Exp. No. 727, 375–397, 1990. Séminaire Bourbaki, Vol. 1989/90. ↑ 55, 70

[OU14] Thomas Occhipinti et Douglas Ulmer : Low-dimensional factors of superelliptic jacobians. *European Journal of Mathematics*, 1(2):279–285, 2014. ↑ 135

[Poo07] Bjorn Poonen : Gonality of modular curves in characteristic p. *Math. Res. Lett.*, 14(4):691–701, 2007. ↑ 10, 32, 74

[PS00] Jérôme Pesenti et Lucien Szpiro : Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques. *Compositio Math.*, 120(1):83–117, 2000. ↑ 58

[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. ↑ 73

[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. ↑ 67

[Ros02] Michael ROSEN : *Number theory in function fields*, volume 210 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. ↑ 55, 64, 75

[RV99] Dinakar RAMAKRISHNAN et Robert J. VALENZA : *Fourier analysis on number fields*, volume 186 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999. ↑ 56, 70

[Saw92] Yoshiaki SAWABE : Legendre character sums. *Hiroshima Math. J.*, 22(1):15–22, 1992. ↑ 97

[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. ↑ 63

[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. ↑ 56, 61, 163, 195

[Shi86] Tetsuji SHIODA : An explicit algorithm for computing the Picard number of certain algebraic surfaces. *Amer. J. Math.*, 108(2):415–432, 1986. ↑ 16, 39, 111

[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. ↑ 26, 49, 126, 133, 134

[Shi90] Tetsuji SHIODA : On the Mordell-Weil lattices. *Comment. Math. Univ. St. Paul.*, 39(2):211–240, 1990. ↑ 59, 61, 62

[Shi92] Tetsuji SHIODA : Some remarks on elliptic curves over function fields. *Astérisque*, (209):12, 99–114, 1992. Journées Arithmétiques, 1991 (Geneva). ↑ 67, 164

[Shy77] Jih Min SHYR : On some class number relations of algebraic tori. *Michigan Math. J.*, 24(3):365–377, 1977. ↑ 15, 38

[Sie35] Carl Ludwig SIEGEL : Über die Classenzahl quadratischer Zahlkörper. *Acta Arith.*, 1:83–86, 1935. ↑ 13, 35, 77

[Sie69] Carl Ludwig SIEGEL : Abschätzung von Einheiten. *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II*, 1969:71–86, 1969. ↑ 14, 36, 77

[Sil86a] Joseph H. SILVERMAN : Heights and elliptic curves. *In Arithmetic geometry (Storrs, Conn., 1984)*, pages 253–265. Springer, New York, 1986. ↑ 58, 60

[Sil86b] Joseph H. SILVERMAN : The theory of height functions. *In Arithmetic geometry (Storrs, Conn., 1984)*, pages 151–166. Springer, New York, 1986. ↑ 61

[Sil94] Joseph H. SILVERMAN : *Advanced topics in the arithmetic of elliptic curves*, volume 151 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. ↑ 55, 57, 58, 59, 60, 61, 62, 145, 179, 192, 193, 194, 209

[Sil09] Joseph H. SILVERMAN : *The arithmetic of elliptic curves*, volume 106 de *Graduate Texts in Mathematics*. Springer, Dordrecht, second édition, 2009. ↑ 55, 56, 57, 60, 61, 65, 66, 69, 161, 163, 192, 195, 208

[SK79] Tetsuji SHIODA et Toshiyuki KATSURA : On Fermat varieties. *Tôhoku Math. J. (2)*, 31(1):97–115, 1979. ↑ 17, 28, 39, 51, 71, 111, 133, 164

[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. ↑ 55, 56, 57, 58, 59, 61, 62, 71, 162, 178, 194, 195

[Sta74] Harold M. STARK : Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23:135–152, 1974. ↑ 15, 37

[Sti90] Ludwig STICKELBERGER : Über eine Verallgemeinerung der Kreistheilung. *Math. Ann.*, 37(3):321–367, 1890. ↑ 129

[Szp90] Lucien SZPIRO : Discriminant et conducteur des courbes elliptiques. *Astérisque*, (183):7–18, 1990. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). ↑ 58, 60

[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. ↑ 71

[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. ↑ 9, 31, 59, 60, 145, 161, 179, 192, 209

[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. ↑ 16, 71

[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. ↑ 16, 39, 61, 67, 69, 70, 71, 72

[TŠ67] John T. Tate et Igor R. Šafarevič : The rank of elliptic curves. *Dokl. Akad. Nauk SSSR*, 175:770–773, 1967. ↑ 18, 40, 76, 111, 113

[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. ↑ 15, 37, 38

[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. ↑ 15, 37

[Ulm] Douglas Ulmer : Jacobi sums, Fermat jacobians, and ranks of abelian varieties over towers of function fields. http ://arxiv.org/abs/math/0609716. ↑ 135

[Ulm02] Douglas Ulmer : Elliptic curves with large rank over function fields. *Ann. of Math. (2)*, 155(1):295–315, 2002. ↑ 18, 20, 40, 43, 68, 76, 80, 89, 111, 113, 164

[Ulm07] 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. ↑ 25, 49, 76, 94, 154, 171, 187, 202, 207, 224

[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. ↑ 55, 57, 58, 59, 62, 64, 65, 66, 67, 70, 71, 72, 73, 74, 76, 145, 154, 163, 171, 177, 185, 194, 202

[Ulm13] Douglas Ulmer : On Mordell-Weil groups of Jacobians over function fields. *J. Inst. Math. Jussieu*, 12(1):1–29, 2013. ↑ 21, 44, 73, 153, 177, 180, 181, 185

[Ulm14a] Douglas Ulmer : Explicit points on the Legendre curve. *J. Number Theory*, 136:165–194, 2014. ↑ 21, 44, 76, 143, 144, 147, 153, 154, 178

[Ulm14b] Douglas Ulmer : Explicit points on the Legendre curve III. *Algebra Number Theory*, 8(10):2471–2522, 2014. ↑ 21, 44, 143

[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. ↑ 15, 38

[vF14] Machiel van Frankenhuijsen : *The Riemann hypothesis for function fields : Frobenius flow and shift operators*, volume 80. Cambridge University Press, 2014. ↑ 55

[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. ↑ 15, 37

[Was97] Lawrence C. Washington : *Introduction to cyclotomic fields*, volume 83 de *Graduate Texts in Mathematics*. Springer-Verlag, New York, second édition, 1997. ↑ 96, 116, 129

[Wei49] André Weil : Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949. ↑ 28, 51, 63, 102, 105, 164

[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. ↑ 21, 44, 65, 83

[Yui94] Noriko Yui : A note on the norms of algebraic numbers associated to Jacobi sums. *J. Number Theory*, 47(1):106–129, 1994. ↑ 133, 164

[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. ↑ 15, 37

[Zyk15] Alexey Zykin : Asymptotic properties of zeta functions over finite fields. *Finite Fields Appl.*, 35:247–283, 2015. ↑ 15, 19, 37, 42, 84