Bounds on special values of L-functions of elliptic curves in an Artin-Schreier family

Richard Griffon
Mathematisch Instituut, Universiteit Leiden

Abstract – We study a certain Artin-Schreier family of elliptic curves over the function field $K = \mathbb{F}_q(t)$. We prove an asymptotic estimate on the special values of their L-function in terms of the degree of their conductor; we show that the special values are, in a sense, 'asymptotically as large as possible'. We also provide an explicit expression for their L-function.

The proof of the main result uses this expression and a detailed study of the distribution of character sums related to Kloosterman sums. Via the BSD conjecture, the main result translates into an analogue of the Brauer–Siegel theorem for these elliptic curves.

Keywords: Elliptic curves over function fields in characteristic p, Explicit computation of L-functions, Special values of L-functions, BSD conjecture, Kloosterman sums, Sato–Tate distribution.

2010 Math. Subj. Classification: 11G05, 11G40, 11M38, 11F67, 11L05, 11J20.

E-mail: r.m.m.griffon@math.leidenuniv.nl

Introduction

Let $\mathbb{F}_q$ be a finite field of odd characteristic p and $K = \mathbb{F}_q(t)$. Consider a nonisotrivial elliptic curve E defined over K, and its associated L-function[1] $L(E,T)$. *Via* a cohomological interpretation, Grothendieck has proved that, even though $L(E,T)$ is *a priori* defined as a formal power series in T, it is actually a polynomial with integral coefficients, whose degree we denote by $b(E)$. Moreover, $L(E,T)$ satisfies the expected functional equation relating $L(E,T)$ to $L(E,1/q^2T)$.

Define $\rho(E)$ to be the order of vanishing of $L(E,T)$ at the central point $T = q^{-1}$ and the *special value* of $L(E,T)$ by $L^*(E,1) := \lim_{T\to q^{-1}}(1-qT)^{-\rho(E)}\cdot L(E,T)$. These invariants both appear in the conjecture of Birch and Swinnerton-Dyer[2] through which they are related to 'arithmetic' invariants of E.

We will be interested in comparing the size of the special value $L^*(E,1)$ to the degree $b(E)$ of the L-function. It is relatively straightforward to prove that

$$-1 \leq \frac{\log L^*(E,1)}{\log\left(q^{b(E)}\right)} \leq 0 + o(1) \qquad (\text{as } b(E)\to\infty), \tag{1}$$

and it seems natural to ask about the optimality of such bounds. In other words, given a family $\mathscr{E}$ of nonisotrivial elliptic curves E over K with $b(E)\to\infty$, we investigate the asymptotic behaviour of the ratio $\log(L^*(E,1))/\log\left(q^{b(E)}\right)$ as E runs through $\mathscr{E}$. Does this ratio have a limit? If so, what is this limit?

These questions are still wide open and, as far as the author knows, they have only been settled for a very limited number of special families $\mathscr{E}$ (see [HP16, Thm. 7.12], [Gri18a, Coro. 5.1], [Gri18b, Thm. 4.2] and [Gri16, Thm. 9]). These examples are known as 'Kummer families' of elliptic curves: one obtains them by pulling-back an elliptic curve E_1/K by the map $t\mapsto t^d$ for larger and larger integers d which are coprime to q. In those cases, the ratio in (1) does have a limit, and this limit is 0.

In this article, we answer the two questions above for an 'Artin–Schreier family' of elliptic curves over K. More precisely, we prove

[1] Since the base field K is fixed and all the invariants of E we consider are relative to K, we drop the dependency on K from the notations.

[2] Hereafter abbreviated as BSD

Theorem A – *Let $\mathbb{F}_q$ be a finite field of odd characteristic p and $K = \mathbb{F}_q(t)$. Fix $\gamma \in \mathbb{F}_q^\times$ and, for all integers $a \geq 1$, let $E_{a,\gamma}$ be the elliptic curve over K given by the affine Weierstrass model*

$$E_{a,\gamma} : \quad y^2 = x\,(x + 16\gamma)\left(x + \wp_a(t)^2\right), \qquad \text{with } \wp_a(t) = t^{q^a} - t \in \mathbb{F}_q[t].$$

Then, as $a \to \infty$, the limit below exists and is 0:

$$\lim_{a\to\infty} \frac{\log L^*(E_{a,\gamma}, 1)}{\log\left(q^{b(E_{a,\gamma})}\right)} = 0. \tag{2}$$

The name of 'Artin–Schreier family' stems from its construction: starting with the elliptic curve E_γ/K given by $y^2 = x(x + 16\gamma)(x + t^2)$, one obtains $E_{a,\gamma}$ by pulling back E_γ by the Artin–Schreier map $t \mapsto \wp_a(t)$ for any $a \geq 1$. This family of elliptic curves $\{E_{a,\gamma}\}_{a\geq 1}$ was previously studied in [PU16] where, among other things, the authors prove that $E_{a,\gamma}$ satisfies the BSD conjecture. Following [PU16, §7.3], we note the ressemblance between $E_{a,\gamma}$ and a Legendre elliptic curve. We refer to Theorem 6.1 for a more quantitative version of (2).

Once again, prior to Theorem A, the only known examples of families of elliptic curves exhibiting a behaviour such as (2) were Kummer families. We also remark that the strategy of proof of (2) markedly differs from the one used in our previous works [Gri16], [Gri18a] and [Gri18b]; we comment further on this difference and on the reason for adopting a new approach in Remark 6.2.

From Theorem A and from the BSD conjecture, we will deduce (see Theorem 7.1):

Theorem B – *Let $\mathbb{F}_q$ be a finite field of odd characteristic and $K = \mathbb{F}_q(t)$. For any $\gamma \in \mathbb{F}_q^\times$ and any integer $a \geq 1$, the Tate–Shafarevich group $Ш(E_{a,\gamma})$ is finite. Furthermore, one has*

$$\lim_{a\to\infty} \frac{\log\left(|Ш(E_{a,\gamma})| \cdot \mathrm{Reg}(E_{a,\gamma})\right)}{\log H(E_{a,\gamma})} = 1,$$

where $\mathrm{Reg}(E_{a,\gamma})$ denotes the Néron–Tate regulator of $E_{a,\gamma}$, and $H(E_{a,\gamma})$ its exponential differential height (see §1.1–§1.3 for definitions).

Following [HP16], we view this result as an analogue of the Brauer–Siegel theorem for the sequence of elliptic curves $\{E_{a,\gamma}\}_{a\geq 1}$. We further comment on this result in section 7.

Let us give an outline of the proof of Theorem A as we describe the structure of the paper and state the other results contained in it. In section 1, we start by reviewing the construction of the elliptic curves $E_{a,\gamma}$ and by computing some of their invariants. We also recall the definition of their L-function and state the BSD conjecture (proved by Pries and Ulmer for $E_{a,\gamma}$, *cf.* [PU16]).

In the following two sections, we compute the L-function of $E_{a,\gamma}$; the relevant objects are introduced in section 2. In particular, a central role is played by angles of some Kloosterman sums. For the purpose of this introduction let us only say that, to any place $v \neq 0, \infty$ of K, we will attach a character sum $\mathrm{K}_\gamma(v)$. The sum $\mathrm{K}_\gamma(v)$ is a real number satisfying $|\mathrm{K}_\gamma(v)| < 2q^{d_v/2}$ where d_v is the degree of v. Hence there exists an angle $\theta_v \in (0, \pi)$ such that $\mathrm{K}_\gamma(v) = 2q^{d_v/2} \cdot \cos\theta_v$. The reader is referred to §2.2 and §3.4 for precise definitions. Section 3 is devoted to the calculation of the L-function itself, which results in the following expression:

Theorem C – *For all integers $a \geq 1$, we denote by $P_q(a)$ the set of places $v \neq 0, \infty$ of K whose degree d_v divides a. Then, for all $\gamma \in \mathbb{F}_q^\times$, the L-function of $E_{a,\gamma}$ is given by*

$$L(E_{a,\gamma}, T) = \prod_{v\in P_q(a)} \left(1 - (qT)^{d_v}\right)\left(1 - \mathrm{e}^{2i\theta_v}(qT)^{d_v}\right)\left(1 - \mathrm{e}^{-2i\theta_v}(qT)^{d_v}\right), \tag{3}$$

where, for all $v \in P_q(a)$, $\theta_v \in (0, \pi)$ is as above (see §2.2 and §3.4 for a precise definition).

This result is proved by a 'point-counting' argument, directly from the definition of $L(E_{a,\gamma}, T)$, through manipulations of character sums over finite fields. Given the paucity of tables of L-functions of elliptic curves over K of large conductor, such an explicit expression of $L(E_{a,\gamma}, T)$ may be of independent interest.

As a by-product, Theorem C yields a closed formula for the analytic rank $\mathrm{ord}_{T=q^{-1}} L(E_{a,\gamma}, T)$. Using that the BSD conjecture is proven for $E_{a,\gamma}$, we recover a result of [PU16] stating that the ranks of $E_{a,\gamma}(K)$ are unbounded as $a \to \infty$; more precisely, we show in Corollary 3.8 that $\mathrm{rank}\, E_{a,\gamma}(K) = q^a/a + O\left(q^{a/2}\right)$.

From Theorem C, we also derive (Proposition 3.7 and (3.15)) an explicit expression for the special value $L^*(E_{a,\gamma},1)$. In the notations of (3), we obtain an expression of the shape

$$\frac{\log L^*(E_{a,\gamma},1)}{b(E_{a,\gamma})} = \frac{\log\binom{\text{positive}}{\text{integer}}}{b(E_{a,\gamma})} + \frac{1}{b(E_{a,\gamma})}\cdot \sum_{v\in P_q(a)} \log\sin^2\theta_v, \tag{4}$$

where, $b(E_{a,\gamma}) \gg q^a$, as will be shown in §1.2. Estimating the first term is straightforward: it is $o(1)$ as $a\to\infty$ and thus does not play any role in the asymptotics. In order to prove the limit in Theorem A, we have to investigate the behaviour of the second term: specifically, we need to show that it is $o(1)$ too. The size of this term visibly depends on how the angles $\{\theta_v\}_{v\in P_q(a)}$ distribute in the interval $[0,\pi]$. Since $t\mapsto \log\sin^2 t$ tends to $-\infty$ at 0 and π, this size also depends on how close the angles θ_v can be to the endpoints of $(0,\pi)$. Therefore we devote sections 4 and 5 to studying the distribution of the angles $\{\theta_v\}_{v\in P_q(a)}$ in more detail. The two main results in these sections can be stated as follows:

Theorem D – *Notations being as above,*

(i - Theorem 5.6) For all continuously differentiable functions $g:[0,\pi]\to\mathbb{C}$,

$$\left|\frac{1}{|P_q(a)|}\sum_{v\in P_q(a)} g(\theta_v) - \frac{2}{\pi}\int_0^\pi g(t)\cdot\sin^2 t\,\mathrm{d}t\right| \ll_q \frac{a^{1/2}}{q^{a/4}}\cdot\int_0^\pi |g'(t)|\,\mathrm{d}t.$$

(ii - Corollary 4.5) There is a constant $c>0$ such that $\min\{\theta_v,\pi-\theta_v\}\geq (q^a)^{-c}$ for all $v\in P_q(a)$.

By the work of Katz, it is known that the angles of Kloosterman sums become equidistributed in $[0,\pi]$ with respect to the Sato–Tate measure (see [Kat88]). It turns out that the same statement holds for the angles $\{\theta_v\}_{v\in P_q(a)}$ (see Theorem 5.5). The proof relies on an adaptation of Katz's method in [Kat88, Chap. 3] and results of Fu and Liu in [FL05]. This equidistribution result, however, is not sufficient for our purpose: we need a more effective version such as Theorem D(i). The effective version (Theorem 5.6) follows from Theorem 5.5 after a more detailed analysis using tools from equidistribution theory (see [Nie91]).

The main goal of section 4 is to prove Theorem D(ii); we actually prove a more general result there (see Theorem 4.1). The proof has a diophantine approximation flavour and the main tool is a version of Liouville's inequality (as in [MW94]).

Combining the two results in Theorem D and approximating $t\mapsto\log\sin^2 t$ by sufficiently regular functions, we prove (Theorem 6.3) that

$$\frac{1}{|P_q(a)|}\sum_{v\in P_q(a)}\log\sin^2\theta_v \xrightarrow[a\to\infty]{} \frac{2}{\pi}\int_0^\pi \log\sin^2 t\cdot\sin^2 t\,\mathrm{d}t = \log(\mathrm{e}/4). \tag{5}$$

Theorem A then follows rather easily (see Theorem 6.1), since (5) implies that the second term in (4) is indeed $o(1)$ as $a\to\infty$. Finally, section 7 is devoted to the proof of Theorem B (see Theorem 7.1).

1 The Artin-Schreier family of elliptic curves $E_{a,\gamma}$

Throughout this article, we fix a finite field $\mathbb{F}_q$ of characteristic $p\geq 3$, and we denote by $K=\mathbb{F}_q(t)$ the function field of the projective line $\mathbb{P}^1_{/\mathbb{F}_q}$.

In this section, we explain in some detail how the curves $E_{a,\gamma}$ are constructed and we collect elementary facts about them. We also setup some notations and conventions that will be in force for the rest of the paper. For a nice account of the theory of elliptic curves over K, the reader may consult [Ulm11].

For all integers $a\geq 1$, we let $\wp_a(t)=t^{q^a}-t\in\mathbb{F}_q[t]$. For any $\gamma\in\mathbb{F}_q^\times$ and any $a\geq 1$, we consider the elliptic curve $E_{a,\gamma}$ defined over K by the affine Weierstrass model:

$$E_{a,\gamma}:\quad y^2 = x\,(x+16\gamma)\,\big(x+\wp_a(t)^2\big)\,. \tag{1.1}$$

The sequence $\{E_{a,\gamma}\}_{a\geq 1}$ is called an *Artin-Schreier family* of elliptic curves over K. This terminology comes from the following observations. Let E_γ/K be the elliptic curve given by $y^2=x(x+16\gamma)(x+t^2)$. Then, for all $a\geq 1$, the curve $E_{a,\gamma}$ is the pullback of E_γ under the Artin-Schreier map $\mathbb{P}^1_{/\mathbb{F}_q}\to\mathbb{P}^1_{/\mathbb{F}_q}$ given by $t\mapsto\wp_a(t)$. Hence, studying $E_{a,\gamma}$ over $K=\mathbb{F}_q(t)$ is equivalent to studying E_γ over the Artin-Schreier extension $\mathbb{F}_q(u_a)$ of $\mathbb{F}_q(t)$, where $\wp_a(u_a)=t$.

These elliptic curves $E_{a,\gamma}$ were studied in [PU16, §6.4, §7.3] where, among other things, it was shown that they satisfy the BSD conjecture (see §1.3 below). In their paper, Pries and Ulmer construct the curves $E_{a,\gamma}$ as follows. For any $\gamma \in \mathbb{F}_q^\times$, we let $f_\gamma : \mathbb{P}^1_{/K} \to \mathbb{P}^1_{/K}$ be the map $[x_0 : x_1] \mapsto x_0/x_1 + \gamma x_1/x_0$. Consider the curve $Z_{a,\gamma} \subset \mathbb{P}^1_{/K} \times \mathbb{P}^1_{/K}$ defined over K by

$$f_\gamma([x_0 : x_1]) - f_\gamma([y_0 : y_1]) = \wp_a(t),$$

in the $([x_0 : x_1], [y_0 : y_1])$-coordinates on $\mathbb{P}^1_{/K} \times \mathbb{P}^1_{/K}$. This curve is smooth of genus 1 and admits one K-rational point $([0 : 1], [0 : 1])$. The curve $Z_{a,\gamma}$ is given in the affine (x, y)-coordinates on $\mathbb{A}^2_{/K}$ by

$$(x - y)(xy - \gamma) = \wp_a(t) \cdot xy.$$

The change of coordinates $(x, y) \mapsto (u, v) = \left(-\gamma \cdot \dfrac{\wp_a(t) - x + y}{x - y}, \gamma\wp_a(t) \cdot \dfrac{y(\wp_a(t) + y - x) + 2\gamma}{x^2 - y^2}\right)$ then brings $Z_{a,\gamma}$ into the affine Weierstrass form

$$E^\circ_{a,\gamma} : \qquad v^2 - \wp_a(t) \cdot uv = u^3 - 2\gamma \cdot u^2 + \gamma^2 \cdot u. \tag{1.2}$$

One finally passes from $E^\circ_{a,\gamma}$ to $E_{a,\gamma}$ by means of the 2-isogeny $\phi : E^\circ_{a,\gamma} \to E_{a,\gamma}$ given by

$$(u, v) \mapsto (x, y) = \left(\frac{4v(v - \wp_a(t)u)}{u^2}, \frac{4(2v - \wp_a(t)u)(u^2 - \gamma^2)}{u^2}\right).$$

From the model (1.1), it is straightforward to compute the j-invariant $j(E_{a,\gamma})$ of $E_{a,\gamma}$ and obtain that

$$j(E_{a,\gamma}) = \frac{\left(\wp_a(t)^4 - 16\gamma \cdot \wp_a(t)^2 + 2^8\gamma^2\right)^3}{\gamma^2 \cdot \wp_a(t)^4 \cdot \left(\wp_a(t)^2 - 16\gamma\right)^2} \in K.$$

As a rational function of t, the j-invariant $j(E_{a,\gamma})$ is visibly nonconstant and separable. In particular, the curve $E_{a,\gamma}$ is not isotrivial.

We also would like to point out that $E_{a,\gamma}$ is 'almost' a Legendre curve. More precisely, in the setting of [BH12], the curve $E_{a,\gamma}$ can be obtained as follows. Starting from the Legendre elliptic curve $E_{0,\gamma}/K$ given by

$$E_{0,\gamma} : \quad y^2 = x(x - 1)\left(x - (16\gamma)^{-1} \cdot t^2\right),$$

one takes a quadratic twist by $-(16\gamma)^{-1}$, obtaining $E'_{0,\gamma}$ defined by $y^2 = x(x+1)\left(1 + (16\gamma)^{-1} \cdot t^2\right)$. Pulling back $E'_{0,\gamma}$ along $\wp_a : \mathbb{P}^1 \to \mathbb{P}^1$, one recovers the curve $E_{a,\gamma}$ defined by (1.1).

1.1 Bad reduction and invariants

For any place v of K, we denote by d_v or $\deg v$ the degree of v and $\mathbb{F}_v$ the residue field at v. We identify finite places of K with monic irreducible polynomials in $\mathbb{F}_q[t]$; we also identify the residue field at $v \neq \infty$ with $\mathbb{F}_q[t]/(B_v)$ if $B_v \in \mathbb{F}_q[t]$ is the monic irreducible polynomial corresponding to v.

Let us describe the reductions of $E_{a,\gamma}$ at places of K and compute its relevant invariants. A straightforward computation of the discriminant of the model (1.1) of $E_{a,\gamma}$ gives that

$$\Delta = 2^{12}\gamma^2 \cdot \wp_a(t)^4 \cdot \left(\wp_a(t)^2 - 16\gamma\right)^2. \tag{1.3}$$

The finite places of bad reduction of $E_{a,\gamma}$ are then the monic irreducible divisors of Δ in $\mathbb{F}_q[t]$. By a routine application of Tate's algorithm (see [Sil94, Chap. IV, §9] for instance), one can give a more precise description:

Proposition 1.1 – *Let $Z_{a,\gamma}$ be the set of places of K that divide $\wp_a(t) \cdot (\wp_a(t)^2 - 16\gamma)$. Then $E_{a,\gamma}$ has good reduction outside $S = Z_{a,\gamma} \cup \{\infty\}$. The reduction of $E_{a,\gamma}$ at places $v \in S$ is as follows:*

Place v of K	*Reduction type of $E_{a,\gamma}$ at v*	$\operatorname{ord}_v \Delta_{\min}(E_{a,\gamma})$	$\operatorname{ord}_v \mathcal{N}(E_{a,\gamma})$
$v \mid \wp_a(t)$	*Multiplicative (of type $\mathbf{I}_4$)*	4	1
$v \mid \wp_a(t)^2 - 16\gamma$	*Multiplicative (of type $\mathbf{I}_2$)*	2	1
∞	*Split multiplicative (of type $\mathbf{I}_{4q^a}$)*	$4q^a$	1

In this table, for all places v of bad reduction for $E_{a,\gamma}$, we have denoted by $\operatorname{ord}_v \Delta_{\min}(E_{a,\gamma})$ (resp. $\operatorname{ord}_v \mathcal{N}(E_{a,\gamma})$) the valuation at v of the minimal discriminant of $E_{a,\gamma}$ (resp. of the conductor of $E_{a,\gamma}$). See [Sil94, Chap. IV, §9], [Ulm11, Lect. 1 §8] for the definitions of these local invariants.

From this local information, one deduces the values of the following global invariants (we refer to [Ulm11, Lect. 1] for their definition). The minimal discriminant divisor $\Delta_{\min}(E_{a,\gamma})$ has degree $\deg \Delta_{\min}(E_{a,\gamma}) = 12q^a$, and the conductor $\mathcal{N}(E_{a,\gamma}) \in \mathrm{Div}(\mathbb{P}^1)$ has degree $\deg \mathcal{N}(E_{a,\gamma}) = 3q^a + 1$. Indeed, since both $\wp_a(t)$ and $\wp_a(t)^2 - 16\gamma$ are squarefree in $\mathbb{F}_q[t]$, one has

$$\sum_{v|\wp_a(t)} \deg v = \deg \wp_a(t) = q^a \quad \text{and} \quad \sum_{v|\wp_a(t)^2-16\gamma} \deg v = \deg(\wp_a(t)^2 - 16\gamma) = 2q^a.$$

Hence the exponential differential height $H(E_{a,\gamma})$ is q^{q^a} since, by definition (see §2 in [Ulm11, Lect. 3]), it is given by $H(E_{a,\gamma}) := q^{(\deg \Delta_{\min}(E_{a,\gamma}))/12}$. Summarising these calculations, we have

$$\deg \Delta_{\min}(E_{a,\gamma}) = 12q^a, \quad \deg \mathcal{N}(E_{a,\gamma}) = 3q^a + 1, \quad \text{and} \quad H(E_{a,\gamma}) = q^{q^a}. \tag{1.4}$$

Remark 1.2 As is clear from comparing (1.3) and the third column of the table in Proposition 1.1, the discriminant Δ of the Weierstrass model (1.1) has the same valuation as $\Delta_{\min}(E_{a,\gamma})$ at all finite places of K. Therefore, the model (1.1) is a minimal integral model of $E_{a,\gamma}$ at all places $v \neq \infty$ of K.

1.2 Definitions of L-function, analytic rank and special value

For any place v of K, with degree d_v and residue field $\mathbb{F}_v$, we denote by $(\widetilde{E_{a,\gamma}})_v$ the reduction modulo v of a minimal integral model of $E_{a,\gamma}$ at v: $(\widetilde{E_{a,\gamma}})_v$ is thus a plane cubic curve over $\mathbb{F}_v$. By definition, the L-function of $E_{a,\gamma}$ is the power series in T given by

$$L(E_{a,\gamma}, T) = \prod_{v \text{ good}} \left(1 - a_v \cdot T^{d_v} + q^{d_v} \cdot T^{2d_v}\right)^{-1} \cdot \prod_{v \text{ bad}} \left(1 - a_v \cdot T^{d_v}\right)^{-1} \in \mathbb{Z}[[T]], \tag{1.5}$$

where the products are over places of K where $E_{a,\gamma}$ has good (resp. bad) reduction, and where[3]

$$a_v := q^{d_v} + 1 - |(\widetilde{E_{a,\gamma}})_v(\mathbb{F}_v)|.$$

We refer to [BH12, §2.2] and [Ulm11, Lect.1 §9, Lect. 3 §6] for more details.

Since $E_{a,\gamma}$ is not isotrivial, a theorem of Grothendieck shows that $L(E_{a,\gamma}, T)$ is actually a polynomial in T with integral coefficients whose degree is denoted by $b(E_{a,\gamma})$. Further, by the Grothendieck–Ogg–Shafarevich formula and our computation in (1.4) of the degree of $\mathcal{N}(E_{a,\gamma})$, we know that

$$b(E_{a,\gamma}) = \deg L(E_{a,\gamma}, T) = \deg \mathcal{N}(E_{a,\gamma}) - 4 = 3(q^a - 1). \tag{1.6}$$

In section 3, we will compute the polynomial $L(E_{a,\gamma}, T)$ explicitly. For now, we only note that it makes sense to define the following two quantities:

Definition 1.3 Let $\rho(E_{a,\gamma})$ be the *analytic rank of* $E_{a,\gamma}$ *i.e.*, the multiplicity of $T = q^{-1}$ as a root of $L(E_{a,\gamma}, T)$. Further, define the *special value of* $L(E_{a,\gamma}, T)$ *at* $T = q^{-1}$ to be

$$L^*(E_{a,\gamma}, 1) := \left.\frac{L(E_{a,\gamma}, T)}{(1 - qT)^\rho}\right|_{T=q^{-1}} \in \mathbb{Z}[q^{-1}] \smallsetminus \{0\}, \quad \text{where } \rho = \rho(E_{a,\gamma}). \tag{1.7}$$

Remark 1.4 The special value $L^*(E_{a,\gamma}, 1)$ is 'usually' defined as the first nonzero coefficient in the Taylor expansion around $s = 1$ of the function $s \mapsto L(E_{a,\gamma}, q^{-s})$. Our definition (1.7) differs from that more 'usual' one by a factor $(\log q)^\rho$. We prefer to use the normalisation (1.7) because it ensures that $L^*(E_{a,\gamma}, 1) \in \mathbb{Q}^*$. This choice is consistent with our normalisation of $\mathrm{Reg}(E_{a,\gamma})$, see §1.3 below.

1.3 The BSD conjecture

The Mordell–Weil theorem implies that $E_{a,\gamma}(K)$ is a finitely generated abelian group (*cf.* [Ulm11, Lect. 1, Thm. 5.1]). Since the canonical Néron–Tate height $\widehat{h} : E_{a,\gamma}(K) \to \mathbb{Q}$ is quadratic, it induces a $\mathbb{Z}$-bilinear pairing $\langle \cdot, \cdot \rangle : E_{a,\gamma}(K) \times E_{a,\gamma}(K) \to \mathbb{Q}$, which is nondegenerate modulo $E_{a,\gamma}(K)_{\mathrm{tors}}$ (*cf.* [Sil94, Chap. III, Thm. 4.3]). We can then define the *Néron-Tate regulator* of $E_{a,\gamma}$ by

$$\mathrm{Reg}(E_{a,\gamma}) := \left|\det\left(\langle P_i, P_j \rangle\right)_{1 \leq i,j \leq r}\right| \in \mathbb{Q}^*,$$

[3] When $E_{a,\gamma}$ has bad reduction at v, note that a_v equals 0 (resp. +1, −1) if $E_{a,\gamma}$ has additive (resp. split multiplicative, nonsplit multiplicative) reduction at v.

for any choice of a $\mathbb{Z}$-basis $P_1, \dots, P_r \in E_{a,\gamma}(K)$ of $E_{a,\gamma}(K)/E_{a,\gamma}(K)_{\mathrm{tors}}$. Note that we normalise $\langle \cdot, \cdot \rangle$ to have values in $\mathbb{Q}$: we may do so since, in our context, this height pairing has an interpretation as an intersection pairing on the minimal regular model of $E_{a,\gamma}$ (see [Sil94, Chap. III, §9]).

Let us also recall that the *Tate–Shafarevich group* of $E_{a,\gamma}$ is defined by

$$Ш(E_{a,\gamma}) := \ker\left(\mathrm{H}^1(K, E_{a,\gamma}) \longrightarrow \prod_v \mathrm{H}^1(K_v, (E_{a,\gamma})_v) \right),$$

see [Ulm11, Lect. 1 §11] for more details. In Theorem 1.5 right below, we will see that $Ш(E_{a,\gamma})$ is finite.

It has been conjectured by Birch, Swinnerton-Dyer and Tate that the 'analytically defined' quantities $\rho(E_{a,\gamma})$ and $L^*(E_{a,\gamma}, 1)$ have an arithmetic interpretation (see [Tat66, Conj. B]). Even though this conjecture is still open in general, it has been proved by Pries and Ulmer for $E_{a,\gamma}$ in [PU16]. Let us state their result as follows:

Theorem 1.5 (Pries - Ulmer) – *For all $\gamma \in \mathbb{F}_q^\times$ and all integers $a \geq 1$, the elliptic curve $E_{a,\gamma}/K$ satisfies the full Birch and Swinnerton-Dyer conjecture. That is to say,*

- *The Tate–Shafarevich group $Ш(E_{a,\gamma})$ is finite.*
- *The rank of $E_{a,\gamma}(K)$ is equal to $\rho(E_{a,\gamma}) = \mathrm{ord}_{T=q^{-1}} L(E_{a,\gamma}, T)$.*
- *Moreover, one has*

$$L^*(E_{a,\gamma}, 1) = \frac{|Ш(E_{a,\gamma})| \cdot \mathrm{Reg}(E_{a,\gamma})}{H(E_{a,\gamma})} \cdot \frac{\tau(E_{a,\gamma}) \cdot q}{|E_{a,\gamma}(K)_{\mathrm{tors}}|^2}, \tag{1.8}$$

where $\tau(E_{a,\gamma})$ denotes the Tamagawa number of $E_{a,\gamma}$.

Proof: We only sketch a proof and refer the interested reader to [PU16, §3] for more details. As we have seen at the beginning of this section, $E_{a,\gamma}$ is 2-isogenous to $E^\circ_{a,\gamma}$. Since $E_{a,\gamma}$ and $E^\circ_{a,\gamma}$ are linked by an isogeny of degree prime to the characteristic of K, Theorem 7.3 in [Mil86, Chap. I] implies that the BSD conjecture holds for $E_{a,\gamma}$ if and only if it does for $E^\circ_{a,\gamma}$. Hence Theorem 1.5 will follow if we prove that $E^\circ_{a,\gamma}$ satisfies the BSD conjecture.

We have also shown that $E^\circ_{a,\gamma}$ is birational to the curve $Z_{a,\gamma} \subset \mathbb{P}^1 \times \mathbb{P}^1$ which, by construction, is given in affine coordinates by an equation of the form $f_\gamma(x) - f_\gamma(y) = \wp_a(t)$ where f_γ is a certain rational function on $\mathbb{P}^1$ over K and $\wp_a(t) \in \mathbb{F}_q[t]$ is a separable additive polynomial. Under these conditions, Corollary 3.1.4 of [PU16] proves that $E^\circ_{a,\gamma}$ satisfies the BSD conjecture.

The crucial point of their proof is the following: given the specific shape of the equation of $Z_{a,\gamma}$ to which $E^\circ_{a,\gamma}$ is birational, the minimal regular model $\mathcal{E}^\circ_{a,\gamma} \to \mathbb{P}^1$ over $\mathbb{F}_q$ of the curve $E^\circ_{a,\gamma}/K$ is dominated by a product of curves $\mathcal{C}_{a,\gamma} \times \mathcal{C}_{a,\gamma} \dashrightarrow \mathcal{E}^\circ_{a,\gamma}$ over $\mathbb{F}_q$ (where $\mathcal{C}_{a,\gamma}$ is actually the curve defined in Remark 2.3 below). The Tate conjecture (T) asserts that the order of the pole of the zeta function of a surface $S/\mathbb{F}_q$ equals the rank of the Néron–Severi group of S (see [Tat66, Conj. C], or §10–§13 in [Ulm11, Lect. 2]). Conjecture (T) is proved for surfaces that are dominated by products of curves. In particular, (T) holds for the surface $\mathcal{E}^\circ_{a,\gamma}/\mathbb{F}_q$. On the other hand, it is known that conjecture (T) for $\mathcal{E}^\circ_{a,\gamma}/\mathbb{F}_q$ is equivalent to the BSD conjecture for the generic fiber of $\mathcal{E}^\circ_{a,\gamma} \to \mathbb{P}^1$ *i.e.*, for the elliptic curve $E^\circ_{a,\gamma}/K$ (Theorem 8.1 in [Ulm11, Lect. 2]). Hence the result. □

In section 6 we give bounds on the special value $L^*(E_{a,\gamma}, 1)$ on the left-hand side of (1.8) and, in section 7, we deduce from these an estimate on the asymptotically significant quantities on the right-hand side of (1.8). For completeness, let us recall here the following bounds (which we will need to prove Theorem 7.1).

Proposition 1.6 – *Let E be a nonisotrivial elliptic curve over K. Then*

(i) $|E(K)_{\mathrm{tors}}| \ll_q 1$, *(ii)* $\log \tau(E) = o\big(\log H(E)\big)$ *as* $H(E) \to \infty$.

Proof: The first bound is the analogue for elliptic curves over $K = \mathbb{F}_q(t)$ of Merel's uniform bound on torsion for elliptic curves over $\mathbb{Q}$. There are several proofs of *(i)* and we refer the reader to [Ulm11, Lect. I §7] for a survey and a sketch of proof (by a modular method). The bound *(ii)* on the Tamagawa number is a consequence of Theorem 1.22 of [HP16] in the case when E is semistable or $p > 3$. A self-contained (and elementary) proof for all elliptic curves over K can also be found in [Gri16, Théorème 1.5.4]. □

2 The sums $\mathcal{K}_\gamma(v)$ and the sets $P_q(a)$

The goal of this section is to introduce the objects which appear in the L-function of $E_{a,\gamma}$.

We fix a finite field $\mathbb{F}_q$ of odd characteristic and a nontrivial additive character ψ_q on $\mathbb{F}_q$, which we assume to take values in the cyclotomic field $\mathbb{Q}(\zeta_p)$. For instance, a standard choice of ψ_q is the map $\psi_q : x \mapsto \zeta_p^{\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}$ where ζ_p is a primitive pth root of unity and $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace map.

For any finite extension $\mathbb{F}$ of $\mathbb{F}_q$, we denote by $\mathrm{tr}_{\mathbb{F}/\mathbb{F}_q} : \mathbb{F} \to \mathbb{F}_q$ the relative trace and we 'lift' ψ_q to a nontrivial additive character $\psi_{\mathbb{F}} : \mathbb{F} \to \mathbb{Q}(\zeta_p)^\times$ on $\mathbb{F}$ by putting $\psi_{\mathbb{F}} := \psi_q \circ \mathrm{tr}_{\mathbb{F}/\mathbb{F}_q}$.

2.1 Kloosterman sums

For a finite field $\mathbb{F}$ of odd characteristic p, a nontrivial additive character ψ on $\mathbb{F}$ with values in the cyclotomic field $\mathbb{Q}(\zeta_p)$, and a parameter $\alpha \in \mathbb{F}^\times$, we define the *Kloosterman sum* $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)$ by:

$$\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha) := -\sum_{x\in\mathbb{F}^\times} \psi\left(x + \frac{\alpha}{x}\right). \tag{2.1}$$

As a sum of pth roots of unity, $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)$ is an algebraic integer in $\mathbb{Q}(\zeta_p)$. For our purpose, it is convenient to normalise the sum by a -1 sign. Let us gather in one proposition several classical facts about the Kloosterman sums that will be useful in this article.

Proposition 2.1 – *Let $\mathbb{F}, \psi$ and α be as above. Then:*

(i) $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)$ *is a totally real algebraic integer in $\mathbb{Q}(\zeta_p)$ i.e.,* $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha) \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

(ii) $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)$ *satisfies 'Salié's formula':*

$$\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha) = -\sum_{y\in\mathbb{F}} \lambda(y^2 - 4\alpha)\cdot\psi(y), \tag{2.2}$$

where $\lambda : \mathbb{F}^\times \to \{\pm 1\}$ is the unique multiplicative character on $\mathbb{F}^\times$ of exact order 2 (extended by $\lambda(0) := 0$ to the whole of $\mathbb{F}$).

(iii) *If $\mathbb{F}$ contains $\mathbb{F}_q$, one has* $\mathrm{Kl}_{\mathbb{F}}(\psi_q \circ \mathrm{tr}_{\mathbb{F}/\mathbb{F}_q};\alpha) = \mathrm{Kl}_{\mathbb{F}}(\psi_q \circ \mathrm{tr}_{\mathbb{F}/\mathbb{F}_q};\alpha^q)$.

(iv) *There exist two algebraic integers $\mathsf{kl}_{\mathbb{F}}(\psi;\alpha)$ and $\mathsf{kl}'_{\mathbb{F}}(\psi;\alpha)$ such that $\mathsf{kl}_{\mathbb{F}}(\psi;\alpha)\cdot\mathsf{kl}'_{\mathbb{F}}(\psi;\alpha) = |\mathbb{F}|$ and,*

$$\text{for any finite extension } \mathbb{F}'/\mathbb{F}, \quad \mathrm{Kl}_{\mathbb{F}'}(\psi\circ\mathrm{tr}_{\mathbb{F}'/\mathbb{F}};\alpha) = \mathsf{kl}_{\mathbb{F}}(\psi;\alpha)^{[\mathbb{F}':\mathbb{F}]} + \mathsf{kl}'_{\mathbb{F}}(\psi;\alpha)^{[\mathbb{F}':\mathbb{F}]}. \tag{2.3}$$

The pair $\{\mathsf{kl}_{\mathbb{F}}(\psi;\alpha), \mathsf{kl}'_{\mathbb{F}}(\psi;\alpha)\}$ is uniquely determined by $\mathbb{F}, \psi, \alpha$.

(v) $\mathsf{kl}_{\mathbb{F}}(\psi;\alpha)$ *and* $\mathsf{kl}'_{\mathbb{F}}(\psi;\alpha)$ *have magnitude $|\mathbb{F}|^{1/2}$ in any complex embedding. In particular, in any complex embedding of $\mathbb{Q}(\zeta_p)$, the sum $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)$ satisfies $|\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)| \le 2|\mathbb{F}|^{1/2}$ ('Weil bound').*

(vi) *In any complex embedding of $\mathbb{Q}(\zeta_p)$, one has*

$$0 < |\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)| < 2|\mathbb{F}|^{1/2}. \tag{2.4}$$

Proof: The reader can confer [LN97, Chap. 5, §5] and [vdGvdV91, §3] for proofs of these classical results about Kloosterman sums: (i) and (iii) are easily checked; items (ii), (iv) and (v) are Theorems 5.47, 5.43 and 5.44 in [LN97], respectively; (vi) is proved in Corollary 3.2 of [vdGvdV91]. □

2.2 The sums $\mathcal{K}_\gamma(v)$

Assume a parameter $\gamma \in \mathbb{F}_q^\times$ is given. A place $v \neq 0, \infty$ of K with degree d_v corresponds to a monic irreducible polynomial $B_v \in \mathbb{F}_q[t]$ of degree d_v, with $B_v \neq t$. Choose a root $\beta_v \in \overline{\mathbb{F}_q}^\times$ of B_v: we claim that the value of the Kloosterman sum $\mathrm{Kl}_{\mathbb{F}_v}(\psi_{\mathbb{F}_v};\gamma\beta_v^2)$ does not depend on the choice of β_v. Indeed, given one such β_v the $d_v - 1$ other choices are of the form $\beta_v{}^{q^j}$ (with $j \in \{1, 2, \ldots, d_v - 1\}$) because the d_v different roots of B_v in $\overline{\mathbb{F}_q}$ are all conjugate under the action of the Galois group $\mathrm{Gal}(\mathbb{F}_v/\mathbb{F}_q)$. A repeated application of Proposition 2.1(iii) then proves the claim. Therefore the following definition makes sense:

Definition 2.2 Let $\mathbb{F}_q$ be a finite field of characteristic p, ψ_q be a nontrivial additive character on $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q^\times$. For any place $v \neq 0, \infty$ of $K = \mathbb{F}_q(t)$ corresponding to a monic irreducible $B_v \in \mathbb{F}_q[t]$, we let

$$\mathcal{K}_\gamma(v) := \mathrm{Kl}_{\mathbb{F}_v}(\psi_{\mathbb{F}_v};\gamma\beta_v^2) = -\sum_{x\in\mathbb{F}_v^\times} \psi_q\circ\mathrm{tr}_{\mathbb{F}_v/\mathbb{F}_q}\left(x + \frac{\gamma\cdot\beta_v^2}{x}\right), \tag{2.5}$$

for any choice of $\beta_v \in \overline{\mathbb{F}_q}^\times$ such that $B_v(\beta_v) = 0$.

Note that $\mathcal{K}_\gamma(v)$ depends on $\mathbb{F}_q$ and ψ_q, but we chose not to include these in the notation for brevity.

For any place $v \neq 0, \infty$, Proposition 2.1(iv)-(v) shows that there exist a unique pair $\{\mathbf{kl}_\gamma(v), \mathbf{kl}'_\gamma(v)\}$ of conjugate algebraic integers, which have magnitude $|\mathbb{F}_v|^{1/2} = q^{d_v/2}$ in any complex embedding and such that

$$\mathrm{K}_\gamma(v) = \mathbf{kl}_\gamma(v) + \mathbf{kl}'_\gamma(v). \tag{2.6}$$

In other words, we denote by $\{\mathbf{kl}_\gamma(v), \mathbf{kl}'_\gamma(v)\}$ the pair of algebraic integers $\{\mathsf{kl}_{\mathbb{F}_v}(\psi_{\mathbb{F}_v}; \gamma\beta_v^2), \mathsf{kl}'_{\mathbb{F}_v}(\psi_{\mathbb{F}_v}; \gamma\beta_v^2)\}$.

Remark 2.3 These sums $\mathrm{K}_\gamma(v)$ appear in the zeta function of a curve over $\mathbb{F}_q$. Namely, consider the hyperelliptic curve $\mathcal{C}_{a,\gamma}$ over $\mathbb{F}_q$ defined as a smooth projective model of the affine curve $\wp_a(y) = x + \gamma/x$. A computation, which probably goes back to Weil, shows that the zeta function of $\mathcal{C}_{a,\gamma}/\mathbb{F}_q$ is given by

$$Z(\mathcal{C}_{a,\gamma}/\mathbb{F}_q; U) = \frac{\prod_v \left(1 - \mathbf{kl}_\gamma(v) \cdot U^{d_v}\right)\left(1 - \mathbf{kl}'_\gamma(v) \cdot U^{d_v}\right)}{(1-U)(1-q\cdot U)},$$

where the product is over all places $v \neq 0, \infty$ of K whose degrees divide a (see [vdGvdV91]).

2.3 The sets $P_q(a)$

Definition 2.4 For any integer $a \geq 1$, we denote by $P_q(a)$ the set of places v of K, with $v \notin \{0, \infty\}$, whose degree d_v divides a. In the identification between finite places of K and monic irreducible polynomials, $P_q(a)$ corresponds to the set $\{B \in \mathbb{F}_q[t] : B \text{ monic, irreducible s.t. } \deg B \mid a \text{ and } B \neq t\}$. Equivalently, $P_q(a)$ is the set of closed points on the multiplicative group $\mathbb{G}_m = \mathbb{P}^1 \smallsetminus \{0, \infty\}$ over $\mathbb{F}_q$ whose degree divides a.

In what follows, we will frequently need the following estimates, which we record here for convenience.

Lemma 2.5 – *Given a finite field $\mathbb{F}_q$, one has*

(i) $|P_q(a)| = q^a/a + O\big(q^{a/2}\big)$ *for all* $a \geq 1$. (ii) $q^a \ll_q a \cdot |P_q(a)| \ll_q q^a$ *for all* $a \geq 1$.

The involved constant are effective and depend at most on q.

Proof: For all $n \geq 1$, we denote by $\pi_q(n)$ the number of places $v \neq 0, \infty$ of K of degree $d_v = n$. In other words, $\pi_q(n)$ is the number of closed points of degree n of $\mathbb{G}_m$ over $\mathbb{F}_q$.

The 'Prime Number Theorem' for $\mathbb{F}_q[t]$ states that $\pi_q(n) = q^n/n + O_q(q^{n/2})$ for all $n \geq 1$ where the hidden constant can be given explicitly (see [Bru92, Prop. 6.3] for example). On the other hand, it is clear from the definition that $|P_q(a)| = \sum_{n|a} \pi_q(n)$. The estimate of $\pi_q(n)$ and this relation directly imply (i). From this, one easily deduces (ii). □

3 The L-function

With the notations introduced in the previous section, we can now state our first main result:

Theorem 3.1 – *Let $\mathbb{F}_q$ be a finite field of odd characteristic p and $K = \mathbb{F}_q(t)$. For any $\gamma \in \mathbb{F}_q^\times$ and any integer $a \geq 1$, consider the elliptic curve $E_{a,\gamma}/K$ given by (1.1). The L-function of $E_{a,\gamma}$ is given by*

$$L(E_{a,\gamma}, T) = \prod_{v \in P_q(a)} \left(1 - q^{d_v} \cdot T^{d_v}\right)\left(1 - \mathbf{kl}_\gamma(v)^2 \cdot T^{d_v}\right)\left(1 - \mathbf{kl}'_\gamma(v)^2 \cdot T^{d_v}\right), \tag{3.1}$$

where $\mathbf{kl}_\gamma(v)$, $\mathbf{kl}'_\gamma(v)$ are the algebraic integers associated to $\mathrm{K}_\gamma(v)$ (see (2.5) and (2.6)).

The proof of this theorem occupies the rest of the present section. Our strategy is loosely based on the computation in [CHU14, §3.2]: to give an expression of $L(E_{a,\gamma}, T)$, we rely on an explicit 'point-counting' argument with character sums. This requires showing an identity for counting solutions to 'Artin–Schreier equations' in terms of character sums, as well as a relation between the character sums that appear in the argument and the sums $\mathrm{K}_\gamma(v)$ introduced above. We first give in the next subsection a proof of these two facts, and then prove Theorem 3.1 in §3.2.

Remark 3.2 Before moving on to the proof of this theorem, we note the following:

(1) Even though the sums $\mathrm{K}_\gamma(v)$ for $v \in P_q(a)$ individually depend on the choice of a nontrivial additive character ψ_q on $\mathbb{F}_q$, the L-function $L(E_{a,\gamma}, T) \in \mathbb{Z}[T]$ does not. Indeed, changing the choice of ψ_q amounts to permuting the factors in (3.1).

(2) Note that $\sum_{v \in P_q(a)} d_v = |\mathbb{G}_m(\mathbb{F}_{q^a})| = q^a - 1$. Thus, as a polynomial in T, the L-function $L(E_{a,\gamma}, T)$ has degree $3(q^a - 1) = \deg \mathcal{N}(E_{a,\gamma}) - 4$. This is consistent with the expected degree, see (1.6).

(3) For any integer $a \geq 1$, the L-function of the base change of $E_{a,\gamma}$ to $K_a := \mathbb{F}_{q^a}(t)$ admits a somewhat simpler expression. Indeed, for all $\gamma \in \mathbb{F}_q^\times$ and $a \geq 1$, the L-function of $E_{a,\gamma}/K_a$ is given by

$$L(E_{a,\gamma}/K_a, T) = \prod_{\beta \in \mathbb{F}_{q^a}^\times} (1 - q^a \cdot T) \left(1 - (\mathsf{kl}_\beta)^2 \cdot T\right) \left(1 - (\mathsf{kl}'_\beta)^2 \cdot T\right),$$

where, for all $\beta \in \mathbb{F}_{q^a}^\times$, kl_β and kl'_β are the two algebraic integers associated to the Kloosterman sum $\mathrm{Kl}_{\mathbb{F}_{q^a}}(\psi_{\mathbb{F}_{q^a}}; \gamma\beta^2)$. This follows directly from (3.1).

(4) Recall the elliptic curves $E^\circ_{a,\gamma}$ introduced at the beginning of §1 and given by (1.2). Since isogenous elliptic curves share the same L-function (by [Mil86, Chap. I, Lemma 7.1]), Theorem 3.1 also shows that the L-function of $E^\circ_{a,\gamma}$ is given by (3.1).

(5) It is perhaps illuminating to comment on the appearance of Kloosterman sums in $L(E_{a,\gamma}, T)$. Choosing a prime $\ell \neq p$, we denote by $\mathrm{H}^i(X) = \mathrm{H}^i_{\text{ét}}(X \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)$ the i-th ℓ-adic étale cohomology group of a smooth projective variety $X/\mathbb{F}_q$. Let $\mathcal{E}^\circ_{a,\gamma} \to \mathbb{P}^1$ denote the minimal regular model of $E^\circ_{a,\gamma}$. The cohomological interpretation of L-functions of Grothendieck implies that $L(E^\circ_{a,\gamma}, T)$ is essentially the 'interesting part' of the zeta function of the surface $\mathcal{E}_{a,\gamma}/\mathbb{F}_q$ *i.e.*, $L(E^\circ_{a,\gamma}, T)$ is a factor of the characteristic polynomial of the Frobenius Frob_q acting on $H^2(\mathcal{E}^\circ_{a,\gamma})$.

By the construction of $E^\circ_{a,\gamma}$ in §1, $\mathcal{E}^\circ_{a,\gamma}$ is a smooth model of a quotient of $\mathcal{C}_{a,\gamma} \times \mathcal{C}_{a,\gamma}$ by the action of a certain finite group G_a, where $\mathcal{C}_{a,\gamma}/\mathbb{F}_q$ is the curve introduced in Remark 2.3 (see [PU16, §7.3] for a more detailed presentation). In particular, $\mathrm{H}^2(\mathcal{E}^\circ_{a,\gamma})$ can be seen as a subspace of $\mathrm{H}^2((\mathcal{C}_{a,\gamma} \times \mathcal{C}_{a,\gamma})/G_a)$, itself a subspace of $\mathrm{H}^2(\mathcal{C}_{a,\gamma} \times \mathcal{C}_{a,\gamma})$. Hence, by Künneth's formula, $L(E^\circ_{a,\gamma}, T)$ divides the characteristic polynomial of Frob_q acting on $\mathrm{H}^1(\mathcal{C}_{a,\gamma}) \otimes \mathrm{H}^1(\mathcal{C}_{a,\gamma})$.

As was noted in Remark 2.3, the numerator of the zeta function of $\mathcal{C}_{a,\gamma}$ *i.e.*, the characteristic polynomial of Frob_q acting on $\mathrm{H}^1(\mathcal{C}_{a,\gamma})$, involves Kloosterman sums $\mathrm{K}_\gamma(v)$. Hence, the eigenvalues of Frob_q acting on $\mathrm{H}^1(\mathcal{C}_{a,\gamma}) \otimes \mathrm{H}^1(\mathcal{C}_{a,\gamma})$ are products of the form $\mathrm{K}_\gamma(v_1)\mathrm{K}_\gamma(v_2)$. Being a factor of the characteristic polynomial of Frob_q acting on $\mathrm{H}^1(\mathcal{C}_{a,\gamma}) \otimes \mathrm{H}^1(\mathcal{C}_{a,\gamma})$, the L-function $L(E^\circ_{a,\gamma}, T)$ has to involve some of the products $\mathrm{K}_\gamma(v_1)\mathrm{K}_\gamma(v_2)$.

Working out the details of this sketchy computation could lead to a different proof of Theorem 3.1.

3.1 Point-counting and character sums

For any finite finite field $\mathbb{F}$ of odd characteristic, we fix a nontrivial additive character ψ on $\mathbb{F}$, and we denote by $\lambda : \mathbb{F}^\times \to \{\pm 1\}$ the unique quadratic character on $\mathbb{F}^\times$, extended to the whole of $\mathbb{F}$ by $\lambda(0) := 0$.

For any $\gamma \in \mathbb{F}^\times$ and $\beta \in \mathbb{F}$, we consider the following double character sum

$$M_{\mathbb{F}}(\beta, \gamma) := \sum_{x \in \mathbb{F}} \sum_{z \in \mathbb{F}} \lambda\left(x(x + 16\gamma)(x + z^2)\right) \cdot \psi(\beta z),$$

Up to a trivial term, we identify the character sum $M_{\mathbb{F}}(\beta, \gamma)$ as the square of a Kloosterman sum:

Proposition 3.3 – *Notations being as above, we have*

$$M_{\mathbb{F}}(\beta, \gamma) = \begin{cases} 1 & \text{if } \beta = 0 \\ \mathrm{Kl}_{\mathbb{F}}\left(\psi; \gamma \cdot \beta^2\right)^2 - |\mathbb{F}| & \text{if } \beta \neq 0. \end{cases} \tag{3.2}$$

In order to prove this identity, we begin by recording the following 'point-counting' lemma:

Lemma 3.4 – *For any $z \in \mathbb{F}$ and $\gamma \in \mathbb{F}^\times$, consider*

$$X_{\mathbb{F},\gamma}(z) := \left\{(u, v) \in \mathbb{F}^2 : v^2 - (u^2 - uz - 4\gamma)v + \gamma z^2 = 0\right\} \subset \mathbb{F}^2.$$

We have

$$|X_{\mathbb{F},\gamma}(z)| = |\mathbb{F}| \cdot (1 + \delta_{z,0}) - 1 + \sum_{x \in \mathbb{F}} \lambda\left(x(x + 16\gamma)(x + z^2)\right), \tag{3.3}$$

where $\delta_{z,0} = 1$ if $z = 0$ and $\delta_{z,0} = 0$ otherwise.

Proof: Let us start by splitting the set $X_{\mathbb{F},\gamma}(z)$ into the two disjoint subsets $X_0 := \{(u, v) \in X_{\mathbb{F},\gamma}(z) : v = 0\}$ and $X_1 := X_{\mathbb{F},\gamma}(z) \smallsetminus X_0$. Computing $|X_0|$ is straightforward: if $z = 0$, any pair $(u, 0)$ with $u \in \mathbb{F}$ belongs to X_0 and, if $z \neq 0$, no such pair belongs to $X_{\mathbb{F},\gamma}(z)$. Therefore, we have $|X_0| = |\mathbb{F}| \cdot \delta_{z,0}$.

To count the number of elements in X_1, let us introduce an auxiliary set

$$Y_{\mathbb{F},\gamma}(z) := \left\{(x, y) \in \mathbb{F}^2 : y^2 = x(x + 16\gamma)(x + z^2)\right\} \subset \mathbb{F}^2,$$

which we also split into two parts: $Y_0 := \{(x,y) \in Y_{\mathbb{F},\gamma}(z) : x = 0\}$ and $Y_1 := Y_{\mathbb{F},\gamma}(z) \smallsetminus Y_0$. The two maps

$$\begin{array}{ccc} X_1 & \longrightarrow & Y_1 \\ (u,v) & \longmapsto & \big(4v, 4v(2u-z)\big) \end{array} \qquad \text{and} \qquad \begin{array}{ccc} Y_1 & \longrightarrow & X_1 \\ (x,y) & \longmapsto & \big((y+zx)/(2x), x/4\big). \end{array}$$

are easily checked to be well-defined and inverse to each other. Thus, we have $|X_1| = |Y_1|$ and the Lemma will be proved once we have related $|Y_1|$ to the character sum in (3.3). Grouping points $(x,y) \in Y_1$ according to their x-coordinates, we obtain that:

$$|Y_1| = \sum_{x \in \mathbb{F}^\times} \big(1 + \lambda\big(x(x+16\gamma)(x+z^2)\big)\big) = |\mathbb{F}| - 1 + \sum_{x \in \mathbb{F}} \lambda\big(x(x+16\gamma)(x+z^2)\big).$$

Since $|X_{\mathbb{F},\gamma}(z)| = |X_0| + |X_1|$ and $|X_1| = |Y_1|$, we conclude that (3.3) holds. □

Proof (of Proposition 3.3): We treat the case where $\beta = 0$ first: we have to prove that

$$\sum_{x \in \mathbb{F}} \sum_{z \in \mathbb{F}} \lambda\left(x(x+16\gamma)(x+z^2)\right) = 1.$$

This identity follows easily upon using the following equality (see [LN97, Thm. 5.48]):

$$\forall b, c \in \mathbb{F}, \quad \sum_{y \in \mathbb{F}} \lambda(y^2 + by + c) = \begin{cases} |\mathbb{F}| - 1 & \text{if } b^2 = 4c, \\ -1 & \text{otherwise.} \end{cases}$$

It remains to prove the Proposition in the case where $\beta \neq 0$. If $\beta \neq 0$, the character $x \mapsto \psi(\beta x)$ is nontrivial, and we can expand $\mathrm{Kl}_{\mathbb{F}}\big(\psi, \gamma\beta^2\big)^2$ as a double character sum using Salié's formula (2.2): we obtain that

$$\begin{aligned} \mathrm{Kl}_{\mathbb{F}}\big(\psi, \gamma\beta^2\big)^2 &= \left(\sum_{u \in \mathbb{F}} \lambda(u^2 - 4\gamma) \cdot \psi(\beta u)\right)^2 = \sum_{u_1 \in \mathbb{F}} \sum_{u_2 \in \mathbb{F}} \lambda\left((u_1^2 - 4\gamma)(u_2^2 - 4\gamma)\right) \cdot \psi\big(\beta(u_1 + u_2)\big) \\ &= \sum_{z \in \mathbb{F}} \left(\sum_{u \in \mathbb{F}} \lambda\left((u^2 - 4\gamma)((u-z)^2 - 4\gamma)\right)\right) \cdot \psi(\beta z). \end{aligned} \tag{3.4}$$

The last line follows from the first by letting $(u, z) = (u_1, u_1 + u_2)$. For a given $z \in \mathbb{F}$, notice that

$$\forall u \in \mathbb{F}, \qquad (u^2 - 4\gamma)((u-z)^2 - 4\gamma) = (u^2 - zu - 4\gamma)^2 - 4\gamma z^2,$$

which is the discriminant of the quadratic equation $V^2 - (u^2 - zu - 4\gamma) \cdot V + \gamma z^2 = 0$ with unknown V. Hence, the number of solutions $v \in \mathbb{F}$ to this equation is given by

$$\left|\left\{v \in \mathbb{F} : v^2 - (u^2 - zu - 4\gamma) \cdot v + \gamma z^2 = 0\right\}\right| = 1 + \lambda\left((u^2 - zu - 4\gamma)^2 - 4\gamma z^2\right).$$

Therefore we can rewrite the inner sum (over $u \in \mathbb{F}$) in (3.4) as

$$\begin{aligned} \sum_{u \in \mathbb{F}} \lambda\left((u^2 - 4\gamma)((u-z)^2 - 4\gamma)\right) &= -|\mathbb{F}| + \sum_{u \in \mathbb{F}} \left(1 + \lambda\left((u^2 - zu - 4\gamma)^2 - 4\gamma z^2\right)\right) \\ &= -|\mathbb{F}| + \sum_{u \in \mathbb{F}} \left|\left\{v \in \mathbb{F} : v^2 - (u^2 - zu - 4\gamma) \cdot v + \gamma z^2 = 0\right\}\right| \\ &= -|\mathbb{F}| + |X_{\mathbb{F},\gamma}(z)|, \end{aligned}$$

where $X_{\mathbb{F},\gamma}(z)$ is the set introduced in Lemma 3.4. In that same Lemma 3.4, we have proved that

$$\forall z \in \mathbb{F}, \qquad |X_{\mathbb{F},\gamma}(z)| - |\mathbb{F}| = |\mathbb{F}| \cdot \delta_{z,0} - 1 + \sum_{x \in \mathbb{F}} \lambda\left(x(x+16\gamma)(x+z^2)\right).$$

On multiplying this identity by $\psi(\beta z)$ and summing over all $z \in \mathbb{F}$, we deduce from (3.4) that

$$\mathrm{Kl}_{\mathbb{F}}\big(\psi; \gamma\beta^2\big)^2 = \sum_{z \in \mathbb{F}} (|\mathbb{F}| \cdot \delta_{z,0} - 1)\psi(\beta z) + M_{\mathbb{F}}(\beta, \gamma) = |\mathbb{F}| + M_{\mathbb{F}}(\beta, \gamma).$$

Indeed, the sum $\sum_{z \in \mathbb{F}} \psi(\beta z)$ vanishes because $x \mapsto \psi(\beta x)$ is nontrivial. This concludes the proof. □

In the proof of Theorem 3.1, we will also need the following 'counting lemma':

Lemma 3.5 – *Let $\mathbb{F}_q$ be a finite field and ψ_q be a nontrivial additive character on $\mathbb{F}_q$. For any finite extension $\mathbb{F}$ of $\mathbb{F}_q$ and any $z \in \mathbb{F}$, one has*

$$|\{\tau \in \mathbb{F} : \wp_a(\tau) = z\}| = \sum_{\beta \in \mathbb{F}_{q^a} \cap \mathbb{F}} \psi_{\mathbb{F}}(\beta \cdot z). \tag{3.5}$$

Proof: For the duration of the proof, we write $\mathbb{F} = \mathbb{F}_{q^n}$ and we let $b = \gcd(a, n)$; note that $\mathbb{F}_{q^a} \cap \mathbb{F}_{q^n} = \mathbb{F}_{q^b}$. The map $\wp_a : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is an $\mathbb{F}_{q^b}$-linear endomorphism of $\mathbb{F}_{q^n}$ whose kernel is $\mathbb{F}_{q^b}$. In particular, the image of $\wp_a$ must have dimension $\dim_{\mathbb{F}_{q^b}}(\mathbb{F}_{q^n}) - 1 = n/b - 1$. The trace $t := \mathrm{tr}_{q^n/q^b} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^b}$ is a surjective $\mathbb{F}_{q^b}$-linear map, so that its kernel H is a sub-$\mathbb{F}_{q^b}$-vector space of $\mathbb{F}_{q^n}$ of dimension $n/b - 1$. Recall that $t \circ \wp_a = 0$ on $\mathbb{F}_{q^n}$, thus we have $\operatorname{Im} \wp_a \subset H$. Since these two subspaces have the same dimension, they coincide. This shows that, for $z \in \mathbb{F}_{q^n}$,

$$|\{\tau \in \mathbb{F}_{q^n} : \wp_a(\tau) = z\}| = \begin{cases} 0 & \text{if } t(z) \neq 0, \\ |\ker \wp_a| = q^b & \text{if } t(z) = 0. \end{cases}$$

On the other hand, for a given $z \in \mathbb{F}_{q^n}$, we notice that

$$\sum_{\beta \in \mathbb{F}_{q^b}} \psi_{\mathbb{F}_{q^n}}(\beta \cdot z) = \sum_{\beta \in \mathbb{F}_{q^b}} \psi_{\mathbb{F}_{q^b}} \circ \mathrm{tr}_{q^n/q^b}(\beta \cdot z) = \sum_{\beta \in \mathbb{F}_{q^b}} \psi_{\mathbb{F}_{q^b}} \circ \left(\beta \cdot \mathrm{tr}_{q^n/q^b}(z)\right) = \begin{cases} 0 & \text{if } t(z) \neq 0, \\ q^b & \text{if } t(z) = 0, \end{cases}$$

because $t = \mathrm{tr}_{q^n/q^b}$ is $\mathbb{F}_{q^b}$-linear. Combining the two displayed equalities, we obtain the result. □

3.2 Proof of Theorem 3.1

We start by giving a 'concrete' expression for $L(E_{a,\gamma}, T)$ in terms of the number of rational points on the reductions of $E_{a,\gamma}$ at places of K. To that end, we introduce the following notations: for any $n \geq 1$ and any $\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})$, denote by v_τ the place of K corresponding to τ and by $(\widetilde{E_{a,\gamma}})_\tau$ the reduction of a integral minimal model of $E_{a,\gamma}$ at v_τ (a cubic plane curve over $\mathbb{F}_{v_\tau}$, not necessarily smooth). We then let

$$A_{a,\gamma}(\tau, q^n) := q^n + 1 - |(\widetilde{E_{a,\gamma}})_\tau(\mathbb{F}_{q^n})|.$$

With these notations, we have:

Lemma 3.6 – *The L-function of $E_{a,\gamma}$ is given by*

$$\log L(E_{a,\gamma}, T) = \sum_{n=1}^{\infty} \left(\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A_{a,\gamma}(\tau, q^n) \right) \cdot \frac{T^n}{n}. \tag{3.6}$$

Proof: Starting from the definition (1.5) of the L-function of $E_{a,\gamma}$, expanding $\log L(E_{a,\gamma}/K, T)$ as a power series in T and rearranging terms yields the desired expression for $L(E_{a,\gamma}, T)$.

See [BH12, §2.2] or [CHU14, §3.2] for more details. □

The next step is to find a more tractable expression of the inner sums in (3.6). For any finite extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, we again let $\lambda : \mathbb{F}_{q^n}^\times \to \{\pm 1\}$ be the unique nontrivial character of $\mathbb{F}_{q^n}^\times$ of order 2. For any $\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})$, we choose an affine model $y^2 = f_\tau(x)$ of $(\widetilde{E_{a,\gamma}})_\tau$ (with $f_\tau(x) \in \mathbb{F}_{v_\tau}[x]$ monic of degree 3): a standard computation then yields that

$$A_{a,\gamma}(\tau, q^n) = q^n + 1 - |(\widetilde{E_{a,\gamma}})_\tau(\mathbb{F}_{q^n})| = q^n - \sum_{x \in \mathbb{F}_{q^n}} (1 + \lambda(f_\tau(x))) = -\sum_{x \in \mathbb{F}_{q^n}} \lambda(f_\tau(x)). \tag{3.7}$$

Since $E_{a,\gamma}$ has split multiplicative reduction at ∞ (see Proposition 1.1), we have $A_{a,\gamma}(\infty, q^n) = 1$. Moreover, by Remark 1.2, we may choose $f_\tau(x) = x(x + 16\gamma)(x + \wp_a(\tau)^2)$ for any $\tau \in \mathbb{F}_{q^n}$. Summing identity (3.7) over all $\tau \in \mathbb{F}_{q^n}$ for this choice of $f_\tau(x)$, we obtain that

$$-\sum_{\tau \in \mathbb{F}_{q^n}} A_{a,\gamma}(\tau, q^n) = \sum_{x \in \mathbb{F}_{q^n}} \sum_{\tau \in \mathbb{F}_{q^n}} \lambda\left(x(x + 16\gamma)(x + \wp_a(\tau)^2)\right).$$

We know from Lemma 3.5 that, for any $z \in \mathbb{F}_{q^n}$,

$$|\{\tau \in \mathbb{F}_{q^n} : \wp_a(\tau) = z\}| = \sum_{\beta \in \mathbb{F}_{q^a} \cap \mathbb{F}_{q^n}} \psi_{q^n}(\beta \cdot z).$$

Therefore, we deduce that

$$-\sum_{\tau\in\mathbb{F}_{q^n}} A_{a,\gamma}(\tau,q^n)=\sum_{x\in\mathbb{F}_{q^n}}\sum_{z\in\mathbb{F}_{q^n}}|\{\tau\in\mathbb{F}_{q^n}:\wp_a(\tau)=z\}|\cdot\lambda\left(x(x+16\gamma)(x+z^2)\right)$$
$$=\sum_{\beta\in\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n}}\left(\sum_{x\in\mathbb{F}_{q^n}}\sum_{z\in\mathbb{F}_{q^n}}\lambda\left(x(x+16\gamma)(x+z^2)\right)\cdot\psi_{q^n}(\beta\cdot z)\right)=\sum_{\beta\in\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n}}M_{q^n}(\beta,\gamma),$$

where $M_{q^n}(\beta,\gamma)$ is the double character sum that we studied in §3.1 (with $\mathbb{F}=\mathbb{F}_{q^n}$). Proposition 3.3, together with our computation of $A_{a,\gamma}(\infty,q^n)$, then leads to

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})} A_{a,\gamma}(\tau,q^n)=-\sum_{\beta\in(\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n})\smallsetminus\{0\}}\left(\mathrm{Kl}_{q^n}\left(\psi_{q^n},\gamma\beta^2\right)^2-q^n\right). \tag{3.8}$$

For each $\beta\in\mathbb{F}_{q^n}^\times$, Proposition 2.1(iv) proves the existence of two algebraic integers $\mathsf{kl}_{\mathbb{F}_{q^n}}(\psi_{q^n};\gamma\beta^2)$ and $\mathsf{kl}'_{\mathbb{F}_{q^n}}(\psi_{q^n};\gamma\beta^2)$ whose product is $|\mathbb{F}_{q^n}|=q^n$ and whose sum is $\mathrm{Kl}_{q^n}(\psi_{q^n};\gamma\beta^2)$. We thus have

$$\mathrm{Kl}_{q^n}\left(\psi_{q^n},\gamma\beta^2\right)^2-q^n=\left\{\mathsf{kl}_{q^n}\left(\psi_{q^n};\gamma\beta^2\right)+\mathsf{kl}'_{q^n}\left(\psi_{q^n};\gamma\beta^2\right)\right\}^2-q^n=\mathsf{kl}_{q^n}\left(\psi_{q^n};\gamma\beta^2\right)^2+\mathsf{kl}'_{q^n}\left(\psi_{q^n};\gamma\beta^2\right)^2+q^n.$$

Hence, for all $n\geq 1$, (3.8) can be rewritten as

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})} A_{a,\gamma}(\tau,q^n)=-\sum_{\beta\in(\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n})\smallsetminus\{0\}}\left(\mathsf{kl}_{q^n}\left(\psi_{q^n};\gamma\beta^2\right)^2+\mathsf{kl}'_{q^n}\left(\psi_{q^n};\gamma\beta^2\right)^2+q^n\right) \tag{3.9}$$

For any $\beta\in\mathbb{F}_{q^a}^\times$, we let $d_\beta:=[\mathbb{F}_q(\beta):\mathbb{F}_q]$ be the degree of β over $\mathbb{F}_q$. Such a β also belongs to $\mathbb{F}_{q^n}$ if and only if d_β divides n *i.e.*, if and only if $\mathbb{F}_{q^n}$ is an extension of $\mathbb{F}_{q^{d_\beta}}$. Therefore, by Proposition 2.1(iv) one has

$$\mathrm{Kl}_{q^n}(\psi_{q^n},\gamma\beta^2)=\mathrm{Kl}_{q^n}\left(\psi_{q^{d_\beta}}\circ\mathrm{tr}_{q^n/q^{d_\beta}};\gamma\beta^2\right)=\mathsf{kl}_{q^{d_\beta}}(\psi_{q^{d_\beta}};\gamma\beta^2)^{n/d_\beta}+\mathsf{kl}'_{q^{d_\beta}}(\psi_{q^{d_\beta}};\gamma\beta^2)^{n/d_\beta}.$$

For brevity, we temporarily write $\boldsymbol{\omega}_1(\beta):=\mathsf{kl}_{q^{d_\beta}}\left(\psi_{q^{d_\beta}};\gamma\beta^2\right)^2$, $\boldsymbol{\omega}_2(\beta):=\mathsf{kl}'_{q^{d_\beta}}\left(\psi_{q^{d_\beta}};\gamma\beta^2\right)^2$ and $\boldsymbol{\omega}_3(\beta):=q^{d_\beta}$. We deduce from (3.9) that

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})} A_{a,\gamma}(\tau,q^n)=-\sum_{\beta\in(\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n})\smallsetminus\{0\}}\left(\boldsymbol{\omega}_1(\beta)^{n/d_\beta}+\boldsymbol{\omega}_2(\beta)^{n/d_\beta}+\boldsymbol{\omega}_3(\beta)^{n/d_\beta}\right).$$

Upon multiplying both sides of this identity by T^n/n and summing over all integers $n\geq 1$, we arrive at

$$-\log L(E_{a,\gamma},T)=\sum_{n\geq 1}\left(\sum_{\beta\in(\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n})\smallsetminus\{0\}}\left(\boldsymbol{\omega}_1(\beta)^{n/d_\beta}+\boldsymbol{\omega}_2(\beta)^{n/d_\beta}+\boldsymbol{\omega}_3(\beta)^{n/d_\beta}\right)\right)\cdot\frac{T^n}{n},$$

and exchanging the order of summation (setting $m=n/d_\beta$) leads to

$$-\log L(E_{a,\gamma},T)=\sum_{\beta\in\mathbb{F}_{q^a}^\times}\left(\sum_{m\geq 1}\left(\boldsymbol{\omega}_1(\beta)^m+\boldsymbol{\omega}_2(\beta)^m+\boldsymbol{\omega}_3(\beta)^m\right)\cdot\frac{T^{md_\beta}}{md_\beta}\right)$$
$$=\sum_{\beta\in\mathbb{F}_{q^a}^\times}-\frac{1}{d_\beta}\cdot\log\left(\prod_{i=1}^{3}\left(1-\boldsymbol{\omega}_i(\beta)\cdot T^{d_\beta}\right)\right) \tag{3.10}$$

Moreover, as we have explained in §2.2, for each $\beta\in\mathbb{F}_{q^a}^\times$ with degree d_β, the triple $\{\boldsymbol{\omega}_1(\beta),\boldsymbol{\omega}_2(\beta),\boldsymbol{\omega}_3(\beta)\}$ is constant along the Galois orbit $\{\beta,\beta^q,\ldots,\beta^{q^{d_\beta-1}}\}$ *i.e.*, the closed point of $\mathbb{G}_m$ corresponding to β. Consequently, for a closed point v of $\mathbb{G}_m$ whose degree divides a, we may define $\boldsymbol{\omega}_i(v)$ to be $\boldsymbol{\omega}_i(\beta)$ for any choice of $\beta\in v$. Each term $\log(1-\boldsymbol{\omega}_i(v)T^{d_v})$ (for $i=1,2,3$) appears $d_v=d_\beta$ times in (3.10) and we may thus rewrite the sum over $\beta\in\mathbb{F}_{q^a}^\times$ there as a sum over closed points of $\mathbb{G}_m$ whose degrees divide a:

$$\log L(E_{a,\gamma},T)=\sum_{v\in P_q(a)}\log\left(\prod_{i=1}^{3}\left(1-\boldsymbol{\omega}_i(v)\cdot T^{d_v}\right)\right)$$

Exponentiating this identity and replacing the $\boldsymbol{\omega}_i(v)$'s by their value (see §2.2) concludes the calculation of the L-function of $E_{a,\gamma}$ over K. □

3.3 Rank and special value

From the factored expression of $L(E_{a,\gamma}, T)$ obtained in Theorem 3.1, one can deduce explicit expressions of the analytic rank $\rho(E_{a,\gamma})$ and of the special value $L^*(E_{a,\gamma}, 1)$ (as defined in §1.2).

Proposition 3.7 – *For any $\gamma \in \mathbb{F}_q^\times$ and any integer $a \geq 1$, we have*

$$\rho(E_{a,\gamma}) = |P_q(a)| \tag{3.11}$$

$$\text{and} \quad L^*(E_{a,\gamma}, 1) = \prod_{v \in P_q(a)} 4 \deg v \cdot \prod_{v \in P_q(a)} \left(1 - \frac{\mathrm{K}_\gamma(v)^2}{4q^{\deg v}}\right). \tag{3.12}$$

Proof: For each $v \in P_q(a)$, let

$$g_v(T) := \left(1 - q^{d_v} \cdot T^{d_v}\right) \left(1 - \mathbf{kl}_\gamma(v)^2 \cdot T^{d_v}\right) \left(1 - \mathbf{kl}'_\gamma(v)^2 \cdot T^{d_v}\right)$$

be the corresponding factor of $L(E_{a,\gamma}, T)$ (as in Theorem 3.1). The factor $1 - q^{d_v} \cdot T^{d_v}$ has a simple zero at $T = q^{-1}$ and neither of the other two factors of $g_v(T)$ vanishes at $T = q^{-1}$. Indeed, neither of $\mathbf{kl}_\gamma(v)^2$ and $\mathbf{kl}'_\gamma(v)^2$ can equal q^{d_v} since $|\mathrm{K}_\gamma(v)| = |\mathbf{kl}_\gamma(v) + \mathbf{kl}'_\gamma(v)|$ is strictly smaller than $2q^{d_v/2}$ by Proposition 2.1(vi). Hence, $g_v(T)$ has a simple zero at $T = q^{-1}$ and we have

$$\rho(E_{a,\gamma}) = \mathrm{ord}_{T=q^{-1}} L(E_{a,\gamma}, T) = \sum_{v \in P_q(a)} \mathrm{ord}_{T=q^{-1}} g_v(T) = |P_q(a)|,$$

which proves (3.11). Next, by definition (*cf.* (1.7)) of the special value $L^*(E_{a,\gamma}, 1)$, we have

$$L^*(E_{a,\gamma}, 1) = \frac{L(E_{a,\gamma}, T)}{(1 - qT)^\rho}\bigg|_{T=q^{-1}} = \prod_{v \in P_q(a)} \left(\frac{g_v(T)}{1 - qT}\bigg|_{T=q^{-1}}\right).$$

Besides, a straightforward computation yields

$$\frac{g_v(T)}{1 - qT}\bigg|_{T=q^{-1}} = d_v \cdot \left(1 - \frac{\mathbf{kl}_\gamma(v)^2}{q^{d_v}}\right)\left(1 - \frac{\mathbf{kl}'_\gamma(v)^2}{q^{d_v}}\right) = d_v \cdot \frac{4q^{d_v} - \mathrm{K}_\gamma(v)^2}{q^{d_v}}.$$

Combining the last two displayed identities directly leads to the desired expression for $L^*(E_{a,\gamma}, 1)$. □

Since the curve $E_{a,\gamma}$ satisfies the BSD conjecture (see Theorem 1.5), Proposition 3.7 implies that $\mathrm{rank}\, E_{a,\gamma}(K) = |P_q(a)|$. It is worthwhile to note that the Mordell-Weil rank of $E_{a,\gamma}(K)$ is actually independent of $\gamma \in \mathbb{F}_q^\times$ (this is evident from (3.11)). By Lemma 2.5(i), we therefore have

$$\mathrm{rank}\, E_{a,\gamma}(K) = \frac{q^a}{a} + O\big(q^{a/2}\big) \qquad (\text{as } a \to \infty). \tag{3.13}$$

In particular, this yields that $\mathrm{rank}\, E_{a,\gamma}(K) \gg_q q^a/a$, and we retrieve the following result of 'unbounded rank' (see [PU16, Coro. 2.7.3]).

Corollary 3.8 (Pries - Ulmer) – *Let $\mathbb{F}_q$ be a finite field of odd characteristic and $K = \mathbb{F}_q(t)$. For all $\gamma \in \mathbb{F}_q^\times$, the rank of $E_{a,\gamma}(K)$ is unbounded as $a \geq 1$ tends to infinity.*

Let us also compare (3.13) to the upper bound of [Bru92, Prop. 6.9], which states that

$$\mathrm{rank}\, E_{a,\gamma}(K) \ll_q \frac{\deg \mathcal{N}(E_{a,\gamma})}{\log \deg \mathcal{N}(E_{a,\gamma})}.$$

From §1.1, we know that $q^a \ll \deg \mathcal{N}(E_{a,\gamma}) \ll q^a$; hence (3.13) shows that $\mathrm{rank}\, E_{a,\gamma}(K)$ attains Brumer's upper bound (up to constants depending on q).

3.4 Angles of the sums $\mathrm{K}_\gamma(v)$

For any $v \in P_q(a)$, we know that $\mathrm{K}_\gamma(v)$ is a real algebraic integer with $|\mathrm{K}_\gamma(v)| \leq 2q^{d_v/2}$ in any complex embedding (see items (i), (iv), (v) in Proposition 2.1). Thus, there exists a unique angle $\boldsymbol{\theta}_\gamma(v) \in [0, \pi]$ such that

$$\mathrm{K}_\gamma(v) = 2q^{d_v/2} \cdot \cos \boldsymbol{\theta}_\gamma(v). \tag{3.14}$$

Note that the individual angles $\boldsymbol{\theta}_\gamma(v)$ depend on a choice of complex embedding $\mathbb{Q}(\zeta_p) \hookrightarrow \mathbb{C}$, but that the set $\{\boldsymbol{\theta}_\gamma(v)\}_{v\in P_q(a)}$ does not.

We can then rewrite the expression of $L^*(E_{a,\gamma},1)$ obtained in Proposition 3.7 in terms of these angles:

$$L^*(E_{a,\gamma},1) = \prod_{v\in P_q(a)} 4\deg v \cdot \prod_{v\in P_q(a)} \sin^2\big(\boldsymbol{\theta}_\gamma(v)\big). \tag{3.15}$$

In section 6, we will prove upper and lower bounds on the size of $L^*(E_{a,\gamma},1)$ in terms of the degree $b(E_{a,\gamma})$ of the L-function. From the above expression, it is obvious that this size crucially depends on how the angles $\{\boldsymbol{\theta}_\gamma(v)\}_{v\in P_q(a)}$ are distributed in $[0,\pi]$ when $a\to\infty$. Therefore, we spend the next two sections describing this distribution in some detail.

4 Small angles of Kloosterman sums

In this section, we work in the following setting. Let $\mathbb{F}$ be a finite field of odd characteristic p, and ψ be a nontrivial additive character on $\mathbb{F}$. We assume that ψ takes values in $\mathbb{Q}(\zeta_p)$ and we pick a complex embedding $\mathbb{Q}(\zeta_p)\hookrightarrow\mathbb{C}$.

For any $\alpha\in\mathbb{F}^\times$ the Kloosterman sum $\mathrm{Kl}_\mathbb{F}(\psi;\alpha)$ is a real algebraic integer with $|\mathrm{Kl}_\mathbb{F}(\psi;\alpha)|\le 2|\mathbb{F}|^{1/2}$ (see Proposition 2.1(i), (iv) and (v)). Thus there is a well-defined angle $\theta_\mathbb{F}(\psi,\alpha)\in[0,\pi]$ associated to the Kloosterman sum by

$$\mathrm{Kl}_\mathbb{F}(\psi;\alpha) := 2|\mathbb{F}|^{1/2}\cdot\cos\theta_\mathbb{F}(\psi;\alpha).$$

Further, as noted in Proposition 2.1(vi), the angle $\theta_\mathbb{F}(\psi;\alpha)$ cannot be 0 or π since $\mathrm{Kl}_\mathbb{F}(\psi;\alpha)$ 'never attains the Weil bound'. In this section, we investigate how close $\theta_\mathbb{F}(\psi;\alpha)$ can be to 0 and π; we prove the following result, which may be of independent interest.

Theorem 4.1 – *There exists an effectively computable constant $c_p>0$ (depending at most on p) such that the following holds: for any finite field $\mathbb{F}$ of characteristic p, any nontrivial additive character ψ on $\mathbb{F}$ and any $\alpha\in\mathbb{F}^\times$, one has*

$$|\theta_\mathbb{F}(\psi;\alpha)| > |\mathbb{F}|^{-c_p} \qquad \text{and} \qquad |\pi-\theta_\mathbb{F}(\psi;\alpha)| > |\mathbb{F}|^{-c_p}.$$

Moreover $c_p=2(p-1)$ is a suitable value of the constant.

Before we start the proof, we recall for convenience the following version of Liouville's inequality:

Theorem 4.2 (Liouville's inequality) – *Let $P\in\mathbb{Z}[X]$ be a polynomial of degree N. For any algebraic number $z\in\overline{\mathbb{Q}}$, let D_z be its degree over $\mathbb{Q}$ and $h(z)$ denote its logarithmic absolute Weil height.*

Either $P(z)=0$ or

$$|P(z)| \ge \|P\|_1^{-D_z+1}\cdot\exp\left(-N\cdot D_z\cdot h(z)\right), \tag{4.1}$$

in any complex embedding of $\mathbb{Q}(z)$, where $\|P\|_1$ is the sum of the absolute values of the coefficients of P.

See the introduction of [MW94] and the proof of Lemma 5 in *loc.cit.* for this version and its proof.

Proof (of Theorem 4.1): We let $\mathbb{F},\psi$ and α be as in the statement of Theorem 4.1; we choose an embedding $\overline{\mathbb{Q}}\hookrightarrow\mathbb{C}$ which is compatible with our choice of $\mathbb{Q}(\zeta_p)\hookrightarrow\mathbb{C}$. By Proposition 2.1(iv), we can write

$$\mathrm{Kl}_\mathbb{F}(\psi;\alpha) = \mathsf{kl}_\mathbb{F}(\psi;\alpha)+\mathsf{kl}'_\mathbb{F}(\psi;\alpha),$$

for two algebraic integers $\mathsf{kl}_\mathbb{F}(\psi;\alpha)$, $\mathsf{kl}'_\mathbb{F}(\psi;\alpha)$ of magnitude $|\mathbb{F}|^{1/2}$ whose product is $|\mathbb{F}|$. In the given complex embedding, $\mathsf{kl}_\mathbb{F}(\psi;\alpha)$ and $\mathsf{kl}'_\mathbb{F}(\psi;\alpha)$ are complex conjugates: one of them thus has nonnegative imaginary part *i.e.*, equals $|\mathbb{F}|^{1/2}\cdot\mathrm{e}^{i\theta_\mathbb{F}(\psi;\alpha)}$ by Proposition 2.1(v). Without loss of generality, we may and do assume that it is $\mathsf{kl}_\mathbb{F}(\psi;\alpha)$. Consider the ratio $z:=\mathsf{kl}_\mathbb{F}(\psi;\alpha)/|\mathbb{F}|^{1/2}=\mathrm{e}^{i\theta_\mathbb{F}(\psi;\alpha)}\in\overline{\mathbb{Q}}$ and write $L:=\mathbb{Q}(z)\subset\overline{\mathbb{Q}}$.

We have

Lemma 4.3 – *z has degree $D_z\le 2(p-1)$ and height $h(z)\le\log\sqrt{|\mathbb{F}|}$. Moreover, $z\neq\pm1$.*

Proof: By Proposition 2.1(i), we have $\mathrm{Kl}_\mathbb{F}(\psi;\alpha)\in\mathbb{Q}(\zeta_p+\zeta_p^{-1})$. Further, Proposition 2.1(iv) implies that $\mathsf{kl}_\mathbb{F}(\psi;\alpha)$ and $\mathsf{kl}'_\mathbb{F}(\psi;\alpha)$ are the roots of $X^2-\mathrm{Kl}_\mathbb{F}(\psi;\alpha)\cdot X+|\mathbb{F}|$; it is then clear that the degree of $\mathsf{kl}_\mathbb{F}(\psi;\alpha)$ over $\mathbb{Q}$ is $\le 2[\mathbb{Q}(\zeta_p+\zeta_p^{-1}):\mathbb{Q}]=p-1$. We thus have

$$D_z=[L:\mathbb{Q}]\le[\mathbb{Q}\big(|\mathbb{F}|^{1/2},\mathsf{kl}_\mathbb{F}(\psi;\alpha)\big):\mathbb{Q}]\le 2[\mathbb{Q}(\zeta_p+\zeta_p^{-1}):\mathbb{Q}]\le 2(p-1),$$

as was to be shown. Since $|\mathsf{kl}_{\mathbb{F}}(\psi;\alpha)| = |\mathbb{F}|^{1/2}$, we infer that $|z| = 1$ in any complex embedding of L, therefore the archimedean places of L do not contribute to $h(z)$. We deduce further that z is a unit at all finite places of L which are not above p; hence these places do not contribute to $h(z)$ either. It remains to consider finite places $\mathfrak{P}$ of L lying above p: since both $\mathsf{kl}_{\mathbb{F}}(\psi;\alpha)$ and $\mathsf{kl}'_{\mathbb{F}}(\psi;\alpha) = |\mathbb{F}|/\mathsf{kl}_{\mathbb{F}}(\psi;\alpha)$ are algebraic integers, the contributions of $\mathfrak{P}$ to $h(z)$ is $\leq \frac{1}{2}\cdot\frac{\mathrm{ord}_{\mathfrak{P}}(|\mathbb{F}|)}{[L:\mathbb{Q}]}$. By summing these, we conclude that $h(z) \leq \frac{1}{2}\log|\mathbb{F}|$.

Finally, Proposition 2.1(vi) shows that $\theta_{\mathbb{F}}(\psi;\alpha) \notin \{0,\pi\}$, and the last assertion easily follows. □

Upon applying Liouville's inequality (4.1) to z with $P = X \pm 1$ and using Lemma 4.3, we obtain that

$$\begin{aligned}\log|z\pm 1| &\geq (-D_z+1)\cdot\log 2 - D_z\cdot h(z) \geq -D_z\cdot\left(\log 2 + \log\sqrt{|\mathbb{F}|}\right)\\ &> -D_z\cdot\log|\mathbb{F}| \geq -2(p-1)\cdot\log|\mathbb{F}|. \end{aligned} \tag{4.2}$$

Noting that the the graph of $t\mapsto|\sin t|$ lies below its tangents at $t=\pi/2$, one sees that $|e^{it}-1|\leq|t|$ for all $t\in[0,\pi]$. From this inequality and the lower bound (4.2) on $|z-1|$, we deduce that

$$|\theta_{\mathbb{F}}(\psi;\alpha)| \geq |e^{i\theta_{\mathbb{F}}(\psi;\alpha)}-1| = |z-1| > |\mathbb{F}|^{-c_p},$$

where $c_p = 2(p-1)$. To get the lower bound on $|\theta_{\mathbb{F}}(\psi;\alpha)-\pi|$, we use the lower bound on $|z+1|$ in (4.2) and the inequality stating that $|e^{it'}+1|\leq|\pi-t'|$ for all $t'\in[0,\pi]$. This concludes the proof of Theorem 4.1. □

Let us deduce two corollaries from Theorem 4.1. The first one can be viewed as a slight improvement on the Weil bound on Kloosterman sums (*i.e.*, an effective version of Proposition 2.1(vi)):

Corollary 4.4 – *For any finite field $\mathbb{F}$ of characteristic $p\geq 3$, any nontrivial additive character ψ on $\mathbb{F}$ and any $\alpha\in\mathbb{F}^\times$, we have*

$$|\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)| \leq 2|\mathbb{F}|^{1/2}\cdot\left(1-\frac{2}{\pi^2}\cdot|\mathbb{F}|^{-2c_p}\right),$$

where c_p is the constant in Theorem 4.1.

Proof: By construction, we have $|\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)| = 2|\mathbb{F}|^{1/2}\cdot|\cos\theta_{\mathbb{F}}(\psi;\alpha)|$. Theorem 4.1 implies that $\theta_{\mathbb{F}}(\psi;\alpha)$ lies in $[Q,\pi-Q]$ with $Q=(q^a)^{-c_p}$. The Corollary follows from the elementary observation that

$$\forall\theta\in[Q,\pi-Q],\quad |\cos\theta| = \sqrt{1-\sin^2\theta} \leq 1-\frac{\sin^2\theta}{2} \leq 1-\frac{2\min\{\theta,\pi-\theta\}^2}{\pi^2} \leq 1-\frac{2Q^2}{\pi^2}.$$ □

The second corollary is more central to our study of the size of $L^*(E_{a,\gamma},1)$, *cf.* §6.1.

Corollary 4.5 – *Let $\mathbb{F}_q$ be a finite field of characteristic $p\geq 3$ equipped with a nontrivial additive character ψ_q. For any $\gamma\in\mathbb{F}_q^\times$ and any integer $a\geq 1$, the angles $\boldsymbol{\theta}_\gamma(v)$ for $v\in P_q(a)$ defined in §3.4 satisfy*

$$(q^a)^{-c_p} \leq \boldsymbol{\theta}_\gamma(v) \leq \pi - (q^a)^{-c_p}, \tag{4.3}$$

where c_p is the constant in Theorem 4.1 above.

Proof: For all $v\in P_q(a)$, the residue field $\mathbb{F}_v$ is a subfield of $\mathbb{F}_{q^a}$ and we may choose β_v as in §2.2. Upon noting that $|\mathbb{F}_v|\leq q^a$, the Corollary immediately follows from Theorem 4.1 applied to $\mathbb{F}=\mathbb{F}_v$, $\psi=\psi_q\circ\mathrm{tr}_{\mathbb{F}_v/\mathbb{F}_q}$ and $\alpha=\gamma\beta_v^2$. □

5 Distribution of the sums $\mathcal{K}_\gamma(v)$

In this section, we fix again a finite field $\mathbb{F}_q$ of odd characteristic p, an element $\gamma\in\mathbb{F}_q^\times$ and a nontrivial additive character ψ_q on $\mathbb{F}_q$ with values in $\mathbb{Q}(\zeta_p)$. For any finite extension $\mathbb{F}/\mathbb{F}_q$, we continue denoting by $\psi_{\mathbb{F}}$ the composition $\psi_q\circ\mathrm{tr}_{\mathbb{F}/\mathbb{F}_q}$ of ψ_q with the trace $\mathrm{tr}_{\mathbb{F}/\mathbb{F}_q}:\mathbb{F}\to\mathbb{F}_q$.

Loosely speaking, we show that, asymptotically as $a\to\infty$, the numbers $q^{-d_v/2}\cdot\mathcal{K}_\gamma(v)$ with $v\in P_q(a)$ (see §2.2) are distributed in $[-2,2]$ as 'the traces of random matrices in $\mathrm{SU}(2,\mathbb{C})$'. In order to make this statement more precise and to prove it, we begin by introducing the necessary notations and notions.

Choose a prime number $\ell\neq p$, an algebraic closure $\overline{\mathbb{Q}_\ell}$ of $\mathbb{Q}_\ell$, an embedding $\overline{\mathbb{Q}}\hookrightarrow\overline{\mathbb{Q}_\ell}$, and a field isomorphism $\overline{\mathbb{Q}_\ell}\simeq\mathbb{C}$. Through this isomorphism, we view ψ_q as a $\overline{\mathbb{Q}_\ell}$-valued additive character on $\mathbb{F}_q$.

We fix a separable closure K^{sep} of K. The set of places $v\neq 0,\infty$ of K can be identified with the set of closed points of the multiplicative group $\mathbb{G}_m=\mathbb{P}^1\smallsetminus\{0,\infty\}$ over $\mathbb{F}_q$. For a finite extension $\mathbb{F}/\mathbb{F}_q$ and a point $\alpha\in\mathbb{G}_m(\mathbb{F})$, we denote by $\mathrm{Fr}_{\mathbb{F},\alpha}$ the geometric Frobenius of $\mathbb{G}_m$ at α, which we view as a conjugacy class in the profinite group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. For any closed point v of $\mathbb{G}_m$, we choose $\beta_v\in v$ and we let $\mathrm{Fr}_v := \mathrm{Fr}_{\mathbb{F}_v,\beta_v}$.

5.1 Angles of Kloosterman sums

Let us start by redefining the angles $\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha)$ from a representation-theoretic point of view. The reader is referred to [Kat88, Chapter 3] or [Fis95] for more detailed presentations.

In Chapter 4 of [Kat88], Katz has constructed a lisse $\overline{\mathbb{Q}_\ell}$-sheaf $\mathcal{K}l^\circ$ on $\mathbb{G}_m$ whose Frobenius traces are Kloosterman sums ($\mathcal{K}l^\circ$ is the so-called *Kloosterman sheaf*). Taking a suitable Tate twist, one obtains a lisse $\overline{\mathbb{Q}_\ell}$-sheaf $\mathcal{K}l = \mathcal{K}l^\circ(1/2)$ of rank 2 on $\mathbb{G}_m$ which is pure of weight 0.

By definition, $\mathcal{K}l$ 'is' a continuous 2-dimensional $\overline{\mathbb{Q}_\ell}$-representation $\kappa : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{GL}(2,\overline{\mathbb{Q}_\ell})$ which is unramified outside $\{0,\infty\}$ and which satisfies the following. For all places $v \neq 0,\infty$ of K, the eigenvalues of $\kappa(\mathrm{Fr}_v)$ have magnitude[4] 1 ('pure of weight 0') and the trace of $\kappa(\mathrm{Fr}_v)$ is:

$$\mathrm{Trace}\left(\kappa(\mathrm{Fr}_v)\right) = |\mathbb{F}_v|^{-1/2} \cdot \mathrm{Kl}_{\mathbb{F}_v}(\psi_{\mathbb{F}_v};\beta_v),$$

where $\beta_v \in \mathbb{G}_m(\overline{\mathbb{F}_q})$ is a choice of element in the closed point of $\mathbb{G}_m$ corresponding to v, as in §2.2. Note that, even though Fr_v is only defined up to conjugation in $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, its $\mathrm{Trace}\left(\kappa(\mathrm{Fr}_v)\right)$ is well-defined.

Katz has shown that the image of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ under κ is contained in $\mathrm{SL}(2,\overline{\mathbb{Q}_\ell})$ (in other words, the representation κ has trivial determinant, see [Kat88, Chap. 11]). *Via* the chosen isomorphism $\overline{\mathbb{Q}_\ell} \simeq \mathbb{C}$, we may view $\kappa(\mathrm{Gal}(K^{\mathrm{sep}}/K))$ as a subgroup of $\mathrm{SL}(2,\mathbb{C})$. The special unitary group $H := \mathrm{SU}(2,\mathbb{C})$ is a maximal compact subgroup of $\mathrm{SL}(2,\mathbb{C})$ and, since $\mathrm{SL}(2,\mathbb{C})$ is semisimple, such a H is uniquely determined up to conjugation. For any place $v \neq 0,\infty$, let $\kappa(\mathrm{Fr}_v)^{\mathrm{s.s.}}$ be the semisimplification of $\kappa(\mathrm{Fr}_v)$: the closure of the subgroup of $\mathrm{SL}(2,\mathbb{C})$ generated by all the $\kappa(\mathrm{Fr}_v)^{\mathrm{s.s.}}$ is compact and thus, up to conjugation in $\mathrm{SL}(2,\mathbb{C})$, lies in H.

We denote by $H^\natural$ the set of conjugacy classes of H and we equip $H^\natural$ with the measure $\mu^\natural$ obtained as the direct image of the Haar measure on H normalised to have total mass 1. The trace of $M \in H$ (or of any element in its conjugacy class) is the sum of two conjugate complex number of magnitude 1, so it is a real number in $[-2,2]$. More precisely, a matrix $M \in H$ is conjugate (in H) to a diagonal matrix $\mathrm{Diag}(\mathrm{e}^{i\theta_M},\mathrm{e}^{-i\theta_M})$ for some unique $\theta_M \in [0,\pi]$ and $\mathrm{Trace}\, M = 2\cos\theta_M$. Hence, the set $H^\natural$ endowed with $\mu^\natural$ can be identified with the interval $[0,\pi]$ endowed with the Sato–Tate measure $\mu_{\mathrm{ST}} := \frac{2}{\pi}\sin^2\theta\,\mathrm{d}\theta$ (see [Kat88, Chap. 13]). We identify any angle $\theta \in [0,\pi]$ with the conjugacy class of $\mathrm{Diag}(\mathrm{e}^{i\theta},\mathrm{e}^{-i\theta}) \in H^\natural$, which we also denote by the same symbol θ.

We are now ready to (re)define angles of Kloosterman sums. For any finite extension $\mathbb{F}/\mathbb{F}_q$ and any $\alpha \in \mathbb{G}_m(\mathbb{F})$, the semisimplification of $\kappa(\mathrm{Fr}_{\mathbb{F},\alpha}) \in \mathrm{SL}(2,\mathbb{C})$ is $\mathrm{SL}(2,\mathbb{C})$-conjugate to an element of H, and we can define $\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha) \in H^\natural$ to be the conjugacy class in H of this element. In the identification between $H^\natural$ and $[0,\pi]$, this gives us a well-defined angle $\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha) \in [0,\pi]$, see [Kat88, §3.3].

For any finite extension $\mathbb{F}/\mathbb{F}_q$ and any $\alpha \in \mathbb{G}_m(\mathbb{F})$, we thus have

$$2\cdot\cos\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha) = \mathrm{Trace}\left(\kappa(\mathrm{Fr}_{\mathbb{F},\alpha})^{\mathrm{s.s.}}\right) = \mathrm{Trace}\left(\kappa(\mathrm{Fr}_{\mathbb{F},\alpha})\right) = |\mathbb{F}|^{-1/2}\cdot\mathrm{Kl}_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha),$$

so that the new definition of $\cos\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha)$ coincides with the one given at the beginning of section 4.

Definition 5.1 Fix a finite field $\mathbb{F}_q$ equipped with a nontrivial additive character ψ_q and $\gamma \in \mathbb{F}_q^\times$. For any place $v \neq 0,\infty$ of K, let $\boldsymbol{\theta}_\gamma(v)$ be the angle associated to the Kloosterman sum $\mathrm{K}_\gamma(v) = \mathrm{Kl}_{\mathbb{F}_v}(\psi_{\mathbb{F}_v};\gamma\beta_v^2)$ by the construction above. In other words, we put $\boldsymbol{\theta}_\gamma(v) := \theta_{\mathbb{F}_v}(\psi_{\mathbb{F}_v};\gamma\beta_v^2) \in \mathrm{SU}(2,\mathbb{C})^\natural$.

Remark 5.2 Let $\mathbb{F}$ be the finite extension of $\mathbb{F}_q$ with $[\mathbb{F}:\mathbb{F}_q] = a$. For an element $\alpha \in \mathbb{G}_m(\mathbb{F})$, let w be the closed point of $\mathbb{G}_m$ corresponding to α (*i.e.*, w is the $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbit of α). The residue field $\mathbb{F}_w$ is then a subfield of $\mathbb{F}$ and $\mathrm{Fr}_{\mathbb{F},\alpha} = (\mathrm{Fr}_w)^{[\mathbb{F}:\mathbb{F}_w]}$ as conjugacy classes in $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. Therefore $\kappa(\mathrm{Fr}_{\mathbb{F},\alpha}) = \kappa(\mathrm{Fr}_w)^{[\mathbb{F}:\mathbb{F}_w]}$ and

$$\tfrac{a}{\deg w}\cdot\theta_{\mathbb{F}_w}(\psi_{\mathbb{F}_w};\alpha) = [\mathbb{F}:\mathbb{F}_w]\cdot\theta_{\mathbb{F}_w}(\psi_{\mathbb{F}_w};\alpha) \equiv \theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha) \bmod \pi.$$

In particular, when v is a closed point of $\mathbb{G}_m$ whose degree divides a and when $\beta_v \in v$, by our definition $\boldsymbol{\theta}_\gamma(v) = \theta_{\mathbb{F}_v}(\psi_{\mathbb{F}_v};\gamma\beta_v^2)$, the above relation reads

$$\tfrac{a}{\deg v}\cdot\boldsymbol{\theta}_\gamma(v) \equiv \theta_{\mathbb{F}}(\psi_{\mathbb{F}};\gamma\beta_v^2) \bmod \pi.$$

5.2 Statement of results

Denote by μ_{ST} the Sato–Tate measure $\frac{2}{\pi}\sin^2\theta\,\mathrm{d}\theta$ on $[0,\pi]$. A sequence of Borel measures $\{\mu_i\}_{i\geq 1}$ on $[0,\pi]$ is said to *converge weak-* to* μ_{ST} if, for every continuous $\mathbb{C}$-valued function f on $[0,\pi]$, the sequence of integrals $\int_{[0,\pi]} f\,\mathrm{d}\mu_i$ converges to $\int_{[0,\pi]} f\,\mathrm{d}\mu_{\mathrm{ST}}$ as $i\to\infty$.

[4] Here we view $\kappa(\mathrm{Fr}_v) \in \overline{\mathbb{Q}_\ell}$ as an element of $\mathbb{C}$ by means of the chosen isomorphism $\overline{\mathbb{Q}_\ell} \simeq \mathbb{C}$

Our results concern two sequences of probability measures that we now introduce.

Definition 5.3 We fix a finite field $\mathbb{F}_q$ of characteristic $p \geq 3$, a nontrivial additive character ψ_q on $\mathbb{F}_q$ and $\gamma \in \mathbb{F}_q^\times$. For an integer $a \geq 1$, we again denote by $P_q(a)$ the set of closed points of $\mathbb{G}_m$ whose degrees divide a. For all integers $a \geq 1$, we define

$$\nu(\mathbb{F}_q, \psi_q, \gamma; a) := \frac{1}{|P_q(a)|} \cdot \sum_{v \in P_q(a)} \delta\{\boldsymbol{\theta}_\gamma(v)\},$$

where $\delta\{x\}$ denotes the Dirac delta measure at $x \in [0, \pi]$. For all finite extensions $\mathbb{F}/\mathbb{F}_q$, we also define

$$\xi(\mathbb{F}_q, \psi_q, \gamma; \mathbb{F}) := \frac{1}{|\mathbb{G}_m(\mathbb{F})|} \cdot \sum_{\beta \in \mathbb{G}_m(\mathbb{F})} \delta\big\{\theta_{\mathbb{F}}(\psi_{\mathbb{F}}; \gamma\beta^2)\big\}.$$

In what follows, we abbreviate $\nu(\mathbb{F}_q, \psi_q, \gamma; a)$ by ν_a and $\xi(\mathbb{F}_q, \psi_q, \gamma; \mathbb{F}_{q^a})$ by ξ_a.

Clearly, both ν_a and ξ_a are Borel measures on $[0, \pi]$ with total mass 1. It follows from the discussion in §5.1 that we may view ν_a and ξ_a as measures on $H^\natural$; we use both points of view interchangeably. Moreover, we note that ξ_a is also given by[5]

$$\xi_a = \xi(\mathbb{F}_q, \psi_q, \gamma; \mathbb{F}_{q^a}) = \frac{1}{|\mathbb{G}_m(\mathbb{F}_{q^a})|} \cdot \sum_{v \in P_q(a)} \deg v \cdot \delta\big\{\tfrac{a}{\deg v} \cdot \boldsymbol{\theta}_\gamma(v)\big\}, \tag{5.1}$$

where $\frac{a}{\deg v} \cdot \boldsymbol{\theta}_\gamma(v)$ is to be understood modulo π (see Remark 5.2).

Remark 5.4 In terms of the measure ν_a, Corollary 4.5 can be reinterpreted as follows: given $\mathbb{F}_q$, ψ_q and γ as above, for any $a \geq 1$ the support of the probability measure ν_a on $[0, \pi]$ is contained in $[(q^a)^{-c_p}, \pi - (q^a)^{-c_p}]$.

We can now state the two main results of this section. First we show that the angles $\{\boldsymbol{\theta}_\gamma(v)\}_{v \in P_q(a)}$ are asymptotically equidistributed with respect to the Sato–Tate measure as $a \to \infty$. Namely,

Theorem 5.5 – *Assume we are given a datum $\mathbb{F}_q, \psi_q, \gamma$ as above. Then the sequences $\{\xi_a\}_{a \geq 1}$ and $\{\nu_a\}_{a \geq 1}$ of Borel probability measures both converge weak-$*$ to the Sato–Tate measure μ_{ST} when $a \to \infty$.*

This statement concretely means that, for all continuous functions f on $[0, \pi]$, we have

$$\frac{1}{|P_q(a)|} \cdot \sum_{v \in P_q(a)} f\big(\boldsymbol{\theta}_\gamma(v)\big) = \int_{[0,\pi]} f \, \mathrm{d}\nu_a \xrightarrow[a \to \infty]{} \int_{[0,\pi]} f \, \mathrm{d}\mu_{\mathrm{ST}} = \frac{2}{\pi} \int_0^\pi f(t) \sin^2(t) \, \mathrm{d}t. \tag{5.2}$$

It will be proven in Propositions 5.7 and 5.9 by a suitable adaptation of the arguments in [Kat88, Chap.3] and [FL05, §2].

In the course of proving Theorem 6.3, we will need a more effective version of (5.2): indeed, we require an estimate of the rate at which $\int_{[0,\pi]} f \, \mathrm{d}\nu_a$ converges to $\int_{[0,\pi]} f \, \mathrm{d}\mu_{\mathrm{ST}}$, at least for a smaller class of functions f. This is the object of the second result in this section:

Theorem 5.6 – *Assume we are given a datum $\mathbb{F}_q, \psi_q, \gamma$ as above. For any continuously differentiable function g on $[0, \pi]$, we have*

$$\left| \int_{[0,\pi]} g \, \mathrm{d}\nu_a - \int_{[0,\pi]} g \, \mathrm{d}\mu_{\mathrm{ST}} \right| \ll_q \frac{a^{1/2}}{q^{a/4}} \cdot \int_0^\pi |g'(t)| \, \mathrm{d}t \qquad (\textit{as } a \to \infty). \tag{5.3}$$

This will follow from the proof of Theorem 5.5 coupled with tools from distribution theory (see [Nie91]).

The proofs will also show that the constants in Theorems 5.5 and 5.6 are effective and depend at most on q (and neither on the choice of ψ_q nor on the value of $\gamma \in \mathbb{F}_q^\times$).

5.3 Equidistribution of $\boldsymbol{\theta}_\gamma(v)$'s

In this subsection, we prove Theorem 5.5 in two steps (Propositions 5.7 and 5.9). Let us first make a reduction (see [Kat88, §3.4, §3.5] for more details). We need to show that, for all complex-valued continuous functions f on $[0, \pi]$, we have

$$\int_{[0,\pi]} f \, \mathrm{d}\xi_a, \quad \int_{[0,\pi]} f \, \mathrm{d}\nu_a \xrightarrow[a \to \infty]{} \int_{[0,\pi]} f \, \mathrm{d}\mu_{\mathrm{ST}}.$$

[5] The measure ξ_a is the measure denoted by X_a in [Kat88, §3.5] applied to our situation.

Since $H = \mathrm{SU}(2,\mathbb{C})$ is compact and since $[0,\pi]$ can be identified with $H^\natural$, there is a natural correspondence between the space of continuous functions on $[0,\pi]$ and the space $\mathscr{C}^0_{cent}(H)$ of continuous central functions on H. When $\mathscr{C}^0_{cent}(H)$ is endowed with the topology of the supremum norm, the Peter–Weyl theorem asserts that the vector subspace generated by characters of irreducible finite-dimensional representations of H is dense in $\mathscr{C}^0_{cent}(H)$. By density, Theorem 5.5 will follow if we can show that, for all irreducible finite-dimensional representations Λ of H,

$$\int_{H^\natural} \mathrm{Trace}\,\Lambda\,\mathrm{d}\xi_a, \quad \int_{H^\natural} \mathrm{Trace}\,\Lambda\,\mathrm{d}\nu_a \xrightarrow[a\to\infty]{} \int_{H^\natural} \mathrm{Trace}\,\Lambda\,\mathrm{d}\mu^\natural.$$

If Λ_0 is trivial, $\mathrm{Trace}\,\Lambda_0$ is the trivial character $\mathbf{1}$ on H and the above limits clearly hold because the measures ν_a, ξ_a and $\mu^\natural$ on $H^\natural$ all have total mass 1. Now, when Λ is a nontrivial irreducible finite-dimensional representation of H, the integral $\int_{H^\natural} \mathrm{Trace}\,\Lambda\,\mathrm{d}\mu^\natural$ on the right-hand side vanishes by orthogonality of characters. Hence, the proof of Theorem 5.5 reduces to that of the following statement[6]: *for any nontrivial irreducible finite-dimensional representation Λ of $H = \mathrm{SU}(2,\mathbb{C})$, one has*

$$\int_{H^\natural} \mathrm{Trace}\,\Lambda\,\mathrm{d}\xi_a, \quad \int_{H^\natural} \mathrm{Trace}\,\Lambda\,\mathrm{d}\nu_a \xrightarrow[a\to\infty]{} 0.$$

We actually prove slightly more precise estimates.

Proposition 5.7 – *Fix $\mathbb{F}_q, \psi_q$ and $\gamma \in \mathbb{F}_q^\times$ as in §5.2. Let Λ be a nontrivial irreducible representation of $H = \mathrm{SU}(2,\mathbb{C})$. For all $a \geq 1$, one has*

$$\left| \int_{H^\natural} \mathrm{Trace}\,\Lambda\,\mathrm{d}\xi_a \right| \ll_q \frac{\dim \Lambda}{q^{a/2}}. \tag{5.4}$$

Proof: For any finite extension $\mathbb{F}/\mathbb{F}_q$, notice that

$$\begin{aligned}\sum_{\beta\in\mathbb{F}^\times} \mathrm{Trace}\,\Lambda\big(\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\gamma\beta^2)\big) &= \sum_{\alpha'\in\mathbb{F}^\times} (1+\lambda_{\mathbb{F}}(\alpha'))\cdot \mathrm{Trace}\,\Lambda\big(\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\gamma\alpha')\big)\\ &= \sum_{\alpha\in\mathbb{F}^\times} \mathrm{Trace}\,\Lambda\big(\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha)\big) + \lambda_{\mathbb{F}}(\gamma^{-1})\cdot \sum_{\alpha\in\mathbb{F}^\times} \lambda_{\mathbb{F}}(\alpha)\cdot \mathrm{Trace}\,\Lambda\big(\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha)\big),\end{aligned}$$

where $\lambda_{\mathbb{F}}$ denotes the unique nontrivial character of order 2 on $\mathbb{F}^\times$. Therefore, one has

$$\left|\sum_{\beta\in\mathbb{F}^\times} \mathrm{Trace}\,\Lambda\big(\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\gamma\beta^2)\big)\right| \leq \left|\sum_{\alpha\in\mathbb{F}^\times} \mathrm{Trace}\,\Lambda\big(\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha)\big)\right| + \left|\sum_{\alpha\in\mathbb{F}^\times} \lambda_{\mathbb{F}}(\alpha)\cdot \mathrm{Trace}\,\Lambda\big(\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha)\big)\right|. \tag{5.5}$$

For any multiplicative character χ on $\mathbb{F}_q^\times$ and any finite extension $\mathbb{F}/\mathbb{F}_q$, we denote by $\chi_{\mathbb{F}} := \chi\circ \mathbf{N}_{\mathbb{F}/\mathbb{F}_q}$ the character on $\mathbb{F}^\times$ 'lifted' by the norm $\mathbf{N}_{\mathbb{F}/\mathbb{F}_q} : \mathbb{F}\to\mathbb{F}_q$. The crucial input is a result of Fu and Liu (see Lemma 4 in [FL05]) who have proved that, for every multiplicative character χ on $\mathbb{F}_q$, one has

$$\left|\sum_{\alpha\in\mathbb{G}_m(\mathbb{F})} \chi_{\mathbb{F}}(\alpha)\cdot \mathrm{Trace}\,\Lambda\big(\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\alpha)\big)\right| \leq \frac{\dim\Lambda}{2}\cdot |\mathbb{F}|^{1/2}.$$

Applying this inequality successively to both multiplicative characters on $\mathbb{F}_q$ whose order divides 2, we deduce from (5.5) that

$$\left|\sum_{\beta\in\mathbb{F}^\times} \mathrm{Trace}\,\Lambda\big(\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\gamma\beta^2)\big)\right| \leq (\dim\Lambda)\cdot |\mathbb{F}|^{1/2}.$$

Therefore, for any finite extension $\mathbb{F}/\mathbb{F}_q$, we have proved that

$$\left|\int_{H^\natural} \mathrm{Trace}\,\Lambda\,\mathrm{d}\xi(\mathbb{F}_q,\psi_q,\gamma;\mathbb{F})\right| = \left|\frac{1}{|\mathbb{G}_m(\mathbb{F})|}\sum_{\beta\in\mathbb{F}^\times} \mathrm{Trace}\,\Lambda\big(\theta_{\mathbb{F}}(\psi_{\mathbb{F}};\gamma\beta^2)\big)\right| \ll_q \dim\Lambda\cdot|\mathbb{F}|^{-1/2}.$$

Specialising to $\mathbb{F} = \mathbb{F}_{q^a}$ yields the desired estimate since $\xi_a = \xi(\mathbb{F}_q,\psi_q,\gamma;\mathbb{F}_{q^a})$. □

[6] This is the analogue in the Sato–Tate context of Weyl's criterion for uniform distribution (see [KN06, Chap. 4, §1]).

Remark 5.8 Let us suggest an alternative way of proving Proposition 5.7. Denote again by $\mathcal{K}l$ the Kloosterman sheaf (suitably twisted to be pure of weight 0) whose existence was proved by Katz. For a given $\gamma \in \mathbb{F}_q^\times$, consider the morphism $f : \mathbb{G}_m \to \mathbb{G}_m$ given by $\beta \mapsto \gamma\beta^2$, and put $\mathcal{G}_\gamma := f^*\mathcal{K}l$. Then $\mathcal{G}_\gamma$ is again a lisse $\overline{\mathbb{Q}_\ell}$-sheaf of rank 2 on $\mathbb{G}_m$ which is pure of weight 0. Moreover, for all places $v \neq 0, \infty$ of K, one has

$$\mathrm{Trace}\big(\mathcal{G}_\gamma(\mathrm{Fr}_v)\big) = |\mathbb{F}_v|^{-1/2} \cdot \mathrm{Kl}_{\mathbb{F}_v}(\psi_{\mathbb{F}_v}; \gamma\beta_v^2) = |\mathbb{F}_v|^{-1/2} \cdot \mathrm{K}_\gamma(v).$$

In the case where $\gamma = 1$, Remark 1 in [FL05] sketches a proof that $\mathcal{G}_\gamma$ satisfies the assumptions of §3.1-§3.3 in [Kat88]. One could therefore prove Proposition 5.7 by making use of [Kat88, §3.6].

This argument should carry over, *mutatis mutandis*, to the case of an arbitrary $\gamma \neq 0$.

To complete the proof of Theorem 5.5, it remains to show that $\{\nu_a\}_{a\geq 1}$ also converges (weak-$*$) to μ_{ST}.

Proposition 5.9 – *Fix a datum $\mathbb{F}_q, \psi_q$ and $\gamma \in \mathbb{F}_q^\times$ as in §5.2. Let Λ be a nontrivial irreducible representation of $H = \mathrm{SU}(2,\mathbb{C})$. For all $a \geq 1$, one has*

$$\left|\int_{H^\natural} \mathrm{Trace}\,\Lambda \,\mathrm{d}\nu_a\right| \ll_q \dim\Lambda \cdot \frac{a}{q^{a/2}}. \tag{5.6}$$

Proof: Consider the measure $\omega_a := |\mathbb{G}_m(\mathbb{F}_{q^a})| \cdot \xi_a - a|P_q(a)| \cdot \nu_a$ on $H^\natural$ (or $[0,\pi]$). By (5.1), we have

$$\omega_a = \sum_{\substack{v\in P_q(a)\\ \deg v<a}} \Big(\deg v \cdot \delta\big\{\tfrac{a}{\deg v}\boldsymbol{\theta}_\gamma(v)\big\} - a\cdot\delta\{\boldsymbol{\theta}_\gamma(v)\}\Big) = \sum_{\substack{b|a\\ b<a}} \sum_{\substack{v \text{ s.t.}\\ \deg v=b}} \big(b\cdot\delta\big\{\tfrac{a}{b}\boldsymbol{\theta}_\gamma(v)\big\} - a\cdot\delta\{\boldsymbol{\theta}_\gamma(v)\}\big)\,.$$

Let $N_a := \sum_{b|a,\, b<a} \pi_q(b)\cdot(b+a)$, where $\pi_q(b)$ denotes the number of places $v \neq 0,\infty$ of K with $\deg v = b$. As is clear from the right-most expression above, ω_a is a sum of N_a Dirac delta measures supported at points of $H^\natural$. By straightforward estimates using the 'Prime Number Theorem' for $\mathbb{F}_q[t]$ (see Lemma 2.5), one can show that

$$N_a = \sum_{\substack{b|a\\ b<a}} \pi_q(b)\cdot(b+a) \leq 2a\cdot\sum_{\substack{b|a\\ b<a}}\pi_q(b) \ll_q a\cdot\sum_{1\leq b\leq a/2} q^b \ll_q a\cdot q^{a/2}.$$

Since, for any $z \in K$, the eigenvalues of $\Lambda(z)$ all have magnitude 1, we have $|\mathrm{Trace}\,\Lambda(z)| \leq \dim\Lambda$. Hence we find that

$$\left|\int_{H^\natural} \mathrm{Trace}\,\Lambda\,\mathrm{d}\omega_a\right| \leq N_a\cdot\dim\Lambda \ll_q \dim\Lambda\cdot a\cdot q^{a/2} \tag{5.7}$$

Now we notice that

$$\nu_a = \frac{|\mathbb{G}_m(\mathbb{F}_{q^a})|}{a|P_q(a)|}\cdot\xi_a + \frac{1}{a|P_q(a)|}\cdot\omega_a,$$

where $a|P_q(a)| \gg_q q^a$ and $|\mathbb{G}_m(\mathbb{F}_{q^a})| \ll_q a|P_q(a)|$, again by Lemma 2.5. Therefore, combining (5.4) in the previous Proposition and inequality (5.7), we deduce that

$$\begin{aligned}\left|\int_{H^\natural}\mathrm{Trace}\,\Lambda\,\mathrm{d}\nu_a\right| &\leq \frac{|\mathbb{G}_m(\mathbb{F}_{q^a})|}{a|P_q(a)|}\cdot\left|\int_{H^\natural}\mathrm{Trace}\,\Lambda\,\mathrm{d}\xi_a\right| + \frac{1}{a|P_q(a)|}\left|\int_{H^\natural}\mathrm{Trace}\,\Lambda\,\mathrm{d}\omega_a\right|\\ &\ll_q \dim\Lambda\cdot\left(q^{-a/2} + \frac{a\cdot q^{a/2}}{q^a}\right) \ll_q \dim\Lambda\cdot\frac{a}{q^{a/2}}.\end{aligned}$$

This concludes the proof of the Proposition and, by the discussion at the beginning of this subsection, that of Theorem 5.5. □

5.4 Effectivity of the equidistribution

The nontrivial irreducible representations of $H = \mathrm{SU}(2,\mathbb{C})$ are exactly the symmetric powers $\mathrm{Symm}^n(\mathrm{std})$ of the standard representation $\mathrm{std} : H \hookrightarrow \mathrm{GL}(2,\mathbb{C})$. Moreover, if $\Lambda_n = \mathrm{Symm}^n(\mathrm{std})$ for some $n \geq 1$, then Λ_n has dimension $n+1$ and the trace function $\mathrm{Trace}\,\Lambda_n : H^\natural \to \mathbb{R}$ corresponds to the map[7] $\theta \mapsto \sin\big((n+1)\theta\big)/\sin\theta$ in the identification of $H^\natural$ with $[0,\pi]$.

It is convenient to denote by $\mathscr{M}_n(a)$, the 'nth moment' of $\{\boldsymbol{\theta}_\gamma(v)\}_{v\in P_q(a)}$ *i.e.*,

$$\mathscr{M}_n(a) := \int_{H^\natural}\mathrm{Trace}\,\Lambda_n\,\mathrm{d}\nu_a = \frac{1}{|P_q(a)|}\cdot\sum_{v\in P_q(a)}\frac{\sin\big((n+1)\boldsymbol{\theta}_\gamma(v)\big)}{\sin\boldsymbol{\theta}_\gamma(v)}. \tag{5.8}$$

With this notation, the result of Proposition 5.9 can be rewritten as follows. Given a datum $\mathbb{F}_q, \psi_q, \gamma \in \mathbb{F}_q^\times$ as in §5.2 and an integer $n \geq 1$, one has

$$\forall a \geq 1, \qquad |\mathscr{M}_n(a)| \ll_q (n+1)\cdot a q^{-a/2}. \tag{5.9}$$

[7] so that $\mathrm{Trace}\,\Lambda_n(\theta) = U_n(\cos\theta)$, where U_n is the nth Chebyshev polynomial of the second kind.

To measure 'how far' from being perfectly equidistributed with respect to the Sato–Tate distribution the angles $\boldsymbol{\theta}_\gamma(v)$ are, it is customary to introduce the *star discrepancy* $\mathcal{D}^*_{q,\gamma}(a)$:

$$\mathcal{D}^*_{q,\gamma}(a) := \sup_x \left| \int_{[0,x)} \mathrm{d}\nu_a - \int_{[0,x)} \mathrm{d}\mu_{\mathrm{ST}} \right| = \sup_x \left| \frac{|\{v \in P_q(a) : \boldsymbol{\theta}_\gamma(v) \in [0,x)\}|}{|P_q(a)|} - \int_{[0,x)} \mathrm{d}\mu_{\mathrm{ST}} \right|,$$

where the supremums are taken over $x \in [0,\pi]$. This definition is the direct analogue of the star discrepancy for the uniform measure (see [KN06, Chap.2, §1]) in the context of μ_{ST}. The interest of finding good upper bounds on $\mathcal{D}^*_{q,\gamma}(a)$ is exemplified by the following result, which is similar to Koksma's inequality (see Theorem 5.1 in [KN06, Chap.2]).

Theorem 5.10 (Niederreiter) – *For any function $g : [0,\pi] \to \mathbb{R}$ of total bounded variation $\mathscr{V}(g)$, one has*

$$\left| \int_{[0,\pi]} g \,\mathrm{d}\nu_a - \int_{[0,\pi]} g \,\mathrm{d}\mu_{\mathrm{ST}} \right| \leq \mathcal{D}^*_{q,\gamma}(a) \cdot \mathscr{V}(g). \tag{5.10}$$

This statement is essentially[8] Corollary 2 in [Nie91], the proof of which is based on an adaptation to the Sato–Tate context of the proof of Koksma's inequality for the uniform measure (see [KN06, p. 143]).

Note that, for a continuously differentiable function g, one has $\mathscr{V}(g) = \int_0^\pi |g'(t)|\,\mathrm{d}t$. Therefore, Theorem 5.6 follows directly from Theorem 5.10 and the following:

Proposition 5.11 – *The star discrepancy of $\{\boldsymbol{\theta}_\gamma(v)\}_{v \in P_q(a)}$ is bounded by*

$$\mathcal{D}^*_{q,\gamma}(a) \ll_q \frac{a^{1/2}}{q^{a/4}}.$$

Proof: Niederreiter has proved in [Nie91] a variant of the 'Erdös–Turán inequality' in the Sato–Tate context. Just as the Erdös–Turán theorem (see [KN06, Chap.2, Thm. 2.5]), his result gives an upper bound on $\mathcal{D}^*_{q,\gamma}(a)$ in terms of 'exponential sums', here the moments $\mathscr{M}_n(a)$ defined in (5.8). Let us state Lemma 3 in [Nie91] as follows[9]: for any odd positive integer N, we have

$$\mathcal{D}^*_{q,\gamma}(a) \ll \frac{1}{N} + \sum_{n=1}^{2N-1} \frac{n+1}{n(n+2)} \cdot |\mathscr{M}_n(a)|, \tag{5.11}$$

As was noted in (5.9), Proposition 5.9 reads: $|\mathscr{M}_n(a)| \ll_q (n+1) \cdot a q^{-a/2}$. Also remark that

$$\sum_{n=1}^{2N-1} \frac{(n+1)^2}{n(n+2)} \leq 2N - 1 + \sum_{n=1}^{\infty} \frac{1}{n^2+2n} = 2N - 1 + 3/4 \ll N.$$

Hence, for all odd $N \geq 1$, (5.11) leads to $\mathcal{D}^*_{q,\gamma}(a) \ll_q N^{-1} + a q^{-a/2} \cdot N$. Choosing N to be the largest odd integer smaller than $(a^{-1} q^{a/2})^{1/2}$, we have $N^{-1} \ll a^{1/2} q^{-a/4}$ and we obtain the desired bound. □

6 Bounds on the special value

By definition (1.3), the special value $L^*(E_{a,\gamma}, 1)$ is the value at $T = q^{-1}$ of a polynomial with integral coefficients of degree $\leq b(E_{a,\gamma})$. Therefore, $L^*(E_{a,\gamma}, 1)$ is of the form $n/q^{b(E_{a,\gamma})}$ for some integer $n \geq 1$, and we deduce the following 'trivial' lower bound on $L^*(E_{a,\gamma}, 1)$:

$$\frac{\log L^*(E_{a,\gamma}, 1)}{\log\left(q^{b(E_{a,\gamma})}\right)} = \frac{\log n}{\log\left(q^{b(E_{a,\gamma})}\right)} - 1 \geq -1. \tag{6.1}$$

On the other hand, using techniques from classical complex analysis, Hindry and Pacheco show the following upper bound on $L^*(E_{a,\gamma}, 1)$ (see Theorem 7.5 in [HP16]):

$$\frac{\log L^*(E_{a,\gamma}, 1)}{\log\left(q^{b(E_{a,\gamma})}\right)} \ll_q \frac{\log\log b(E_{a,\gamma})}{\log b(E_{a,\gamma})}.$$

In this section, we prove the main theorem of this article (Theorem A in the introduction), which provides a significant improvement on (6.1):

[8] Instead of considering the measure μ_{ST} on $[0,\pi]$, Niederreiter works on the interval $[-1,1]$ endowed with the direct image of μ_{ST} under $t \mapsto \cos t$ (the 'semi-circle measure'); the translation to our setting is straightforward.

[9] See previous footnote. Note that [Nie91] actually gives explicit constants in (5.11).

Theorem 6.1 – *Let $\mathbb{F}_q$ be a finite field of odd characteristic p and $K = \mathbb{F}_q(t)$. There exist positive constants C_1, C_2 (depending at most on q and p) such that the following holds. For all $\gamma \in \mathbb{F}_q^\times$ and all integers $a \geq 1$, the special value $L^*(E_{a,\gamma}, 1)$ satisfies:*

$$-C_1 \cdot \frac{1}{\log b(E_{a,\gamma})} \leq \frac{\log L^*(E_{a,\gamma},1)}{\log\left(q^{b(E_{a,\gamma})}\right)} \leq C_2 \cdot \frac{\log\log b(E_{a,\gamma})}{\log b(E_{a,\gamma})} \quad (as\ a \to \infty). \tag{6.2}$$

We will prove this Theorem in §6.2. The upper bound in (6.2) does not radically improve on the upper bound of Hindry and Pacheco (*loc. cit.*) but, since our proof is rather short, we decided to include it here for completeness. Our proof of the lower bound in (6.2), on the other hand, is much more involved: the crucial step is the computation of a 'Sato–Tate limit', using the results of sections 4 and 5 (see the next subsection). For later use (in section 7), we note that Theorem 6.1 implies that

$$|\log L^*(E_{a,\gamma},1)| = o\big(b(E_{a,\gamma})\big) \qquad (\text{as } a \to \infty).$$

Remark 6.2 In [Gri16, Gri18a, Gri18b], the author has also proved, for other families of elliptic curves, lower bounds on special values of L-functions which are similar to (6.2). However, the approach used in those papers for proving such bounds noticeably differs from the strategy of proof of Theorem 6.1: let us investigate what comes out of our previous method for the sequence $\{E_{a,\gamma}\}_{a\geq 1}$ at hand.

The proof of Proposition 3.7 implies that

$$L^*(E_{a,\gamma},1) = \underbrace{\prod_{v\in P_q(a)} d_v}_{:=\Pi_1} \cdot \underbrace{\prod_{v\in P_q(a)} \left(1-\mathbf{kl}_\gamma(v)^2 q^{-d_v}\right)\left(1-\mathbf{kl}'_\gamma(v)^2 q^{-d_v}\right)}_{:=\Pi_2}.$$

The product Π_1 is an integer and can be shown to satisfy $\log \Pi_1 = o\big(b(E_{a,\gamma})\big)$ as $a \to \infty$ (see (6.5) and its proof), hence it is negligible for our purpose. As for the second term Π_2, by construction of the special value, it is of the form

$$\Pi_2 = \frac{N_{a,\gamma}}{q^{e_{a,\gamma}}} \text{ for some integers } e_{a,\gamma} \geq 0 \text{ and } N_{a,\gamma} \geq 1 \text{ with } \gcd(N_{a,\gamma}, q) = 1.$$

The proofs of [Gri18a, Thm. 4.1] and [Gri18b, Thm. 4.2] are essentially based on the observation that *to prove the desired lower bound on* $\log L^*(E_{a,\gamma},1)$*, it is* sufficient *to show that the exponent* $e_{a,\gamma}$ *is* $o\big(b(E_{a,\gamma})\big)$ *as* $a \to \infty$. Let us show that this asymptotic relation does not hold here.

To do so, we keep track of the contribution to the exponent $e_{a,\gamma}$ of each factor in Π_2. Fix a prime ideal $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ above p and denote by $\mathrm{ord}_{\mathfrak{P}}$ the $\mathfrak{P}$-adic valuation on $\overline{\mathbb{Q}}$ so normalised that $\mathrm{ord}_{\mathfrak{P}}(q) = 1$. For any $v \in P_q(a)$, one has $\mathrm{ord}_{\mathfrak{P}}(q^{d_v}) = d_v$ and it can be shown that $\{\mathrm{ord}_{\mathfrak{P}}\,\mathbf{kl}_\gamma(v), \mathrm{ord}_{\mathfrak{P}}\,\mathbf{kl}'_\gamma(v)\} = \{0, d_v\}$. Indeed, we know from Proposition 2.1 that $\mathbf{kl}_\gamma(v)$ and $\mathbf{kl}'_\gamma(v)$ are algebraic integers whose product is $|\mathbb{F}_v| = q^{d_v}$ and whose sum is $\mathrm{K}_\gamma(v)$. Besides it is known that $\mathrm{K}_\gamma(v) \equiv 1 \bmod \mathfrak{P}$ (see [vdGvdV91, Prop. 3.1(v)] for instance). Hence one of $\mathbf{kl}_\gamma(v)$ or $\mathbf{kl}'_\gamma(v)$ is a $\mathfrak{P}$-adic unit, so that the other has $\mathfrak{P}$-adic valuation d_v.

A quick computation then shows that the vth factor of Π_2 has $\mathfrak{P}$-adic valuation $-d_v$ *i.e.*, is of the form

$$\left(1-\mathbf{kl}_\gamma(v)^2 q^{-d_v}\right)\left(1-\mathbf{kl}'_\gamma(v)^2 q^{-d_v}\right) = q^{-d_v} \cdot \big(\text{a certain algebraic integer with } \mathrm{ord}_{\mathfrak{P}} = 0\big)$$

Taking the product of these factors over $v \in P_q(a)$, we deduce that (*cf.* (1.6)):

$$e_{a,\gamma} = \sum_{v\in P_q(a)} d_v = |\mathbb{G}_m(\mathbb{F}_{q^a})| = q^a - 1 = \frac{b(E_{a,\gamma})}{3}.$$

Since $e_{a,\gamma}$ is not $o\big(b(E_{a,\gamma})\big)$, this '$p$-adic valuation' method only yields a much weaker lower bound on the special value $L^*(E_{a,\gamma},1)$ than the one in (6.2): namely,

$$\log L^*(E_{a,\gamma},1)/\log\left(q^{b(E_{a,\gamma})}\right) \geq -1/3 + o(1) \qquad (\text{as } a \to \infty).$$

This is why we rely instead on studying the distribution of the angles $\{\boldsymbol{\theta}_\gamma(v)\}_{v\in P_q(a)}$ in $[0,\pi]$.

6.1 Evaluation of a Sato–Tate limit

In this subsection, we show the following result, which is the crucial input in our proof of the lower bound in Theorem 6.1. For any integer $a \geq 1$, we again denote by $\nu_a = \nu(\mathbb{F}_q, \psi_q, \gamma; a)$ the probability measure on $[0,\pi]$ introduced in §5.2.

Theorem 6.3 – *Let $\mathbb{F}_q$ be a finite field equipped with a nontrivial additive character ψ_q, and $\gamma \in \mathbb{F}_q^\times$. Then*

$$\int_{[0,\pi]} \log \sin^2 \, \mathrm{d}\nu_a \xrightarrow[a\to\infty]{} \int_{[0,\pi]} \log \sin^2 \mathrm{d}\mu_{\mathrm{ST}}. \tag{6.3}$$

More concretely, this statement means that

$$\frac{1}{|P_q(a)|} \sum_{v \in P_q(a)} \log\left(\sin^2 \boldsymbol{\theta}_\gamma(v)\right) \xrightarrow[a\to\infty]{} \frac{2}{\pi} \int_0^\pi \log(\sin^2 t) \cdot \sin^2 t \, \mathrm{d}t = \log \frac{e}{4},$$

the evaluation of the integral on the right-hand side being a routine exercise in calculus.

Proof: For conciseness, we denote by $w : [0,\pi] \to \mathbb{R}$ the function given by $w(t) := -\log(\sin^2 t)$ if $t \neq 0, \pi$ and $w(0) = w(\pi) := 0$. Once and for all, pick a nondecreasing continuously differentiable function $\phi_0 : [0,1] \to \mathbb{R}$ such that $\phi_0 \equiv 0$ on $[0,1/3]$ and $\phi_0 \equiv 1$ on $[2/3,1]$. For all $\epsilon \in (0,1)$, we define a function $\phi_\epsilon : [0,\pi] \to \mathbb{R}$ by

$$\phi_\epsilon(t) = \begin{cases} \phi_0(t/\epsilon) & \text{if } t \in [0,\epsilon], \\ 1 & \text{if } t \in [\epsilon, \pi-\epsilon], \\ \phi_0((\pi-t)/\epsilon) & \text{if } t \in [\pi-\epsilon, \pi], \end{cases}$$

and we let $w_\epsilon := w \cdot \phi_\epsilon$. By construction, w_ϵ is a continuously differentiable function on $[0,\pi]$ such that $w_\epsilon \leq w$ on $[0,\pi]$, $w \equiv w_\epsilon$ on $[\epsilon, \pi-\epsilon]$, and $w_\epsilon \equiv 0$ on $[0,\epsilon/3] \cup [\pi-\epsilon/3, \pi]$. Furthermore, we have the following analytic estimates:

Lemma 6.4 – *Notations being as above, for all $\epsilon \in (0,1)$, we have*

$$\text{(i)} \quad \int_0^\pi |w_\epsilon'(t)| \, \mathrm{d}t \ll |\log \epsilon|, \qquad \text{(ii)} \quad \int_0^\pi (w(t) - w_\epsilon(t)) \cdot \sin^2(t) \cdot \, \mathrm{d}t \ll \epsilon |\log \epsilon|.$$

The constants depend only on the choice of ϕ_0.

We postpone the proof of this Lemma until the end of the subsection, and we now prove that $\int_{[0,\pi]} w \, \mathrm{d}\nu_a$ converges to $\int_{[0,\pi]} w \, \mathrm{d}\mu_{\mathrm{ST}}$ when $a \to \infty$. For any $\epsilon \in (0,1)$, note that

$$\left| \int w \, \mathrm{d}\nu_a - \int w \, \mathrm{d}\mu_{\mathrm{ST}} \right| \leq \underbrace{\int |w - w_\epsilon| \, \mathrm{d}\nu_a}_{:=T_1} + \underbrace{\left| \int w_\epsilon \, \mathrm{d}\nu_a - \int w_\epsilon \, \mathrm{d}\mu_{\mathrm{ST}} \right|}_{:=T_2} + \underbrace{\int |w_\epsilon - w| \, \mathrm{d}\mu_{\mathrm{ST}}}_{:=T_3}.$$

Let us bound each of these three terms using the results in sections 4 and 5.

For $\epsilon > 0$ sufficiently small, we claim that the first term T_1 vanishes. Indeed, $w \equiv w_\epsilon$ on $[\epsilon, \pi-\epsilon]$ and, as we pointed out in Remark 5.4, Corollary 4.5 shows that the support of ν_a is contained in $[(q^a)^{-c_p}, \pi-(q^a)^{-c_p}]$. Therefore, for any $\epsilon < (q^a)^{-c_p}$, w and w_ϵ coincide (at least) on the support of ν_a, so that we have $T_1 = 0$. Next, the function w_ϵ being continuously differentiable on $[0,\pi]$, we can use our effective equidistribution result (Theorem 5.6) to control the second term T_2. Precisely, Theorem 5.6 yields

$$T_2 = \left| \int w_\epsilon \, \mathrm{d}\nu_a - \int w_\epsilon \, \mathrm{d}\mu_{\mathrm{ST}} \right| \ll_q \frac{a^{1/2}}{q^{a/4}} \cdot \int_0^\pi |w_\epsilon'(t)| \, \mathrm{d}t \ll_q \frac{a^{1/2}}{q^{a/4}} \cdot |\log \epsilon|,$$

where the rightmost upper bound is Lemma 6.4(i). Finally, Lemma 6.4(ii) proves that $T_3 \ll \epsilon |\log \epsilon|$.

In summary, for all $\epsilon > 0$ such that $\epsilon < (q^a)^{-c_p}$, we have

$$\left| \int_{[0,\pi]} w \, \mathrm{d}\nu_a - \int_{[0,\pi]} w \, \mathrm{d}\mu_{\mathrm{ST}} \right| \ll_q \frac{a^{1/2}}{q^{a/4}} \cdot |\log \epsilon| + \epsilon |\log \epsilon|.$$

Upon choosing $\epsilon = (q^a)^{-\gamma}$ where $\gamma = 2\max\{c_p, 4^{-1}\}$, we conclude that

$$\left| \int_{[0,\pi]} w \, \mathrm{d}\nu_a - \int_{[0,\pi]} w \, \mathrm{d}\mu_{\mathrm{ST}} \right| \ll_q \gamma a \cdot \frac{a^{1/2}}{q^{a/4}} + \frac{\gamma a}{q^{a \cdot \gamma}} \ll_{q,p} \frac{a^{3/2}}{q^{a/4}},$$

which proves Theorem 6.3. We even obtain a more quantitative version of (6.3):

$$\frac{1}{|P_q(a)|} \sum_{v \in P_q(a)} \log\left(\sin^2 \boldsymbol{\theta}_\gamma(v)\right) = \log(\mathrm{e}/4) + O\left(\frac{a^{3/2}}{q^{a/4}}\right) \quad (\text{as } a \to \infty),$$

where the implicit constant depends at most on q and p (and the choice of the auxiliary function ϕ_0). □

Proof (of Lemma 6.4): Since both w and w_ϵ are symmetric around $\pi/2$, it is sufficient to prove (i) and (ii) where the integrals are replaced by integrals over $[0,\pi/2]$. We also note that, for all $t \in (0,\pi/2]$, one has $0 \le w(t) \le 2\log\frac{\pi}{2t}$. This follows from the classical estimate: $\sin t \ge \frac{2t}{\pi}$ for $t \in [0,\pi/2]$.

To prove (i), we study separately the integrals over $(0,\epsilon)$ and over $[\epsilon,\pi/2]$. Since w and w_ϵ coincide on $[\epsilon,\pi/2]$, we have

$$\forall t \in [\epsilon,\pi/2], \quad |w_\epsilon'(t)| = |w'(t)| = 2\left|\frac{\cos t}{\sin t}\right| \le \frac{2}{|\sin t|} \le \frac{\pi}{t},$$

by the classical estimate mentioned above. Hence we have $\int_\epsilon^{\pi/2} |w_\epsilon'(t)|\,\mathrm{d}t \le \pi\int_\epsilon^{\pi/2} t^{-1}\,\mathrm{d}t \ll |\log\epsilon|$. On the interval $(0,\epsilon)$, we use the fact that $w_\epsilon = w\phi_\epsilon$ to deduce that

$$\forall t \in (0,\epsilon), \quad |w_\epsilon'(t)| \le |w'(t)|\cdot\phi_\epsilon(t) + |w(t)|\cdot|\phi_\epsilon'(t)| \le \frac{\pi}{t}\cdot\phi_\epsilon(t) + |w(t)|\cdot\frac{\|\phi_0'\|_\infty}{\epsilon},$$

where $\|\phi_0'\|_\infty$ denotes the supnorm of ϕ_0' on $[0,\pi]$. By the upper bound on $w(t)$ at the beginning of the proof and the fact that $\phi_\epsilon \equiv 0$ on $[0,\epsilon/3)$, we obtain that

$$\forall t \in (0,\epsilon), \quad |w_\epsilon'(t)| \le \frac{3\pi}{\epsilon} + \frac{2\|\phi_0'\|_\infty}{\epsilon}\cdot\log\frac{\pi}{2t},$$

and from there, that

$$\int_0^\epsilon |w_\epsilon'(t)|\,\mathrm{d}t \le 3\pi + \frac{2\|\phi_0'\|_\infty}{\epsilon}\cdot\int_0^\epsilon \log\frac{\pi}{2t}\,\mathrm{d}t \ll 1 + \frac{\|\phi_0'\|_\infty}{\epsilon}\cdot\epsilon|\log\epsilon| \ll |\log\epsilon|.$$

Summing the contributions of $\int_0^\epsilon$ and $\int_\epsilon^{\pi/2}$, we conclude that (i) holds, with a constant depending only on ϕ_0. We now show that (ii) holds: by the symmetry of $w - w_\epsilon$ and since $w \equiv w_\epsilon$ on $[\epsilon,\pi/2]$, it suffices to prove that $\int_0^\epsilon |w(t) - w_\epsilon(t)|\sin^2 t\,\mathrm{d}t \ll \epsilon|\log\epsilon|$. By construction of ϕ_ϵ, we notice that

$$\int_0^\epsilon |w(t) - w_\epsilon(t)|\cdot\sin^2 t\,\mathrm{d}t \le \int_0^\epsilon w(t)\cdot\sin^2 t\,\mathrm{d}t \le \int_0^\epsilon w(t)\,\mathrm{d}t \overset{(*)}{\le} 2\int_0^\epsilon \log\frac{\pi}{2t}\,\mathrm{d}t \ll \epsilon|\log\epsilon|,$$

where inequality $(*)$ follows from the upper bound on $w(t)$ given at the beginning of the proof. □

6.2 Proof of Theorem 6.1

In (3.12) and (3.15), we have proved that

$$L^*(E_{a,\gamma},1) = \prod_{v\in P_q(a)} 4\deg v\cdot\prod_{v\in P_q(a)}\left(1 - \frac{\mathrm{K}_\gamma(v)^2}{4q^{\deg v}}\right) = \prod_{v\in P_q(a)} 4\deg v\cdot\prod_{v\in P_q(a)}\sin^2\big(\boldsymbol{\theta}_\gamma(v)\big).$$

Therefore, we have

$$\frac{\log L^*(E_{a,\gamma},1)}{\log\left(q^{b(E_{a,\gamma})}\right)} = \underbrace{\frac{1}{\log\left(q^{b(E_{a,\gamma})}\right)}\cdot\sum_{v\in P_q(a)}\log(4\deg v)}_{:=A_1} \underbrace{- \frac{1}{\log\left(q^{b(E_{a,\gamma})}\right)}\sum_{v\in P_q(a)} -\log\left(\sin^2\boldsymbol{\theta}_\gamma(v)\right)}_{:=A_2}, \tag{6.4}$$

and we estimate the terms A_1 and A_2 separately. First of all, we deduce from Lemma 2.5(ii) that

$$\sum_{v\in P_q(a)}\log(4\deg v) \le \log(4a)\cdot|P_q(a)| \ll_q \frac{\log a\cdot q^a}{a}.$$

And, since we know by (1.6) that $q^a \ll b(E_{a,\gamma}) \ll q^a$, this yields

$$0 \le A_1 \ll_q \frac{\log a}{a} \ll_q \frac{\log\log b(E_{a,\gamma})}{\log b(E_{a,\gamma})}, \qquad (\text{as } a\to\infty). \tag{6.5}$$

Let us now bound A_2. Recall from §6.1 that $w : [0,\pi] \to \mathbb{R}$ denotes the function $t \mapsto -\log\left(\sin^2 t\right)$. It is clear that A_2 is nonnegative, and that one can write:

$$0 \le A_2 = \frac{|P_q(a)|}{\log\left(q^{b(E_{a,\gamma})}\right)}\cdot\frac{1}{\log\left(q^{b(E_{a,\gamma})}\right)}\sum_{v\in P_q(a)} w\big(\boldsymbol{\theta}_\gamma(v)\big) = \frac{|P_q(a)|}{\log\left(q^{b(E_{a,\gamma})}\right)}\cdot\int_{[0,\pi]} w\,\mathrm{d}\nu_a.$$

By (1.6) again, we have $b(E_{a,\gamma}) \gg q^a$ and, since Lemma 2.5(ii) yields that $|P_q(a)| \ll_q q^a/a$, we see that $|P_q(a)|/b(E_{a,\gamma}) \ll_q a^{-1}$. Moreover, by Theorem 6.3, we have

$$\int_{[0,\pi]} w \, \mathrm{d}\nu_a = \log(4/\mathrm{e}) + O_{p,q}\left(\frac{a^{3/2}}{q^{a/4}}\right) \ll_{p,q} 1 \qquad (\text{as } a \to \infty).$$

Putting these estimates together, we infer that

$$0 \le A_2 \ll_{q,p} \frac{1}{a} \ll_{q,p} \frac{1}{\log b(E_{a,\gamma})} \qquad (\text{as } a \to \infty). \tag{6.6}$$

Summing the inequalities (6.5) and (6.6), we finally obtain that

$$-\frac{1}{\log b(E_{a,\gamma})} \ll_{q,p} \frac{\log L^*(E_{a,\gamma},1)}{\log\left(q^{b(E_{a,\gamma})}\right)} = A_1 - A_2 \ll_q \frac{\log\log b(E_{a,\gamma})}{\log b(E_{a,\gamma})} \qquad (\text{as } a \to \infty).$$

This concludes the proof of Theorem 6.1. □

7 Application to an analogue of the Brauer–Siegel theorem

In this section, we deduce from Theorem 6.1 and from the BSD conjecture that the following theorem holds (stated as Theorem B in the introduction).

Theorem 7.1 – *Let $\mathbb{F}_q$ be a finite field of odd characteristic and $K := \mathbb{F}_q(t)$. For all $\gamma \in \mathbb{F}_q^\times$ and all integers $a \ge 1$, consider the elliptic curve $E_{a,\gamma}/K$ as above. Then the Tate–Shafarevich group $Ш(E_{a,\gamma})$ is finite and, as $a \to \infty$,*

$$\log\big(|Ш(E_{a,\gamma})| \cdot \mathrm{Reg}(E_{a,\gamma})\big) \sim \log H(E_{a,\gamma}). \tag{7.1}$$

Alternatively, (7.1) can be rewritten under the form

$$\forall \epsilon > 0, \quad H(E_{a,\gamma})^{1-\epsilon} \ll_{q,\epsilon} |Ш(E_{a,\gamma})| \cdot \mathrm{Reg}(E_{a,\gamma}) \ll_{q,\epsilon} H(E_{a,\gamma})^{1+\epsilon} \qquad (\text{as } a \to \infty). \tag{7.2}$$

The upper bound in (7.2) was essentially conjectured by Lang for elliptic curves over $\mathbb{Q}$ with finite Tate–Shafarevich groups[10] (see [Lan83, Conj.1]). Theorem 7.1 thus provides an unconditional example where this conjecture holds for elliptic curves over $K = \mathbb{F}_q(t)$. The lower bound in (7.2) further proves that the exponent 1 of the height is optimal, in the sense that 1 cannot be replaced by any smaller number.

One may also view Theorem 7.1 as an analogue of the Brauer–Siegel theorem for the elliptic curves $E_{a,\gamma}$. The Brauer–Siegel theorem states that, as F runs through a sequence of number fields of given degree n over $\mathbb{Q}$ and whose discriminants Δ_F tend, in absolute value, to $+\infty$, one has

$$\forall \epsilon > 0, \quad \Delta_F^{1/2-\epsilon} \ll_{n,\epsilon} |Cl(F)| \cdot R(F) \ll_{n,\epsilon} \Delta_F^{1/2+\epsilon} \qquad (\text{as } |\Delta_F| \to \infty), \tag{7.3}$$

where $Cl(F)$ denotes the class group of F and $R(F)$ its regulator of units. At least formally, (7.2) is very similar to (7.3). A more detailed analogy is explained in [Hin07] and [HP16].

Proof: We know from Theorem 1.5 that the BSD conjecture holds for $E_{a,\gamma}$. In particular, the Tate–Shafarevich group $Ш(E_{a,\gamma})$ is indeed finite and the special value $L^*(E_{a,\gamma},1)$ satisfies (1.8). The BSD formula (1.8) and Proposition 1.6 then imply the estimate:

$$\frac{\log\big(|Ш(E_{a,\gamma})| \cdot \mathrm{Reg}(E_{a,\gamma})\big)}{\log H(E_{a,\gamma})} = 1 + \frac{\log L^*(E_{a,\gamma},1)}{\log H(E_{a,\gamma})} + o(1) \qquad (\text{as } a \to \infty).$$

Therefore, to conclude the proof of Theorem 7.1, it remains to show that $|\log L^*(E_{a,\gamma},1)| = o\big(\log H(E_{a,\gamma})\big)$ or, alternatively, that

$$|\log L^*(E_{a,\gamma},1)| = o\big(b(E_{a,\gamma})\big) \qquad (\text{as } a \to \infty)$$

because, by (1.4), $\log H(E_{a,\gamma})$ and $b(E_{a,\gamma})$ have the same order of magnitude as $a \to \infty$. But we have already proved in Theorem 6.1 that this asymptotic estimate holds. □

[10] Note though that Lang uses a different normalisation of the height: his (naïve) height has an exponent 1/12 instead of our exponent 1.

Acknowledgements It is a pleasure to thank Marc Hindry and Douglas Ulmer for their encouragements and for some useful comments on earlier versions of this work. The author would also like to thank Bruno Anglès, Peter Bruin and Peter Koymans for fruitful discussions about various parts of the paper.

This work has been carried out at Universiteit Leiden, whose financial support and perfect working conditions are gratefully acknowledged. The author is also partially supported by the ANR project 'FLAIR' (Grant ANR-17-CE40-0012).

References

[BH12] Salman Baig and Chris Hall. Experimental data for Goldfeld's conjecture over function fields. *Exp. Math.*, 21(4):362–374, 2012.

[Bru92] Armand Brumer. The average rank of elliptic curves. I. *Invent. Math.*, 109(3):445–472, 1992.

[CHU14] Ricardo P. Conceição, Chris Hall, and Douglas Ulmer. Explicit points on the Legendre curve II. *Math. Res. Lett.*, 21(2):261–280, 2014.

[Fis95] Benji Fisher. Equidistribution theorems. *Astérisque*, (228):3, 69–79, 1995. Columbia University Number Theory Seminar (New York, 1992).

[FL05] Lei Fu and Chunlei Liu. Equidistribution of Gauss sums and Kloosterman sums. *Math. Z.*, 249(2):269–281, 2005.

[Gri16] Richard Griffon. *Analogues du théorème de Brauer-Siegel pour quelques familles de courbes elliptiques.* PhD thesis, Université Paris Diderot, July 2016. (available at math.leidenuniv.nl/~griffonrmm/thesis/Griffon_thesis.pdf).

[Gri18a] Richard Griffon. Analogue of the Brauer–Siegel theorem for Legendre elliptic curves. *Journal of Number Theory*, (to appear), 2018. (DOI:10.1016/j.jnt.2018.05.006).

[Gri18b] Richard Griffon. Explicit L-functions and a Brauer-Siegel theorem for Hessian elliptic curves. *Journal de Théorie des Nombres de Bordeaux*, (to appear), 2018. (Preprint ArXiv:1709.02761).

[Hin07] Marc Hindry. Why is it difficult to compute the Mordell-Weil group? In *Diophantine geometry*, volume 4 of *CRM Series*, pages 197–219. Ed. Norm., Pisa, 2007.

[HP16] Marc Hindry and 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.

[Kat88] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups.* Princeton University Press, Princeton, NJ, 1988.

[KN06] Lauwrens Kuipers and Harald Niederreiter. *Uniform distribution of sequences.* Dover Publications, New York, 2006.

[Lan83] Serge Lang. Conjectured Diophantine estimates on elliptic curves. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 155–171. Birkhäuser Boston, Boston, MA, 1983.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, second edition, 1997. With a foreword by P. M. Cohn.

[Mil86] James S. Milne. *Arithmetic duality theorems*, volume 1 of *Perspectives in Mathematics.* Boston Academic Press. Inc. Harcourt Brace Jovanovich, 1986.

[MW94] Maurice Mignotte and Michel Waldschmidt. On algebraic numbers of small height: linear forms in one logarithm. *J. Number Theory*, 47(1):43–62, 1994.

[Nie91] Harald Niederreiter. The distribution of values of Kloosterman sums. *Arch. Math.*, 56(3):270–277, 1991.

[PU16] Rachel Pries and Douglas Ulmer. Arithmetic of abelian varieties in Artin-Schreier extensions. *Trans. Amer. Math. Soc.*, 368(12):8553–8595, 2016.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1994.

[Tat66] John T. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages 415–440 (Exp. No. 306). Soc. Math. France, Paris, 1965/66.

[Ulm11] Douglas Ulmer. Elliptic curves over function fields. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 211–280. Amer. Math. Soc., Providence, RI, 2011.

[vdGvdV91] Gerard van der Geer and Marcel van der Vlugt. Kloosterman sums and the p-torsion of certain Jacobians. *Math. Ann.*, 290(3):549–563, 1991.

Mathematisch Instituut, Universiteit Leiden, PO Box 9512, 2300 RA Leiden, The Netherlands.
E-mail: r.m.m.griffon@math.leidenuniv.nl