Elliptic curves with large Tate–Shafarevich groups over $\mathbb{F}_q(t)$

Richard Griffon and Guus de Wit

Abstract. Let $\mathbb{F}_q$ be a finite field of odd characteristic p. We exhibit elliptic curves over the rational function field $K = \mathbb{F}_q(t)$ whose Tate-Shafarevich groups are large. Precisely, we consider certain infinite sequences of explicit elliptic curves E the Tate–Shafarevich group $Ш(E)$ of which, we prove, is finite and satisfies $|Ш(E)| = H(E)^{1+o(1)}$ as $H(E) \to \infty$, where $H(E)$ denotes the exponential differential height of E. We further show that, despite being large, these Tate–Shafarevich groups have trivial p-primary part.

The proof involves explicitly computing the L-functions of these elliptic curves, proving the BSD conjecture for them, and obtaining estimates on the size of the central value of their L-function.

Introduction

0.1. The size of Tate–Shafarevich groups of elliptic curves. Fix a finite field $\mathbb{F}_q$ of odd characteristic p and let $K := \mathbb{F}_q(t)$ denote the rational function field over $\mathbb{F}_q$. Let E be an elliptic curve over K which, we assume, is non-isotrivial (*i.e.*, its j-invariant $j(E) \in K$ does not lie in $\mathbb{F}_q$). One attaches to E its Tate–Shafarevich group, denoted by $Ш(E)$. Among other reasons, the arithmetic significance of $Ш(E)$ stems from its measuring, in a certain sense, how badly the local–global principle fails for E. The Tate–Shafarevich group remains a mysterious object; for instance, the finiteness of $Ш(E)$ is still conjectural in general, even though it has been proved in a number of cases. Let us assume for now that $Ш(E)$ is indeed finite: what can then be said about its size? There are several natural choices of numerical invariants of E to compare $|Ш(E)|$ to. Here, we choose the exponential differential height $H(E)$ and the conductor $N(E)$: these are defined by

$$H(E) := q^{\frac{1}{12}\deg \Delta_{\min}(E)} \qquad \text{and} \qquad N(E) := q^{\deg \mathcal{N}(E)},$$

where $\Delta_{\min}(E)$ and $\mathcal{N}(E)$ denote the minimal discriminant and the conductor divisors of E, respectively. Goldfeld and Szpiro [**1**] have proven upper bounds on the order of $Ш(E)$ in terms of these two invariants.

Let us quote a special case of their result:

Theorem 1 (Goldfeld–Szpiro [**1**]). *Let E be a non-isotrivial elliptic curve over K. Assume that E has finite Tate–Shafarevich group.*

2010 *Mathematics Subject Classification.* Primary 11G05, 11G40; Secondary 14G10, 11L05.

Key words and phrases. Elliptic curves over function fields, Tate-Shafarevich groups, Explicit computation of L-functions, BSD conjecture, Gauss and Kloosterman sums.

Correspondence to be sent to richard.griffon@unibas.ch.

(i) Then, for all $\varepsilon > 0$, one has $|Ш(E)| \ll_{q,\varepsilon} H(E)^{1+\varepsilon}$.
(ii) If, moreover, $j(E) \in K$ is not a p-th power in K, then, for all $\varepsilon > 0$, one has $|Ш(E)| \ll_{q,\varepsilon} N(E)^{1/2+\varepsilon}$.

In this statement[1], item *(ii)* follows from item *(i)* by applying Szpiro's inequality for elliptic curves with separable j-invariants. It is then natural to wonder about the optimality of *(i)* and *(ii)*: apart from the ε's, are the exponents of the height (1) and of the conductor (1/2) in these upper bounds best possible? In other words, as E ranges over all elliptic curves over K, what is the largest power of $H(E)$ – or $N(E)$ – that does appear in $|Ш(E)|$, up to a $\pm\varepsilon$ for all $\varepsilon > 0$?

In the analogous setting of elliptic curves over $\mathbb{Q}$, the analogue of Theorem 1 is known to be a consequence of the ABC conjecture (see §1–3 in [**1**]). Moreover, de Weger [**21**] conjectures that the exponents 1 and 1/2 should indeed be optimal in that context (see Conjectures 2 and 4 in [**21**]). Following the analogy between the arithmetics of elliptic curves over $\mathbb{Q}$ and over K, one can translate the statement of de Weger's conjecture (the quantities $H(E)$ and $N(E)$ here correspond to the 1/12-th power of the minimal discriminant and to the conductor of an elliptic curve over $\mathbb{Q}$, respectively). This translation results in the following:

Conjecture 2 (de Weger [**21**]). *Assuming finiteness of the relevant Tate–Shafarevich groups,*

(i) For any $\varepsilon > 0$, there are infinitely many elliptic curves E/K such that
$$|Ш(E)| \gg_{q,\varepsilon} H(E)^{1-\varepsilon}.$$
(ii) For any $\varepsilon > 0$, there are infinitely many elliptic curves E/K such that
$$|Ш(E)| \gg_{q,\varepsilon} N(E)^{1/2-\varepsilon}.$$

In the same paper, de Weger proves, conditionally to the Birch and Swinnerton-Dyer (BSD) conjecture, that (the analogue of) Conjecture 2*(i)* holds for elliptic curves over $\mathbb{Q}$. Prior to [**21**], Mai and Murty [**10**, Theorem 2] had shown, again conditionally to the BSD conjecture, a weaker version of Conjecture 2*(ii)* for elliptic curves over $\mathbb{Q}$, with the exponent 1/2 replaced by 1/4. Both of these results rely on considering sequences of well-chosen quadratic twists of a given elliptic curve.

In the context of elliptic curves over K, the above-stated Conjecture 2*(i)* is not difficult to prove. One can indeed take advantage of the existence of inseparable isogenies of large degree to construct sequences of elliptic curves over K with large Tate–Shafarevich groups (see §1.5, where we build one such example). In such sequences, the inseparability degree of the j-invariant grows to infinity. Moreover, by construction of these sequences, the elliptic curves therein are K-isogenous: one cannot, therefore, hope to deduce from these any result towards Conjecture 2*(ii)*. One also notices that the p-primary parts of the Tate–Shafarevich groups of the elliptic curves belonging to these sequences are "large"; and that, actually, the order of the p-primary part already accounts for the observed "large Ш" phenomenon.

We are therefore led to ask the following questions:

Question *1 For a given $\varepsilon > 0$, are there infinitely many* pairwise non K-isogenous *elliptic curves E/K such that $|Ш(E)| \gg_{q,\varepsilon} H(E)^{1-\varepsilon}$?*

[1]For two functions $f(x)$, $g(x)$ defined on $[0, \infty)$, we use Vinogradov's notation "$f(x) \ll_a g(x)$" to mean that there exists a constant $C > 0$, depending at most on the parameters a, such that $|f(x)| \leq Cg(x)$ for $x \to \infty$. This is synonymous with Landau's notation "$f(x) = O_a(g(x))$".

QUESTION *2 If so, is the fact that their Tate–Shafarevich groups are "large" always explained by a "large p-primary part of* Ш*" phenomenon?*

QUESTION *3 In the first question, can one also require that the j-invariants of the involved elliptic curves have bounded inseparability degree?*

In this paper, we give positive answers to the first and third questions:

THEOREM A. *For all* $\varepsilon > 0$*, there are infinitely many* pairwise non K-isogenous *elliptic curves* E/K *with separable j-invariant and finite Tate–Shafarevich group, such that*

$$|Ш(E)| \geq H(E)^{1-\varepsilon}.$$

We also prove a result in direction of Conjecture 2*(ii)*, with the same exponent $1/4$ as in [**10**]:

THEOREM B. *For all* $\varepsilon > 0$*, there are infinitely many* pairwise non $\overline{K}$-isomorphic *elliptic curves* E/K *with separable j-invariant and finite Tate–Shafarevich group, such that*

$$|Ш(E)| \geq N(E)^{1/4-\varepsilon}.$$

In contrast to the aforementioned results concerning elliptic curves over $\mathbb{Q}$, Theorems A and B are unconditional, and the involved elliptic curves are not quadratic twists of each other. Our proof is constructive and effective in that we exhibit sequences of elliptic curves over K satisfying these properties and we provide explicit bounds on the order of their Tate–Sharafarevich groups.

Finally, for all the elliptic curves in these sequences, we prove that the p-primary parts of their Tate–Shafarevich groups are trivial, thus answering in the negative the second question raised above.

0.2. Elliptic curves with large Tate–Shafarevich groups. Theorems A and B both follow from our main theorem, which we now state. Let $\mathbb{F}_q$ be a finite field of odd characteristic p. For any parameter $\gamma \in \mathbb{F}_q^\times$ and any integer $a \geq 1$, we write $\wp_a(t) := t^{q^a} - t \in \mathbb{F}_q[t]$ and consider the elliptic curve $E_{\gamma,a}$ defined over K by the Weierstrass model:

$$E_{\gamma,a} : \qquad y^2 = x\big(x^2 + \wp_a(t)x + \gamma\big). \tag{1}$$

The main result of this paper is the following:

THEOREM C. *In the above setting,*

(1) As $\gamma \in \mathbb{F}_q^\times$ *and* $a \geq 1$ *vary, the curves* $E_{\gamma,a}$ *are pairwise neither* $\overline{K}$*-isomorphic nor* K*-isogenous. Moreover, the j-invariant* $j(E_{\gamma,a})$ *is separable.*

(2) For any $\gamma \in \mathbb{F}_q^\times$ *and* $a \geq 1$*, the Tate–Shafarevich group* $Ш(E_{\gamma,a})$ *is finite.*

(3) Given $\gamma \in \mathbb{F}_q^\times$*, as* $a \to \infty$*, we have*

$$|Ш(E_{\gamma,a})| = H(E_{\gamma,a})^{1+o(1)}.$$

(4) For any $\gamma \in \mathbb{F}_q^\times$ *and* $a \geq 1$*, the p-primary part of* $Ш(E_{\gamma,a})$ *is trivial.*

One can reformulate *(3)* as follows: given $\varepsilon > 0$, for any $\gamma \in \mathbb{F}_q^\times$ and any large enough integer $a \geq 1$ (depending on ε), we have

$$H(E_{\gamma,a})^{1-\varepsilon} \leq |Ш(E_{\gamma,a})| \leq H(E_{\gamma,a})^{1+\varepsilon}.$$

It is then clear that, for a given $\varepsilon > 0$, all but finitely many of the $E_{a,\gamma}$'s satisfy $|Ш(E_{\gamma,a})| \geq H(E_{\gamma,a})^{1-\varepsilon}$. Further, we will see that $H(E_{\gamma,a}) = N(E_{\gamma,a})^{1/4}$, so that $|Ш(E_{\gamma,a})| \geq N(E_{\gamma,a})^{1/4-\varepsilon}$ holds for all but finitely many of the $E_{\gamma,a}$'s.

In particular, Theorem C does imply Theorems A and B.

0.3. Organisation of the paper. We now explain the overall strategy of the proof of Theorem C as we describe the plan of the paper. The first section briefly recalls the definitions and main properties of the objects that will be used throughout the paper. In the last subsection §1.5, we show how the Frobenius isogenies allow one to construct sequences of elliptic curves with large Tate–Shafarevich groups (thus proving Conjecture 2*(i)* above). We found it worthwhile to include this construction since the argument in §1.5 illustrates on a simple example the general structure of the proof of Theorem C.

The elliptic curves $E_{\gamma,a}$ are introduced in section 2, where we also calculate some of their more easily accessible invariants: their height and conductor, their Tamagawa number, as well as the torsion subgroup of $E_{\gamma,a}(K)$. The curves $E_{\gamma,a}$ were first studied by Pries and Ulmer in [**13**]: we recall in §2.2 how they were constructed there, and some of the results of [**13**]. Item *(1)* of Theorem C is proved in Proposition 2.4.

A large part of the proof of Theorem C is analytic, in that we rely on a detailed study of the relevant L-functions. Our first main goal is therefore to obtain an explicit expression for the L-function of $E_{\gamma,a}$. To that end, we introduce some notation in section 3. We define a certain finite set $P_q(a)$ of places of K and, to each place $v \in P_q(a)$ we attach in §3.3 two character sums over the residue field of K at v: a Gauss sum $\mathbf{g}(v)$ and a Kloosterman sum $\mathbf{Kl}_\gamma(v)$. We then show (see Theorem 4.1) that, for any integer $a \geq 1$ and any $\gamma \in \mathbb{F}_q^\times$, the L-function $L(E_{\gamma,a}, T)$ of $E_{\gamma,a}$ admits the following expression:

$$L(E_{\gamma,a}, T) = \prod_{v \in P_q(a)} \left(1 - \mathbf{g}(v)\mathbf{Kl}_\gamma(v)T^{\deg v} + \mathbf{g}(v)^2 q^{\deg v} T^{2\deg v}\right). \tag{2}$$

This identity is proved in section 4 by an elementary method based on the definition of $L(E_{\gamma,a}, T)$ and manipulation of character sums. This result, which is instrumental in the proof of our main theorem, may be of independent interest.

Using (2) and arithmetic properties of Gauss and Kloosterman sums, we elucidate in Theorem 5.2 the p-adic valuations of the zeros of $L(E_{\gamma,a}, T)$. As a consequence, we deduce that $L(E_{\gamma,a}, T)$ does not vanish at the central point $T = q^{-1}$ for its functional equation (see Theorem 5.3). This non-vanishing result is enough to ensure that the BSD conjecture holds for $E_{\gamma,a}$ (Corollary 5.4) which, in turn, has several important corollaries for our study. First, the Tate–Shafarevich group $Ш(E_{\gamma,a})$ is indeed (unconditionally) finite, as claimed in Theorem C*(2)*. Secondly, we derive from the BSD formula and from our computations in section 2 that

$$|Ш(E_{\gamma,a})| = q^{-1} H(E_{\gamma,a}) \cdot L(E_{\gamma,a}, q^{-1}). \tag{3}$$

Lastly – even though this is less central to our point – the Mordell–Weil group $E_{\gamma,a}(K)$ is finite and, taking into account our description of its torsion subgroup, we conclude that $E_{\gamma,a}(K) = \{\mathcal{O}, (0,0)\}$.

In light of the link (3) between the order of the Tate–Shafarevich group and the central value of $L(E_{\gamma,a}, T)$, we estimate the size of $|Ш(E_{\gamma,a})|$ in terms of $H(E_{\gamma,a})$

by proving adequate upper and lower bounds on $L(E_{\gamma,a}, q^{-1})$. Specifically, in order to show that Theorem C*(3)* holds, we need to prove that

$$-o(1) \leq \frac{\log L(E_{\gamma,a}, q^{-1})}{\log H(E_{\gamma,a})} \leq o(1) \qquad (\text{as } a \to \infty). \tag{4}$$

The proof of these inequalities is carried out in section 7. Proving the lower bound in (4) is the crucial step. After evaluating expression (2) for $L(E_{\gamma,a}, T)$ at $T = q^{-1}$, straightforward analytical considerations yield that $L(E_{\gamma,a}, q^{-1})$ can be bounded from below by

$$\log L(E_{\gamma,a}, q^{-1}) \geq \sum_{v \in P_q(a)} w\left(\frac{\mathsf{Kl}_\gamma(v)}{2q^{\deg v/2}}\right), \quad \text{where } w(x) := \log|x^2(1-x^2)|.$$

For any place $v \in P_q(a)$, the algebraic number $\mathsf{Kl}_\gamma(v)/2q^{\deg v/2}$ is known to be totally real; moreover, its image in any complex embedding of $\overline{\mathbb{Q}}$ lies in the interval $[-1, 1]$ by the Weil bound for Kloosterman sums. It is apparent that the size of the right-hand side of the previous display depends on how the set

$$\Theta_{\gamma,a} := \{\mathsf{Kl}_\gamma(v)/2q^{\deg v/2}\}_{v \in P_q(a)}$$

is distributed in $[-1, 1]$. We study the relevant aspects of the distribution of $\Theta_{\gamma,a}$ in section 6. Namely, we first recall from [**3**] an effective version of an asymptotic equidistribution statement, the qualitative form of which says that, asymptotically as $a \to \infty$, the set $\Theta_{\gamma,a}$ becomes equidistributed in $[-1, 1]$ with respect to the measure $\frac{2}{\pi}\sqrt{1-x^2}\,\mathrm{d}x$. Next we prove a quantitative version of the fact that $\Theta_{\gamma,a}$ "avoids" the points $-1, 0$ and 1, which are the poles of $x \mapsto w(x)$ on $[-1, 1]$.

We then conclude the proof of the lower bound in (4) by coupling these two facts about $\Theta_{\gamma,a}$ with a suitable approximation of w on $[-1, 1]$. The resulting estimates (4) constitute Theorem 7.1. We combine these to (3) in §8.2 to complete the proof of Theorem C*(3)*.

Finally, in order to prove Theorem C*(4)*, we show that $|Ш(E_{\gamma,a})|$ is relatively prime to p (see Theorem 8.1). To do so, we start from the BSD formula (3): instead of estimating the "archimedean size" of the central value $L(E_{\gamma,a}, q^{-1})$ as we did above, we now estimate its "p-adic size". The p-adic valuation of $L(E_{\gamma,a}, q^{-1})$ visibly depends on the p-adic valuations of the zeros of $L(E_{\gamma,a}, T)$. The above-mentioned Theorem 5.2 allows us to obtain the desired result, in §8.1.

1. Invariants of elliptic curves over function fields

Let $\mathbb{F}_q$ be a finite field of characteristic p and $K := \mathbb{F}_q(t)$ denote the field of rational functions on the projective line $\mathbb{P}^1_{/\mathbb{F}_q}$. For simplicity, and since we will not need the general case, we assume throughout that $p \neq 2$. Let M_K denote the set of all places v of K; the set M_K may be identified with the set of closed points of $\mathbb{P}^1_{/\mathbb{F}_q}$. Among those is the degree-1 closed point $\infty = [0 : 1]$; we write M_K° for the set $M_K \setminus \{\infty\}$ of closed points of $\mathbb{A}^1_{/\mathbb{F}_q} = \mathbb{P}^1_{\mathbb{F}_q} \setminus \{\infty\}$. There is a 1-to-1 correspondence between M_K° and the set of monic irreducible elements of $\mathbb{F}_q[t]$.

In this section, we introduce the relevant invariants of elliptic curves over K. For a more detailed introduction to the arithmetic of elliptic curves over function fields and their invariants, the reader is referred to [**19**]. Some of the results quoted in this section are valid more generally for elliptic curves (or even abelian varieties) over a function field of positive characteristic, but we only state the special cases

that are required for our purpose. We do not mention K in the notation used for the invariants of elliptic curves over K which we consider: unless explicitly noted otherwise, these invariants are relative to K.

1.1. Conductor and height. Let E be a non-isotrivial elliptic curve over K (*i.e.*, its j-invariant $j(E)$ is not a constant rational function). We denote by $\Delta_{\min}(E)$ its minimal discriminant divisor, which is a divisor on $\mathbb{P}^1_{/\mathbb{F}_q}$. The *exponential differential height* $H(E)$ is defined by

$$H(E) := q^{\frac{1}{12}\deg \Delta_{\min}(E)}.$$

The conductor divisor $\mathcal{N}(E)$ of E is also a divisor on $\mathbb{P}^1_{/\mathbb{F}_q}$ (see [**16**, Chap. IV, §10] for the precise definition). We then let

$$N(E) := q^{\deg \mathcal{N}(E)}.$$

We will call $N(E)$ the "*(numerical) conductor*" of E. An easy inequality between the conductor and the minimal discriminant divisors yields that $N(E)^{1/12} \leq H(E)$. In the other direction, Szpiro's inequality states that

$$H(E) \leq N(E)^{1/2},$$

provided that $j(E) \in K$ is not a p-th power in K (see [**1**, Thm. 3] and the references in that article). Note that two K-isogenous elliptic curves have the same numerical conductor (see §1.3).

1.2. The Tate–Shafarevich group. Fix a separable closure K^{sep} of K and consider the Galois cohomology group $\mathrm{H}^1(K,E) := \mathrm{H}^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), E(K^{\mathrm{sep}}))$. For any place $v \in M_K$, there is a similarly defined group $\mathrm{H}^1(K_v,E)$, where K_v denotes the completion of K at v. Recall that the *Tate–Shafarevich group of* E is defined by:

$$Ш(E) := \ker\left(\mathrm{H}^1(K,E) \longrightarrow \prod_{v\in M_K} \mathrm{H}^1(K_v,E)\right),$$

where the product runs over all places v of K and the arrow is the product of the canonical restriction maps $\mathrm{H}^1(K,E) \to \mathrm{H}^1(K_v,E)$.

Perhaps a more illuminating way of thinking about $Ш(E)$ is to observe that it is in bijection with the set of K-isomorphism classes of pairs (C,ϕ), where C/K is a curve of genus 1 which has at least one K_v-rational point for all places $v \in M_K$ and ϕ is a K-isomorphism between E and $\mathrm{Jac}(C)$ (see [**17**, Chap. X, §3-4] for more details). One can show that the class of such a pair (C,ϕ) is trivial in $Ш(E)$ if and only if C has a K-rational point. This point of view makes it clearer that $Ш(E)$ measures a local-global obstruction.

By construction, the Tate–Shafarevich group $Ш(E)$ is a torsion abelian group. It is conjectured, but not known in general, that $Ш(E)$ is finite (in the cases we study, we will show that it is indeed finite).

1.3. The L-function. For any place $v \in M_K$, we denote by $\mathbb{F}_v$ the residue field of K at v, which is a finite extension of $\mathbb{F}_q$, and by $\deg v = [\mathbb{F}_v : \mathbb{F}_q]$ the degree of v. For such a v, let $(\widetilde{E})_v$ denote the reduction of E at v. This plane cubic curve over $\mathbb{F}_v$ is not necessarily smooth: we say that E has *good reduction at* v if it is, and that E has *bad reduction at* v otherwise. In both cases, it makes sense to count

$\mathbb{F}_v$-rational points on $(\widetilde{E})_v$. For any $v \in M_K$, put $a_v(E) := |\mathbb{F}_v| + 1 - |(\widetilde{E})_v(\mathbb{F}_v)|$ and define the *L-function of* E by the formal Euler product

$$L(E,T) := \prod_{v \in M_K} L_v(E,T)^{-1}, \tag{1.1}$$

where the product runs over all places of K and where

$$L_v(E,T) = \begin{cases} 1 - a_v(E)T^{\deg v} + q^{d_v}T^{2\deg v} & \text{if } E \text{ has good reduction at } v, \\ 1 - a_v(E)T^{\deg v} & \text{if } E \text{ has bad reduction at } v. \end{cases} \tag{1.2}$$

By the Hasse bound, the Euler product in (1.1) *a priori* converges on the complex disk $\left\{T \in \mathbb{C} : |T| < q^{-3/2}\right\}$. However, deep results of Grothendieck and Deligne (among others) actually prove that $L(E,T)$ is a polynomial with integral coefficients in T, with constant coefficient 1. The degree $b(E)$ of that polynomial is given by the Grothendieck–Ogg–Shafarevich formula, which states that $\deg L(E,T) = \deg \mathcal{N}(E) - 4$. Moreover, the L-function satisfies the expected functional equation: $L(E,T) = \pm 1 \cdot (qT)^{b(E)} \cdot L(E, 1/q^2T)$. Lastly, $L(E,T)$ satisfies the Riemann Hypothesis *i.e.*, the complex zeros of $z \mapsto L(E,z)$ have magnitude q^{-1}.

In particular, the value of $L(E,T)$ at the central point for its functional equation (*viz.* $T = q^{-1}$) is a rational number, and the Riemann Hypothesis allows one to see that $L(E,q^{-1})$ is non-negative.

Recall that two K-isogenous elliptic curves E and E' have the same L-function: see [**5**, App. C] for a proof. In particular, their L-functions have the same degree and the Grothendieck–Ogg–Shafarevich formula implies that $\deg \mathcal{N}(E) = \deg \mathcal{N}(E')$, so that the numerical conductors $N(E)$ and $N(E')$ coincide.

By the results recalled in the previous paragraph, the L-function of E can be written as a product of the form

$$L(E,T) = \prod_{k=1}^{b(E)} (1 - z_k T),$$

for some algebraic integers z_k. These z_k's are the inverse zeros of the polynomial $L(E,T)$. We choose a prime ideal $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ above p and denote by $\mathrm{ord}_{\mathfrak{P}} : \overline{\mathbb{Q}}^{\times} \to \mathbb{Q}$ the corresponding discrete valuation, so normalised that $\mathrm{ord}_{\mathfrak{P}}(q) = 1$. For all $k \in \{1, \dots, b(E)\}$, we let $\lambda_k = \mathrm{ord}_{\mathfrak{P}}(z_k) \in \mathbb{Q}$. The functional equation of $L(E,T)$ implies that both z_k and q^2/z_k are algebraic integers, so that $0 \leq \lambda_k \leq 2$ for all k. Renumbering the z_k's if necessary, we can assume that $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_{b(E)}$. Thus ordered, the sequence $\{\lambda_1, \lambda_2, \dots, \lambda_{b(E)}\}$ will be called the *p-adic slope sequence of* $L(E,T)$. It then follows from the functional equation satisfied by $L(E,T)$ that one has $\lambda_{b(E)-k} = 2 - \lambda_k$ for any $k \in \{1, \dots, b(E)\}$.

1.4. The BSD conjecture. Birch and Swinnerton-Dyer (and Tate, in this context) conjectured that the analytic behaviour of the L-function $z \mapsto L(E,z)$ around $z = q^{-1}$ encodes arithmetic information about E. The reader is referred to [**18**], [**1**, §4] or [**19**] for more detailed accounts of the BSD conjecture.

In the case that $L(E,T)$ does not vanish at $T = q^{-1}$, which is the most relevant for our purpose, their conjecture is entirely proved. We state the end result as follows:

THEOREM 1.1 (BSD conjecture for elliptic curves of analytic rank 0). *Let E be a non-isotrivial elliptic curve over K. Assume that $L(E, q^{-1}) \neq 0$. Then the following statements hold:*

(1) The Mordell–Weil group $E(K)$ is finite (i.e., $E(K)$ is torsion).
(2) The Tate–Shafarevich group $Ш(E)$ is finite.
(3) Moreover, one has

$$L(E, q^{-1}) = \frac{|Ш(E)|}{H(E)} \cdot \frac{q \cdot \tau(E)}{|E(K)|^2}, \tag{1.3}$$

where $\tau(E)$ denotes the Tamagawa number of E (i.e., the product over all places v of K of the number of connected components of the fiber over v of the Néron model of E).

We sketch a proof of this theorem. Write $\rho_E = \mathrm{ord}_{T=q^{-1}} L(E, T)$ for the *analytic rank of E i.e.*, the multiplicity of q^{-1} as a root of $L(E, T)$. Tate [**18**] has proved that $0 \leq \mathrm{rank}_{\mathbb{Z}} E(K) \leq \rho_E$. By assumption we have $\rho_E = 0$ here, so that $\mathrm{rank}_{\mathbb{Z}} E(K)$ vanishes too: hence the finiteness of $E(K)$. Moreover, we have $\rho_E = \mathrm{rank}_{\mathbb{Z}} E(K)$ (this equality is the so-called "weak BSD conjecture").

On the other hand, deep results by Tate [**18**] and Milne [**12**] show that the "weak BSD conjecture" implies the whole BSD conjecture. More precisely, they prove the equivalence:

$$\rho_E = \mathrm{rank}_{\mathbb{Z}} E(K) \iff \exists\ \ell \text{ prime} : Ш(E)[\ell^\infty] \text{ is finite} \iff \text{the BSD conjecture holds for } E/K.$$

Milne [**12**] assumes that $p \neq 2$, but note that the equivalence is now known to hold even in even characteristic, by subsequent work of Kato and Trihan [**8**].

Therefore, the equality $\rho_E = \mathrm{rank}_{\mathbb{Z}} E(K)$ implies *(2)* and *(3)*.

1.5. Large Ш via Frobenius isogenies. This section is inspired by [**20**, §5]: our main purpose here is to illustrate, on a very simple example, the steps that we shall follow to prove that some elliptic curves have a large Tate–Shafarevich group.

Let E be a non-isotrivial elliptic curve over $K = \mathbb{F}_q(t)$ and, for any integer $n \geq 1$, let E_n denote the base change of E/K under the p^n-th power Frobenius morphism $\mathrm{Fr}_{p^n} : K \to K$. In other words, we put $E_n = E \times_K K$ where the underlying map $K \to K$ is Fr_{p^n}. The induced map $F_{p^n} : E \to E_n$ is a purely inseparable isogeny of degree p^n (see [**19**, p. 225]). We obtain in this manner a sequence $(E_n)_{n \geq 1}$ of elliptic curves over K. One obviously has $j(E_n) = j(E)^{p^n}$, so that the inseparability degree of $j(E_n)$ is unbounded as n varies. Moreover, we have $N(E_n) = N(E)$ since the curves are K-isogenous (see §1.1). For the same reason, we have $L(E_n, T) = L(E, T)$ for all $n \geq 1$. On the other hand, the proof of Theorem 5.1 in [**20**] shows that the height $H(E_n)$ tends to infinity as $n \to \infty$.

Now let us *assume that E is chosen so that $L(E, q^{-1})$ is non-zero.* Clearly, the central value $L(E_n, q^{-1})$ is then also non-zero for any $n \geq 1$. This implies that the full BSD conjecture holds for all the elliptic curves E_n in the sequence (see Theorem 1.1). In particular, the Tate–Shafarevich groups $Ш(E_n)$ are all finite. Furthermore, the BSD formula (1.3) states that

$$L(E_n, q^{-1}) = \frac{|Ш(E_n)|}{H(E_n)} \cdot \frac{q \cdot \tau(E_n)}{|E_n(K)_{\mathrm{tors}}|^2}.$$

The growth of $\tau(E_n)$ can be estimated in terms of $H(E_n)$: [**6**, Thm. 1.22] or [**2**, Thm. 1.5.4] yield that $\log \tau(E_n) = o\big(\log H(E_n)\big)$ as $n \to \infty$. Further, there is a uniform bound on torsion subgroups of elliptic curves over K (see Proposition 7.1 in [**19**, Lect. 1] for instance): here, this shows that $|E_n(K)_{\mathrm{tors}}|$ remains bounded as $n \to \infty$. From the last displayed identity and these two bounds, we deduce that:

$$\frac{\log |Ш(E_n)|}{\log H(E_n)} = 1 + \frac{\log L(E_n, q^{-1})}{\log H(E_n)} + o(1) \qquad (\text{as } n \to \infty).$$

Since $L(E_n, q^{-1}) = L(E, q^{-1}) = O(1)$, we therefore obtain that

$$\log |Ш(E_n)| \sim \log H(E_n) \qquad (\text{as } n \to \infty).$$

In other words, we have $|Ш(E_n)| = H(E_n)^{1+o(1)}$ as $n \to \infty$, so that the elliptic curves E_n do have "large Tate–shafarevich groups".

Let us denote by $v_p : \mathbb{Q}^\times \to \mathbb{Q}$ the p-adic valuation on $\mathbb{Q}$, normalised so that $v_p(q) = 1$. We now evaluate the p-adic valuations of both sides of the BSD formula (instead of their logarithm, as we just did). The above mentioned upper bound on $\tau(E_n)$ also yields that $v_p(\tau(E_n)) = O\big(v_p(H(E_n))\big)$ as $n \to \infty$. Hence, we have

$$\frac{v_p(|Ш(E_n)|)}{v_p(H(E_n))} \geq 1 + \frac{v_p(L(E_n, q^{-1}))}{v_p(H(E_n))} + o(1) = 1 + o(1).$$

Besides, the order of $Ш(E_n)[p^\infty]$ equals $q^{v_p(|Ш(E_n)|)}$. Since $v_p(H(E_n))$ is none other than $\log H(E_n)/\log q$, we deduce from the above that

$$|Ш(E_n)[p^\infty]| \geq H(E_n)^{1+o(1)} \qquad (\text{as } n \to \infty).$$

Therefore, the "large Ш" phenomenon for the elliptic curves in the sequence $(E_n)_{n\geq 1}$ is "explained" by a large p-primary part of Ш.

The set of elliptic curves E to which this construction applies is non-empty. For instance, consider the Legendre elliptic curve E/K given by $y^2 = x(x-1)(x-t)$. This curve is non-isotrivial, and a straighforward application of Tate's algorithm shows that the conductor divisor $\mathcal{N}(E)$ has degree 4. The Grothendieck–Ogg–Shafarevich formula then predicts that $\deg L(E, T) = 0$. This forces the L-function to be trivial (*i.e.*, $L(E, T) = 1$); in particular, $L(E, q^{-1})$ is non-zero.

The previous paragraph shows that we have:

Proposition 1.2. *For any integer $n \geq 1$, consider the elliptic curve E_n defined over K by*

$$E_n : \qquad y^2 = x\big(x-1\big)\big(x-t^{p^n}\big).$$

For all $n \geq 1$, the Tate–Shafarevich group $Ш(E_n)$ is finite and, as $n \to \infty$, one has

$$|Ш(E_n)| = H(E_n)^{1+o(1)}.$$

This proposition proves that Conjecture 2*(i)* in the introduction is true. To prove Theorem C, we rely on a somewhat similar strategy: the various steps we follow in the rest of the paper are but more elaborate versions of the ones in the proof of Proposition 1.2.

Remark 1.3. In case the characteristic p of K is congruent to 1 modulo 6, the authors of [**4**] have very recently produced a sequence of elliptic curves over K with large Tate–Shafarevich groups, the p-primary parts of which are trivial. In contrast to the elliptic curves studied in the present paper, though, the elliptic curves forming the sequence of [**4**], being sextic twists of $y^2 = x^3 + 1$ over K, are

all isotrivial and are all $\overline{K}$-isomorphic (they have j-invariant 0). Theorem C is also independent of the congruence of p modulo 6.

2. The elliptic curves $E_{\gamma,a}$

Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$, $K = \mathbb{F}_q(t)$ and M_K be the set of places of K. Recall that we identify, as we may, the set $M_K^\circ = M_K \setminus \{\infty\}$ both with the set of monic irreducible polynomials in $\mathbb{F}_q[t]$ and with the set of closed points of $\mathbb{A}^1_{/\mathbb{F}_q} = \mathbb{P}^1_{/\mathbb{F}_q} \setminus \{\infty\}$.

For any integer $a \geq 1$, we let $\wp_a(t) := t^{q^a} - t \in \mathbb{F}_q[t]$.

2.1. Definition. Let γ be a nonzero element of $\mathbb{F}_q$ and $a \geq 1$ be an integer. We let $E_{\gamma,a}$ be the elliptic curve over K given by the affine Weierstrass model

$$E_{\gamma,a}: \qquad y^2 = x^3 + \wp_a(t)x^2 + \gamma x. \tag{2.1}$$

Its j-invariant is easily computed to be

$$j(E_{\gamma,a}) = 2^8 \cdot \frac{(\wp_a(t)^2 - 3\gamma)^3}{\gamma^2(\wp_a(t)^2 - 4\gamma)}, \tag{2.2}$$

and the discriminant of the model (2.1) is $\Delta_{\gamma,a} = 2^4\gamma^2(\wp_a(t)^2 - 4\gamma)$. Note that the j-invariant is not constant, hence the curve $E_{\gamma,a}$ is non-isotrivial. We also remark that $j(E_{\gamma,a})$ is not a p-th power in K *i.e.*, $j(E_{\gamma,a})$ is separable.

Even though the model (2.1) still makes sense when $p = 2$ or $\gamma = 0$, the expression of its discriminant $\Delta_{\gamma,a}$ shows that the curve $E_{\gamma,a}$ defined by (2.1) is not smooth in these cases. Hence our assuming that $p \neq 2$ and $\gamma \neq 0$ to ensure that $E_{\gamma,a}$ is a *bona fide* elliptic curve.

2.2. Construction of $E_{\gamma,a}$. The sequences $\{E_{\gamma,a}\}_{a\geq 1}$ are essentially some of the titular Artin–Schreier families of elliptic curves studied in [**13**] (see §6.2 there). We briefly give more details about how the sequences $\{E_{\gamma,a}\}_{a\geq 1}$ were constructed in *loc. cit.* and "compare" them to other similarly constructed sequences.

The basic input of the construction in [**13**] is a pair (f, g) of rational functions $\mathbb{P}^1_{/\mathbb{F}_q} \to \mathbb{P}^1_{/\mathbb{F}_q}$ whose divisors satisfy mild conditions. The output is a sequence, indexed by powers Q of q, of smooth projective surfaces X_Q over $\mathbb{F}_q$, each equipped with a natural fibration $\pi_Q : X_Q \to \mathbb{P}^1_{/\mathbb{F}_q}$ and admitting a dominant rational map $C_{f,Q} \times C_{g,Q} \dashrightarrow X_Q$ from the product of two curves $C_{f,Q}$, $C_{g,Q}$ defined over $\mathbb{F}_q$ in terms of f and g. One of the main results of [**13**] is that the Jacobian variety of the generic fiber of π_Q satisfies the BSD conjecture.

Pries and Ulmer further classify (see Proposition 3.1.5 and §4.2 in [**13**]) the various polar behaviours of f and g for which the resulting sequence $(X_Q)_Q$ is a sequence of elliptic surfaces (*i.e.*, for which the generic fiber of π_Q is an elliptic curve over K). This classification results in seven "types" of pairs (f, g).

The elliptic curve $E_{\gamma,a}$ defined by (2.1) corresponds to the case $(2, 1+1)$ of their construction. Specifically, one starts with $f(u) = u^2$ (one double pole at $\infty \in \mathbb{P}^1_{/\mathbb{F}_q}$) and $g(v) = v + \gamma/v$ (one simple pole at 0 and one simple pole at ∞). One obtains, for any power Q of q, a smooth projective surface X_Q over $\mathbb{F}_q$ which is birational to the affine surface Y_Q defined in affine coordinates (u, v, t) by

$$Y_Q: \qquad f(u) - g(v) = t^Q - t.$$

The surface X_Q is equipped with a surjective morphism $\pi_Q : X_Q \to \mathbb{P}^1_{/\mathbb{F}_q}$, which extends the natural projection $Y_Q \to \mathbb{A}^1_{/\mathbb{F}_q}$ given by $(u, v, t) \mapsto t$. Writing $Q = q^a$ for some integer $a \geq 1$, the elliptic curve $E_{\gamma,a}$ over K then arises as the generic fiber of π_Q. The model (2.1) for $E_{\gamma,a}/K$ indeed appears naturally by putting the equation for the generic fiber of π_Q into Weierstrass form.

We wish to remark that one other case of the Pries–Ulmer construction is, for a good choice of parameters, "isogenous" to the case $(2, 1 + 1)$. Given an element $\gamma \in \mathbb{F}_q^\times$, consider the two rational maps $f, g : \mathbb{P}^1_{/\mathbb{F}_q} \to \mathbb{P}^1_{/\mathbb{F}_q}$ given by $f(u) = u^2$ and $g(v) = v^2 + \gamma/v^2$. In the terminology of [**13**], this input data has type $(2, 2 + 2)$ since f has a single double pole at ∞, and g has double poles at 0 and at ∞. For any power Q of q, let X_Q be the smooth projective surface over $\mathbb{F}_q$, fibered over $\mathbb{P}^1_{/\mathbb{F}_q}$ *via* $\pi_Q : X_Q \to \mathbb{P}^1_{/\mathbb{F}_q}$, which is birational to the affine surface Y_Q over $\mathbb{F}_q$ given by

$$Y_Q : \qquad f(u) - g(v) = t^Q - t$$

and such that the morphism $\pi_Q : X_Q \to \mathbb{P}^1_{/\mathbb{F}_q}$ extending $(u, v, t) \in Y_Q \mapsto t \in \mathbb{A}^1_{/\mathbb{F}_q}$ is minimal. Writing $Q = q^a$ for some integer $a \geq 1$, we denote by $E'_{\gamma,a}/K$ the generic fiber of π_Q. By construction, after clearing denominators, the curve $E'_{\gamma,a}$ is given in affine coordinates $(u, v) \in \mathbb{A}^2_{/K}$ by

$$E'_{\gamma,a} : \qquad u^2v^2 = v^4 + \wp_a(t)v^2 + \gamma.$$

The change of coordinates $(u, v) \mapsto (x, y) = \big(2v(u + v), 4v\big(uv + v^2 + \wp_a(t)\big)\big)$ then provides the following affine Weierstrass model for $E'_{\gamma,a}$ over K:

$$E'_{\gamma,a} : \qquad y^2 = \big(x + \wp_a(t)\big)\big(x^2 - 4\gamma\big).$$

Our main observation is:

PROPOSITION 2.1. *For any $\gamma \in \mathbb{F}_q^\times$ and any $a \geq 1$, the elliptic curve $E'_{\gamma,a}$ defined over K by the affine Weierstrass model*

$$E'_{\gamma,a} : \qquad y^2 = \big(x + \wp_a(t)\big)\big(x^2 - 4\gamma\big)$$

is 2-isogenous to $E_{\gamma,a}$ over K.

PROOF. Using the formulae in [**17**, Chap. III, Ex. 4.5], we find that the map

$$\phi : (x, y) \in E_{\gamma,a} \mapsto \big(y^2/x^2 - \wp_a(t), y\big(1 - \gamma/x^2\big)\big) \in E'_{\gamma,a},$$

which is clearly defined over K, provides the desired 2-isogeny. □

Since they are K-isogenous, the elliptic curves $E_{\gamma,a}$ and $E'_{\gamma,a}$ have the same conductor, they share the same L-function, and their Mordell-Weil ranks are equal. Therefore, our main results about the elliptic curves $E_{\gamma,a}$ (such as the explicit expression for their L-function, and the fact that they have large Tate-Shafarevich groups) are also valid for the curves $E'_{\gamma,a}$.

Furthermore, we know by [**13**, Coro. 3.1.4] that, for all $\gamma \in \mathbb{F}_q^\times$ and $a \geq 1$, the elliptic curves $E_{\gamma,a}$ and $E'_{\gamma,a}$ satisfy the BSD conjecture. The "geometric" calculations of [**13**, §6.2] also show that the Mordell-Weil group $E_{\gamma,a}(K)$ has rank 0. We will recover these two facts *via* a different method, as corollaries of our explicit expression for the L-function of $E_{\gamma,a}$ (see Theorem 5.3 and Corollary 5.4).

2.3. Bad reduction and invariants. We let $B_{\gamma,a} \subset M_K^\circ$ denote the subset corresponding to monic irreducible polynomials in $\mathbb{F}_q[t]$ which divide $\wp_a(t)^2 - 4\gamma$. Equivalently, $B_{\gamma,a}$ is the set of places $v \in M_K^\circ$ dividing the discriminant of the Weierstrass model (2.1) for $E_{\gamma,a}$.

PROPOSITION 2.2. *For any $\gamma \in \mathbb{F}_q^\times$ and any integer $a \geq 1$, the elliptic curve $E_{\gamma,a}$ has good reduction outside $B_{\gamma,a} \cup \{\infty\}$. Moreover, its places of bad reduction are as follows:*

Place v	*Reduction at v*	$\delta_v(E_{\gamma,a})$	$\nu_v(E_{\gamma,a})$
$v \in B_{\gamma,a}$	*Multiplicative (fiber of type $\mathbf{I}_1$)*	1	1
∞	*Additive (fiber of type $\mathbf{I}^*_{4q^a}$)*	$4q^a + 6$	2

where, for any place $v \in M_K$, we have denoted by $\delta_v(E_{\gamma,a})$ (resp. by $\nu_v(E_{\gamma,a})$) the order at v of the minimal discriminant divisor of $E_{\gamma,a}$ (resp. of its conductor divisor).

PROOF. This follows from a routine application of Tate's algorithm to compute the type of the fibers of bad reduction (as explained in [**16**, §IV.9]). □

From the above proposition, we deduce explicit expressions for the exponential differential height $H(E_{\gamma,a})$ and the "numerical" conductor $N(E_{\gamma,a})$ of $E_{\gamma,a}$ (as defined in §1.1):

$$H(E_{\gamma,a}) = q^{\frac{1}{12}\deg \Delta_{\min}(E_{\gamma,a})} = q^{(q^a+1)/2}, \quad \text{and} \quad N(E_{\gamma,a}) = q^{\deg \mathcal{N}(E_{\gamma,a})} = q^{2(q^a+1)}. \tag{2.3}$$

Indeed, since $p \neq 2$ and $\gamma \neq 0$, the polynomial $\wp_a(t)^2 - 4\gamma \in \mathbb{F}_q[t]$ is squarefree, and therefore we have

$$\sum_{v \in B_{\gamma,a}} \deg v = \sum_{v \mid \wp_a(t)^2 - 4\gamma} \deg v = \deg\left(\wp_a(t)^2 - 4\gamma\right) = 2q^a.$$

It is clear from (2.3) that we have $H(E_{\gamma,a}) = N(E_{\gamma,a})^{1/4}$.

The *Tamagawa number* $\tau(E_{\gamma,a})$ of $E_{\gamma,a}$ is the product over all places $v \in M_K$ of the number of components in the special fiber of the Néron model of $E_{\gamma,a}$ at v. It is also readily calculated from the above proposition with the help of the table on p. 365 of [**16**]. We find that the only contribution to $\tau(E_{\gamma,a})$ comes from the fiber above ∞: since the special fiber of $E_{\gamma,a}$ at ∞ has Kodaira type $\mathbf{I}^*_{4q^a}$, its group of components is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. We obtain that

$$\tau(E_{\gamma,a}) = 4. \tag{2.4}$$

REMARK 2.3. For the computation of the L-function in section 4, it will be useful to have minimal integral models of $E_{\gamma,a}$ at places in M_K° at our disposal. For a place $v \in M_K^\circ$, we find by comparing the valuation at v of the discriminant $\Delta_{\gamma,a}$ of the model (2.1) with the valuation at v of the minimal discriminant in the above table, that the Weierstrass model (2.1) is minimal and integral at v.

This computation of the invariants of $E_{\gamma,a}$ yields the following:

PROPOSITION 2.4. *As γ varies in $\mathbb{F}_q^\times$ and as $a \geq 1$ varies among integers, the elliptic curves $E_{\gamma,a}$ are pairwise non $\overline{K}$-isomorphic and pairwise non K-isogenous.*

PROOF. Two elliptic curves over K are $\overline{K}$-isomorphic if and only if they have the same j-invariant. It is obvious from (2.2) that $\deg j(E_{\gamma,a}) = 4a$ is strictly increasing when $a \geq 1$ grows. Also apparent on (2.2) is the fact that, for a fixed a, the position of the poles of $j(E_{\gamma,a})$ varies with $\gamma \in \mathbb{F}_q^\times$. Hence the first assertion.

In a similar vein, it follows from (2.3) that $\deg \mathcal{N}(E_{\gamma,a})$ increases with $a \geq 1$. Since two K-isogenous elliptic curves have equal conductor divisors, we conclude that $E_{\gamma,a}$ and $E_{\gamma,a'}$ cannot be K-isogenous for any $a \neq a'$. For a given $a \geq 1$ and distinct $\gamma, \gamma' \in \mathbb{F}_q^\times$, the curves $E_{\gamma,a}$ and $E_{\gamma',a}$ are not K-isogenous either, since the sets $B_{\gamma,a} \cup \{\infty\}$ and $B_{\gamma',a} \cup \{\infty\}$ of places where they have bad reduction differ (*i.e.* their conductor divisors have different supports). □

2.4. Torsion subgroup. We conclude this section by elucidating the structure of the torsion subgroup of the Mordell-Weil group $E_{\gamma,a}(K)$:

THEOREM 2.5. *For any $\gamma \in \mathbb{F}_q^\times$ and any integer $a \geq 1$, let $P_0 \in E_{\gamma,a}(K)$ be the point with coordinates $(0,0)$ in the Weierstrass model* (2.1)*. Then we have $E_{\gamma,a}(K)_{\mathrm{tors}} = \{\mathcal{O}, P_0\}$.*

We will show later on (Corollary 5.4) that the whole group $E_{\gamma,a}(K)$ is torsion, so that the above result provides a complete list of the K-rational points on $E_{\gamma,a}$.

PROOF. We see on (2.2) that the j-invariant of $E_{\gamma,a}$ is not a p-th power in K, so that Proposition 7.1 in [**19**, Lect. I] ensures that $E_{\gamma,a}(K)_{\mathrm{tors}}$ contains no point with p-th power order.

As was shown in the previous subsection, $E_{\gamma,a}$ has additive reduction at ∞. We may thus make use of Lemma 7.8 of [**15**], which asserts that the prime-to-p part of $E_{\gamma,a}(K)_{\mathrm{tors}}$ embeds into the group G_∞ of components of the special fiber at ∞ of the Néron model of $E_{\gamma,a}$. Since the reduction at ∞ is of type $\mathbf{I}^*_{4q^a}$, the table in §7.2 of [**15**] tells us that $G_\infty \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

Combining the last two paragraphs, we deduce that $E_{\gamma,a}(K)_{\mathrm{tors}}$ is isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2$. In particular, the torsion subgroup of $E_{\gamma,a}(K)$ consists only of 2-torsion points and we infer that $E_{\gamma,a}(K)_{\mathrm{tors}} = E_{\gamma,a}(K)[2]$.

The 2-torsion subgroup of $E_{\gamma,a}(\overline{K})$ is readily computed: it consists of 4 points, given in the homogenised version of (2.1) by

$$\mathcal{O} = [0:1:0], \quad P_0 = [0:0:1],$$
$$P_+ = \left[\wp_a(t) + \sqrt{\wp_a(t)^2 - 4\gamma} : 0 : -2\right], \quad P_- = \left[\wp_a(t) - \sqrt{\wp_a(t)^2 - 4\gamma} : 0 : -2\right].$$

Since $p \neq 2$ and $\gamma \neq 0$, the polynomial $\wp_a(t)^2 - 4\gamma \in \mathbb{F}_q[t]$ is squarefree, so that only the first two points are K-rational (the latter two are rational over the quadratic extension $K(\sqrt{\wp_a(t)^2 - 4\gamma})$ of K). We deduce that $E_{\gamma,a}(K)[2] = \{\mathcal{O}, P_0\}$. □

3. Preliminaries on character sums

In the next section (see Theorem 4.1), we will compute an explicit expression for the L-function of the curve $E_{\gamma,a}$ introduced above. To carry out this computation, we first need to set up some notation and conventions. These will be in force for the rest of the paper.

3.1. Gauss sums and Kloosterman sums. Let $\mathbb{F}$ be a finite field of odd characteristic p. Any additive character ψ on $\mathbb{F}$ may and will be assumed to take values in the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. For any finite extension $\mathbb{F}'/\mathbb{F}$, we denote the trace map by $\mathrm{Tr}_{\mathbb{F}'/\mathbb{F}} : \mathbb{F}' \to \mathbb{F}$. If ψ is an additive character on $\mathbb{F}$, then the composition $\psi \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}}$ is an additive character on $\mathbb{F}'$.

We denote by $\lambda : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times$ (or $\lambda_{\mathbb{F}}$ if confusion is likely to arise) the unique nontrivial multiplicative character of order 2 on $\mathbb{F}^\times$. We extend λ to the whole of $\mathbb{F}$ by setting $\lambda(0) := 0$.

Definition 3.1. For any additive character ψ on $\mathbb{F}$, define the *quadratic Gauss sum* $\mathrm{G}_{\mathbb{F}}(\psi, \lambda)$ by

$$\mathrm{G}_{\mathbb{F}}(\psi, \lambda) := -\sum_{x \in \mathbb{F}} \lambda(x)\psi(x).$$

Note our choice of normalising $\mathrm{G}_{\mathbb{F}}(\psi, \lambda)$ by multiplying the sum by -1. By construction, the sum $\mathrm{G}_{\mathbb{F}}(\psi, \lambda)$ is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta_p)$. Recall the following facts about Gauss sums:

(Ga 1) For any nontrivial additive character ψ on $\mathbb{F}$, any $\alpha \in \mathbb{F}^\times$ and any finite extension $\mathbb{F}'/\mathbb{F}$, define $\psi_{\mathbb{F}'}^{(\alpha)}$ by $x \mapsto \psi \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}}(\alpha x)$. (This map $\psi_{\mathbb{F}'}^{(\alpha)}$ is a nontrivial additive character on $\mathbb{F}'$.) Letting $\alpha' := \alpha^{|\mathbb{F}|}$, one has

$$\mathrm{G}_{\mathbb{F}'}(\psi_{\mathbb{F}'}^{(\alpha')}, \lambda_{\mathbb{F}'}) = \mathrm{G}_{\mathbb{F}'}(\psi_{\mathbb{F}'}^{(\alpha)}, \lambda_{\mathbb{F}'}).$$

(Ga 2) For any nontrivial additive character ψ on $\mathbb{F}$ and any finite extension $\mathbb{F}'/\mathbb{F}$, one has

$$\mathrm{G}_{\mathbb{F}'}(\psi \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}}, \lambda_{\mathbb{F}'}) = \mathrm{G}_{\mathbb{F}}(\psi, \lambda_{\mathbb{F}})^{[\mathbb{F}':\mathbb{F}]}.$$

(Ga 3) For any nontrivial additive character ψ on $\mathbb{F}$, one has $|\mathrm{G}_{\mathbb{F}}(\psi, \lambda)| = |\mathbb{F}|^{1/2}$ in any complex embedding of $\mathbb{Q}(\zeta_p)$.

(Ga 4) For any nontrivial additive character ψ on $\mathbb{F}$, the quotient $\mathrm{G}_{\mathbb{F}}(\psi, \lambda)/|\mathbb{F}|^{1/2}$ is a 4th root of unity (which may be explicitly determined).

These results are quite classical, and the reader is referred to [**9**, Chap. V, §2] for their proofs.

Definition 3.2. For $\alpha \in \mathbb{F}$ and an additive character ψ on $\mathbb{F}$, define the *Kloosterman sum* $\mathrm{Kl}_{\mathbb{F}}(\psi; \alpha)$ by

$$\mathrm{Kl}_{\mathbb{F}}(\psi; \alpha) := -\sum_{x \in \mathbb{F}^\times} \psi\left(x + \frac{\alpha}{x}\right). \tag{3.1}$$

Again, we point out our choice of normalising the sum by multiplying it by -1. One can show that the Kloosterman sum $\mathrm{Kl}_{\mathbb{F}}(\psi; \alpha)$ is a totally real algebraic integer in $\mathbb{Q}(\zeta_p)$ *i.e.*, $\mathrm{Kl}_{\mathbb{F}}(\psi; \alpha) \in \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. We remind the reader of the following facts about Kloosterman sums:

(Kl 1) For any nontrivial additive character ψ on $\mathbb{F}$ and any $\alpha \in \mathbb{F}^\times$, one has the identity (sometimes called Salié's formula):

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

(Kl 2) For any nontrivial additive character ψ on $\mathbb{F}$, any $\alpha \in \mathbb{F}$ and any finite extension $\mathbb{F}'/\mathbb{F}$, letting $\alpha' = \alpha^{|\mathbb{F}|}$, one has

$$\mathrm{Kl}_{\mathbb{F}'}(\psi \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}}; \alpha') = \mathrm{Kl}_{\mathbb{F}'}(\psi \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}}; \alpha).$$

(Kl 3) For any nontrivial additive character ψ on $\mathbb{F}$ and any $\alpha \in \mathbb{F}^\times$, there is a unique pair $\{\mathsf{kl}_{\mathbb{F}}(\psi;\alpha), \mathsf{kl}'_{\mathbb{F}}(\psi;\alpha)\}$ of algebraic integers, whose product is $|\mathbb{F}|$ and such that, for any finite extension $\mathbb{F}'/\mathbb{F}$, one has

$$\mathrm{Kl}_{\mathbb{F}'}(\psi \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}};\alpha) = \mathsf{kl}_{\mathbb{F}}(\psi;\alpha)^{[\mathbb{F}':\mathbb{F}]} + \mathsf{kl}'_{\mathbb{F}}(\psi;\alpha)^{[\mathbb{F}':\mathbb{F}]}.$$

(Kl 4) For any nontrivial additive character ψ on $\mathbb{F}$ and any $\alpha \in \mathbb{F}^\times$, one has $|\mathsf{kl}_{\mathbb{F}}(\psi;\alpha)| = |\mathsf{kl}'_{\mathbb{F}}(\psi;\alpha)| = |\mathbb{F}|^{1/2}$ in any complex embedding of $\overline{\mathbb{Q}}$. In particular, one has $|\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)| \leq 2|\mathbb{F}|^{1/2}$ in any complex embedding of $\mathbb{Q}(\zeta_p)$.

These results are classical: see [**9**, Chap. V, §5] for proofs thereof. For convenience, we also state here a fact that will only be proved later on (see Lemma 5.1 and Remark 6.2):

(Kl 5) For any nontrivial additive character ψ on $\mathbb{F}$ and any $\alpha \in \mathbb{F}^\times$, $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)$ is a p-adic unit in $\mathbb{Q}(\zeta_p)$. In particular, one has $0 < |\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)| < 2|\mathbb{F}|^{1/2}$ in any complex embedding of $\mathbb{Q}(\zeta_p)$.

3.2. Places of degree dividing a. Let $\mathbb{F}_q$ be a finite field of odd characteristic, and let $K := \mathbb{F}_q(t)$ denote the rational function field over $\mathbb{F}_q$.

Definition 3.3. For any integer $a \geq 1$, let $P_q(a)$ denote the set of places $v \in M_K$ such that $v \neq 0, \infty$ and $\deg v \mid a$. That is to say, $P_q(a)$ is the set of closed points of the multiplicative group $\mathbb{G}_{m/\mathbb{F}_q} = \mathbb{P}^1_{\mathbb{F}_q} \setminus \{0,\infty\}$ whose degree divides a. In the usual identification between places in M_K° and monic irreducible elements of $\mathbb{F}_q[t]$, the set $P_q(a)$ corresponds to the set of monic irreducible polynomials $B \in \mathbb{F}_q[t]$ such that $B \neq t$ and $\deg B \mid a$.

The latter interpretation allows for an easy estimation of the cardinality $|P_q(a)|$. Indeed the Prime Number Theorem for $\mathbb{F}_q[t]$ states that, for any integer $n \geq 1$, the number $\pi_q(n)$ of monic irreducible polynomials in $\mathbb{F}_q[t]$ of degree n satisfies: $q^n/n - q^{n/2} \leq \pi_q(n) \leq q^n/n$ (see, for instance, [**14**, Thm. 2.2] and its proof). Noting that $|P_q(a)| = -1 + \sum_{n|a} \pi_q(n)$, we deduce the existence of constants $c_q, c'_q > 0$, depending at most on q, such that

$$\forall a \geq 1, \qquad c'_q \cdot \frac{q^a}{a} \leq |P_q(a)| \leq c_q \cdot \frac{q^a}{a}. \tag{3.2}$$

3.3. The sums $\mathbf{g}(v)$ and $\mathbf{Kl}_\gamma(v)$. Let $\mathbb{F}_q$ be a finite field of odd characteristic p, and endow $\mathbb{F}_q$ with a nontrivial additive character ψ_q taking values in the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. For any finite extension $\mathbb{F}/\mathbb{F}_q$ we "lift" ψ_q to a nontrivial character $\psi_{\mathbb{F}}$ on $\mathbb{F}$ by composing ψ_q with the relative trace map; *i.e.*, we let $\psi_{\mathbb{F}} := \psi_q \circ \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q}$.

Definition 3.4. Let $\gamma \in \mathbb{F}_q^\times$ and $a \geq 1$ be an integer. For any place $v \in P_q(a)$, we denote by $\mathbb{F}_v$ the residue field of K at v, and by $d_v := [\mathbb{F}_v : \mathbb{F}_q]$ the degree of v.

Viewing v as the $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbit of an $\overline{\mathbb{F}_q}$-rational point of $\mathbb{G}_{m/\mathbb{F}_q}$, we may pick an element $\beta_v \in \mathbb{F}_v^\times \subset \overline{\mathbb{F}_q}^\times$ representing that orbit v. (The choices of representatives of v in $\overline{\mathbb{F}_q}^\times$ are then $\beta_v, \beta_v^q, \beta_v^{q^2}, \ldots, \beta_v^{q^{d_v-1}}$.) The map $\psi_{\mathbb{F}_v}^{(\beta_v)} : x \mapsto \psi_q \circ \mathrm{Tr}_{\mathbb{F}_v/\mathbb{F}_q}(\beta_v x)$ defines a nontrivial additive character on $\mathbb{F}_v$.

- We denote the Gauss sum $\mathrm{G}_{\mathbb{F}_v}(\psi_{\mathbb{F}_v}^{(\beta_v)}, \lambda_{\mathbb{F}_v})$ by $\mathbf{g}(v)$. A repeated application of (Ga 1) shows that the definition of $\mathbf{g}(v)$ makes sense, in that the value of the sum $\mathrm{G}_{\mathbb{F}_v}(\psi_{\mathbb{F}_v}^{(\beta_v)}, \lambda_{\mathbb{F}_v})$ does not depend on a particular choice of representative β_v for the orbit v.

- We denote the Kloosterman sum $\mathrm{Kl}_{\mathbb{F}_v}(\psi_{\mathbb{F}_v}^{(\beta_v)};\gamma)$ by $\mathsf{Kl}_\gamma(v)$, and we let $\{\mathsf{kl}_\gamma(v),\mathsf{kl}'_\gamma(v)\}$ be the pair of algebraic integers attached to the Kloosterman sum $\mathsf{Kl}_\gamma(v)$ as in (Kl 3). Again, these definitions make sense: repeated applications of (Kl 2) imply that the value of $\mathrm{Kl}_{\mathbb{F}_v}(\psi_{\mathbb{F}_v}^{(\beta_v)};\gamma)$, and hence the pair of algebraic integers attached to it by (Kl 3), do not depend on the choice of β_v in v.

4. The L-function of $E_{\gamma,a}$

The main objective of this section is to provide an explicit expression for the L-function of the elliptic curve $E_{\gamma,a}$. The resulting formula will prove instrumental for the proof of our main theorem. In the notation set up in the previous section, the result is as follows:

THEOREM 4.1. *Let $\mathbb{F}_q$ be a finite field of odd characteristic. For any $\gamma\in\mathbb{F}_q^\times$ and any $a\geq 1$, consider the elliptic curve $E_{\gamma,a}$ over $K=\mathbb{F}_q(t)$ defined by* (2.1). *The L-function $L(E_{\gamma,a},T)\in\mathbb{Z}[T]$ of $E_{\gamma,a}$ is given by:*

$$L(E_{\gamma,a},T)=\prod_{v\in P_q(a)}\big(1-\mathbf{g}(v)\mathsf{kl}_\gamma(v)T^{\deg v}\big)\big(1-\mathbf{g}(v)\mathsf{kl}'_\gamma(v)T^{\deg v}\big), \tag{4.1}$$

where $P_q(a)$ denotes the set of places defined in §3.2, and $\mathbf{g}(v)$, $\mathsf{kl}_\gamma(v)$, $\mathsf{kl}'_\gamma(v)$ denote the algebraic integers attached to any $v\in P_q(a)$ in §3.3.

The proof of this theorem occupies the rest of the section: the next subsection proves a useful identity between character sums, and the following subsection contains the computation leading to Theorem 4.1.

REMARK 4.2. (1) Given the definition of $\{\mathsf{kl}_\gamma(v),\mathsf{kl}'_\gamma(v)\}$ and formula (Kl 3), an equivalent way of formulating (4.1) is:

$$L(E_{\gamma,a},T)=\prod_{v\in P_q(a)}\big(1-\mathbf{g}(v)\mathsf{Kl}_\gamma(v)T^{\deg v}+\mathbf{g}(v)^2q^{\deg v}T^{2\deg v}\big). \tag{4.2}$$

(2) To define the sums $\mathbf{g}(v)$ and $\mathsf{Kl}_\gamma(v)$ for a place $v\in P_q(a)$, we started by fixing a nontrivial additive character ψ_q on $\mathbb{F}_q$. We remark that the expression for the L-function of $E_{\gamma,a}$ obtained in Theorem 4.1 is independent of this choice. Indeed, a different choice of ψ_q has the sole effect of permuting the factors in (4.1), for the L-function $L(E_{\gamma,a},T)$ has integral coefficients.

(3) By definition, we have $\sum_{v\in P_q(a)}\deg v=|\mathbb{G}_m(\mathbb{F}_{q^a})|=q^a-1$. Hence, as a polynomial in T, the L-function of $E_{\gamma,a}$ has degree

$$b(E_{\gamma,a})=\deg L(E_{\gamma,a},T)=2(q^a-1).$$

This is compatible with the Grothendieck–Ogg–Shafarevich formula and the value of $\deg\mathcal{N}(E_{\gamma,a})$ found in (2.3). Note that $b(E_{\gamma,a})$ is even.

4.1. An identity between character sums. For this subsection, we let $\mathbb{F}$ be a finite field of odd characteristic, which we equip with an additive character ψ. Denote by $\lambda_{\mathbb{F}}=\lambda:\mathbb{F}^\times\to\{\pm1\}$ the unique quadratic character on $\mathbb{F}^\times$, extended by $\lambda(0):=0$. For any $\gamma\in\mathbb{F}^\times$, define the double character sum

$$S(\mathbb{F},\psi,\gamma):=\sum_{z\in\mathbb{F}}\sum_{x\in\mathbb{F}}\lambda(x^3+zx^2+\gamma x)\psi(z).$$

Note that the terms with $x = 0$ do not contribute to the sum since $\lambda(0) = 0$. We may therefore disregard these terms and use the multiplicativity of λ to get:

$$S(\mathbb{F}, \psi, \gamma) = \sum_{x \neq 0} \lambda(x^2) \left\{ \sum_{z \in \mathbb{F}} \lambda\left(z + \frac{x^2 + \gamma}{x}\right) \psi(z) \right\}.$$

For a given $x \in \mathbb{F}^\times$, we put $u = z + (x^2 + \gamma)/x$ in the sum displayed between brackets: using the additivity of ψ and the definition of $\mathrm{G}_{\mathbb{F}}(\psi, \lambda)$, we obtain that

$$\sum_{z \in \mathbb{F}} \lambda\left(z + \frac{x^2 + \gamma}{x}\right) \psi(z) = \psi\left(-x - \frac{\gamma}{x}\right) \sum_{u \in \mathbb{F}} \lambda(u)\psi(u) = -\psi\left(-x - \frac{\gamma}{x}\right) \cdot \mathrm{G}_{\mathbb{F}}(\psi, \lambda).$$

Multiplying this identity by $\lambda(x^2)$, and summing over all $x \in \mathbb{F}^\times$ then yields that

$$S(\mathbb{F}, \psi, \gamma) = -\mathrm{G}_{\mathbb{F}}(\psi, \lambda) \cdot \sum_{x \in \mathbb{F}^\times} \lambda(x)^2 \psi\left(-x - \frac{\gamma}{x}\right).$$

Noting that $\lambda(x)^2 = 1$ for all $x \neq 0$ (because λ has order 2) and reindexing the sum by setting $y = -x$ entails that

$$S(\mathbb{F}, \psi, \gamma) = -\mathrm{G}_{\mathbb{F}}(\psi, \lambda) \cdot \sum_{y \in \mathbb{F}^\times} \psi\left(y + \frac{\gamma}{y}\right) = \mathrm{G}_{\mathbb{F}}(\psi, \lambda) \cdot \mathrm{Kl}_{\mathbb{F}}(\psi; \gamma).$$

We have thus proved:

LEMMA 4.3. *In the above setting, one has* $S(\mathbb{F}, \psi, \gamma) = \mathrm{G}_{\mathbb{F}}(\psi, \lambda) \cdot \mathrm{Kl}_{\mathbb{F}}(\psi; \gamma)$, *where the Gauss and Kloosterman sums are as defined in §3.1.*

Additionally, it is immediate to check that all three sums in the above identity vanish when ψ is trivial.

4.2. Proof of Theorem 4.1. Fix a parameter $\gamma \in \mathbb{F}_q^\times$ and an integer $a \geq 1$ as in the statement of the theorem. Our starting point for the computation is expression (4.3) below for the L-function of $E_{\gamma,a}$.

For any $\tau \in \overline{\mathbb{F}_q}$, we denote by $v_\tau \in M_K^\circ$ the corresponding place of K; we pick a minimal integral Weierstrass (affine) model of $E_{\gamma,a}/K$ at v_τ of the form $y^2 = f_\tau(x,t)$ where $f_\tau(x,t)$ is a monic cubic polynomial in x, with coefficients in $\mathbb{F}_q[t]$. Recall that $\lambda_{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n} \to \{\pm 1\}$ denotes the unique character of exact order 2 on $\mathbb{F}_{q^n}^\times$, extended by $\lambda_{\mathbb{F}_{q^n}}(0) := 0$ to the whole of $\mathbb{F}_{q^n}$. With this notation, one has the equality of formal power series:

$$\log L(E_{\gamma,a}, T) = -\sum_{n=1}^{\infty} \left(\sum_{\tau \in \mathbb{F}_{q^n}} \sum_{x \in \mathbb{F}_{q^n}} \lambda_{\mathbb{F}_{q^n}}\big(f_\tau(x,\tau)\big) \right) \frac{T^n}{n}. \tag{4.3}$$

This expression can be derived from the definition (1.1)-(1.2) of the L-function, just as in [**3**] (see Lemma 4.6 and the following paragraph there) or [**4**, §4]. Here, we have implicitly used the fact that $E_{\gamma,a}$ has additive reduction at the place ∞ (see Proposition 2.2) to ignore the local term corresponding to this place. At a place of additive reduction, the local Euler factor of $L(E_{\gamma,a}, T)$ in (1.2) is indeed trivial.

We next aim at giving a more explicit expression of the inner double sums in (4.3). As was pointed out in Remark 2.3, one can choose, for any $\tau \in \overline{\mathbb{F}_q}$,

$$f_\tau(x,t) = x^3 + \wp_a(t)x^2 + \gamma x.$$

For any integer $n \geq 1$, the inner double sum in (4.3) can thus be rewritten as

$$\sum_{\tau\in\mathbb{F}_{q^n}} \sum_{x\in\mathbb{F}_{q^n}} \lambda_{\mathbb{F}_{q^n}}\big(f_\tau(x,\tau)\big) = \sum_{z\in\mathbb{F}_{q^n}} \sum_{x\in\mathbb{F}_{q^n}} \big|\big\{\tau\in\mathbb{F}_{q^n} : \wp_a(\tau)=z\big\}\big| \cdot \lambda_{\mathbb{F}_{q^n}}\big(x^3+zx^2+\gamma x\big).$$

Moreover, Lemma 4.5 in [**3**] asserts that, for any $z \in \mathbb{F}_{q^n}$,

$$\big|\big\{\tau\in\mathbb{F}_{q^n} : \wp_a(\tau)=z\big\}\big| = \sum_{\beta\in\mathbb{F}_{q^n}\cap\mathbb{F}_{q^a}} \psi_q\circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta x).$$

For all $\beta \in \mathbb{F}_{q^n}$, the map $z \mapsto \psi_q \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta z)$ is an additive character on $\mathbb{F}_{q^n}$, which we denote by $\psi_{q^n}^{(\beta)}$. Hence, for any integer $n \geq 1$, we have

$$\sum_{\tau\in\mathbb{F}_{q^n}} \sum_{x\in\mathbb{F}_{q^n}} \lambda_{\mathbb{F}_{q^n}}\big(f_\tau(x)\big) = \sum_{\beta\in\mathbb{F}_{q^n}\cap\mathbb{F}_{q^a}} S(\mathbb{F}_{q^n}, \psi_{q^n}^{(\beta)}, \gamma),$$
$$\text{where } S(\mathbb{F}_{q^n}, \psi_{q^n}^{(\beta)}, \gamma) = \sum_{z\in\mathbb{F}_{q^n}} \sum_{x\in\mathbb{F}_{q^n}} \lambda_{\mathbb{F}_{q^n}}(x^3+zx^2+\gamma x)\psi_{q^n}^{(\beta)}(z).$$

Lemma 4.3 above now yields that $S(\mathbb{F}_{q^n}, \psi_{q^n}^{(\beta)}, \gamma) = \mathrm{G}_{\mathbb{F}_{q^n}}(\psi_{q^n}^{(\beta)}, \lambda) \cdot \mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n}^{(\beta)}; \gamma)$ for all $\beta \in \mathbb{F}_{q^n}$, where the Gauss and Kloosterman sums are as in §3.1. Combining the above equalities, we obtain that

$$-\log L(E_{\gamma,a}, T) = \sum_{n=1}^{\infty} \left(\sum_{\beta\in\mathbb{F}_{q^n}\cap\mathbb{F}_{q^a}} \mathrm{G}_{\mathbb{F}_{q^n}}(\psi_{q^n}^{(\beta)}, \lambda) \cdot \mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n}^{(\beta)}; \gamma) \right) \frac{T^n}{n}. \tag{4.4}$$

When $\beta = 0$, the additive character $\psi_{q^n}^{(\beta)}$ is trivial, so both $\mathrm{G}_{\mathbb{F}_{q^n}}(\psi_{q^n}^{(\beta)}, \lambda)$ and $\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n}^{(\beta)}; \gamma)$ vanish. For any $\beta \in (\mathbb{F}_{q^a} \cap \mathbb{F}_{q^n}) \setminus \{0\}$, we denote the place of K containing β by $v_\beta \in M_K^\circ$ (equivalently, v_β is the $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbit of β). The place v_β is not $0 \in M_K^\circ$ and has degree $\deg v_\beta = [\mathbb{F}_q(\beta) : \mathbb{F}_q]$, which divides both a and n. In particular, v_β belongs to $P_q(a)$.

Lemma 4.4. *In the notation of §3.3, one has* $\mathrm{G}_{\mathbb{F}_{q^n}}(\psi_{q^n}^{(\beta)}, \lambda) = \mathbf{g}(v_\beta)^{n/\deg v_\beta}$ *and* $\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n}^{(\beta)}; \gamma) = \mathbf{kl}_\gamma(v_\beta)^{n/\deg v_\beta} + \mathbf{kl}'_\gamma(v_\beta)^{n/\deg v_\beta}$.

Proof. For brevity, we write $d = \deg v_\beta$ (recall that d divides n). By multiplicativity of the trace in towers of extensions and because $\beta \in \mathbb{F}_{q^d}$, we have $\psi_{\mathbb{F}_{q^n}}^{(\beta)} = \psi_{\mathbb{F}_{q^d}}^{(\beta)} \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}$. Moreover, $\lambda = \lambda_{\mathbb{F}_{q^n}}$ coincides with $\lambda_{\mathbb{F}_{q^d}} \circ \mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}$. Hence, the Hasse–Davenport relation for Gauss sums (Ga 2) implies that

$$\mathrm{G}_{\mathbb{F}_{q^n}}(\psi_{q^n}^{(\beta)}, \lambda) = \mathrm{G}_{\mathbb{F}_{q^n}}(\psi_{q^d}^{(\beta)} \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}, \lambda_{\mathbb{F}_{q^d}} \circ \mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^d}}) = \mathrm{G}_{\mathbb{F}_{q^d}}(\psi_{q^d}^{(\beta)}, \lambda_{\mathbb{F}_{q^d}})^{[\mathbb{F}_{q^n}:\mathbb{F}_{q^d}]}.$$

Since, by definition, we have $\mathbf{g}(v_\beta) = \mathrm{G}_{\mathbb{F}_{q^d}}(\psi_{q^d}^{(\beta)}, \lambda_{\mathbb{F}_{q^d}})$, the first identity is proved. The second identity is proved in a similar fashion, using the Hasse–Davenport relation for Kloosterman sums (Kl 3). □

Plugging the identities of Lemma 4.4 into (4.4) and exchanging the order of summation yields that

$$\begin{aligned}&-\log L(E_{\gamma,a},T)\\&\quad=\sum_{\beta\in\mathbb{F}_{q^a}\setminus\{0\}}\sum_{\substack{n\geq 1\\ \deg v_\beta\mid n}}\left(\left(\mathbf{g}(v_\beta)\mathbf{kl}_\gamma(v_\beta)\right)^{n/\deg v_\beta}+\left(\mathbf{g}(v_\beta)\mathbf{kl}'_\gamma(v_\beta)\right)^{n/\deg v_\beta}\right)\frac{T^n}{n}.\end{aligned}$$

Upon reindexing the second sum (by setting $m=n/\deg v_\beta$), we obtain that

$$\begin{aligned}-\log L(E_{\gamma,a},T)=\sum_{\beta\in\mathbb{F}_{q^a}^\times}\frac{1}{\deg v_\beta}\Bigg\{&\sum_{m=1}^{\infty}\frac{(\mathbf{g}(v_\beta)\mathbf{kl}_\gamma(v_\beta)T^{\deg v_\beta})^m}{m}\\&+\sum_{m=1}^{\infty}\frac{(\mathbf{g}(v_\beta)\mathbf{kl}'_\gamma(v_\beta)T^{\deg v_\beta})^m}{m}\Bigg\}.\end{aligned}$$

Whence we have, by the formal power series identity $-\log(1-u)=\sum_{m=1}^{\infty}\frac{u^m}{m}$,

$$\begin{aligned}&\log L(E_{\gamma,a},T)\\&\quad=\sum_{\beta\in\mathbb{F}_{q^a}^\times}\frac{1}{\deg v_\beta}\log\left((1-\mathbf{g}(v_\beta)\mathbf{kl}_\gamma(v_\beta)T^{\deg v_\beta})(1-\mathbf{g}(v_\beta)\mathbf{kl}'_\gamma(v_\beta)T^{\deg v_\beta})\right).\end{aligned}$$

Finally we group the indices $\beta\in\mathbb{F}_{q^a}^\times$ corresponding to the same $v\in P_q(a)$, and get:

$$\begin{aligned}&\log L(E_{\gamma,a},T)\\&\quad=\sum_{v\in P_q(a)}\sum_{\beta\in v}\frac{1}{\deg v}\log\left((1-\mathbf{g}(v)\mathbf{kl}_\gamma(v)T^{\deg v})(1-\mathbf{g}(v)\mathbf{kl}'_\gamma(v)T^{\deg v})\right)\\&\quad=\sum_{v\in P_q(a)}\log\left((1-\mathbf{g}(v)\mathbf{kl}_\gamma(v)T^{\deg v})(1-\mathbf{g}(v)\mathbf{kl}'_\gamma(v)T^{\deg v})\right).\end{aligned}$$

To conclude the proof of Theorem 4.1, there only remains to exponentiate this identity. □

5. Non-vanishing of $L(E_{\gamma,a},T)$ at the central point and consequences

As before, let $\mathbb{F}_q$ be a finite field of odd characteristic p and $K:=\mathbb{F}_q(t)$. For any parameter $\gamma\in\mathbb{F}_q^\times$ and any integer $a\geq 1$, we consider the elliptic curve $E_{\gamma,a}$ defined over K by (2.1). In this section, we describe the behaviour of the L-function $z\mapsto L(E_{\gamma,a},z)$ around $z=1$ (see Theorem 5.3). We first gather some information about its p-adic slope sequence from Theorem 4.1 and results about Gauss and Kloosterman sums. We then derive an important corollary of this analytic study, namely the BSD conjecture for the elliptic curves $E_{\gamma,a}$ (see Corollary 5.4).

5.1. p-adic slopes of $L(E_{\gamma,a},T)$. We choose, once and for all, a prime ideal $\mathfrak{P}$ of $\overline{\mathbb{Q}}$ above p. We denote by $\mathrm{ord}_{\mathfrak{P}}:\overline{\mathbb{Q}}^\times\to\mathbb{Q}$ the corresponding discrete valuation, so normalised that $\mathrm{ord}_{\mathfrak{P}}(q)=1$. The goal of this subsection is to compute the p-adic slope sequence of $L(E_{\gamma,a},T)$ explicitly (see §1.3).

We first prove a probably well-known lemma for which we could not find a proof in the literature:

LEMMA 5.1. *Let $\mathbb{F}$ be a finite extension of $\mathbb{F}_q$, and ψ be a nontrivial additive character on $\mathbb{F}$. For any $\alpha \in \mathbb{F}^\times$, consider the Kloosterman sum $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)$ and the pair $\{\mathsf{kl}_{\mathbb{F}}(\psi;\alpha), \mathsf{kl}'_{\mathbb{F}}(\psi;\alpha)\}$ of algebraic integers associated to it by (KI3). Then we have*

$$\{\mathrm{ord}_{\mathfrak{P}}\, \mathsf{kl}_{\mathbb{F}}(\psi;\alpha), \mathrm{ord}_{\mathfrak{P}}\, \mathsf{kl}'_{\mathbb{F}}(\psi;\alpha)\} = \big\{0, [\mathbb{F}:\mathbb{F}_q]\big\}.$$

Equivalently, one has $\mathrm{ord}_{\mathfrak{P}}\, \mathrm{Kl}_{\mathbb{F}}(\psi;\alpha) = 0$.

The last statement is equivalent to the first assertion of (KI5). In the same setting, the $\mathfrak{P}$-adic valuation of the Gauss sum $\mathrm{G}_{\mathbb{F}}(\psi,\lambda)$ is easily determined: (Ga4) shows that the sums $\mathrm{G}_{\mathbb{F}}(\psi,\lambda)$ has the same $\mathfrak{P}$-adic valuation as $|\mathbb{F}|^{1/2}$, so that

$$\mathrm{ord}_{\mathfrak{P}}\, \mathrm{G}_{\mathbb{F}}(\psi,\lambda) = \frac{[\mathbb{F}:\mathbb{F}_q]}{2}. \tag{5.1}$$

PROOF. By construction, $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)$ is an element of $\mathbb{Q}(\zeta_p)$. The unique prime ideal of $\mathbb{Q}(\zeta_p)$ above p is the principal ideal $I = (\zeta_p - 1)$, so that $p \cdot \mathbb{Z}[\zeta_p] = I^{p-1}$. Since $\psi(y)$ is a power of ζ_p for all $y \in \mathbb{F}$, we have $\psi(y) \equiv 1 \bmod I$ and we find that

$$-\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha) \equiv \sum_{x\in\mathbb{F}^\times} 1 \equiv |\mathbb{F}| - 1 \equiv -1 \bmod I,$$

because $|\mathbb{F}|$ is a power of p. In particular, $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha) \not\equiv 0 \bmod p$ in $\overline{\mathbb{Q}}$, and we indeed have $\mathrm{ord}_{\mathfrak{P}}\, \mathrm{Kl}_{\mathbb{F}}(\psi;\alpha) = 0$.

On the other hand, (KI3) implies that the algebraic integers $\mathsf{kl}_{\mathbb{F}}(\psi;\alpha)$ and $\mathsf{kl}'_{\mathbb{F}}(\psi;\alpha)$ satisfy:

$$\mathsf{kl}_{\mathbb{F}}(\psi;\alpha) \cdot \mathsf{kl}'_{\mathbb{F}}(\psi;\alpha) = |\mathbb{F}| \quad \text{and} \quad \mathsf{kl}_{\mathbb{F}}(\psi;\alpha) + \mathsf{kl}'_{\mathbb{F}}(\psi;\alpha) = \mathrm{Kl}_{\mathbb{F}}(\psi;\alpha).$$

The pair $\{v, v'\}$ formed by their $\mathfrak{P}$-adic valuations thus satisfies the following constraints: $v, v' \geq 0$, $v + v' = \mathrm{ord}_{\mathfrak{P}}\, |\mathbb{F}| = [\mathbb{F}:\mathbb{F}_q]$, and $\min\{v, v'\} \leq \mathrm{ord}_{\mathfrak{P}}\, \mathrm{Kl}_{\mathbb{F}}(\psi;\alpha) = 0$. The only pair $\{v, v'\}$ fulfilling these requirements is $\{0, [\mathbb{F}:\mathbb{F}_q]\}$.

Hence the result. □

We can now state and prove the following:

THEOREM 5.2. *Let $\gamma \in \mathbb{F}_q^\times$ and $a \geq 1$. Consider the elliptic curve $E_{\gamma,a}/K$ defined by (2.1), and write $b = \deg L(E_{\gamma,a}, T)$. Recall from Remark 4.2(3) that $b = 2(q^a - 1)$ is even. The L-function $L(E_{\gamma,a}, T)$ has p-adic slope sequence*

$$\lambda_1 = \frac{1}{2},\ \lambda_2 = \frac{1}{2},\ \ldots,\ \lambda_{b/2} = \frac{1}{2},\ \lambda_{b/2+1} = \frac{3}{2},\ \lambda_{b/2+2} = \frac{3}{2},\ \ldots,\ \lambda_b = \frac{3}{2}.$$

PROOF. By definition (see §1.3), the p-adic slope sequence of $L(E_{\gamma,a}, T)$ is the (suitably indexed) multiset of $\mathfrak{P}$-adic valuations of the inverses of zeros of the L-function $z \mapsto L(E_{\gamma,a}, z)$.

Upon staring at the expression for $L(E_{\gamma,a}, T)$ obtained in Theorem 4.1, one immediately sees that an algebraic number $z \in \overline{\mathbb{Q}}$ is the inverse of a zero of $L(E_{\gamma,a}, T)$ if and only if there exists a place $v \in P_q(a)$ with $z^{\deg v} \in \{\mathbf{g}(v)\mathbf{kl}_\gamma(v), \mathbf{g}(v)\mathbf{kl}'_\gamma(v)\}$. In particular, if z is the inverse of a zero of $L(E_{\gamma,a}, T)$, there exists $v \in P_q(a)$ such that $\mathrm{ord}_{\mathfrak{P}}(z^{\deg v})$ equals one of $\mathrm{ord}_{\mathfrak{P}}(\mathbf{g}(v)\mathbf{kl}_\gamma(v))$ or $\mathrm{ord}_{\mathfrak{P}}(\mathbf{g}(v)\mathbf{kl}'_\gamma(v))$.

As can be seen from applying formula (5.1) in the case where $\mathrm{G}_{\mathbb{F}}(\psi,\lambda) = \mathbf{g}(v)$, we have $\mathrm{ord}_{\mathfrak{P}}\, \mathbf{g}(v) = \deg v/2$. The previous lemma applied to $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha) = \mathbf{Kl}_\gamma(v)$

further yields that $\{\mathrm{ord}_{\mathfrak{P}} \mathbf{kl}_\gamma(v), \mathrm{ord}_{\mathfrak{P}} \mathbf{kl}'_\gamma(v)\} = \{0, \deg v\}$. We therefore have

$$\mathrm{ord}_{\mathfrak{P}} z = \frac{\mathrm{ord}_{\mathfrak{P}}(z^{\deg v})}{\deg v} \in \left\{ \frac{\mathrm{ord}_{\mathfrak{P}} \mathbf{g}(v) + \mathrm{ord}_{\mathfrak{P}} \mathbf{kl}_\gamma(v)}{\deg v}, \frac{\mathrm{ord}_{\mathfrak{P}} \mathbf{g}(v) + \mathrm{ord}_{\mathfrak{P}} \mathbf{kl}'_\gamma(v)}{\deg v} \right\} = \left\{ \frac{1}{2}, \frac{3}{2} \right\}.$$

As was recalled in §1.3, the p-adic slope sequence $\{\lambda_k\}_{k=1}^b$ of $L(E_{\gamma,a}, T)$ admits the following symmetry: for a given $s \in [0,2]$, there are as many indices k such that $\lambda_k = s$ as there are indices k' such that $\lambda_{k'} = 2 - s$. From this observation and from the above display, we immediately conclude that, among the b slopes of the L-function $L(E_{\gamma,a}, T)$, half of them equal $1/2$ and the other half equal $3/2$.

The result follows by choosing a suitable numbering of these slopes. □

5.2. Non-vanishing at the central point. The following is a direct consequence of Theorem 5.2:

THEOREM 5.3. *For any $\gamma \in \mathbb{F}_q^\times$ and any $a \geq 1$, the L-function $L(E_{\gamma,a}, T)$ does not vanish at $T = q^{-1}$. In other words, one has $\mathrm{ord}_{T=q^{-1}} L(E_{\gamma,a}, T) = 0$.*

PROOF. Given the expression for $L(E_{\gamma,a}, T)$ of Theorem 4.1, it suffices to show that, for any $v \in P_q(a)$, the two factors

$$1 - \mathbf{g}(v)\mathbf{kl}_\gamma(v) q^{-\deg v} \qquad \text{and} \qquad 1 - \mathbf{g}(v)\mathbf{kl}'_\gamma(v) q^{-\deg v}$$

of $L(E_{\gamma,a}, q^{-1})$ are nonzero. As we have seen in the previous subsection, for all places $v \in P_q(a)$, we have

$$\{\mathrm{ord}_{\mathfrak{P}}(\mathbf{g}(v)\mathbf{kl}_\gamma(v)), \mathrm{ord}_{\mathfrak{P}}(\mathbf{g}(v)\mathbf{kl}'_\gamma(v))\} = \left\{ \frac{\deg v}{2}, \frac{3 \deg v}{2} \right\}.$$

Since $\mathrm{ord}_{\mathfrak{P}}(q^{\deg v}) = \deg v$, neither of $\mathbf{g}(v)\mathbf{kl}_\gamma(v)$ or $\mathbf{g}(v)\mathbf{kl}'_\gamma(v)$ can equal $q^{\deg v}$, and we are done. □

Remark 6.2 outlines an alternative proof of Theorem 5.3: there, we obtain the non-vanishing by relying on the "angular distribution" of the Gauss and Kloosterman sums.

5.3. The BSD conjecture for $E_{\gamma,a}$. Given the non-vanishing of $L(E_{\gamma,a}, T)$ at $T = q^{-1}$, we deduce from the BSD result (see Theorem 1.1) that the BSD conjecture holds for all the elliptic curves $E_{\gamma,a}$.

COROLLARY 5.4. *For all $\gamma \in \mathbb{F}_q^\times$ and all integers $a \geq 1$, one has:*

(1) The Mordell–Weil group $E_{\gamma,a}(K)$ consists of the two points $\mathcal{O}$ and $P_0 = (0,0)$.
(2) The Tate–Shafarevich group $Ш(E_{\gamma,a})$ is finite.
(3) The following identity holds:

$$L(E_{\gamma,a}, q^{-1}) = \frac{|Ш(E_{\gamma,a})|}{q^{-1} \cdot H(E_{\gamma,a})}. \tag{5.2}$$

That the elliptic curves $E_{\gamma,a}$ satisfy the BSD conjecture is not new: as was already mentioned in §2.2, it was first proved by Pries and Ulmer in [**13**], where the proof relies on the geometry of the minimal regular model of $E_{\gamma,a}$. Our proof appears to be largely independent of theirs. Pries and Ulmer have further shown (also by a geometric argument) that $E_{\gamma,a}(K)$ has rank 0 (see §6.2 in [**13**]).

PROOF. By Theorem 1.1*(1)*, the Mordell–Weil group $E_{\gamma,a}(K)$ is finite, hence coincides with its torsion subgroup. Theorem 2.5 then entails the first assertion. The second assertion is copied verbatim from the second item of Theorem 1.1. As for identity (5.2), it suffices to plug the values $|E_{\gamma,a}(K)| = 2$ and $\tau(E_{\gamma,a}) = 4$ (both calculated in §2.3) into the BSD formula (1.3). □

6. Distribution of the Kloosterman sums $\mathsf{Kl}_\gamma(v)$

In this section, we work in the following setting: we fix a finite field $\mathbb{F}_q$ of odd characteristic p, endowed with a nontrivial additive character ψ_q; we also choose, once and for all, an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. For any $\gamma \in \mathbb{F}_q^\times$ and any $a \geq 1$, we consider the elliptic curves $E_{\gamma,a}$ defined by (2.1).

In the next section, we will describe the asymptotic behaviour of $L(E_{\gamma,a}, q^{-1})$ as $a \to \infty$. Doing so will require some knowledge about the "angular distribution" in the complex plane of (the images under ι of) the algebraic integers $\mathbf{kl}_\gamma(v), \mathbf{kl}'_\gamma(v)$, for $v \in P_q(a)$. We therefore lay out, in this section, the relevant facts about that distribution.

6.1. Angles of Gauss and Kloosterman sums. For a place $v \in P_q(a)$, the Weil bounds (Ga 3) and (Kl 4) for Gauss and Kloosterman sums reveal that the images under ι of the algebraic integers $\mathbf{g}(v)$, $\mathbf{kl}_\gamma(v)$ and $\mathbf{kl}'_\gamma(v)$ lie on the complex circle $\{z \in \mathbb{C} : |z| = q^{\deg v/2}\}$. We may therefore introduce the following angles:

DEFINITION 6.1. For a place $v \in P_q(a)$,

- We know from (Ga 4) that the algebraic number $\mathbf{g}(v)/q^{\deg v/2}$ is a 4th root of unity. Thus, there is a unique $\boldsymbol{\varepsilon}(v) \in \{0, \pi/2, \pi, 3\pi/2\}$ such that
$$\iota(\mathbf{g}(v)) = q^{\deg v/2} \mathrm{e}^{i\boldsymbol{\varepsilon}(v)}.$$
- By (Kl 4), the complex number $\iota(\mathbf{Kl}_\gamma(v))$ is real with $|\iota(\mathbf{Kl}_\gamma(v))| \leq 2q^{\deg v/2}$. Hence there exists a unique angle $\boldsymbol{\theta}_\gamma(v) \in [0, \pi]$ such that
$$\iota(\mathbf{Kl}_\gamma(v)) = 2q^{\deg v/2} \cos \boldsymbol{\theta}_\gamma(v).$$

For all $v \in P_q(a)$, we remark that one has

$$\left\{\iota(\mathbf{kl}_\gamma(v)), \iota(\mathbf{kl}'_\gamma(v))\right\} = \left\{q^{\deg v/2}\mathrm{e}^{i\boldsymbol{\theta}_\gamma(v)}, q^{\deg v/2}\mathrm{e}^{-i\boldsymbol{\theta}_\gamma(v)}\right\}.$$

With this new notation, the expression for $L(E_{\gamma,a}, T)$ obtained in Theorem 4.1 becomes:

(6.1)
$$L(E_{\gamma,a}, T) = \prod_{v \in P_q(a)} \left(1 - \mathrm{e}^{i(\boldsymbol{\varepsilon}(v)+\boldsymbol{\theta}_\gamma(v))}(qT)^{\deg v}\right)\left(1 - \mathrm{e}^{i(\boldsymbol{\varepsilon}(v)-\boldsymbol{\theta}_\gamma(v))}(qT)^{\deg v}\right).$$

Note that, whilst the angles $\boldsymbol{\theta}_\gamma(v)$ individually depend on the choice of ι, the set $\{\boldsymbol{\theta}_\gamma(v)\}_{v \in P_q(a)}$ does not: a different choice of ι only permutes the various $\boldsymbol{\theta}_\gamma(v)$, since $L(E_{\gamma,a}, T)$ has integral coefficients.

Evaluating both sides of the above equality at $T = q^{-1}$ yields that

$$L(E_{\gamma,a}, q^{-1}) = \prod_{v \in P_q(a)} \left(1 + \mathrm{e}^{2i\boldsymbol{\varepsilon}(v)} - 2\mathrm{e}^{i\boldsymbol{\varepsilon}(v)} \cos \boldsymbol{\theta}_\gamma(v)\right). \tag{6.2}$$

REMARK 6.2. (1) For any $v \in P_q(a)$, Lemma 5.1 implies that the angle $\boldsymbol{\theta}_\gamma(v)$ does not lie in $\{0, \pi/2, \pi\}$. Indeed, were $\boldsymbol{\theta}_\gamma(v)$ to hit one of $0, \pi/2$ or π, then the sum $\mathbf{Kl}_\gamma(v)$ would equal $+2q^{\deg v/2}, 0$ or $-2q^{\deg v/2}$, respectively. This is incompatible with Lemma 5.1 since $\mathbf{Kl}_\gamma(v)$ would then not be a p-adic unit.

More generally, with the same construction as in Definition 6.1, one can associate an angle $\theta_{\mathbb{F},\psi,\alpha} \in [0,\pi]$ to any of the Kloosterman sums $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)$ introduced in §3.1. A straightforward adaptation of the above argument shows that $\theta_{\mathbb{F},\psi,\alpha} \notin \{0, \pi/2, \pi\}$, which directly implies the second assertion in (Kl 5).

(2) The previous item actually provides a second proof of the non-vanishing of the L-function $L(E_{\gamma,a}, T)$ at $T = q^{-1}$, as follows. It is clear that, for a place $v \in P_q(a)$, the factor indexed by v in the product (6.1) vanishes at $T = q^{-1}$ if and only if $\boldsymbol{\varepsilon}(v) \equiv \pm\boldsymbol{\theta}_\gamma(v) \bmod 2\pi$. By Definition 6.1 above, we know that $\boldsymbol{\varepsilon}(v) \in \{0, \pi/2, 3\pi/2, 2\pi\}$. What we have shown in item (1) proves that the v-th factor in (6.1) does not vanish at $T = q^{-1}$. Hence $L(E_{\gamma,a}, q^{-1})$ is nonzero.

6.2. Angular distribution of the sums $\mathbf{Kl}_\gamma(v)$. Recall that the Sato–Tate measure μ_∞ on $[0,\pi]$ is defined by $\mathrm{d}\mu_\infty := \frac{2}{\pi}\sin^2\theta\,\mathrm{d}\theta$. We denote by μ_a the discrete probability measure on $[0,\pi]$ supported on the set $\{\boldsymbol{\theta}_\gamma(v)\}_{v\in P_q(a)}$ of angles introduced in the previous subsection. In other words, we put

$$\mu_a := \frac{1}{|P_q(a)|}\sum_{v\in P_q(a)} \delta\{\boldsymbol{\theta}_\gamma(v)\},$$

where $\delta\{x\}$ denotes the Dirac delta measure at $x \in [0,\pi]$. Note that μ_a depends neither on the choice of a nontrivial additive character ψ_q on $\mathbb{F}_q$ nor on that of an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. The measure μ_a does depend on $\mathbb{F}_q$ and γ though, but we chose not to reflect this in the notation for brevity.

In a previous work, the first-named author has proved that, as $a \to \infty$, the sequence of measures $(\mu_a)_{a\geq 1}$ converges weak-$*$ to μ_∞ in a quantitative way. More specifically, Theorem 6.6 in [**3**] states that:

THEOREM 6.3. *In the above setting, given any continuously differentiable function $g : [0,\pi] \to \mathbb{C}$ and any $\gamma \in \mathbb{F}_q^\times$, as $a \geq 1$ tends to $+\infty$, one has*

$$\left|\int_{[0,\pi]} g\,\mathrm{d}\mu_a - \int_{[0,\pi]} g\,\mathrm{d}\mu_\infty\right| \ll_q \frac{a^{1/2}}{q^{a/4}}\cdot\int_0^\pi |g'(t)|\,\mathrm{d}t, \tag{6.3}$$

where the implicit constant is effective and depends at most on q.

The reader is referred to section 6 of [**3**] for a detailed proof of that statement. Note that μ_a is the same measure as the one denoted by ν_a there.

6.3. 'Small' angles of Kloosterman sums. As we have seen in Remark 6.2, the fact that $L(E_{\gamma,a}, T)$ does not vanish at $T = q^{-1}$ is equivalent to the statement that none of the angles $\boldsymbol{\theta}_\gamma(v)$ lies in $\{0, \pi/2, \pi\}$. In this subsection, we obtain a quantitative version of the fact that the set $\{\boldsymbol{\theta}_\gamma(v)\}_{v\in P_q(a)}$ "avoids" $\{0, \pi/2, \pi\}$.

THEOREM 6.4. *Let p be an odd prime number. There exists a constant $\sigma_p > 0$, depending at most on p, such that the following holds. Let $\mathbb{F}_q$ be a finite field of characteristic p endowed with a nontrivial additive character ψ_q, and fix an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. For any parameter $\gamma \in \mathbb{F}_q^\times$ and any integer $a \geq 1$, one has*

$$\{\boldsymbol{\theta}_\gamma(v)\}_{v\in P_q(a)} \subset \left[\varepsilon_a, \tfrac{\pi}{2} - \varepsilon_a\right] \cup \left[\tfrac{\pi}{2} + \varepsilon_a, \pi - \varepsilon_a\right] \quad \textit{where } \varepsilon_a = (q^a)^{-\sigma_p}.$$

In other words, the measure μ_a is supported on $\left[\varepsilon_a, \frac{\pi}{2} - \varepsilon_a\right] \cup \left[\frac{\pi}{2} + \varepsilon_a, \pi - \varepsilon_a\right]$.

Corollary 5.5 in [**3**] already shows that $\boldsymbol{\theta}_\gamma(v) \in \left[\varepsilon_a, \pi - \varepsilon_a\right]$ for all $v \in P_q(a)$; so we actually only need to prove that $|\boldsymbol{\theta}_\gamma(v) - \pi/2| \geq \varepsilon_a$. However, for convenience, we give a complete proof of Theorem 6.4.

The main tool to prove this result is the following version of Liouville's inequality, which is taken from the introduction of [**11**]. Let $P \in \mathbb{Z}[X]$ be a polynomial of degree N. For any algebraic number $\kappa \in \overline{\mathbb{Q}}$, let $ht(\kappa)$ denote its absolute logarithmic Weil height. If $P(\kappa) \neq 0$, then

$$\frac{\log|P(\kappa)|}{[\mathbb{Q}(\kappa):\mathbb{Q}]} \geq -\log\|P\|_1 - N \cdot ht(\kappa), \tag{6.4}$$

in any complex embedding of $\mathbb{Q}(\kappa)$. Here we have denoted by $\|P\|_1$ the sum of the absolute values of the coefficients of P. The reader is referred to [**11**] for this statement and its proof.

Proof of Theorem 6.4. In the setting of the theorem, we claim that there exists a constant $\sigma_p > 0$ such that, for all $v \in P_q(a)$, one has

$$\min\{\boldsymbol{\theta}_\gamma(v), |\boldsymbol{\theta}_\gamma(v) - \pi/2|, \pi - \boldsymbol{\theta}_\gamma(v)\} \geq (q^{\deg v})^{-\sigma_p}.$$

Since $\deg v$ divides a for all $v \in P_q(a)$, the theorem clearly follows from this claim.

In order to prove the claim, consider the algebraic number $\kappa := \mathbf{kl}_\gamma(v) q^{-\deg v/2}$. Up to replacing $\mathbf{kl}_\gamma(v)$ by $\mathbf{kl}'_\gamma(v)$, we can assume that $\iota(\kappa) = \mathrm{e}^{i\boldsymbol{\theta}_\gamma(v)}$. It is relatively easy to show that $[\mathbb{Q}(\kappa):\mathbb{Q}] \leq 2(p-1)$ and that $ht(\kappa) \leq \log(q^{\deg v/2})$, see [**3**, Lem. 5.3] for details. Let us now apply Liouville's inequality to κ with the following three polynomials: $P_1 = X - 1$, $P_2 = X + 1$ and $P_3 = X^4 - 1$.

By (KI5) or Remark 6.2, we know that $\kappa \notin \{1, i, -1\}$, so that $P_j(\kappa) \neq 0$ for $j \in \{1, 2, 3\}$. Combined with our estimates of the degree and of the height of κ, Liouville's inequality (6.4) yields that, for $j \in \{1, 2, 3\}$,

$$\begin{aligned} \log|\iota(P_j(\kappa))| &\geq -[\mathbb{Q}(\kappa):\mathbb{Q}](\log 2 + 4ht(\kappa)) \geq -2(p-1)(\log 2 + 2\log q^{\deg v}) \\ &\geq -6(p-1)\log q^{\deg v}. \end{aligned} \tag{6.5}$$

Besides, a quick analysis shows that, for any $\theta \in [0, \pi]$, one has

$$\begin{aligned} &|P_1(\mathrm{e}^{i\theta})| = |\mathrm{e}^{i\theta} - 1| \leq |\theta| = \theta, \\ &|P_2(\mathrm{e}^{i\theta})| = |\mathrm{e}^{i\theta} + 1| = |\mathrm{e}^{i(\theta-\pi)} - 1| \leq |\theta - \pi| = \pi - \theta, \\ \text{and} \quad &|P_3(\mathrm{e}^{i\theta})| = |\mathrm{e}^{4i\theta} - 1| = |\mathrm{e}^{i\theta} - i| \cdot |\mathrm{e}^{i\theta} + i|. \end{aligned}$$

Applying these inequalities to $\theta = \boldsymbol{\theta}_\gamma(v)$ and using (6.5), we directly obtain that

$$\boldsymbol{\theta}_\gamma(v) \geq |P_1(\kappa)| \geq (q^{\deg v})^{-6(p-1)}, \quad \text{and that} \quad \pi - \boldsymbol{\theta}_\gamma(v) \geq |P_2(\kappa)| \geq (q^{\deg v})^{-6(p-1)}.$$

By further noting that $q^{2\deg v} \geq 4$, we also get that

$$|\pi/2 - \boldsymbol{\theta}_\gamma(v)| \geq |P_3(\kappa)|/4 \geq (q^{\deg v})^{-6(p-1)}/4 \geq (q^{\deg v})^{-(6p-4)}.$$

The claim now follows immediately, with $\sigma_p = 6p - 4 > 0$ being a suitable choice of constant. □

7. Estimates of the central value $L(E_{\gamma,a}, q^{-1})$

The goal of this section is to prove a precise asymptotic estimate on the central value $L(E_{\gamma,a}, q^{-1})$ as $a \to \infty$. This will provide the crucial input for our bounds on the size of $Ш(E_{\gamma,a})$ in the next section.

The result is as follows:

THEOREM 7.1. *Let $\mathbb{F}_q$ be a finite field of odd characteristic, and $K = \mathbb{F}_q(t)$. There are positive constants c_1, c_2 (depending at most on q) such that: for any $\gamma \in \mathbb{F}_q^\times$ and any $a \geq 1$, the central value $L(E_{\gamma,a}, q^{-1})$ of the L-function of the elliptic curve $E_{\gamma,a}$ satisfies:*

$$-\frac{c_1}{a} \leq \frac{\log |L(E_{\gamma,a}, q^{-1})|}{\log H(E_{\gamma,a})} \leq \frac{c_2}{a}. \tag{7.1}$$

The proof of this theorem will be given in §7.2 after proving an intermediate result in the following subsection. The upper bound in (7.1) provides a slight improvement on the generic upper bound on the central value: for any non-isotrivial elliptic curve E over K with $L(E, q^{-1}) \neq 0$, it is known that

$$\frac{\log L(E, q^{-1})}{\log H(E)} \leq c_3 \cdot \frac{\log\log\log H(E)}{\log\log H(E)} \qquad (\text{as } H(E) \to \infty),$$

for some constant $c_3 > 0$. This can be proved by using the fact that the zeros of $L(E, T)$ become uniformly equidistributed on the circle $\{z \in \mathbb{C} : |z| = q^{-1}\}$ as $H(E) \to \infty$ (see [**6**, Thm. 7.5]). For easier comparison, note that $\log\log H(E_{\gamma,a})$ has the same order of magnitude as a, as was shown in (2.3).

The lower bound in (7.1) is, on the other hand, much stronger than the generic lower bound on the central value. For a non-isotrivial elliptic curve E with $L(E, q^{-1}) \neq 0$, the latter only yields that

$$-1 + \frac{c_4}{\log H(E)} \leq \frac{\log L(E, q^{-1})}{\log H(E)} \qquad (\text{as } H(E) \to \infty),$$

for some $c_4 < 0$. *Via* the BSD formula, this translates into a lower bound on the order of $Ш(E)$ which is weaker than the one we require to prove Theorem C*(3)*.

7.1. Convergence of a certain sequence. Let $a \in \mathbb{Z}_{\geq 1}$ and $\gamma \in \mathbb{F}_q^\times$. We keep the notation introduced in section 6. Consider the non-negative function $W : [0, \pi] \to \mathbb{R}$ defined by

$$W(\theta) := \begin{cases} -\log\left(\sin^2\theta \cdot \cos^2\theta\right) & \text{if } \theta \in [0,\pi] \setminus \{0, \pi/2, \pi\}, \\ 0 & \text{if } \theta \in \{0, \pi/2, \pi\}. \end{cases}$$

The function $\theta \mapsto W(\theta)$ is continuously differentiable on $(0, \pi/2) \cup (\pi/2, \pi)$ and, for all $\theta \in [0, \pi]$, it satisfies $W(\pi - \theta) = W(\theta)$. Moreover, a routine check shows that W is integrable on $[0, \pi]$ for the Lebesgue measure, as well as for the Sato–Tate measure μ_∞. By Remark 6.2, the function W is also integrable for the measure μ_a introduced in §6.2: it thus makes sense to consider the sequence $I_W = \left(\int_{[0,\pi]} W \, \mathrm{d}\mu_a\right)_{a \geq 1}$. Even though we know, by Theorem 6.3, that $(\mu_a)_{a\geq 1}$ converges weak-$*$ to μ_∞, we cannot directly conclude that the sequence I_W converges because W is not continuous on $[0, \pi]$.

Nonetheless, the goal of this subsection is to show the following:

PROPOSITION 7.2. *In the above setting, the sequence* $\left(\int_{[0,\pi]} W \,\mathrm{d}\mu_a\right)_{a\geq 1}$ *converges to* $\int_{[0,\pi]} W \,\mathrm{d}\mu_\infty$. *More precisely, one has*

$$\left|\int_{[0,\pi]} W \,\mathrm{d}\mu_a - \int_{[0,\pi]} W \,\mathrm{d}\mu_\infty\right| \ll_q \frac{a^{3/2}}{q^{a/4}} \qquad (\text{as } a \to \infty),$$

where the implicit constant is effective and depends at most on q.

Even though the exact value of the limit is of little importance to us, one can actually compute that $\int_{[0,\pi]} W \,\mathrm{d}\mu_\infty = \log(16)$. Using the definition of the measure μ_a, the above result can thus be rewritten in a more explicit form:

$$\frac{1}{|P_q(a)|} \sum_{v\in P_q(a)} \log\big(\sin^2 \boldsymbol{\theta}_\gamma(v) \cdot \cos^2 \boldsymbol{\theta}_\gamma(v)\big) = -\log(16) + O_q\left(\frac{a^{3/2}}{q^{a/4}}\right) \quad (\text{as } a \to \infty).$$

PROOF. We pick, once and for all, a nondecreasing continuously differentiable function $\beta_0 : [0,1] \to [0,1]$ such that $\beta_0(x) = 0$ for all $x \in [0,1/3]$, and $\beta_0(x) = 1$ for all $x \in [2/3,1]$. For a small enough $\varepsilon > 0$, we define a "smoothing" function $\beta_\varepsilon : [0,\pi] \to [0,1]$ as follows: define β_ε on $[0,\pi/2]$ by

$$\beta_\varepsilon(\theta) := \begin{cases} \beta_0(\theta/\varepsilon) & \text{if } \theta \in [0,\varepsilon], \\ 1 & \text{if } \theta \in [\varepsilon, \pi/2-\varepsilon], \\ \beta_0((\pi/2-\theta)/\varepsilon) & \text{if } \theta \in [\pi/2-\varepsilon, \pi/2], \end{cases}$$

and extend it to $[0,\pi]$ by requiring that $\beta_\varepsilon(\pi-\theta) = \beta_\varepsilon(\theta)$ for all $\theta \in [0,\pi]$.

For any $\varepsilon > 0$, we put $W_\varepsilon := W \cdot \beta_\varepsilon$. The function $W_\varepsilon : [0,\pi] \to \mathbb{R}$ is continuously differentiable on the whole interval $[0,\pi]$, it coincides with W on $[\varepsilon, \pi/2-\varepsilon] \cup [\pi/2+\varepsilon, \pi-\varepsilon]$, and it satisfies $W_\varepsilon(\pi-\theta) = W_\varepsilon(\theta)$ for all $\theta \in [0,\pi]$. Let us also record the following estimates:

LEMMA 7.3. *For all* $\varepsilon \in (0,1/4)$, *one has*

(a) $\displaystyle\int_0^\pi |W_\varepsilon'(t)| \,\mathrm{d}t = O\big(|\log\varepsilon|\big)$, *(b)* $\displaystyle\int_{[0,\pi]} |W - W_\varepsilon| \,\mathrm{d}\mu_\infty = O\big(\varepsilon|\log\varepsilon|\big)$.

We postpone proving these two bounds until the end of the section, and carry on with the proof of Proposition 7.2. In the notation introduced above, the triangle inequality yields that

$$\left|\int_{[0,\pi]} W \,\mathrm{d}\mu_a - \int_{[0,\pi]} W \,\mathrm{d}\mu_\infty\right| \leq \int_{[0,\pi]} |W - W_\varepsilon| \,\mathrm{d}\mu_a + \left|\int_{[0,\pi]} W_\varepsilon \,\mathrm{d}\mu_a - \int_{[0,\pi]} W_\varepsilon \,\mathrm{d}\mu_\infty\right| + \int_{[0,\pi]} |W - W_\varepsilon| \,\mathrm{d}\mu_\infty. \tag{7.2}$$

We treat each of the three terms appearing in the right-hand side of this inequality separately.

The third term $\int_{[0,\pi]} |W - W_\varepsilon| \,\mathrm{d}\mu_\infty$ can be directly bounded with the help of Lemma 7.3*(b)*.

To show that the middle term is small when $a \to \infty$, we apply Theorem 6.3 to W_ε, which is permissible since W_ε is continuously differentiable on $[0,\pi]$. We obtain that

$$\left| \int_{[0,\pi]} W_\varepsilon \, \mathrm{d}\mu_a - \int_{[0,\pi]} W_\varepsilon \, \mathrm{d}\mu_\infty \right| \ll_q \frac{a^{1/2}}{q^{a/4}} \cdot \int_0^\pi |W_\varepsilon'(t)| \, \mathrm{d}t \ll_q \frac{a^{1/2}}{q^{a/4}} \cdot |\log \varepsilon|,$$

where the last inequality follows from Lemma 7.3*(a)*.

Finally, we claim that the first term $\int_{[0,\pi]} |W - W_\varepsilon| \, \mathrm{d}\mu_a$ on the right-hand side of (7.2) vanishes provided that $\varepsilon > 0$ is small enough. Indeed, we know by Theorem 6.4 that the support of μ_a is contained in $[\varepsilon_a, \pi/2 - \varepsilon_a] \cup [\pi/2 + \varepsilon_a, \pi - \varepsilon_a]$ where $\varepsilon_a = (q^a)^{-\sigma_p}$ for some constant $\sigma_p > 0$. By the proof of that theorem, one can take $\sigma_p = 6p - 4$. On the other hand, as was noted in a previous paragraph, W and W_ε coincide on $[\varepsilon, \pi/2 - \varepsilon] \cup [\pi/2 + \varepsilon, \pi - \varepsilon]$. Hence, choosing $\varepsilon < \varepsilon_a$, we have $\int_{[0,\pi]} |W - W_\varepsilon| \, \mathrm{d}\mu_a = 0$.

Summing up these three contributions, inequality (7.2) yields that

$$\left| \int_{[0,\pi]} W \, \mathrm{d}\mu_a - \int_{[0,\pi]} W \, \mathrm{d}\mu_\infty \right| \ll_q 0 + \frac{a^{1/2}}{q^{a/4}} \cdot |\log \varepsilon| + \varepsilon |\log \varepsilon|,$$

for all $\varepsilon < \varepsilon_a$. Note that $(q^a)^{-6q} < \varepsilon_a$ because $6q > 6p - 4 = \sigma_p$. We may therefore take $\varepsilon = (q^a)^{-6q}$, and this choice provides the desired bound. □

Proof of Lemma 7.3. Both W and W_ε are periodic of period $\pi/2$ and are symmetric around $\pi/4$ (*i.e.*, $W(\pi/2 - \theta) = W(\theta)$ for all $\theta \in [0, \pi/2]$, and similarly for W_ε). The same holds for $|W_\varepsilon'|$ and $|W - W_\varepsilon|$. We are thus reduced to proving the following two bounds:

(a') $\displaystyle\int_0^{\pi/4} |W_\varepsilon'(t)| \, \mathrm{d}t \ll |\log \varepsilon|,$ *(b')* $\displaystyle\int_{[0,\pi/2]} |W - W_\varepsilon| \, \mathrm{d}\mu_\infty \ll \varepsilon |\log \varepsilon|.$

To that end, we first gather a few useful remarks:

(i) Since $W_\varepsilon = W \cdot \beta_\varepsilon$ and since $0 \le \beta_\varepsilon(t) \le 1$, we have
$$\forall t \in [0,\pi], \qquad |W_\varepsilon'(t)| \le |W'(t)| + |\beta_\varepsilon'(t)| W(t).$$

(ii) By construction of β_ε, we have $|\beta_\varepsilon'(t)| = 0$ for all $t \in [\varepsilon, \pi/4]$ and $|\beta_\varepsilon'(t)| \le M/\varepsilon$ for $t \in [0, \varepsilon]$, where $M := \sup_{x \in [0,1]} |\beta_0'(x)|$.

(iii) The function W_ε is constant (equal to 0) on $[0, \varepsilon/3]$, so that $W_\varepsilon'(t) = 0$ for all $t \in (0, \varepsilon/3)$.

(iv) The functions W and W_ε are symmetric around $\pi/4$, and they coincide on $[\varepsilon, \pi/2 - \varepsilon]$. Moreover, we have
$$\forall t \in [0, \pi/2], \qquad |W(t) - W_\varepsilon(t)| = (1 - \beta_\varepsilon(t)) W(t) \le W(t).$$

(v) For $t \in (0, \pi/4]$, classical convexity inequalities imply that $(\sin t)^{-1} \le \pi/(2t)$ and $(\cos t)^{-1} \le \pi/(\pi - 2t)$. We deduce that
$$W(t) = 2 \log \left((\sin t \cdot \cos t)^{-1} \right) \le 2 \log \left(\frac{\pi^2}{2t(\pi - 2t)} \right) \le 2 \log \frac{\pi}{t},$$
for all t in this interval. In particular, this yields that
$$\int_0^\varepsilon W(t) \, \mathrm{d}t \le -2 \int_0^\varepsilon \log \frac{t}{\pi} \, \mathrm{d}t \ll \varepsilon |\log \varepsilon|.$$

(vi) For all $t \in (0, \pi/4]$, a simple calculation shows that

$$W'(t) = 2\left(\frac{\sin t}{\cos t} - \frac{\cos t}{\sin t}\right) = -\frac{2\cos(2t)}{\sin t \cdot \cos t}.$$

Thus, using the same classical inequalities as in the previous item, we obtain that, for all $t \in (0, \pi/4]$,

$$|W'(t)| \leq \frac{2}{\sin t \cdot \cos t} \leq \frac{2\pi^2}{2t(\pi - 2t)} \leq \frac{2\pi}{t}.$$

We now combine the above items to derive the desired inequalities. First, we have

$$\int_0^\varepsilon |W'_\varepsilon(t)|\,\mathrm{d}t \overset{\text{by (iii)}}{=} \int_{\varepsilon/3}^\varepsilon |W'_\varepsilon(t)|\,\mathrm{d}t \overset{\text{by (i)}}{\leq} \int_{\varepsilon/3}^\varepsilon |W'(t)|\,\mathrm{d}t + \int_{\varepsilon/3}^\varepsilon W(t)|\beta'_\varepsilon(t)|\,\mathrm{d}t$$
$$\overset{\text{by (vi), (ii)}}{\leq} \int_{\varepsilon/3}^\varepsilon \frac{2\pi}{t}\,\mathrm{d}t + \int_{\varepsilon/3}^\varepsilon W(t)\frac{M}{\varepsilon}\,\mathrm{d}t \overset{\text{by (v)}}{\ll} |\log\varepsilon|.$$

Furthermore, we have

$$\int_\varepsilon^{\pi/4} |W'_\varepsilon(t)|\,\mathrm{d}t \overset{\text{by (i)}}{\leq} \int_\varepsilon^{\pi/4} |W'(t)|\,\mathrm{d}t + \int_\varepsilon^{\pi/4} W(t)|\beta'_\varepsilon(t)|\,\mathrm{d}t$$
$$\overset{\text{by (vi), (ii)}}{\leq} \int_\varepsilon^{\pi/4} \frac{2\pi}{t}\,\mathrm{d}t \ll |\log\varepsilon|.$$

Summing the last two displays proves *(a')*. Finally, we notice that

$$\int_{[0,\pi/2]} |W - W_\varepsilon|\,\mathrm{d}\mu_\infty = \frac{2}{\pi}\int_0^{\pi/2} |W(t) - W_\varepsilon(t)|\sin^2(t)\,\mathrm{d}t$$
$$\leq \frac{2}{\pi}\int_0^{\pi/2} |W(t) - W_\varepsilon(t)|\,\mathrm{d}t \overset{\text{by (iv)}}{\leq} \frac{4}{\pi}\int_0^\varepsilon W(t)\,\mathrm{d}t \overset{\text{by (v)}}{\ll} \varepsilon|\log\varepsilon|,$$

which proves *(b')* and concludes the proof of the lemma. □

7.2. Proof of Theorem 7.1. With Proposition 7.2 at hand, we may now proceed to prove Theorem 7.1. In the notation introduced in the previous sections, we begin by taking the logarithm of identity (6.2):

$$\log L(E_{\gamma,a}, q^{-1}) = \log|L(E_{\gamma,a}, q^{-1})|$$
$$= \sum_{v\in P_q(a)} \log\left|1 + \mathrm{e}^{2i\boldsymbol{\varepsilon}(v)} - 2\mathrm{e}^{i\boldsymbol{\varepsilon}(v)}\cos\boldsymbol{\theta}_\gamma(v)\right|$$
$$= \sum_{v\in P_q(a)} \log|F_v(\boldsymbol{\theta}_\gamma(v))|, \tag{7.3}$$

where the functions $F_v : [0, \pi] \to \mathbb{R}$ are defined as follows:

$$\forall v \in P_q(a), \qquad F_v : \theta \mapsto \begin{cases} 2 - 2\cos\theta & \text{if } \boldsymbol{\varepsilon}(v) = 0, \\ -2i\cos\theta & \text{if } \boldsymbol{\varepsilon}(v) = \pi/2, \\ 2 + 2\cos\theta & \text{if } \boldsymbol{\varepsilon}(v) = \pi, \\ 2i\cos\theta & \text{if } \boldsymbol{\varepsilon}(v) = 3\pi/2. \end{cases}$$

Note that $|F_v(\boldsymbol{\theta}_\gamma(v))| > 0$ for all $v \in P_q(a)$ because $\boldsymbol{\theta}_\gamma(v) \notin \{0, \pi/2, \pi\}$ by (KI5) (see Remark 6.2). Straightforward analytic estimates show that, for any place $v \in P_q(a)$, one has

$$\forall \theta \in [0,\pi], \qquad \sin^2\theta \cdot \cos^2\theta \leq |F_v(\theta)| \leq 4.$$

In particular, writing $W(\theta) = -\log\left(\sin^2\theta \cdot \cos^2\theta\right)$ as in §7.1, we obtain that

$$\forall v \in P_q(a), \qquad -W(\boldsymbol{\theta}_\gamma(v)) \leq \log|F_v(\boldsymbol{\theta}_\gamma(v))| \leq \log 4.$$

Summing this chain of inequalities over all $v \in P_q(a)$ and using equality (7.3) yields:

$$\frac{1}{\log H(E_{\gamma,a})} \cdot \sum_{v\in P_q(a)} -W(\boldsymbol{\theta}_\gamma(v)) \leq \frac{\log L(E_{\gamma,a}, q^{-1})}{\log H(E_{\gamma,a})} \leq \log 4 \cdot \frac{|P_q(a)|}{\log H(E_{\gamma,a})}.$$

It is clear from these inequalities that Theorem 7.1 will be proved once we show the following two assertions:

(C_1) There exists a constant $c_1 > 0$ such that

$$\frac{1}{\log H(E_{\gamma,a})} \sum_{v\in P_q(a)} W(\boldsymbol{\theta}_\gamma(v)) \leq \frac{c_1}{a},$$

(C_2) There exists a constant $c_2 > 0$ such that $\dfrac{|P_q(a)|}{\log H(E_{\gamma,a})} \leq \dfrac{c_2}{a}$.

We thus now prove these two claims. The second one (C_2) is a direct consequence of the following two estimates: we know from (2.3) that $\log H(E_{\gamma,a}) \gg_q q^a$, and from (3.2) that $|P_q(a)| \ll_q q^a/a$.

Next we turn to the proof of (C_1): by Proposition 7.2, we have

$$\frac{1}{|P_q(a)|} \sum_{v\in P_q(a)} W(\boldsymbol{\theta}_\gamma(v)) = \int_{[0,\pi]} W \,\mathrm{d}\mu_\infty + O_q\left(\frac{a^{3/2}}{q^{a/4}}\right),$$

as $a \to \infty$, where the implicit constant depends at most on q. Therefore, making use of the estimate in (C_2) which we have just proved, we obtain that

$$\begin{aligned} 0 \leq \frac{1}{\log H(E_{\gamma,a})} \sum_{v\in P_q(a)} W(\boldsymbol{\theta}_\gamma(v)) &= \frac{|P_q(a)|}{\log H(E_{\gamma,a})} \cdot \frac{1}{|P_q(a)|} \sum_{v\in P_q(a)} W(\boldsymbol{\theta}_\gamma(v)) \\ &\leq \frac{c_2}{a}\left(\int_{[0,\pi]} W \,\mathrm{d}\mu_\infty + O_q\left(\frac{a^{3/2}}{q^{a/4}}\right)\right) \leq \frac{c_1}{a}, \end{aligned}$$

for some constant $c_1 > 0$, depending at most on q. This proves the first claim (C_1) and concludes the proof of Theorem 7.1. □

8. Proof of Theorem C

In this section, we gather our results so far to prove our main result (Theorem C in the introduction). We have already proved assertions *(1)* and *(2)* of that theorem: see Proposition 2.4 and Corollary 5.4*(2)*, respectively. In the following two subsections, we prove assertions *(4)* and *(3)* of Theorem C, in this order.

8.1. The p-primary part of $Ш(E_{\gamma,a})$. Let us first prove assertion *(4)* of Theorem C, concerning the p-primary part of $Ш(E_{\gamma,a})$:

THEOREM 8.1. *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 $E_{\gamma,a}$ over K defined by* (2.1)*. Then the p-primary part of $Ш(E_{\gamma,a})$ is trivial. In other words, the integer $|Ш(E_{\gamma,a})|$ is relatively prime to p.*

PROOF. Recall from §5.1 that $\mathrm{ord}_{\mathfrak{P}} : \overline{\mathbb{Q}}^\times \to \mathbb{Q}$ denotes an extension of the p-adic value to $\overline{\mathbb{Q}}$, normalised so that $\mathrm{ord}_{\mathfrak{P}}(q) = 1$. Taking $\mathfrak{P}$-adic valuation of both sides of the BSD formula (5.2), we obtain that

$$\mathrm{ord}_{\mathfrak{P}} |Ш(E_{\gamma,a})| = \mathrm{ord}_{\mathfrak{P}} L(E_{\gamma,a}, q^{-1}) + \mathrm{ord}_{\mathfrak{P}} H(E_{\gamma,a}) - 1. \tag{8.1}$$

Our formula (2.3) for the height of $E_{\gamma,a}$ implies that $\mathrm{ord}_{\mathfrak{P}} H(E_{\gamma,a}) - 1 = (q^a - 1)/2$. To conclude the proof, it thus suffices to see that $\mathrm{ord}_{\mathfrak{P}} L(E_{\gamma,a}, q^{-1}) = -(q^a - 1)/2$. Indeed, one would then deduce from (8.1) that $\mathrm{ord}_{\mathfrak{P}} |Ш(E_{\gamma,a})| = 0$, and this would directly show that $Ш(E_{\gamma,a})$ has trivial p-primary part (by the structure theorem for finite abelian groups).

We now proceed to compute $\mathrm{ord}_{\mathfrak{P}} L(E_{\gamma,a}, q^{-1})$. Evaluating at $T = q^{-1}$ the expression for $L(E_{\gamma,a}, T)$ obtained in Theorem 4.1, and taking $\mathfrak{P}$-adic valuations on both sides of the resulting identity yields that

$$\mathrm{ord}_{\mathfrak{P}} L(E_{\gamma,a}, q^{-1}) = \sum_{v \in P_q(a)} \mathrm{ord}_{\mathfrak{P}} \left(1 - \frac{\mathbf{g}(v)\mathbf{kl}_\gamma(v)}{q^{\deg v}}\right) + \mathrm{ord}_{\mathfrak{P}} \left(1 - \frac{\mathbf{g}(v)\mathbf{kl}'_\gamma(v)}{q^{\deg v}}\right).$$

The results proved in §5.1 imply that, for all places $v \in P_q(a)$, we have

$$\left\{\mathrm{ord}_{\mathfrak{P}} \left(\mathbf{g}(v)\mathbf{kl}_\gamma(v) q^{-\deg v}\right), \mathrm{ord}_{\mathfrak{P}} \left(\mathbf{g}(v)\mathbf{kl}'_\gamma(v) q^{-\deg v}\right)\right\} = \left\{-\frac{\deg v}{2}, \frac{\deg v}{2}\right\}.$$

Using the cases of equality in the non-archimedean triangle inequality, we then obtain that

$$\mathrm{ord}_{\mathfrak{P}} L(E_{\gamma,a}, q^{-1}) = \sum_{v \in P_q(a)} \min\left\{0, -\frac{\deg v}{2}\right\} + \min\left\{0, \frac{\deg v}{2}\right\} = -\frac{1}{2} \sum_{v \in P_q(a)} \deg v.$$

As has already been observed, we have $\sum_{v \in P_q(a)} \deg v = |\mathbb{G}_m(\mathbb{F}_{q^a})| = q^a - 1$. We therefore conclude that $\mathrm{ord}_{\mathfrak{P}} L(E_{\gamma,a}, q^{-1}) = -(q^a - 1)/2$, as was to be shown. □

REMARK 8.2. (1) In a very recent paper [**20**], Ulmer introduces the notion of *dimension of* Ш for abelian varieties over $\mathbb{F}_q(t)$ whose Tate–Shafarevich group is finite. In the special case of $E_{\gamma,a}$, this invariant is defined as follows: for all integers $n \geq 1$, let $K_n := \mathbb{F}_{q^n}(t)$ and consider

$$\dim Ш(E_{\gamma,a}) := \lim_{n \to \infty} \frac{\log \left|Ш\big(E_{\gamma,a} \times_K K_n / K_n\big)[p^\infty]\right|}{\log q^n}.$$

Proposition 4.1 of [**20**] shows that the limit exists and is a nonnegative integer, called the *dimension of* Ш *of* $E_{\gamma,a}$. Further, [**20**, Prop. 4.2] provides an expression for $\dim Ш(E_{\gamma,a})$ in terms of the p-adic slope sequence of the L-function of $E_{\gamma,a}$. Using that expression and our Theorem 5.2, an easy calculation yields that $\dim Ш(E_{\gamma,a}) = 0$.

(2) The previous item shows that the order of the p-primary part of the Tate–Shafarevich group of the base-changed elliptic curve $E_{\gamma,a} \times_K K_n$ over K_n grows slowly with n (its log is $o(n)$). By replacing q by q^n in the proof of Theorem 8.1, one can actually prove the stronger assertion that, for all $n \geq 1$,

$$|Ш(E_{\gamma,a} \times_K K_n/K_n)[p^\infty]| = 1.$$

8.2. The size of $Ш(E_{\gamma,a})$. Finally, we prove assertion *(3)* of Theorem C about the size of $Ш(E_{\gamma,a})$. We actually show a slightly more precise result:

THEOREM 8.3. *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 $a \geq 1$, consider the elliptic curve $E_{\gamma,a}$ over K defined by* (2.1)*. Then, as $a \to \infty$, we have*

$$|Ш(E_{\gamma,a})| = H(E_{\gamma,a})^{1+O_q(1/a)},$$

where the implicit constant is effective and depends at most on q.

Recall from (2.3) that $H(E_{\gamma,a}) = N(E_{\gamma,a})^{1/4}$. Hence, the above implies:

COROLLARY 8.4. *In the same setting, as $a \to \infty$, we have*

$$|Ш(E_{\gamma,a})| = N(E_{\gamma,a})^{1/4+O_q(1/a)}.$$

PROOF (OF THEOREM 8.3). We note that, by (2.3), $\log\log H(E_{\gamma,a})$ and a have the same order of magnitude when $a \to \infty$, the involved constants depending at most on q. The elliptic curve $E_{\gamma,a}$ satisfies the BSD conjecture (see Corollary 5.4): taking the logarithm of both sides of the BSD formula (5.2) and reordering terms yields that

$$\frac{\log|Ш(E_{\gamma,a})|}{\log H(E_{\gamma,a})} = 1 - \frac{\log q}{\log H(E_{\gamma,a})} + \frac{\log L(E_{\gamma,a}, q^{-1})}{\log H(E_{\gamma,a})}. \tag{8.2}$$

The term $\log q/\log H(E_{\gamma,a})$ is clearly $o\big(1/\log\log H(E_{\gamma,a})\big) = o(a^{-1})$ as $a \to \infty$. To control the right-most term, we use our bound on the central value $L(E_{\gamma,a}, q^{-1})$: we deduce from Theorem 7.1 that

$$\frac{\big|\log L(E_{\gamma,a}, q^{-1})\big|}{\log H(E_{\gamma,a})} = O\big(1/\log\log H(E_{\gamma,a})\big) = O(1/a),$$

as $a \to \infty$, where the implicit constant depends at most on q. Plugging these two estimates into (8.2) completes the proof. □

REMARK 8.5. Theorem 8.3 can be interpreted as an analogue of the Brauer–Siegel theorem for the sequences $\{E_{\gamma,a}\}_{a\geq 1}$. We refer the reader to [**6, 7**] for a detailed description of the analogue we have in mind: let us simply recall that Hindry and Pacheco have introduced the *Brauer–Siegel ratio* of an abelian variety with finite Tate–Shafarevich group and that, in the case at hand, the Brauer–Siegel ratio is given by $\mathfrak{Bs}(E_{\gamma,a}) = \log|Ш(E_{\gamma,a})|/\log H(E_{\gamma,a})$. (For an elliptic curve with positive Mordell–Weil rank, the Brauer–Siegel ratio also includes the Néron–Tate regulator.) With this notation, Theorem 8.3 can be rewritten in a compact form:

$$\mathfrak{Bs}(E_{\gamma,a}) = 1 + O_q\big(1/a\big) \qquad (\text{as } a \to \infty). \tag{8.3}$$

There is only a handful of sequences of elliptic curves over K for which one can prove that the Brauer–Siegel ratio has a limit and that this limit is 1 (see [**6, 2, 3, 7**] and references therein). The families studied in the present paper therefore provide further examples of that behaviour. However, it seems interesting to remark that

the sequences $\{E_{\gamma,a}\}_{a\geq 1}$ consist of rank 0 elliptic curves, whereas previous articles considered sequences with unbounded rank.

Acknowledgements

This article is partly based on GdW's Leiden Master's thesis [**22**], written under the supervision of RG. The authors would like to thank Bas Edixhoven, Marc Hindry and Douglas Ulmer for fruitful conversations about this work and useful comments on earlier versions thereof.

GdW received funding from the ALGANT Master Programme during his studies at Università degli studi di Milano and Universiteit Leiden. Work on this project was started at Universiteit Leiden. RG now works at Universität Basel, with funding from the Swiss National Science Foundation (SNSF Professorship #170565 awarded to Pierre Le Boudec). These institutions are gratefully thanked for creating great working conditions, and for their financial support. RG also acknowledges funding from Agence Nationale de la Recherche (Grant ANR-17-CE40-0012 FLAIR).

References

[1] Dorian Goldfeld and Lucien Szpiro. Bounds for the order of the Tate-Shafarevich group. *Compositio Math.*, 97(1-2):71–87, 1995.

[2] Richard Griffon. *Analogues du théorème de Brauer-Siegel pour quelques familles de courbes elliptiques*. PhD thesis, Université Paris Diderot, July 2016.

[3] Richard Griffon. Bounds on special values of L-functions of elliptic curves in an Artin-Schreier family. *European Journal of Mathematics*, 5(2):476–517, 2018.

[4] Richard Griffon and Douglas Ulmer. On the arithmetic of a family of twisted constant elliptic curves. *Pacific J. of Math.* (to appear). Preprint `https://arxiv.org/abs/1903.03901`.

[5] Benedict H. Gross. Lectures on the conjecture of Birch and Swinnerton-Dyer. In *Arithmetic of L-functions*, vol. 18 of *IAS/Park City Math. Ser.*, pp. 169–209. Amer. Math. Soc., Providence, RI, 2011.

[6] 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.

[7] Marc Hindry. Analogues of Brauer-Siegel theorem in arithmetic geometry. In *Arithmetic geometry: computation and applications*, vol. 722 of *Contemp. Math.*, pp. 19–41. Amer. Math. Soc., Providence, RI, 2019.

[8] Kazuya Kato Hindry and Fabien Trihan. On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$. *Invent. Math.*, 153(3):537–592, 2003.

[9] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, second edition, 1997.

[10] Liem Mai and M. Ram Murty. A note on quadratic twists of an elliptic curve. In *Elliptic curves and related topics*, pp. 121–124. American Mathematical Society, 1994.

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

[12] James S. Milne. On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975.

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

[14] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[15] Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. In *Algebraic geometry in East Asia—Seoul 2008*, vol. 60 of *Adv. Stud. Pure Math.*, pp. 51–160. Math. Soc. Japan, Tokyo, 2010.

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

[17] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2nd edition, 2009.
[18] 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.
[19] Douglas Ulmer. Elliptic curves over function fields. In *Arithmetic of L-functions*, vol. 18 of *IAS/Park City Math. Ser.*, pp. 211–280. Amer. Math. Soc., Providence, RI, 2011.
[20] Douglas Ulmer. On the Brauer-Siegel ratio for abelian varieties over function fields. *Algebra & Number Theory*, 13(5):1069–1120, 2019.
[21] Benjamin M. M. de Weger. $A + B = C$ and big Ш's. *Quart. J. Math. Oxford Ser. (2)*, 49(193):105–128, 1998.
[22] Guus de Wit. *Elliptic curves over function fields with large Tate–Shafarevich groups*. Master's thesis, Universiteit Leiden, July 2018. (available at `www.math.u-bordeaux.fr/~ybilu/algant/algant_theses.php`).

Departement Mathematik und Informatik, Universität Basel, Spiegelgasse 1, CH-4051 Basel (Switzerland)
E-mail address: `richard.griffon@unibas.ch`

Mathematisch Instituut, Universiteit Leiden, PO Box 9512, 2300RA Leiden (the Netherlands)
E-mail address: `dewit.guus@gmail.com`