ALGANT MASTER THESIS

Elliptic curves over function fields with large Tate-Shafarevich groups

Presented by

Guus de Wit

Advised by

Dr. R. Griffon

Universiteit Leiden

Università degli
studi di Milano

June, 2018

Contents

Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 5$ and set $K = \mathbb{F}_q(t)$. Let E be a nonisotrivial elliptic curve over K and let Ш denote its Tate-Shafarevich group. It is conjectured that Ш is a finite group. In general, this conjecture is still widely open. However, under the assumption that $|Ш|$ is finite, Goldfeld and Szpiro were able to prove an upper bound on the order of Ш, in the case of function fields. Let $N := q^{\deg \mathcal{N}(E)}$ and $H := q^{(1/12)\deg \Delta_{\min}(E)}$, where $\mathcal{N}(E), \Delta_{\min}(E) \in \mathrm{Div}(\mathbb{P}^1)$ are respectively the conductor and the minimal discriminant of E. The bound found by Goldfeld and Szpiro is the following (see [GS95]):

Theorem (Goldfeld-Szpiro). In the above setting, assume that Ш is finite and that $j(E)$ is not a p-th power. For all $\varepsilon > 0$, there exist constants $c, c' > 0$, depending only on ε and q, such that:

$$|Ш| \leq c \cdot N^{1/2+\varepsilon}, \tag{1}$$

and

$$|Ш| \leq c' \cdot H^{1+\varepsilon}. \tag{2}$$

By the Szpiro inequality, we have $H \leq N^{1/2}$, so (1) follows from (2). The question now arises whether these bounds are optimal for finite Ш. We will prove that this is the case for (2), by examining a certain family of nonisotrivial elliptic curves. We also get an improved optimal version of (1) for this specific family.

For any integer $a \geq 1$, let $\wp_a(t) = t^{q^a} - t$ and we define the elliptic curve E_a over K by the following Weierstrass model:

$$E_a : y^2 = x^3 + \wp_a(t)x^2 - x. \tag{3}$$

We denote the Tate-Shafarevich group of E_a by $Ш(E_a)$ and we will show that for all $a \geq 1$, $Ш(E_a)$ is a finite group (see Corollary 4.6), hence we have an infinite family of elliptic curves over K for which $|Ш| < \infty$ holds. We now also know that the Goldfeld-Szpiro bound holds. The main result will be to improve this upper bound for E_a, and to show that the improved bound is almost optimal by proving the corresponding lower bound. This can be summarised in the following theorem:

Theorem A. Let $K = \mathbb{F}_q(t)$ be of characteristic at least 5, and for any integer $a \geq 1$, let E_a/K be the elliptic curve defined by (3) and set $N_a := q^{\deg \mathcal{N}_a}$, where $\mathcal{N}_a$ is the conductor of E_a. For all $\varepsilon > 0$, there exist constants $c_1, c_2 > 0$, depending only on ε and q, such that for all $a \geq 1$, we have:

$$c_1 \cdot N_a^{1/4-\varepsilon} \leq \big|Ш(E_a)\big| \leq c_2 \cdot N_a^{1/4+\varepsilon}.$$

As a corollary, we will also get the following bounds of $|Ш(E_a)|$ in terms of $H(E_a)$:

Theorem B. In the setting of Theorem A, set $H(E_a) := q^{(1/12)\deg \Delta_{\min}(E_a)}$, where $\Delta_{\min}(E_a)$ is the minimal discriminant of E_a. For all $\varepsilon > 0$, there exist constants $c_1', c_2' > 0$ depending only on ε and q, such that for all $a \geq 1$, we have:

$$c_1' \cdot H(E_a)^{1-\varepsilon} \leq \left|Ш(E_a)\right| \leq c_2' \cdot H(E_a)^{1+\varepsilon}.$$

It follows from Theorem B that the Goldfeld-Szpiro bound is essentially optimal, in the sense that the exponent 1 in (2) is the best possible (it cannot be replaced by a smaller number).

We will now give an outline of the proof of Theorem A. We first focus on finding an explicit expression for the L-function $L(E_a, T)$ of E_a. The main tool in finding the expression will be a certain relation between character sums. Define $P_q(a)$ to be the set of nonzero, finite places v of K with degree d_v dividing a. We will find for all $v \in P_q(a)$ certain algebraic integers $g(v)$, $\alpha(v)$ and $\alpha'(v)$ (see Definitions 1.21 and 1.26 for more details), such that the L-function of E_a is given by:

$$L(E_a, T) = \prod_{v \in P_q(a)} (1 - \alpha(v)g(v)T^{d_v})(1 - \alpha'(v)g(v)T^{d_v}) \in \mathbb{Z}[T]. \tag{4}$$

Defining the special value $L^*(E_a) := L(E_a, q^{-1})$, we will deduce from this expression that $L^*(E_a) \neq 0$, or in other words $\operatorname{ord}_{T=q^{-1}} L(E_a, T) = 0$. It is a result of Tate that for the rank of the Mordell-Weil group of E_a, we have $0 \leq \operatorname{rank} E_a(K) \leq \operatorname{ord}_{T=q^{-1}} L(E_a, T)$, so in particular $\operatorname{rank} E_a(K) = 0$ as well. From this, we deduce that the full BSD conjecture holds for the curves E_a and hence that the Tate-Shafarevich group $Ш(E_a)$ is finite (see section 4 for more details).

To find bounds on the order of $Ш(E_a)$, we first deduce from the BSD conjecture and a computation of the torsion and Tamagawa number of E_a, the following relation:

$$\frac{\log L^*(E_a)}{\log N_a} = \frac{\log |Ш(E_a)|}{\log N_a} - \frac{1}{4} + o(1), \text{ as } a \to \infty \tag{5}$$

and then continue by finding upper and lower bounds for $\frac{\log L^*(E_a)}{\log N_a}$. By proving a bound for the size of $P_q(a)$, we find that there exists a constant $C_2 > 0$, such that for all $a \geq 1$:

$$\frac{\log L^*(E_a)}{\log N_a} \leq \frac{C_2}{a}. \tag{6}$$

Finding a lower bound requires more work. For every place $v \in P_q(a)$, we will prove the existence of an angle $\theta_v \in (0, \pi) \setminus \{\pi/2\}$ from the computation of the L-function, such that we have the following bound for all $a \geq 1$:

$$-\frac{\log L^*(E_a)}{\log N_a} \leq \frac{|P_q(a)|}{\log N_a} \cdot \left(\frac{1}{|P_q(a)|} \sum_{v \in P_q(a)} - \log(\sin^2 \theta_v \cos^2 \theta_v) \right). \tag{7}$$

The first factor of the right hand side of this inequality can easily be seen to be $\frac{|P_q(a)|}{\log N_a} = \mathcal{O}(1/a)$, as $a \to \infty$. The remainder of the proof is focused on proving that the second factor has a limit as $a \to \infty$. Hence there exists a constant $C_1 > 0$, such that for all $a \geq 1$, we have:

$$-\frac{C_1}{a} \leq \frac{\log L^*(E_a)}{\log N_a}. \tag{8}$$

Combining equation (5) with the bounds found in (6) and (8) will then conclude the proof of Theorem A.

We also give a short outline of this thesis: In section 1 we recall the relevant definitions and results on elliptic curves and characters, as well as introducing quadratic Gauss sums and Kloosterman sums with some classical results. In section 2 we will compute some invariants of the family E_a, including the j-invariant, the conductor and the minimal discriminant. We also compute the Tamagawa number of E_a and the torsion subgroup of $E(K)$. Section 3 will be completely dedicated to computing the L-function, and in section 4 we deduce several corollaries from the explicit expression, including the finiteness of $Ш(E_a)$ and the fact that the full BSD conjecture holds. In section 5 we will prove the desired bounds on $\frac{\log L^*(E_a)}{\log N_a}$, from which we will deduce proofs for Theorems A and B in section 6.

1 Background

We let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 5$ with q elements and write $K = \mathbb{F}_q(t)$. Throughout, we fix an algebraic closure $\overline{\mathbb{F}_q}/\mathbb{F}_q$ and for any $n \geq 1$ let $\mathbb{F}_{q^n}$ be the unique subfield of $\overline{\mathbb{F}_q}$ with q^n elements. We also fix a primitive p-th root of unity ζ_p and embeddings $\mathbb{Q}(\zeta_p) \hookrightarrow \overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. When algebraic integers are considered as complex numbers, it is always implicitly under these embeddings.

The next two sections are inspired by Ulmer's Park City lecture notes ([Ulm11]). The reader can confer these notes or [Sil09] for more details.

1.1 Places of K

Consider the projective line $\mathbb{P}^1$ over $\mathbb{F}_q$, and note that $K = \mathbb{F}_q(t) = \mathbb{F}_q(\mathbb{P}^1)$. We let a place v of K be an orbit of the Galois action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on $\mathbb{P}^1(\overline{\mathbb{F}_q})$. Since $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is topologically generated by the Frobenius morphism $\mathrm{Fr}_q \colon x \mapsto x^q$, a place v of K is given by $v = \{\mathrm{Fr}_q^j(P) : j \geq 1\}$, for some point $P \in \mathbb{P}^1(\overline{\mathbb{F}_q})$. Note that $\mathbb{P}^1$ has exactly one point at infinity, which is $\mathbb{F}_q$-rational, and we will denote the place to which this point belongs with ∞. All the other places v of K are called *finite* places of K, and it is a classical fact that there is a bijection between the finite places of K, and the set $\{B \in \mathbb{F}_q[t] : B \text{ monic, irreducible}\}$, and we denote with $B_v \in \mathbb{F}_q[t]$ the monic irreducible polynomial corresponding to a place v of K (see for example [Ulm11, Lect. 1.2]). We set d_v to be the degree of a place v of K. In particular, we have $d_v = \deg B_v$.

We associate the residue field $\mathbb{F}(v) := \mathbb{F}_q[t]/(B_v)$ to a finite place v of K of degree d_v. Note that $\mathbb{F}(v)/\mathbb{F}_q$ is a field extension of degree d_v. Similarly, for the place ∞ of K, we set $\mathbb{F}(\infty) = \mathbb{F}_q$ (as ∞ is a place of degree 1). For any place v of K, we set K_v to be the completion of K at v.

1.2 Elliptic curves over K

We use mostly the definitions as in [Ulm11, Lect. 1]. An *elliptic curve* over K is a smooth cubic plane curve, given by a Weierstrass model of the form:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.1}$$

with $a_1, ..., a_6 \in K$. Let O be the K-rational point $(0 : 1 : 0)$. Setting $x = X/Z$ and $y = Y/Z$, we can also give the Weierstrass model in affine form:

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

Note that O is the only point of E at infinity, in the plane "$Z = 0$". The quantities $b_2, ..., b_8, c_4, c_6, \Delta$ and j are defined as in [Sil09, III.1]. All Weierstrass models that can be obtained from a given model by a change of variables of the form:

$$x = u^2x' + r, y = u^3y' + u^2sx' + t,$$

with $u, r, s, t \in K$, $u \neq 0$, are said to define the same elliptic curve over K. We now define the following:

Definition 1.1. Let E be an elliptic curve over K.

(1) We say that E is *constant* if E can be defined by a Weierstrass model (1.1), with $a_i \in \mathbb{F}_q$ for all i.

(2) We say that E is *isotrivial* if there exists a finite extension K' of K, such that E becomes constant over K'.

(3) We say that E is *nonisotrivial* if it is not isotrivial.

Note that [Ulm11, Rem. 1.1.5] states that E is isotrivial, if and only if $j(E) \in \mathbb{F}_q$. We let $E(K)$ be the set of K-rational points of E. It is a classical fact that $E(K)$ becomes a group under the "chord and tangent" addition (see for example [Sil09, Ch. III.2, Prop.2.2.(f)]. Lang and Néron both proved the following analogue of the classical Mordell-Weil theorem ([Ulm11, Lect. 1, Th. 5.1]):

Theorem 1.2. *Let $K = \mathbb{F}_q(t)$ and E an elliptic curve over K. Then $E(K)$ is a finitely generated abelian group.*

In particular, the torsion subgroup $E(K)_{\text{tors}} \subseteq E(K)$ is finite.

Definition 1.3. For a finite place v of K of degree d_v, let $B_v \in \mathbb{F}_q[t]$ be the corresponding monic irreducible polynomial of degree d_v. We then define $\operatorname{ord}_v \colon K^* \to \mathbb{Z}$, by $\operatorname{ord}_v(f) := \operatorname{ord}_{B_v}(f)$, for all $f \in K$, where ord_{B_v} denotes the multiplicity of B_v in f. For $v = \infty$, we define $\operatorname{ord}_\infty \colon K^* \to \mathbb{Z}$ by $\operatorname{ord}_\infty(f) := -\deg f$, for all $f \in K$. Furthermore, for any place v of K, we set $\operatorname{ord}_v(0) = \infty$.

Definition 1.4. Let v be a place of K and E an elliptic curve over K, given by a Weierstrass model (1.1). We say that the model is *integral at v*, if $\operatorname{ord}_v(a_i) \geq 0$, for all i.

Note that from an elliptic curve E over K given Weierstrass model, and any place v of K, we can always we can always find a model for E that is integral at v, by applying a change of variables as in [Sil09, Ch. III.1], with the formulas from [Sil09, Ch. III.1, Table 3.1]. Note that $\operatorname{ord}_v \Delta \geq 0$ for an integral model at v, so there are models where this valuation is minimal.

Definition 1.5. Let E be an elliptic curve over K and v any place of K. A *minimal integral model of E at v* is an integral model of E at v, such that $\operatorname{ord}_v \Delta$ is minimal among all integral models of E. We set $\Delta_v(E)$ to be the discriminant of a minimal integral model at v.

Definition 1.6. Let E be an elliptic curve over K. We define the *minimal discriminant* $\Delta_{\min}(E)$ of E to be:

$$\Delta_{\min}(E) := \sum_v \operatorname{ord}_v \Delta_v(E) \cdot (v) \in \operatorname{Div}(\mathbb{P}^1),$$

where the sum runs over all the places v of K. This is indeed a divisor, as there are only finitely many places with $\operatorname{ord}_v \Delta_v(E) > 0$. We set $H(E) := q^{(1/12) \deg \Delta_{\min}(E)}$.

Let v be any place of K, and choose a minimal integral model model of E at v:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $\tau \in v$, and $\overline{a}_i \in \mathbb{F}(v)$ be the reduction modulo v, obtained by substituting t with τ and let $(\widetilde{E})_\tau$ be the cubic plane curve defined by:

$$y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6. \tag{1.3}$$

We call $(\widetilde{E})_\tau$ the reduction of E at v. If $\operatorname{ord}_v(\Delta_v(E)) = 0$, (1.3) describes an elliptic curve over $\mathbb{F}(v)$. However, if $\operatorname{ord}_v(\Delta_v(E)) \geq 1$, then $(\widetilde{E})_\tau$ is singular. We use this to define the following:

Definition 1.7. Let E be an elliptic curve over K, and v be any place of K. Then:

(1) If $(\widetilde{E})_\tau$ is a smooth cubic, i.e. an elliptic curve, we say that E has *good reduction at v.*

(2) If $(\widetilde{E})_\tau$ is a nodal cubic, we say that E has *multiplicative reduction at v.* If the tangent lines at the node are rational over $\mathbb{F}(v)$ we say that the reduction is *split multiplicative*, otherwise we say the reduction is *non-split multiplicative.*

(3) If $(\widetilde{E})_\tau$ is a cuspidal cubic, we say that E has *additive reduction.*

If E has either multiplicative or additive reduction at v, we say that E has *bad reduction at v.* In the case of bad reduction at v, write $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}(v))$ for the set of non-singular $\mathbb{F}(v)$-rational points of $(\widetilde{E})_\tau$. Then, we define:

$$E_0(K_v) := \{P \in E(K_v) : \tilde{P} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}(v))\} \tag{1.4}$$

Definition 1.8. Let E be an elliptic curve over K. For a place v of K, we set:

$$n_v(E) := \begin{cases} 0, & \text{if } E \text{ has good reduction at } v \\ 1, & \text{if } E \text{ has multiplicative reduction at } v \\ 2, & \text{if } E \text{ has additive reduction at } v \end{cases}.$$

Furthermore, we define the *conductor of E* to be:

$$\mathcal{N}(E) := \sum_v n_v(E) \cdot (v) \in \operatorname{Div}(\mathbb{P}^1),$$

where the sum runs over all the places v of K. $\mathcal{N}(E)$ is indeed a divisor, as there are only finitely many places of bad reduction. We set $N(E) := q^{\deg \mathcal{N}(E)}$

We also define the Tamagawa number of an elliptic curve E:

Definition 1.9. Let E be an elliptic curve over K, and v any place of K and let K_v be the completion of K at v. We define:

$$c_v(E) := \#(E(K_v)/E_0(K_v)),$$

and the *Tamagawa number* $\tau(E)$ of E as the following product over all places v of E:

$$\tau(E) := \prod_v c_v(E).$$

This is well-defined, as $c_v(E) = 1$ for all places of good reduction and there are only finitely many places of bad reduction.

The next object we want to introduce is the L-function of E. For any place v of K, define:

$$a_v(E) := q^{d_v} + 1 - \#(\widetilde{E})_\tau(\mathbb{F}(v)). \tag{1.5}$$

In the case of bad reduction, the number of points of $(\widetilde{E_a})_\tau(\mathbb{F}(v))$ is known exactly, hence we get:

$$a_v(E) = \begin{cases} q^{\deg v} + 1 - \#(\widetilde{E})_\tau(\mathbb{F}(v)) & \text{, if } E \text{ has good reduction at } v \\ 1 & \text{, if } E \text{ has split multiplicative reduction at } v \\ -1 & \text{, if } E \text{ has non-split multiplicative reduction at } v \\ 0 & \text{, if } E \text{ has additive reduction at } v \end{cases} \tag{1.6}$$

Then we define the L-function $L(E,T)$ of E as the following Euler product:

$$L(E,T) = \prod_{\text{good } v} (1 - a_v(E)T^{d_v} + q^{d_v}T^{2d_v})^{-1} \cdot \prod_{\text{bad } v} (1 - a_v(E)T^{d_v})^{-1}. \tag{1.7}$$

In [Ulm11, Lect. 1.9], the classical Hasse-Weil bound is stated: for all places v of K, we have

$$|a_v(E)| \leq 2\sqrt{q}^{d_v}.$$

This bound implies that the Euler product in (4.3) converges for all T with $|T| < q^{-3/2}$. Furthermore, [Ulm11, Lect 1, Th. 9.3] states that for nonisotrivial elliptic curves, $L(E,T)$ is actually a polynomial in $\mathbb{Z}[T]$.

Finally, we give a definition of the Tate-Shafarevich group. Fix a separable closure K^{sep} of K, and for any place v of K, fix a separable closure K_v^{sep} of K_v. Set $G_K := \text{Gal}(K^{\text{sep}}/K)$, and for any place v, set $G_{K_v} := \text{Gal}(K_v^{\text{sep}}/K_v)$. Then we define the *Tate-Shafarevich group* of E over K, to be:

$$Ш(E) := \ker\left(H^1(G_K, E(K^{\text{sep}})) \to \prod_v H^1(G_{K_v}, E(K_v^{\text{sep}}))\right), \tag{1.8}$$

where the H^1 are the Galois cohomology groups. We only study the order of the Tate-Shafarevich group, hence no introduction into Galois cohomology is given. For more details on this topic, the reader may refer to [Ser97]. Note that Ш(E) is conjectured to be finite, but this is not known in general.

1.3 Characters

This section follows topics on characters as discussed in [LN97, Ch. 5]. Some slight changes in the definitions and notations were made, mostly for notational convenience and we only use the specific characters we are interested in. The results of [LN97] remain true

When we consider a finite field $\mathbb{F}$ of characteristic p, we actually have two interesting abelian groups: the additive group $\mathbb{F}$ and the multiplicative group $\mathbb{F}^*$. For both of these, we define characters we are interested in.

Definition 1.10. Let $\mathbb{F}$ be a finite field of characteristic p. We define an *additive character of* $\mathbb{F}$ to be a group homomorphism $\psi\colon \mathbb{F} \to \mathbb{Q}(\zeta_p)^*$. We call the character $\psi\colon \mathbb{F} \to \mathbb{Q}(\zeta_p)^*$ with $\psi(x) = 1$ for all $x \in \mathbb{F}$ the *trivial additive character* of $\mathbb{F}$. All other additive characters are called *nontrivial.*

Remark 1.11. For the finite field $\mathbb{F}_q$, note that the following map is a nontrivial additive character:

$$\psi_q\colon \mathbb{F}_q \to \mathbb{Q}(\zeta_p)^*, x \mapsto \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}, \tag{1.9}$$

which can be seen by noting that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}\colon \mathbb{F}_q \to \mathbb{F}_p$ is additive and surjective. We call ψ_q the *standard additive character* of $\mathbb{F}_q$. For any finite extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, we write

$$\psi_{q^n} := \psi_q \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\colon \mathbb{F}_{q^n} \to \mathbb{Q}(\zeta_p)^*,$$

which is a nontrivial character of $\mathbb{F}_{q^n}$ (see [LN97, (5.7)]). We call ψ_{q^n} the *standard additive character* of $\mathbb{F}_{q^n}$.

Remark 1.12. Let $n \geq 1$ and $\beta \in \mathbb{F}_{q^n}$. Define the map $\psi_\beta\colon \mathbb{F}_{q^n} \to \mathbb{Q}(\zeta_p)^*$ by $\psi_\beta(x) = \psi_{q^n}(\beta x)$ for all $x \in \mathbb{F}_{q^n}$. Then it can be easily seen that ψ_β is also an additive character on $\mathbb{F}_{q^n}$, which is trival if and only if $\beta = 0$.

Definition 1.13. For any finite field $\mathbb{F}$ of characteristic p, we define the *quadratic character* $\lambda\colon \mathbb{F}^* \to \{\pm 1\}$ by

$$\lambda(x) = \begin{cases} 1, & \text{if } x \text{ is a square in } \mathbb{F} \\ -1, & \text{otherwise} \end{cases}.$$

Remark 1.14. The quadratic character is an example of a *multiplicative character* of $\mathbb{F}$: it is the unique nontrivial homomorphism $\chi\colon \mathbb{F}^* \to \{\pm 1\}$ for which $\chi^2(x) = 1$ holds for all $x \in \mathbb{F}^*$ (see [LN97, Ex. 5.10]). For any winite extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, we will write λ_{q^n} and λ_q for the quadratic characters of $\mathbb{F}_{q^n}$ and $\mathbb{F}_q$ respectively. Note that $\lambda_q \circ \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\colon \mathbb{F}_{q^n}^* \to \{\pm 1\}$ is also a group homomorphism of order exactly 2 (as $\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is multiplicative and surjective), but since λ_{q^n} is the *unique* map with this property, we actually have $\lambda_{q^n} = \lambda_q \circ \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

Remark 1.15. For any finite field $\mathbb{F}$ of characteristic p, we extend the quadratic character $\lambda\colon \mathbb{F}^* \to \{\pm 1\}$ to all of $\mathbb{F}$, by setting $\lambda(0) = 0$.

1.3.1 Gauss sums

Definition 1.16. Let $\mathbb{F}$ be a finite field of characteristic p, ψ an additive character and λ the quadratic character of $\mathbb{F}$. We define the *quadratic Gauss sum*

$\mathrm{G}_{\mathbb{F}}(\lambda, \psi)$ as

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

Remark 1.17. We can actually let this sum run over all of $\mathbb{F}$, if λ is extended as in Remark 1.15. Also, note that we normalize our Gauss sums with a minus sign, contrary to the classical definition in [LN97, Ch. 5.2].

Lemma 1.18. *Let $\mathbb{F}$ be a finite field of characteristic p, λ the quadratic character and ψ the trivial character on $\mathbb{F}$. Then:*

$$\mathrm{G}_{\mathbb{F}}(\lambda, \psi) = 0.$$

Proof. Note that the Gauss sum now reduces to:

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

and this sum vanishes, which is a classical fact that holds for all nontrivial characters (see [LN97, Thm. 5.4]). □

Lemma 1.19. *Let $n \geq 1$ and let $\beta \in \mathbb{F}_{q^n}^*$. Define ψ_β as in Remark 1.12. Let λ_{q^n} be the quadratic character on $\mathbb{F}_{q^n}$. Then we have:*

$$\mathrm{G}_{\mathbb{F}_{q^n}}(\lambda_{q^n}, \psi_\beta) = \lambda_{q^n}(\beta) \cdot \mathrm{G}_{\mathbb{F}_{q^n}}(\lambda_{q^n}, \psi_{q^n})$$

Proof. By writing out the Gauss sum, we find:

$$\begin{aligned}
\mathrm{G}_{\mathbb{F}_{q^n}}(\lambda_{q^n}, \psi_\beta) &= -\sum_{x \in \mathbb{F}_{q^n}^*} \lambda_{q^n}(x)\psi_\beta(x) \\
&= -\sum_{x \in \mathbb{F}_{q^n}^*} \lambda_{q^n}(\beta^2)\lambda_{q^n}(x)\psi_{q^n}(\beta x) \\
&= -\lambda_{q^n}(\beta) \sum_{x \in \mathbb{F}_{q^n}^*} \lambda_{q^n}(\beta x)\psi_{q^n}(\beta x) \\
&= \lambda_{q^n}(\beta) \cdot \mathrm{G}_{\mathbb{F}_{q^n}}(\lambda_{q^n}, \psi_{q^n}),
\end{aligned}$$

where the last line follows from the fact that βx attains all values of $\mathbb{F}_{q^n}^*$ as x runs through $\mathbb{F}_{q^n}^*$, because $\beta \neq 0$.

□

We also have the Hasse-Davenport relation:

Theorem 1.20 (Hasse-Davenport). *Let $m \geq 1$, let ψ be an additive character and λ_{q^m} be the quadratic character of $\mathbb{F}_{q^m}$. Then for all finite extensions $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$, we have:*

$$\mathrm{G}_{\mathbb{F}_{q^n}}(\lambda_{q^m} \circ \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^m}}, \psi \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^m}}) = \mathrm{G}_{\mathbb{F}_{q^m}}(\lambda_{q^m}, \psi)^{n/m}.$$

For a proof of this theorem, see [LN97, Th. 5.14]. Using this, we actually get a relation which will be useful in the computation of the L-function in section 3. For that, we consider the following value:

Definition 1.21. Let $n \geq 1$ and let $\beta \in \mathbb{F}_{q^n}^*$. We write d_β for the degree of β over $\mathbb{F}_q$, and $\lambda_{q^{d_\beta}}$ for the quadratic character on $\mathbb{F}_{q^{d_\beta}}$. Then we define:

$$g(\beta) := \lambda_{q^{d_\beta}}(\beta) \mathrm{G}_{\mathbb{F}_{q^{d_\beta}}}(\lambda_{q^{d_\beta}}, \psi_{q^{d_\beta}})$$

The importance of this definition will become clear later, but for now we prove some facts about it.

Proposition 1.22. *Let $n \geq 1$ and $\beta \in \mathbb{F}_{q^n}^*$.*

(i) We have $\lambda_{q^n}(\beta) \cdot \mathrm{G}_{\mathbb{F}_{q^n}}(\lambda_{q^n}, \psi_{q^n}) = g(\beta)^{n/d_\beta}$.

(ii) For all $\alpha \in \{\beta, \beta^q, ..., \beta^{q^{d_\beta - 1}}\}$ we have $g(\alpha) = g(\beta)$. In other words, the value of $g(\beta)$ is constant along the Galois orbit of β.

(iii) Seeing $g(\beta)$ as a complex number in the complex embedding, we have $g(\beta) = q^{d_\beta/2} e^{i\theta_\beta}$ for some $\theta_\beta \in \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$

Proof. We prove the parts separately:

(i) Since $\beta \in \mathbb{F}_{q^n}$, we have $d_\beta | n$. Note that we have $\psi_{q^n} = \psi_{q^{d_\beta}} \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{d_\beta}}}$ and $\lambda_{q^n} = \lambda_{q^{d_\beta}} \circ \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{d_\beta}}}$ by definition. In particular, we have:

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{d_\beta}}}(\beta) = \beta^{q^{d_\beta}} \beta^{q^{2d_\beta}} \cdots \beta^{q^{(n/d_\beta)d_\beta}} = \beta^{n/d_\beta},$$

as $\beta^{q^{d_\beta}} = \beta$. Combining this with the result of Theorem 1.20, we find:

$$\begin{aligned} \lambda_{q^n}(\beta) \cdot \mathrm{G}_{\mathbb{F}_{q^n}}(\lambda_{q^n}, \psi_{q^n}) =& \lambda_{q^{d_\beta}} \circ \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{d_\beta}}}(\beta) \cdot \\ & \mathrm{G}_{\mathbb{F}_{q^n}}(\lambda_{q^{d_\beta}} \circ \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{d_\beta}}}, \psi_{q^{d_\beta}} \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{d_\beta}}}) \\ =& \lambda_{q^{d_\beta}}\left(\beta^{n/d_\beta}\right) \mathrm{G}_{\mathbb{F}_{q^{d_\beta}}}(\lambda_{q^{d_\beta}}, \psi_{q^{d_\beta}})^{n/d_\beta} \\ =& g(\beta)^{n/d_\beta}, \end{aligned}$$

where on the last line we used the fact that $\lambda_{q^{d_\beta}}$ is multiplicative.

(ii) Note that since q is odd, we have $\lambda_{q^{d_\beta}}(x^q) = (\lambda_{q^{d_\beta}}(x))^q = \lambda_{q^{d_\beta}}(x)$ for all $x \in \mathbb{F}_{q^{d_\beta}}^*$, so in particular we have $\lambda_{q^{d_\beta}}(\beta^q) = \lambda_{q^{d_\beta}}(\beta)$. Also note that $d_\beta = d_{\beta^q}$, hence we now easily find $g(\beta^q) = g(\beta)$. Applying this repeatedly, we get $g(\beta) = g(\beta^q) = \cdots g(\beta^{q^{d_\beta - 1}})$.

(iii) There exist an explicit formula for the value of a quadratic Gauss sum. A proof of this classical fact can be found in [LN97, Th. 5.15]. Our statement is a direct consequence of this formula.

□

1.3.2 Kloosterman sums

Definition 1.23. Let $\mathbb{F}$ be a finite field, $\alpha \in \mathbb{F}^*$ and ψ a nontrivial additive character of $\mathbb{F}$. We define the *Kloosterman sum* $\mathrm{Kl}_{\mathbb{F}}(\psi;\alpha)$ as:

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

We first prove two elementary properties about Kloosterman sums in specific cases of $\mathbb{F}$ and ψ.

Lemma 1.24. *Let $n \geq 1$ and let $\alpha \in \mathbb{F}_{q^n}^*$. Then:*

(i) Let $\beta \in \mathbb{F}_{q^n}^*$ and define the nontrivial additive character $\psi_\beta \colon \mathbb{F}_{q^n} \to \mathbb{Q}(\zeta_p)^*$ by $\psi_\beta(x) = \psi_{q^n}(\beta x)$ for all $x \in \mathbb{F}_{q^n}$, as in Remark 1.12. Then we have:

$$\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_\beta;\alpha) = \mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n};\alpha\beta^2).$$

(ii) For any $j \geq 1$, we have:

$$\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n};\alpha) = \mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n};\alpha^{q^j}).$$

Proof. We prove the two parts separately:

(i) For $x \in \mathbb{F}_{q^n}^*$, write $y := \beta x$, and note that y takes all values of $\mathbb{F}_{q^n}^*$, as x runs over $\mathbb{F}_{q^n}^*$, because $\beta \neq 0$. Using this, we get:

$$\begin{aligned}\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_\beta;\alpha) &= -\sum_{x\in\mathbb{F}_{q^n}^*} \psi_\beta\left(x+\frac{\alpha}{x}\right) = -\sum_{x\in\mathbb{F}_{q^n}^*} \psi_{q^n}\left(\beta x+\frac{\alpha\beta}{x}\right)\\ &= -\sum_{x\in\mathbb{F}_{q^n}^*} \psi_{q^n}\left(\beta x+\frac{\alpha\beta^2}{\beta x}\right) = -\sum_{y\in\mathbb{F}_{q^n}^*} \psi_{q^n}\left(y+\frac{\alpha\beta^2}{y}\right)\\ &= \mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n};\alpha\beta^2)\end{aligned}$$

(ii) Note that $\psi_{q^n} = \psi_q \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ and that for any $x \in \mathbb{F}_{q^n}^*$, we have $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x^q)$. Using this, we find:

$$\begin{aligned}\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n};\alpha) &= -\sum_{x\in\mathbb{F}_{q^n}^*} \psi_q \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(x+\frac{\alpha}{x}\right)\\ &= -\sum_{x\in\mathbb{F}_{q^n}^*} \psi_q \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\left(x+\frac{\alpha}{x}\right)^q\right)\\ &= -\sum_{x\in\mathbb{F}_{q^n}^*} \psi_{q^n}\left(x^q+\frac{\alpha^q}{x^q}\right) = \mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n};\alpha^q),\end{aligned}$$

where the last equality follows as x^q attains all values of $\mathbb{F}_{q^n}^*$, as x runs through $\mathbb{F}_{q^n}^*$.

□

Similar to the Hasse-Davenport theorem in the case of Gauss sums, there is a relation on Kloosterman sums which we will use to define certain values.

Theorem 1.25. *Let $m \geq 1$, $\alpha \in \mathbb{F}_{q^m}^*$ and $\psi\colon \mathbb{F}_{q^m} \to \mathbb{Q}(\zeta_p)^*$ be any nontrivial additive character of $\mathbb{F}_{q^m}$. Then there exist two algebraic integers $\mathrm{kl}_{\mathbb{F}_{q^m}}(\psi;\alpha)$ and $\mathrm{kl}'_{\mathbb{F}_{q^m}}(\psi;\alpha)$, which are uniquely determined by $\mathbb{F}_{q^m}$, ψ and α up to permutation, such that for all finite extensions $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$, we have:*

$$\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^m}};\alpha) = \mathrm{kl}_{\mathbb{F}_{q^m}}(\psi;\alpha)^{n/m} + \mathrm{kl}'_{\mathbb{F}_{q^m}}(\psi;\alpha)^{n/m}.$$

A proof of this theorem can be found in [LN97, Th. 5.43]. We will use it for the following definition:

Definition 1.26. Let $n \geq 1$ and let $\beta \in \mathbb{F}_{q^n}^*$ of degree d_β. Then we define

$$\{\alpha(\beta), \alpha'(\beta)\} := \{\mathrm{kl}_{\mathbb{F}_{q^{d_\beta}}}(\psi_{q^{d_\beta}};-\beta^2), \mathrm{kl}'_{\mathbb{F}_{q^{d_\beta}}}(\psi_{q^{d_\beta}};-\beta^2)\},$$

for the pair $\mathrm{kl}_{\mathbb{F}_{q^{d_\beta}}}(\psi_{q^{d_\beta}};-\beta^2)$ and $\mathrm{kl}'_{\mathbb{F}_{q^{d_\beta}}}(\psi_{q^{d_\beta}};-\beta^2)$ as in Theorem 1.25.

Proposition 1.27. *Let $n \geq 1$ and $\beta \in \mathbb{F}_{q^n}^*$. Then:*

(i) We have $\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n};-\beta^2) = \alpha(\beta)^{n/d_\beta} + \alpha'(\beta)^{n/d_\beta}$.

(ii) For all $\gamma \in \{\beta, \beta^q, ..., \beta^{q^{d_\beta - 1}}\}$, we have $\{\alpha(\gamma), \alpha'(\gamma)\} = \{\alpha(\beta), \alpha'(\beta)\}$, so the values of $\alpha(\beta)$ and $\alpha'(\beta)$ are constant along the Galois orbit of β, up to permuting with each other.

(iii) We have $|\alpha(\beta)| = |\alpha'(\beta)| = q^{d_\beta/2}$ and $\alpha(\beta)$ and $\alpha'(\beta)$ are complex conjugates, when seen as complex numbers in the embedding into $\mathbb{C}$.

Proof. For (i), note that $\psi_{q^n} = \psi_{q^{d_\beta}} \circ \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{d_\beta}}}$ and the result then follows immediately from Theorem 1.25. For part (ii), note that for any j and $\beta' = \beta^{q^j}$, we have $d_{\beta'} = d_\beta$ and using Lemma 1.24.(ii), we find

$$\mathrm{Kl}_{\mathbb{F}_{q^{d_{\beta'}}}}(\psi_{q^{d_{\beta'}}};-(\beta')^2) = \mathrm{Kl}_{\mathbb{F}_{q^{d_\beta}}}(\psi_{q^{d_\beta}};-\beta^2),$$

and hence $\{\alpha(\gamma), \alpha'(\gamma)\} = \{\alpha(\beta), \alpha'(\beta)\}$. The first statement of part (iii) is [LN97, Th. 5.44], and the second statement is actually part of [LN97, Th.5.43] □

We also need a result on bounds of the absolute value of Kloosterman sums.

Proposition 1.28. *For any $n \geq 1$ and $\beta \in \mathbb{F}_{q^n}^*$, we have:*

$$0 < |\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n};-\beta^2)| < 2q^{n/2}.$$

Proof. Note that the second inequality is exactly [vdGvdV91, Cor. (3.2)], and for the first inequality, we use a similar argument. Let $(\zeta_p - 1)$ be the unique prime ideal of $\mathbb{Q}(\zeta_p)$ lying over p, and note that $(p) = (\zeta_p - 1)^{p-1}$ (this is a well known fact about the decomposition of p in $\mathbb{Q}(\zeta_p)$. For a proof of this fact, see for example [IR90, Prop. 13.2.7]). Since ψ_{q^n} takes values in $\{\zeta_p^j : j = 0, ..., p-1\}$, we have for all $x \in \mathbb{F}_{q^n}^*$ that $\psi_{q^n}(x - \beta^2/x) \equiv 1 \mod (\zeta_p - 1)$. Hence:

$$\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n}; -\beta^2) = -\sum_{x \in \mathbb{F}_{q^n}^*} \psi_{q^n}\left(x - \frac{\beta^2}{x}\right) \equiv -(q^n - 1) \equiv 1 \mod (\zeta_p - 1).$$

In particular, we cannot have $\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n}; -\beta^2) = 0$. □

2 The family E_a

For an integer $a \geq 1$, we consider the following elliptic curve over $K = \mathbb{F}_q(t)$:

$$E_a : y^2 = x^3 + \wp_a(t)x^2 - x, \tag{2.1}$$

where $\wp_a(t) = t^{q^a} - t$. From this Weierstrass model and straightforward computations, we deduce the following table of quantities for E_a, as found in [Sil09, III.1].

quantity	value	quantity	value
b_2	$4\wp_a(t)$	c_4	$16(\wp_a(t)^2 + 3)$
b_4	-2	c_6	$-32(2\wp_a(t)^3 + 9\wp_a(t))$
b_6	0	Δ	$16(\wp_a(t)^2 + 4)$
b_8	-1	j	$\frac{256(\wp_a(t)^2+3)^3}{\wp_a(t)^2+4}$

(2.2)

Note that j does not depend on the model of E_a, and since $j \notin \mathbb{F}_q$, we see that E_a is nonisotrivial.

2.1 Reductions

For the computation of the L-function, we need to reduce E_a modulo the places of K and determine minimal integral models at those places.

First we consider the finite places of K, so let v be a place of K with $v \neq \infty$ of degree d_v. We can identify v with a monic irreducible polynomial B_v in $\mathbb{F}_q[t]$ of degree d_v. For a point $\tau \in v$ (i.e. a root $\tau \in \overline{\mathbb{F}_q}$ of B_v), we consider the reduction $(\widetilde{E_a})_\tau$, of (a minimal model at v of) E_a modulo v, by substituting t with τ. To v, we associate the residue field $\mathbb{F}(v) := \mathbb{F}_q[t]/(B_v)$, which is an extension of $\mathbb{F}_q$ of degree d_v. For a general (not necessarily finite) place v of K, we consider $\Delta_v(E_a)$, which is the discriminant of a minimal integral model of E_a at v. These definitions can also be found in section 1.

It is clear that $(\widetilde{E_a})_\tau$ is an elliptic curve if $\mathrm{ord}_v\big(\Delta_v(E_a)\big) = 0$, as we then have $\Delta_v(E_a) \not\equiv 0 \mod v$. So, in that case E_a has good reduction at v. In the other case, when $\mathrm{ord}_v(\Delta_v(E_a)) > 0$, E_a has bad reduction at v. We compute the places of bad reductions and the reduction types explicitly, in the following proposition:

Proposition 2.1. *The following two statements hold:*

(i) We have the following reductions of E_a modulo the places v of K. Note that for a finite place $v \neq \infty$, we denote by $B_v \in \mathbb{F}_q[t]$ the corresponding monic irreducible polynomial.

place v	*Kodaira symbol*	*reduction*
$B_v \nmid \wp_a(t)^2 + 4$	I_0	*good*
$B_v \mid \wp_a(t)^2 + 4$	I_1	*multiplicative*
∞	$I^*_{4q^a}$	*additive*

(2.3)

(ii) For a finite place v of K such that $B_v \mid \wp_a(t)^2 + 4$, a minimimal integral model of E_a at v is given by (2.1).

In order to prove Proposition 2.1, we first need the following lemma.

Lemma 2.2. *The polynomial* $\wp_a(t)^2 + 4 \in \mathbb{F}_q[t]$ *is square-free.*

Proof. Write $f(t) = \wp_a(t)^2 + 4 = t^{2q^a} - 2t^{q^a+1} + t^2 + 4$. Its derivative is $f'(t) = 2q^a t^{2q^a-1} - 2(q^a+1)t^{q^a} + 2t = -2t^{q^a} + 2t$. Then a direct computation yields that:

$$\frac{1}{4} f(t) + \frac{1}{8}\wp_a(t) f'(t) = 1,$$

(note that we used that q is not a power of 2), hence $f(t)$ and $f'(t)$ are coprime in $\mathbb{F}_q[t]$, which implies that $f(t)$ is square-free. □

Now we have the tools we need to prove Proposition 2.1.

Proof of Proposition 2.1. We prove the two parts at the same time, where (ii) will follow from our computation of Kodaira symbol at the finite places of bad reduction. We separate the three cases:

- Let v be a finite place of K, and suppose that $B_v \nmid \wp_a(t)^2 + 4$. Then $B_v \nmid \Delta$ and thus $\mathrm{ord}_v \Delta = 0$. As we saw before, we have good reduction in this case, hence Kodaira symbol I_0.

- Now suppose that $B_v \mid \wp_a(t)^2 + 4$. Note that (2.1) is an integral model of E_a at v. By Lemma 2.2 we know that $\wp_a(t)^2 + 4$ is square-free, hence B_v only occurs once as an irreducible factor of $\wp_a(t)^2 + 4$, from which it is also clear that $\mathrm{ord}_v(\Delta) = 1$, where Δ is the discriminant of model (2.2) of E_a. Since a change of variables could only change $\mathrm{ord}_v(\Delta)$ by a multiple of 12, we know that (2.1) actually is a minimal integral model. Furthermore, if we rewrite the j-invariant to be:

  $$j = \frac{16^3(\wp_a(t)^2 + 3)^3}{16(\wp_a(t)^2 + 4)} = \frac{(\Delta - 16)^3}{\Delta},$$

  we see that the numerator does not vanish modulo v, and hence j has a simple pole at v. Now referencing table 4.1 in [Sil94, IV.9], we see that this specific behavior of the orders of Δ and j at v only happens for reduction type I_1.

- Finally we consider the case $v = \infty$. This place corresponds to the element $u := 1/t \in K$, so we first have to make an integral model at v. Note that we can rewrite (2.1) to:

  $$y^2 = x^3 + (1/u^{q^a} - 1/u)x^2 - x.$$

  Multiplying both sides by u^{6q^a+6} and making the substitutions $x' = u^{q^a+1}x$ and $y' = u^{\frac{3q^a+3}{2}}$ gives us the following integral model of E_a at v:

  $$\begin{aligned} y'^2 &= x'^3 + (1/u^{q^a} - 1/u)u^{q^a+1}x'^2 - u^{2q^a+2}x' \\ &= x'^3 - \wp_a(u)x'^2 - u^{2q^a+2}x'. \end{aligned} \tag{2.4}$$

The corresponding quantities defined in [Sil09, III.1] for this model become:

quantity	value
b'_2	$-4\wp_a(u)$
b'_4	$-2u^{2q^a+2}$
b'_6	0
b'_8	$-u^{4q^a+4}$
Δ'	$16\left(\wp_a(u)^2 + 4u^{2q^a+2}\right)u^{4q^a+4}$

(2.5)

Now we follow Tate's algorithm as described in [Sil94, IV.9] with $\pi = u$, to determine the reduction type. Note that our model is such that $u \mid \Delta'$ and that the singular point of the reduction $\widetilde{E_a}$ at ∞ is at $(0,0)$. Furthermore, we note (in this order) that $u|b_2$, $u^2|a_6$, $u^3|b_8$ and $u^3|b_6$. That leaves us in step 6 of the algorithm, for which we note that we already have $u|a_1, a_2$, $u^2|a_3, a_4$ and $u^3|a_6$. Hence, we are left to study the factorisation of

$$P(T) := T^3 + (1 - u^{q^a-1})T^2 - u^{2q^a}T$$

in the residue field of ∞, i.e $\mathbb{F}_q$ (∞ is a place of degree 1). Note that we have:

$$P(T) \equiv T^3 + T^2 \equiv T^2(T+1),$$

so $P(T)$ has one double root, and one single root in the residue field. This means that the algorithm stops at step 7, and that we have reduction type I_n^*, with

$$n = \mathrm{ord}_\infty(\Delta') - 6 = (4q^a + 6) - 6 = 4q^a$$

and model (2.4) is minimal integral at ∞.

□

2.2 Conductor and minimal discriminant of E_a

It is convenient to introduce the following notation:

Notation 2.3. As we explained in section 1, we can identify a finite place v of K with a monic irreducible polynomial $B_v \in \mathbb{F}_q[t]$, and for any polynomial $P \in \mathbb{F}_q[t]$, we write $v|P$ if $B_v|P$, or in other words $\mathrm{ord}_v(P) > 0$. Note that we only define $v|P$ for $v \neq \infty$.

By our computation of the reductions of E_a at the different places and the definition of the conductor $\mathcal{N}_a \in \mathrm{Div}(\mathbb{P}^1)$ of E_a, we find:

$$\mathcal{N}_a = 2 \cdot (\infty) + \sum_{v|\Delta} 1 \cdot (v). \tag{2.6}$$

To compute the degree of $\mathcal{N}_a$, we use the following lemma:

Lemma 2.4. *We have:*

$$\sum_{v|\Delta} \deg v = 2q^a.$$

Proof. By combining the explicit expression for Δ from (2.2) and Lemma 2.2, we see that we can write:

$$\Delta = 16 \prod_{v \mid \Delta} B_v.$$

Now note that for all places in the product we have $\deg v = \deg B_v$, and by comparing with $\deg \Delta = 2q^a$, we find the desired result. □

Now for the degree of the conductor of E_a, we get the following:

Proposition 2.5. *We have* $\deg \mathcal{N}_a = 2(q^a + 1)$.

Proof. This follows directly by taking the degree of (2.6), which is $\mathbb{Z}$-linear, using Lemma 2.4 and by noting that $\deg(\infty) = 1$. □

In the same way we find an expression for $\Delta_{\min}(E_a) \in \mathrm{Div}(\mathbb{P}^1)$. Using table 4.1 from [Sil94, IV.9], we find that for $v \neq \infty$ with $v \mid \Delta$ that $\mathrm{ord}_v(\Delta_v(E_a)) = 1$, and for $v = \infty$, we find $\mathrm{ord}_\infty(\Delta') = 4q^a + 6$, with Δ' as in (2.5). Hence we have:

$$\Delta_{\min}(E_a) = (4q^a + 6) \cdot (\infty) + \sum_{v \mid \Delta} 1 \cdot (v), \tag{2.7}$$

and in the same way as for the conductor, we find:

Proposition 2.6. *We have* $\deg \Delta_{\min}(E_a) = 6(q^a + 1)$.

Proof. This is completely analogous to the proof of Proposition 2.5. □

Recall that we defined $N_a := q^{\deg \mathcal{N}_a}$ and $H(E_a) := q^{(1/12) \deg \Delta_{\min}(E_a)}$, so we now get the following:

Corollary 2.7. *We have* $N_a = q^{2(q^a+1)}$ *and* $H(E_a) = q^{(q^a+1)/2}$. *Note that the exponents are both integers. Furthermore, we find:*

$$\frac{\log H(E_a)}{\log N_a} = \frac{q^a + 1}{2} \log q \cdot \frac{1}{2(q^a + 1) \log q} = \frac{1}{4}$$

2.3 Tamagawa number and torsion of E_a

For a place v of K, we let K_v be the the completion of K at v, and we define $c_v(E_a) := \#(E_a(K_v)/(E_a)_0(K_v))$ and recall that we defined the Tamagawa number of E_a over K to be the product of c_v over all places of K:

$$\tau(E_a) := \prod_v c_v(E_a). \tag{2.8}$$

We use this definition and the results on reductions from section 2.1 to compute the Tamagawa number of E_a.

Proposition 2.8. *The Tamagawa number of E_a is given by $\tau(E_a) = 4$.*

Proof. Using the reduction types we found in (2.3), and looking at table 4.1 of [Sil94, Ch. IV.9], we find the following values:

place v	$c_v(E_a)$
$v \nmid \wp_a(t)^2+4$	1
$v \mid \wp_a(t)^2+4$	1
∞	4

,

and combining this with (2.8), we easily see that $\tau(E_a)$ is equal to 4. □

We know that the torsion subgroup of $E_a(K)$ is finite, and we can actually compute it explicitly

Proposition 2.9. *The torsion subgroup $E_a(K)_{\text{tors}} \subseteq E_a(K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and it is generated by the point $(0,0)$.*

Proof. For short-hand notation, we will write $T := E_a(K)_{\text{tors}}$. Since E_a is given by the short Weierstrass model (2.1), we know that a point $(x,y) \in E_a(\overline{K})$ is 2-torsion, if and only if $y = 0$. Hence we are looking for solutions of the equation

$$x(x^2 + \wp_a(t)x - 1) = 0,$$

which are exactly given by the following: $x_0 = 0$, $x_1 = (-\wp_a(t) + \sqrt{\wp_a(t)^2+4})/2$ and $x_2 = (-\wp_a(t) - \sqrt{\wp_a(t)^2+4})/2$. Hence the 2-torsion of $E_a(\overline{K})$ is given by:

$$E_a(\overline{E})[2] = \{O, (0,0), (x_1,0), (x_2,0)\},$$

and note that $K(x_1) = K(x_2) = K(\sqrt{\wp_a(t)^2+4})$, which has degree 2 over K because $\wp_a(t)^2+4$ is square-free (see Lemma 2.2), and hence $(x_1,0)$ and $(x_2,0)$ are not K-rational, so:

$$T[2] = \{O, (0,0)\} \cong \mathbb{Z}/2\mathbb{Z}.$$

The next step is to examine $T[p^\infty]$. If we have a nontrivial element $x \in T[p^k]$ for some k, then $[p^{k-1}]x \in T[p]$ is also nontrivial, hence if $T[p^\infty] \neq 0$, then also $T[p] \neq 0$. From [Ulm11, Lect. 1, Prop. 7.3] we then know that $j(E_a) \in K^p$. However, from (2.2) we see that

$$j(E_a) = \frac{256(\wp_a(t)^2+3)^3}{\wp_a(t)^2+4},$$

and we easily see that the numerator is not a p-th power. Hence in fact we have $T[p^\infty] = 0$. Let $T' := \{P \in E_a(K)_{\text{tors}} : \text{ord}(P) \text{ coprime with } p\}$. We now know that $T' = T$. Note that E_a has reduction type $I^*_{4q^a}$, and let $G(I^*_{4q^a})$ be as in [SS10, Par. 7.2], and from [SS10, Lem. 7.3] we know that $G(I^*_{4q^a}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Furthermore, from [SS10, Lem. 7.8], we have an injection $T' \hookrightarrow G(I^*_{4q^a}) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Since $T' = T$ and $T[2] \cong \mathbb{Z}/2\mathbb{Z}$, we must have $T \cong \mathbb{Z}/2\mathbb{Z}$, which concludes our proof. □

3 The L-function

In this section we will compute the L-function of E_a over K. We start with setting up some notation and definitions.

Definition 3.1. Define

$$P_q(a) := \{B \in \mathbb{F}_q[t] : B \text{ monic, irreducible and } \deg(B)|a\} \setminus \{t\},$$

where we also identify the elements of $P_q(a)$ with finite places $v \neq 0$ of K with degree dividing a. Recall that for $v \in P_q(a)$, we have that $g(\beta)$ and $\{\alpha(\beta), \alpha'(\beta)\}$ are the same for any $\beta \in v$, by Propositions 1.22.(ii) and 1.27.(ii). Hence we can set $g(v) := g(\beta)$ and $\{\alpha(v), \alpha'(v)\} := \{\alpha(\beta), \alpha'(\beta)\}$ for any $\beta \in v$.

The main result of this section is:

Theorem 3.2. *The L-function $L(E_a, T)$ is given by:*

$$L(E_a, T) = \prod_{v \in P_q(a)} (1 - \alpha(v)g(v)T^{d_v})(1 - \alpha'(v)g(v)T^{d_v}) \in \mathbb{Z}[T]$$

3.1 Preliminary lemmas

We first state two lemmas that we will use in the computation of the L-function. For any $n \geq 1$ and $\tau \in \mathbb{F}_{q^n} \cup \{\infty\}$, define

$$A_a(\tau, q^n) := q^n + 1 - \left|(\widetilde{E_a})_\tau(\mathbb{F}_{q^n})\right|, \tag{3.1}$$

where $(\widetilde{E_a})_\tau$ denotes the reduction of (a minimal integral model at v) of E_a, modulo the place v to which τ belongs.

Lemma 3.3. *For the L-function of E_a, we have the following:*

$$\log(L(E_a, T)) = \sum_{n=1}^{\infty} \left(\sum_{\tau \in \mathbb{F}_{q^n} \cup \{\infty\}} A_a(\tau, q^n) \right) \frac{T^n}{n}. \tag{3.2}$$

Lemma 3.4. *Let $n \geq 1$ and $z \in \mathbb{F}_{q^n}$. Then we have:*

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

Proofs of these lemmas can be found in [Gri18, Lem. 3.5] and [Gri18, Lem. 2.4] respectively.

3.2 Proof of Theorem 3.2

Note that $(\widetilde{E_a})_\tau$ is a cubic plane curve over the residue field $\mathbb{F}(v)$ of K at v, which is not necessarily smooth. To compute the values of A_a, we use the following lemma:

Lemma 3.5. *Let $n \geq 1$. We distinguish between two cases:*

(i) Let $\tau \in \mathbb{F}_{q^n}$ and let v be the finite place of K to which τ belongs. Then we have an affine model $(\widetilde{E_a})_\tau : y^2 = f_\tau(x)$, with $f_\tau(x) := x^3 + \wp_a(\tau)x^2 - x$. Let $\lambda_{q^n} : \mathbb{F}_{q^n}^* \to \mathbb{C}^*$ be the quadratic multiplicative character of $\mathbb{F}_{q^n}$, extended with $\lambda(0) := 0$. Then we have:

$$A_a(\tau, q^n) = -\sum_{x \in \mathbb{F}_{q^n}} \lambda(f_\tau(x)).$$

(ii) We have $A_a(\infty, q^n) = 0$.

Proof. Note that for (i), we saw in Lemma 2.1, $y^2 = x^3 + \wp_a(t)x^2 - x$ is a minimal integral model at all finite places v, hence we can pick $f_\tau(x) = x^3 + \wp_a(\tau)x^2 - x$. Then we use the following counting argument for the number of points on $(\widetilde{E_a})_\tau$:

$$\begin{aligned}\left|(\widetilde{E_a})_\tau(\mathbb{F}_{q^n})\right| &= 1 + \sum_{x \in \mathbb{F}_{q^n}} |\{y \in \mathbb{F}_{q^n} : y^2 = f_\tau(x)\}| \\ &= 1 + \sum_{x \in \mathbb{F}_{q^n}} (1 + \lambda_{q^n}(f_\tau(x))) \\ &= 1 + q^n + \sum_{x \in \mathbb{F}_{q^n}} \lambda_{q^n}(f_\tau(x)),\end{aligned}$$

where we also counted the point at infinity on $(\widetilde{E_a})_\tau$, which is $\mathbb{F}(v)$-rational, and hence also $\mathbb{F}_{q^n}$-rational. The second equality follows from the fact that $\lambda_{q^n}(\alpha) = 1$ if $\alpha \in \mathbb{F}_{q^n}^*$ is a square, giving two solutions, $\lambda_{q^n}(\alpha) = -1$ if $\alpha \in \mathbb{F}_{q^n}^*$ is not a square, so no solutions, and $\lambda_{q^n}(0) = 0$, giving 1 solution. Using the definition of $A_a(\tau, q^n)$, we then find:

$$A_a(\tau, q^n) = q^n + 1 - \left|(\widetilde{E_a})_\tau(\mathbb{F}_{q^n})\right| = -\sum_{x \in \mathbb{F}_{q^n}} \lambda_{q^n}(f_\tau(x)).$$

Now for (ii), note that E_a has additive reduction at $\tau = \infty$, hence $E' := (\widetilde{E_a})_\tau$ has a cusp over the residue field $\mathbb{F}(v)$, so exactly one singular point P, which is $\mathbb{F}(v)$-rational, hence also $\mathbb{F}_{q^n}$-rational. The set of non-singular $\mathbb{F}_{q^n}$-rational points $E'(\mathbb{F}_{q^n})_{\mathrm{ns}}$ of E' forms a group, for which it is known that $E'(\mathbb{F}_{q^n})_{\mathrm{ns}} \cong \mathbb{F}_{q^n}^+$ (for a proof, see [Sil09, Prop. III.2.5]). Note that $E'(\mathbb{F}_{q^n}) = E'(\mathbb{F}_{q^n})_{\mathrm{ns}} \sqcup \{P\}$, and hence $|E'(\mathbb{F}_{q^n})| = |\mathbb{F}_{q^n}| + 1 = q^n + 1$, from which we get $A_a(\infty, q^n) = 0$. □

Since $A_a(\infty, q^n) = 0$, we ignore the term with $\tau = \infty$. Using the result from Lemma 3.5.(i), we find the following for the coefficients of the series in (3.2):

$$\begin{aligned}-\sum_{\tau \in \mathbb{F}_{q^n}} A_a(\tau, q^n) &= \sum_{x \in \mathbb{F}_{q^n}} \sum_{\tau \in \mathbb{F}_{q^n}} \lambda_{q^n}(x^3 + \wp_a(\tau)x^2 - x) \\ &= \sum_{x \in \mathbb{F}_{q^n}} \sum_{z \in \mathbb{F}_{q^n}} \lambda_{q^n}(x^3 + zx^2 - x) \cdot |\{\tau \in \mathbb{F}_{q^n} : \wp_a(\tau) = z\}| = (*).\end{aligned}$$

Putting $M_{\mathbb{F}_{q^n}}(\beta) := \sum_{x\in\mathbb{F}_{q^n}}\sum_{z\in\mathbb{F}_{q^n}} \lambda_{q^n}(x^3+zx^2-x)\psi_{q^n}(\beta z)$ and using Lemma 3.4, we find:

$$(*) = \sum_{\beta\in\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n}} \left(\sum_{x\in\mathbb{F}_{q^n}}\sum_{z\in\mathbb{F}_{q^n}} \lambda_{q^n}(x^3+zx^2-x)\psi_{q^n}(\beta z)\right) = \sum_{\beta\in\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n}} M_{\mathbb{F}_{q^n}}(\beta).$$

We can write $M_{\mathbb{F}_{q^n}}(\beta)$ as the product of a Kloosterman sum and a Gauss sum, for which we use the results from section 1.3.

Lemma 3.6. *Let $n \geq 1$ and $\beta \in \mathbb{F}_{q^n}$. Then we have:*

$$M_{\mathbb{F}_{q^n}}(\beta) = \begin{cases} \mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n}; -\beta^2)\cdot\lambda_{q^n}(\beta)\mathrm{G}_{\mathbb{F}_{q^n}}(\lambda_{q^n},\psi_{q^n}) & , \textit{if } \beta \neq 0 \\ 0 & , \textit{if } \beta = 0 \end{cases}.$$

Proof. Write $\psi_\beta : \mathbb{F}_{q^n} \to \mathbb{C}^*$ for the additive character on $\mathbb{F}_{q^n}$, defined by $\psi_\beta(z) = \psi_{q^n}(\beta z)$ for all $z \in \mathbb{F}_{q^n}^*$. We can rewrite the expression of $M_{\mathbb{F}_{q^n}}(\beta)$ as follows:

$$\begin{aligned} M_{\mathbb{F}_{q^n}}(\beta) &= \sum_{x\in\mathbb{F}_{q^n}}\sum_{z\in\mathbb{F}_{q^n}} \lambda_{q^n}(x^3+zx^2-x)\psi_{q^n}(\beta z) \\ &= \sum_{x\in\mathbb{F}_{q^n}^*}\sum_{z\in\mathbb{F}_{q^n}} \lambda_{q^n}(x^3+zx^2-x)\psi_\beta(z) \\ &= \sum_{x\in\mathbb{F}_{q^n}^*} \lambda_{q^n}(x^2)\sum_{z\in\mathbb{F}_{q^n}} \lambda_{q^n}(x+z-x^{-1})\psi_\beta(z) \\ &= \sum_{x\in\mathbb{F}_{q^n}^*}\sum_{y\in\mathbb{F}_{q^n}} \lambda_{q^n}(y)\psi(y+x^{-1}-x) \\ &= \left(\sum_{x\in\mathbb{F}_{q^n}^*} \psi_\beta(x^{-1}-x)\right)\cdot\left(\sum_{y\in\mathbb{F}_{q^n}} \lambda_{q^n}(y)\psi_\beta(y)\right) \end{aligned}$$

Now the case when $\beta = 0$ is clear, as then ψ_β becomes the trivial additive character of $\mathbb{F}_{q^n}$, hence the second factor vanishes (see Lemma 1.18). For $\beta \neq 0$, the result now follows from the definitions of quadratic Gauss and Kloosterman sums and applying Lemmas 1.19 and 1.24.(ii). □

This is a very useful result, as we saw in section 1.3 how to write the factors of $M_{\mathbb{F}_{q^n}}(\beta)$ in terms of $g(\beta)$, $\alpha(\beta)$ and $\alpha'(\beta)$. Note that $M_{\mathbb{F}_{q^n}}(\beta)(0) = 0$ for all $n \geq 1$, so removing this term and applying Propositions 1.22.(i) and 1.27.(i), and further rewriting, we get:

$$\begin{aligned}
-\log(L(E_a,T)) &= \sum_{n=1}^{\infty}\left(\sum_{\beta\in(\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n})\setminus\{0\}} M_{\mathbb{F}_{q^n}}(\beta)\frac{T^n}{n}\right)\\
&= \sum_{n=1}^{\infty}\left(\sum_{\beta\in(\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n})\setminus\{0\}} \left[\mathrm{Kl}_{\mathbb{F}_{q^n}}(\psi_{q^n};-\beta^2)\right]\left[\lambda_{q^n}(\beta)\mathrm{G}_{\mathbb{F}_{q^n}}(\lambda_{q^n},\psi_{q^n})\right]\frac{T^n}{n}\right)\\
&= \sum_{n=1}^{\infty}\left(\sum_{\beta\in(\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n})\setminus\{0\}} \left(\alpha(\beta)^{n/d_\beta}+\alpha'(\beta)^{n/db}\right)g(\beta)^{n/d_\beta}\frac{T^n}{n}\right)\\
&= \sum_{n=1}^{\infty}\left(\sum_{\beta\in(\mathbb{F}_{q^a}\cap\mathbb{F}_{q^n})\setminus\{0\}} \left[(\alpha(\beta)g(\beta))^{n/d_\beta}+(\alpha'(\beta)g(\beta))^{n/d_\beta}\right]\frac{T^n}{n}\right)\\
&= \sum_{\beta\in\mathbb{F}_{q^a}^*}\left(\sum_{m\geq 1}\left[(\alpha(\beta)g(\beta))^m+(\alpha'(\beta)g(\beta))^m\right]\frac{T^{md_\beta}}{md_\beta}\right)\\
&= \sum_{\beta\in\mathbb{F}_{q^a}^*}\frac{1}{d_\beta}\left(\sum_{m\geq 1}\frac{(\alpha(\beta)g(\beta)T^{d_\beta})^m}{m}+\frac{(\alpha'(\beta)g(\beta)T^{d_\beta})^m}{m}\right)\\
&= \sum_{\beta\in\mathbb{F}_{q^a}^*}\frac{-1}{d_\beta}\log\left[(1-\alpha(\beta)g(\beta)T^{d_\beta})(1-\alpha'(\beta)g(\beta)T^{d_\beta})\right]
\end{aligned}$$

Note that by Propositions 1.22.(ii) and 1.27.(ii), $\alpha(\beta),\alpha'(\beta)$ and $g(\beta)$ are all constant along the Galois orbit $\{\beta,\beta^q,...,\beta^{q^{d_\beta-1}}\}$ of $\beta\in\mathbb{F}_{q^a}^*$. The Galois orbit of such β is exactly the place v of β in $\mathbb{F}_{q^a}$, which corresponds to a unique monic polynomial B_v, with degree d_β which divides a. Hence grouping the d_β terms in the above sum belonging to the same place as β, and writing $\alpha(v),\alpha'(v)$ and $g(v)$ for their respective values of $\alpha(\beta),\alpha'(\beta)$ and $g(\beta)$, we find:

$$\log(L(E_a,T)) = \sum_{v\in P_q(a)}\log\left[(1-\alpha(v)g(v)T^{d_v})(1-\alpha'(v)g(v)T^{d_v})\right],$$

where $P_q(a) := \{B\in\mathbb{F}_q[t] : B \text{ monic, irreducible and } \deg(B)|a\}\setminus\{t\}$. Finally, exponentiating both sides, we find the expression of the L-function:

$$L(E_a,T) = \prod_{v\in P_q(a)}(1-\alpha(v)g(v)T^{d_v})(1-\alpha'(v)g(v)T^{d_v}) \tag{3.3}$$

4 Consequences of the L-function

4.1 The special value

Define the special value of E_a to be $L^*(E_a) := L(E_a, q^{-1})$. Now that we have an explicit expression for the L-function, we get the following:

$$L^*(E_a) = \prod_{v \in P_q(a)} \left(1 - \frac{\alpha(v)g(v)}{q^{d_v}}\right)\left(1 - \frac{\alpha'(v)g(v)}{q^{d_v}}\right) \in \mathbb{Q}, \tag{4.1}$$

where we use the fact that $L(E_a, T)$ is a polynomial over $\mathbb{Z}$ to see that $L^*(E_a)$ lies in $\mathbb{Q}$. We are interested in whether $L^*(E_a)$ is zero or not. We first introduce the following notation.

Definition 4.1. Let $v \in P_q(a)$. Recalling the results from Proposition 1.27, we can choose $\alpha(v)$ to have non-negative imaginary part and $\alpha'(v)$ be its complex conjugate. We can then define $\theta_v \in [0, \pi]$ to be such that $\alpha(v) = q^{d_v/2}e^{i\theta_v}$ and $\alpha'(v) = q^{d_v/2}e^{-i\theta_v}$.

Similarly, using Proposition 1.22.(iii) we define $\psi_v \in \{0, \pi/2, \pi, 3\pi/2\}$ to be such that $g(v) = q^{d_v/2}e^{i\psi_v}$.

Using this, we can rewrite (4.1) as

$$L^*(E_a) = \prod_{v \in P_q(a)} \left(1 - e^{i(\psi_v + \theta_v)}\right)\left(1 - e^{i(\psi_v - \theta_v)}\right). \tag{4.2}$$

The result about the order of vanishing of $L(E_a, T)$ at q^{-1} is stated in the following Proposition:

Proposition 4.2. *We have* $L^*(E_a) > 0$*, and hence* $\mathrm{ord}_{T=q^{-1}} L(E_a, T) = 0$.

Proof. We will first prove that all the factors in (4.2) are nonzero, from which we conclude that $L^*(E_a) \neq 0$. For this it suffices to prove that for any v, we have $\psi_v \pm \theta_v \notin 2\pi\mathbb{Z}$. This is automatically satisfied if $\theta_v \notin \{0, \pi/2, \pi\}$ for any $v \in P_q(a)$. Let $\beta \in v$ be arbitrary and note that $\{\alpha(\beta), \alpha'(\beta)\} = \{\alpha(v), \alpha'(v)\}$. If $\theta_v \in \{0, \pi\}$, then Theorem 1.25 would imply that:

$$|\mathrm{Kl}_{\mathbb{F}_{q^{d_\beta}}}(\psi_\beta; -\beta^2)| = |\alpha(\beta) + \alpha'(\beta)| = 2q^{d_\beta/2},$$

and similarly if $\theta_v = \pi/2$, we would get

$$|\mathrm{Kl}_{\mathbb{F}_{q^{d_\beta}}}(\psi_\beta; -\beta^2)| = |\alpha(\beta) + \alpha'(\beta)| = 0,$$

which are both in contradiction with Proposition 1.28 , and hence $\theta_v \notin \{0, \pi/2, \pi\}$, so indeed $L^*(E_a) \neq 0$.

Recall the definition of the L-function of E_a:

$$L(E_a, T) = \prod_{\text{good } v} (1 - a_v(E_a)T^{d_v} + q^{d_v}T^{2d_v})^{-1} \cdot \prod_{\text{bad } v} (1 - a_v(E_a)T^{d_v})^{-1}. \tag{4.3}$$

Recall that for all places v of K, we have the Hasse-Weil bound:

$$|a_v(E_a)| \leq 2\sqrt{q}^{d_v}. \tag{4.4}$$

This bound implies that the Euler product in (4.3) converges for all T with $|T| < q^{-3/2}$. Furthermore, for all real T with $|T| < q^{-3/2}$ and all places v of K of good reduction, we have:

$$1-a_v(E_a)T^{d_v}+q^{d_v}T^{2d_v} \geq 1-(2q^{d_v/2})\cdot q^{-3d_v/2}+q^{d_v}q^{-3d_v} = 1-2q^{-d_v}+q^{-2d_v} = (1-q^{-d_v})^2 > 0 \quad (4.5)$$

and for all places v of K of bad reduction, we have $\left|a_v(E_a)\right| \leq 1$, and hence:

$$1-a_v(E_a)T^{d_v} \geq 1-q^{-3d_v/2} > 0. \quad (4.6)$$

Now, for all $T \in \mathbb{R}$ with $|T| < q^{-3/2}$ we know (4.3) converges, and it is a product of positive factors, hence $L(E_a,T) > 0$ for all $T \in (-q^{-3/2}, q^{-3/2})$. Also, from [Ulm11, Lect 1. Thm. 9.3], we know that the zeros of $L(E_a,T)$ all have absolute value q^{-1}, hence there are no zeros of $L(E_a,T)$ on $[q^{-3/2}, q^{-1})$, so $L(E_a,T) > 0$ for all $T \in (-q^{-3/2}, q^{-1})$. Hence by continuity of $T \mapsto L(E_a,T)$, $L^*(E_a) \geq 0$. □

4.2 The BSD conjecture

In general, the BSD conjecture is still an open problem, but there are special cases for which it has been proved. In particular, we will use the following theorem:

Theorem 4.3 (rank 0 BSD). *Let E/K be a nonisotrivial elliptic curve. Assume that $L^*(E) \neq 0$. Then:*

(i) $\operatorname{rank} E(K) = 0$.

(ii) $Ш(E)$ *is finite.*

(iii) We have the following expression for the special value:

$$L^*(E) = \frac{|Ш(E/K)|}{H(E)} \frac{\tau(E)\cdot q}{|E(K)_{\text{tors}}|^2}. \quad (4.7)$$

Sketch of the proof. We only give a sketch of the proof. More details can be found in [Ulm11, Lect. 1, Th. 12.1]. Tate proved the following:

$$0 \leq \operatorname{rank} E(K) \leq \operatorname{ord}_{T=q^{-1}} L(E,T).$$

By the assumption $L^*(E) \neq 0$, we have $\operatorname{ord}_{T=q^{-1}} L(E,T) = 0$, hence also $\operatorname{rank} E(K) = 0$. Later, Kato and Trihan proved that equality between $\operatorname{rank} E(K)$ and $\operatorname{ord}_{T=q^{-1}} L(E,T)$ is equivalent to $Ш(E)$ being finite and also that (4.7) holds in that case. □

Corollary 4.4. *Let $K = \mathbb{F}_q(t)$ with $\operatorname{char}(K) \geq 5$. For any integer $a \geq 1$, let E_a/K be the elliptic curve as defined in (2.1). Then Theorem 4.3 holds for E_a.*

Proof. As we saw in Proposition 4.2, we have $L^*(E_a) \neq 0$ and we proved in section 2 that E_a is nonisotrivial. Hence the results of the theorem hold for E_a. □

In particular, we get the following results:

Corollary 4.5. $\operatorname{rank} E_a(K) = 0$*, and hence* $E_a(K) = E_a(K)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$*.*

Proof. This is a direct consequence of Corollary 4.4 and Proposition 2.9. □

Corollary 4.6. *The Tate-Shafarevich group* $\text{Ш}(E_a)$ *of* E_a/K *is finite.*

4.3 Relation between bounds on $L^*(E_a)$ and $|\text{Ш}(E_a)|$

We can now use the expression from Theorem 4.3.(iii) to relate bounds on $L^*(E_a)$ with bounds on $|\text{Ш}(E_a)|$. For this, it is actually more useful to rewrite (4.7) slightly. Recall that we defined $N_a = q^{\deg \mathcal{N}_a}$. Then from (4.7), we get:

$$\frac{\log L^*(E_a)}{\log N_a} = \frac{\log |\text{Ш}(E_a)|}{\log N_a} + \frac{\log(\tau(E_a)q)}{\log N_a} - \frac{\log H(E_a)}{\log N_a} - \frac{\log |E_a(K)_{\text{tors}}|^2}{\log N_a}, \quad (4.8)$$

which we can make more explicit with the following proposition:

Proposition 4.7. *We have:*

$$\frac{\log L^*(E_a)}{\log N_a} = \frac{\log |\text{Ш}(E_a)|}{\log N_a} - \frac{1}{4} + o(1), \text{ as } a \to \infty. \quad (4.9)$$

Proof. As we saw in Corollary 2.7, we have:

$$\frac{\log H(E_a)}{\log N_a} = \frac{1}{4}.$$

Furthermore, since $\log N_a = 2(q^a + 1)\log q$ and from Propositions 2.8 and 2.9 it follows that $\log(\tau(E_a)q) \leq \log(4q)$ and $\log |E_a(K)_{\text{tors}}|^2 \leq \log 4$ respectively, both other terms are $o(1)$ as $a \to \infty$. □

5 Bounds on the special value

In this section we will find upper and lower bounds on $L^*(E_a)$, which we will then be able to relate to bounds on $|Ш(E_a)|$ using Proposition 4.7. First, we will slightly rewrite (4.2). Let $v \in P_q(a)$ with $\theta_v \in [0, \pi]$ as in Proposition 1.25.(iii), and $\psi_v \in \{0, \pi/2, \pi, 3\pi/2\}$ as in Proposition 1.20.(iii). Consider the occuring term of v in (4.2):

$$(1 - e^{i\psi_v} e^{i\theta_v})(1 - e^{i\psi_v} e^{-i\theta_v}) = 1 - e^{i\psi_v}(2\cos\theta_v) + e^{2i\psi_v},$$

and define $F_v \colon [0, \pi] \to \mathbb{R}$ by $F_v(\theta) := 1 - e^{i\psi_v}(2\cos\theta) + e^{2i\psi_v}$. From Proposition 4.2, we know that $L^*(E_a) > 0$, so $|L^*(E_a)| = L^*(E_a)$ and we can write:

$$L^*(E_a) = \prod_{v \in P_q(a)} |F_v(\theta_v)|. \tag{5.1}$$

Since ψ_v can attain only 4 different values, we list the possible values of $F_v(\theta)$ for all $\theta \in [0, \pi]$ explicitly:

ψ_v	$F_v(\theta)$
0	$2 - 2\cos\theta$
$\frac{\pi}{2}$	$-2i\cos\theta$
π	$2 + 2\cos\theta$
$\frac{3\pi}{2}$	$2i\cos\theta$

(5.2)

5.1 Upper bound

The main result of this section is as follows:

Theorem 5.1. *Let $N_a := q^{\deg \mathcal{N}_a}$. There exists a constant $c_q > 0$ depending only on q, such that for all $a \geq 1$:*

$$\frac{\log L^*(E_a)}{\log N_a} \leq \frac{c_q}{a}.$$

We will get this upper bound by bounding each factor in (5.1) and the number of factors. Note that from (5.2) we easily get $|F_v(\theta_v)| \leq 4$, independently of the value of ψ_v. For the number of terms, we need to bound $|P_q(a)|$ (recall that $P_q(a) = \{B \in \mathbb{F}_q[t] : B \text{ monic, irreducible, } \deg(B)|a\} \setminus \{t\}$). First, we define $\pi_q(n) := \#\{B \in \mathbb{F}_q[t] : B \text{ monic irreducible of degree } n\}$, and we use the following result:

Lemma 5.2. *For all $n \geq 1$, we have $\pi_q(n) = \frac{q^n}{n} + \mathcal{O}(q^{n/2})$, where the implicit constant depends only on q, and can be chosen to be at most 2.*

Proof. Note that the affine curve $\mathbb{A}^1$ has exactly q^n $\mathbb{F}_{q^n}$-rational points. If we group these by places, we get the following:

$$q^n = \sum_{d|n} d \cdot \#\{v \text{ finite place of } K : \deg v = d\} = \sum_{d|n} d \cdot \pi_q(d), \tag{5.3}$$

where we used the correspondence between finite places of K of degree d and monic irreducible polynomials of $\mathbb{F}_q[t]$ of degree d. Now let $\mu \colon \mathbb{N} \to \mathbb{N}$ be the Möbius function. By the Möbius inverion formula, we find from (5.3):

$$n\pi_q(n) = \sum_{d|n} \mu(n/d)q^d = q^n + \sum_{\substack{d|n \\ d<n}} \mu(n/d)q^d,$$

and hence:

$$\left|\pi_q(n) - \frac{q^n}{n}\right| \leq \frac{1}{n}\sum_{\substack{d|n \\ d<n}} q^d \leq \frac{1}{n}\sum_{d=1}^{n/2} q^d \leq \frac{q}{n} \cdot \frac{q^{n/2}-1}{q-1} = \mathcal{O}\left(\frac{q^{n/2}}{n}\right),$$

from which the desired result follows and it can be easily seen that the constant can be chosen to be $q/(q-1)$. □

A bound on $|P_q(a)|$ is now easily deduced

Lemma 5.3. *We have* $|P_q(a)| = \frac{q^a}{a} + \mathcal{O}(q^{a/2})$ *as* $a \to \infty$*, where the implicit constant depends only on* q*.*

Proof. Rewrite $|P_q(a)|$ (for $a \geq 2$) as follows:

$$\begin{aligned} |P_q(a)| &= \sum_{\substack{n|a \\ n\geq 2}} \pi_q(n) + (\pi_q(1) - 1) = \sum_{\substack{n|a \\ n\geq 2}} \left(\frac{q^n}{n} + \mathcal{O}(q^{n/2})\right) + (q-1) \\ &= \frac{q^a}{a} + \mathcal{O}(q^{a/2}) + \sum_{\substack{n|a \\ 2\leq n\leq a/2}} \left(\frac{q^n}{n} + \mathcal{O}(q^{n/2})\right) + \mathcal{O}(1), \text{ as } a \to \infty \end{aligned} \tag{5.4}$$

and for the remaining sum term, we find:

$$\begin{aligned} \sum_{\substack{n|a \\ 2\leq n\leq a/2}} \left(\frac{q^n}{n} + \mathcal{O}(q^{n/2})\right) &\leq \sum_{n=1}^{a/2} \left(\frac{q^n}{n} + \mathcal{O}(q^{n/2})\right) \leq a \cdot \left(\frac{2q^a}{a} + \mathcal{O}(q^{a/4})\right) \\ &= \mathcal{O}(q^{a/2}), \text{ as } a \to \infty \end{aligned}$$

and hence (5.4) actually reduces to:

$$|P_q(a)| = \frac{q^a}{a} + \mathcal{O}(q^{a/2}), \text{ as } a \to \infty.$$

□

We now have enough tools to prove Theorem 5.1.

Proof of Theorem 5.1. Using (5.1) and the fact that $|F_v(\theta_v)| \leq 4$, we get:

$$\frac{\log L^*(E_a)}{\log N_a} = \frac{1}{\log N_a} \sum_{v\in P_q(a)} \log|F_v(\theta_v)| \leq \frac{\log 4}{\log N_a}|P_q(a)|.$$

Recall that $\deg \mathcal{N}_a = 2(q^a+1)$, and hence $\log N_a = 2(q^a+1)\log q$. Combining this with Lemma 5.3, we get

$$\begin{aligned}\frac{\log L^*(E_a)}{\log N_a} &\leq \frac{\log 4}{2(q^a+1)\log q} \cdot \left(\frac{q^a}{a} + \mathcal{O}(q^{a/2}\right) \\ &\leq \frac{\log 4}{a} + \mathcal{O}(q^{-a/2}) \\ &\leq \frac{c_q}{a},\end{aligned}$$

for some $c_q > 0$ depending only on q. □

5.2 Lower bound

First we give a lower bound on the terms $|F_v(\theta_v)|$ appearing in (5.1).

Lemma 5.4. *Let $v \in P_q(a)$. Then for all $\theta \in [0,\pi]$, we have*

$$|F_v(\theta)| \geq \sin^2\theta\cos^2\theta,$$

and $\sin^2\theta_v\cos^2\theta_v > 0$.

Proof. The second part follows from the fact that $\sin^2\theta_v\cos^2\theta_v = 0$, if and only if $\theta_v \in \{0,\pi/2,\pi\}$, but as we saw in the proof of Proposition 4.2, this is not possible.

For the first part, note that $|F_v(\theta)|$ is either of the following options:

$$|F_v(\theta)| = \begin{cases} 2(1-\cos\theta) & \text{, if } \psi_v = 0 \\ 2|\cos\theta| & \text{, if } \psi_v \in \{\pi/2, 3\pi/2\} \\ 2(1+\cos\theta) & \text{, if } \psi_v = \pi \end{cases}.$$

Define $G\colon [0,\pi] \to \mathbb{R}$ by $G(\theta) := 2\min\{1-\cos\theta, |\cos\theta|, 1+\cos\theta\}$, and note that $|F_v(\theta)| \geq G(\theta)$ for all $\theta \in [0,\pi]$. Note that:

$$G(\theta) = \begin{cases} 2(1-\cos\theta) & \text{, if } \theta \in [0,\pi/3] \\ 2|\cos\theta| & \text{, if } \theta \in [\pi/3, 2\pi/3] \\ 2(1+\cos\theta) & \text{, if } \theta \in [2\pi/3,\pi] \end{cases}.$$

We will prove that $G(\theta) \geq \sin^2\theta\cos^2\theta$ on all three of the intervals. Note that for $\theta \in [\pi/3, 2\pi/3]$ we get:

$$\cos^2\theta\sin^2\theta \leq \cos^2\theta \leq |\cos\theta| \leq 2|\cos\theta| = G(\theta).$$

Note that the maps G and $\theta \mapsto \sin^2\theta\cos^2\theta$ are both symmetric around $\theta = \pi/2$, so we prove the desired inequality on $[0,\pi/3]$, from which the inequality on $[2\pi/3,\pi]$ will follow from symmetry. Note that $G(0) = \sin^2 0\cos^2 0 = 0$, and furthermore, we have:

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}\theta}\left[2 - 2\cos\theta - \sin^2\theta\cos^2\theta\right] &= 2\sin\theta - \left(2\sin\theta\cos^3\theta + 2\sin^3\theta\cos\theta\right) \\ &= 2\sin\theta - 2\sin\theta\cos\theta\left(\cos^2\theta + \sin^2\theta\right) \\ &= 2\sin\theta(1-\cos\theta),\end{aligned}$$

and for all $\theta \in [0, \pi/3]$, we have $2\sin\theta(1-\cos\theta) \geq 0$, so indeed the inequality $G(\theta) \geq \sin^2\theta\cos^2\theta$ holds on $[0, \pi/3]$, hence also on $[2\pi/3, \pi]$ and hence on all of $[0, \pi]$. □

Now we define the function $w\colon [0, \pi] \to \mathbb{R}$ by:

$$w(\theta) := \begin{cases} 0 & \text{, if } \theta \in \{0, \pi/2, \pi\} \\ -\log(\sin^2\theta\cos^2\theta) & \text{, otherwise} \end{cases} \tag{5.5}$$

Let $v \in P_q(a)$. Since $|F_v(\theta_v)| > 0$, $\log|F_v(\theta_v)|$ is well-defined and from Lemma 5.4 it follows that

$$-\log(|F_v(\theta_v)|) \leq w(\theta_v).$$

Using this and (5.1), we get the following:

$$-\frac{\log L^*(E_a)}{\log N_a} = \frac{1}{\log N_a} \sum_{v \in P_q(a)} -\log|F_v(\theta_v)| \leq \frac{|P_q(a)|}{\log N_a} \cdot \left(\frac{1}{|P_q(a)|} \sum_{v \in P_q(a)} w(\theta_v) \right) \tag{5.6}$$

and finding a lower bound for $\frac{\log L^*(E_a)}{\log N_a}$ is equivalent to finding an upper bound for (5.6). As we saw in the proof of Theorem 5.1, we have:

$$\frac{|P_q(a)|}{\log N_a} = \mathcal{O}\left(1/a\right), \text{ as } a \to \infty, \tag{5.7}$$

so it remains to examine the second factor of the right hand side of (5.6). We introduce the following notation:

Definition 5.5. Let $f\colon [0, \pi] \to \mathbb{R}$ be a function. Then for any $a \geq 1$, we define:

$$\operatorname{Avg}(f, a) := \frac{1}{|P_q(a)|} \sum_{v \in P_q(a)} f(\theta_v).$$

The main result of the remainder of this section is the following:

Theorem 5.6. *There exists a constant $C \in \mathbb{R}$, such that:*

$$\operatorname{Avg}(w, a) \overset{a\to\infty}{\longrightarrow} C. \tag{5.8}$$

This theorem will provide us with the desired lower bound:

Corollary 5.7. *There exists a constant $c_q' > 0$ depending only on q, such that for all $a \geq 1$ we have:*

$$-\frac{c_q'}{a} \leq \frac{\log L^*(E_a)}{\log N_a}. \tag{5.9}$$

Proof. This follows directly by combining (5.6), (5.7) and (5.8). □

To prove Theorem 5.6, we use the two theorems below. First we introduce another new notation:

Definition 5.8. Let $g\colon [0,\pi] \to \mathbb{R}$ be a function, and write

$$\int_{\mathrm{ST}} g := \int_0^\pi g(\theta) \cdot \frac{2}{\pi} \sin^2 \theta \, \mathrm{d}\theta, \tag{5.10}$$

whenever this integral is well-defined. In this integral, g is said to be integrated with respect to the *Sato-Tate measure.*

Theorem 5.9 (Griffon). *There exists a constant $c_q > 0$, depending only on q, such that for all continuously differentiable functions $g\colon [0,\pi] \to \mathbb{R}$, we have:*

$$\left| \mathrm{Avg}(g,a) - \int_{\mathrm{ST}} g \right| \leq c_q \cdot \frac{a^{1/2}}{q^{a/4}} \cdot \int_0^\pi |g'(t)| \, \mathrm{d}t, \ \text{ as } a \to \infty. \tag{5.11}$$

Theorem 5.10 (Griffon). *There exists a constant $\gamma_p > 0$ depending only on p, such that for all $a \geq 1$ and $v \in P_q(a)$, we have:*

(i) $\theta_v > (q^a)^{-\gamma_p}$

(ii) $\pi - \theta_v > (q^a)^{-\gamma_p}$

(iii) $|\pi/2 - \theta_v| > (q^a)^{-\gamma_p}$

Proofs of Theorems 5.9 and 5.10 can be found in [Gri18, Thm 5.6] and [Gri18, Thm. 4.1] respectively.

5.2.1 Proof of Theorem 5.6

As in Theorem 5.9 we are going to compare $\mathrm{Avg}(w,a)$ to an integral, which will give us the constant $C \in \mathbb{R}$:

Lemma 5.11. *Let $w\colon [0,\pi] \to \mathbb{R}$ be as in* (5.5). *There exists a real number $C \in \mathbb{R}$, such that*

$$\int_{\mathrm{ST}} w = C, \tag{5.12}$$

in other words: the integral converges.

Proof. Define the function $\varphi\colon [0,\pi] \to \mathbb{R}$ by $\theta \mapsto -\log(\sin^2\theta \cos^2\theta)\sin^2\theta$. Note that φ is symmetric around $\pi/2$. Furthermore, φ is continuous on $[0,\pi/2)$, hence locally integrable on $[0,\pi/2)$. Now, around $\pi/2$, the Taylor expansion of φ is given by:

$$2\log(x-\pi/2) + (x-\pi/2)^2(-2\log(x-\pi/2) - 4/3) + \mathcal{O}\left((x-\pi/2)^4\right),$$

which is locally integrable around $\pi/2$, hence φ is integrable on $[0,\pi/2]$, and by symmetry on all of $[0,\pi]$. Hence $\int_{\mathrm{ST}} w$ converges. □

Remark 5.12. One can actually compute the integral in Lemma 5.11, to get $C = \log 16$.

However, we cannot apply Theorem 5.9 directly to w, as w is not continuous. To fix this, we will multiply w with a smoothing function. Choose a non-decreasing continuously differentiable function $g_0\colon [0,1] \to \mathbb{R}$, such that:

$$g_0(x) = \begin{cases} 0, & \text{if } x \in [0,1/3] \\ 1, & \text{if } x \in [2/3,1] \end{cases} \tag{5.13}$$

and define the following smoothing functions:

Definition 5.13. Let $\varepsilon \in (0,1)$ and define the continuously differentiable function $g_\varepsilon\colon [0,\pi/2] \to \mathbb{R}$ by:

$$g_\varepsilon(x) := \begin{cases} g_0(x/\varepsilon) & , \text{if } x \in [0,\varepsilon] \\ 1 & , \text{if } x \in [\varepsilon, \pi/2-\varepsilon] \\ g_0((\pi/2-x)/\varepsilon) & , \text{if } x \in [\pi/2-\varepsilon, \pi/2] \end{cases}$$

and extend g_ε to a continuously differentiable function on $[0,\pi]$, by setting $g_\varepsilon(x) := g_\varepsilon(x-\pi/2)$, for all $x \in [\pi/2,\pi]$.

Using this, we define for any $\varepsilon \in (0,\pi/4)$ the function $w_\varepsilon\colon [0,\pi] \to \mathbb{R}$ by

$$w_\varepsilon(\theta) := w(\theta)g_\varepsilon(\theta), \text{ for all } \theta \in [0,\pi]. \tag{5.14}$$

Note that w_ε is a continuously differentiable function, and we have $w_\varepsilon(\theta) = w(\theta)$ for all $\theta \in [\varepsilon, \pi/2-\varepsilon] \cup [\pi/2+\varepsilon, \pi-\varepsilon]$. Also, note that both w and g_ε are periodic with period $\pi/2$, and on the interval $[0,\pi/2]$, they are both symmetric around $\pi/4$. Hence, w_ε is also periodic with period $\pi/2$, and symmetric around $\pi/4$.

We use the triangle inequality to get the following bound:

$$\begin{aligned}\left|\operatorname{Avg}(w,a) - \int_{\mathrm{ST}} w\right| \le \left|\operatorname{Avg}(w,a) - \operatorname{Avg}(w_\varepsilon,a)\right| + \left|\operatorname{Avg}(w_\varepsilon,a) - \int_{\mathrm{ST}} w_\varepsilon\right| \\ + \left|\int_{\mathrm{ST}} w_\varepsilon - \int_{\mathrm{ST}} w\right|,\end{aligned} \tag{5.15}$$

for which we will bound the 3 terms on the right hand side separately.

Proposition 5.14. *Let γ_p be as in Theorem 5.10. Then we have for all $0 < \varepsilon < \min\{(q^a)^{-\gamma_p}, \pi/4\}$:*

$$\left|\operatorname{Avg}(w,a) - \operatorname{Avg}(w_\varepsilon,a)\right| = 0. \tag{5.16}$$

Proof. Note that by the choice of ε, we have for all $v \in P_q(a)$ that $\theta_v \in [\varepsilon, \pi/2-\varepsilon] \cup [\pi/2+\varepsilon, \pi-\varepsilon]$. Hence for all v, we have $w(\theta_v) = w_\varepsilon(\theta_v)$, and hence:

$$\left|\operatorname{Avg}(w,a) - \operatorname{Avg}(w_\varepsilon,a)\right| = \left|\operatorname{Avg}(w - w_\varepsilon,a)\right| = 0$$

□

We will need to bound sin and cos. Since these functions are both concave on the interval $[0,\pi/2]$, we get the following linear bounds for all $\theta \in [0,\pi/2]$:

$$\begin{aligned}\sin\theta &\ge \frac{2\theta}{\pi}, \\ \cos\theta &\ge \frac{2(\pi/2-\theta)}{\pi}.\end{aligned} \tag{5.17}$$

For the second and third term of (5.15), we will first prove the following lemma:

Lemma 5.15. *For $\varepsilon \in (0, \pi/4)$, we have:*

$$\int_0^\pi \left|w'_\varepsilon(\theta)\right| \mathrm{d}\theta = \mathcal{O}(|\log \varepsilon|).$$

Proof. Note that since w_ε is symmetric around $x = \pi/4$, and periodic with period $\pi/2$ the same is also true for $|w'_\varepsilon|$. Using this, we can write:

$$\int_0^\pi \left|w'_\varepsilon(\theta)\right| \mathrm{d}\theta = 4\int_0^{\pi/4} \left|w'_\varepsilon(\theta)\right| \mathrm{d}\theta = 4\left(\int_0^\varepsilon \left|w'_\varepsilon(\theta)\right| \mathrm{d}\theta + \int_\varepsilon^{\pi/4} \left|w'_\varepsilon(\theta)\right| \mathrm{d}\theta\right), \tag{5.18}$$

and we will bound both integrals on the right hand side separately. Note that we have:

$$|w'_\varepsilon(\theta)| = \left|g_\varepsilon(\theta)w'(\theta) + w(\theta)g'_\varepsilon(\theta)\right| \leq \left|w'(\theta)\right| + w(\theta)|g'_\varepsilon(\theta)| \tag{5.19}$$

and we will find upper bounds for the different factors on the right hand side. To bound $|g'_\varepsilon(\theta)|$, note that on the interval $[0, \pi/4]$, we have by construction of g_ε:

$$g'_\varepsilon(\theta) = \left\{ \begin{array}{cl} \frac{1}{\varepsilon}g'_0(\theta/\varepsilon) & \text{, if } \theta \in [0,\varepsilon] \\ 0 & \text{, if } \theta \in [\varepsilon, \pi/4] \end{array} \right. .$$

Denote with $\|g'_0\|_\infty := \max_{x\in[0,1]} |g'_0(x)|$. Then we get:

$$\left|g'_\varepsilon(\theta)\right| \leq \left\{ \begin{array}{cl} \frac{1}{\varepsilon}\|g'_0\|_\infty & \text{, if } \theta \in [0,\varepsilon] \\ 0 & \text{, if } \theta \in [\varepsilon, \pi/4] \end{array} \right. . \tag{5.20}$$

Now we find an upper bound for $w(\theta)$. Note that by (5.17), we have for all $\theta \in (0, \pi/4]$: $(\sin\theta)^{-1} \leq \frac{\pi}{2\theta}$ and $(\cos\theta)^{-1} \leq \frac{\pi}{2(\pi/2-\theta)}$. Hence for all $\theta \in (0, \pi/4]$, we have:

$$w(\theta) = 2\log((\sin\theta\cos\theta)^{-1}) \leq 2\log\left(\frac{\pi^2}{4\theta(\pi/2-\theta)}\right) \leq 2\log\left(\frac{\pi}{\theta}\right), \tag{5.21}$$

where for the last inequality we used that $\pi/2 - \theta \geq \pi/4$. Using this, we get:

$$\int_0^\varepsilon w(\theta)\,\mathrm{d}\theta \ \leq\ -2\int_0^\varepsilon \log\left(\frac{\theta}{\pi}\right)\mathrm{d}\theta \ =\ -2\left[\theta\log\left(\frac{\theta}{\pi}\right) - \theta\right]_0^\varepsilon \ =\ \mathcal{O}(\varepsilon|\log\varepsilon|). \tag{5.22}$$

For the final factor $\left|w'(\theta)\right|$, note that we have:

$$w'(\theta) = 2\left(\frac{\sin\theta}{\cos\theta} - \frac{\cos\theta}{\sin\theta}\right) = 2\left(\frac{\sin^2\theta - \cos^2\theta}{\sin\theta\cos\theta}\right) = -2\left(\frac{\cos 2\theta}{\sin\theta\cos\theta}\right),$$

and combining this with (5.17), we find for $\theta \in (0, \pi/4]$:

$$\left|w'(\theta)\right| \leq \frac{2}{\sin\theta\cos\theta} \leq \frac{2}{\frac{2\theta}{\pi}\cdot\frac{2(\pi/2-\theta)}{\pi}} = \frac{\pi^2}{2\theta(\pi/2-\theta)} \leq \frac{2\pi}{\theta}, \tag{5.23}$$

where we again used that $\pi/2 - \theta \geq \pi/4$.

Now that we have bounds for all factors, we will find upper bounds for the integrals in (5.18). For the first integral, note that $w_\varepsilon(\theta) = 0$ for $\theta \in [0, \varepsilon/3]$, hence $w_\varepsilon'(\theta) = 0$ for $\theta \in (0, \varepsilon/3)$, and we get using (5.19):

$$\int_0^\varepsilon \left|w_\varepsilon'(\theta)\right| \mathrm{d}\theta = \int_{\varepsilon/3}^\varepsilon \left|w_\varepsilon'(\theta)\right| \mathrm{d}\theta \leq \int_{\varepsilon/3}^\varepsilon \left|w'(\theta)\right| \mathrm{d}\theta + \int_{\varepsilon/3}^\varepsilon w(\theta)\left|g_\varepsilon'(\theta)\right| \mathrm{d}\theta. \quad (5.24)$$

From (5.23) we get for all $\theta \in [\varepsilon/3, \varepsilon]$ that $\left|w'(\theta)\right| \leq \frac{2\pi}{(\varepsilon/3)} = \frac{6\pi}{\varepsilon}$. Combined with (5.20) and (5.22), we find for (5.24):

$$\begin{aligned}\int_0^\varepsilon \left|w_\varepsilon'(\theta)\right| \mathrm{d}\theta \leq \int_0^\varepsilon \frac{6\pi}{\varepsilon} \mathrm{d}\theta + \frac{\|g_0'\|_\infty}{\varepsilon} \int_0^\varepsilon w(\theta) \, \mathrm{d}\theta = 6\pi + \frac{\|g_0'\|_\infty}{\varepsilon} \mathcal{O}(\varepsilon|\log \varepsilon|) \\ = \mathcal{O}(|\log \varepsilon|). \quad (5.25)\end{aligned}$$

For the second integral of the right hand side of (5.18), note that $|g_\varepsilon'(\theta)| = 0$ for all $\theta \in [\varepsilon, \pi/4]$. Then from (5.19) and (5.23) it follows that:

$$\begin{aligned}\int_\varepsilon^{\pi/4} \left|w_\varepsilon'(\theta)\right| \mathrm{d}\theta \leq \int_\varepsilon^{\pi/4} |w'(\theta)| \, \mathrm{d}\theta \leq \int_\varepsilon^{\pi/4} \frac{2\pi}{\theta} \mathrm{d}\theta = 2\pi(\log \frac{\pi}{4} - \log \varepsilon) \\ = \mathcal{O}(|\log \varepsilon|). \quad (5.26)\end{aligned}$$

Now combining (5.18) with (5.25) and (5.26), concludes our proof. □

Proposition 5.16. *Let $\varepsilon \in (0, \pi/4)$. Then we have the following bound:*

$$\left|\mathrm{Avg}(w_\varepsilon, a) - \int_{\mathrm{ST}} w_\varepsilon\right| = \mathcal{O}\left(\frac{a^{1/2}}{q^{a/4}} |\log \varepsilon|\right), \quad \textit{as } a \to \infty. \quad (5.27)$$

Proof. Since $w_\varepsilon \colon [0, \pi] \to \mathbb{R}$ is continuously differentiable, we can apply Theorem 5.9. Combining this with the result of Lemma 5.15, we get the desired bound. □

Proposition 5.17. *Let $\varepsilon \in (0, \varepsilon)$. Then we have the following bound:*

$$\left|\int_{\mathrm{ST}} w - \int_{\mathrm{ST}} w_\varepsilon\right| = \mathcal{O}(\varepsilon|\log \varepsilon|). \quad (5.28)$$

Proof. We can bound the third term of (5.15) as follows:

$$\begin{aligned}\left|\int_{\mathrm{ST}} w - \int_{\mathrm{ST}} w_\varepsilon\right| &= \left|\int_{\mathrm{ST}} w - w_\varepsilon\right| \leq \frac{2}{\pi} \int_0^\pi \left|w(\theta) - w_\varepsilon(\theta)\right| \sin^2(\theta) \, \mathrm{d}\theta \\ &\leq \frac{2}{\pi} \int_0^\pi (1 - g_\varepsilon(\theta)) w(\theta) \, \mathrm{d}\theta = \frac{8}{\pi} \int_0^{\pi/4} (1 - g_\varepsilon(\theta)) w(\theta) \, \mathrm{d}\theta \\ &= \frac{8}{\pi} \int_0^\varepsilon w(\theta) \, \mathrm{d}\theta,\end{aligned}$$

where we used the fact that $w - w_\varepsilon$ is symmetric around $x = \pi/4$ and periodic with period $\pi/2$. We also used that $g_\varepsilon(\theta) = 1$ for $\theta \in [\varepsilon, \pi/4]$. Using (5.22) from the proof of Lemma 5.15 now concludes our proof. □

Proof of Theorem 5.6. Let $C = \int_{\mathrm{ST}} w$ be as in Lemma 5.11 and γ_p be as in Theorem 5.10. Choose $\gamma > \max\{\gamma_p, 1/4\}$ and set $\varepsilon = (q^a)^{-\gamma}$. In particular, we then have $0 < \varepsilon < \min\{\pi/4, (q^a)^{-\gamma_p}\}$, so we can use the results from Propositions 5.14, 5.16 and 5.17. Hence:

$$\begin{aligned}\left|\mathrm{Avg}(w,a) - \mathrm{Avg}(w_\varepsilon, a)\right| &= 0,\\ \left|\mathrm{Avg}(w_\varepsilon, a) - \int_{\mathrm{ST}} w_\varepsilon\right| &= \mathcal{O}\left(\frac{a^{1/2}}{q^{a/4}}|\log\varepsilon|\right), \text{ as } a \to \infty.,\\ \left|\int_{\mathrm{ST}} w - \int_{\mathrm{ST}} w_\varepsilon\right| &= \mathcal{O}(\varepsilon|\log\varepsilon|).\end{aligned}$$

Then from (5.15) and noting that $\varepsilon = (q^a)^{-\gamma} < q^{-a/4}$, we get:

$$\begin{aligned}\left|\mathrm{Avg}(w,a) - C\right| &= 0 + \mathcal{O}\left(\frac{a^{1/2}}{q^{a/4}} \cdot a\gamma\log(q)\right) + \mathcal{O}\left(\frac{1}{q^{a\gamma}} \cdot a\gamma\log(q)\right)\\ &= \mathcal{O}\left(\frac{a^{3/2}}{q^{a/4}}\right) + \mathcal{O}\left(\frac{a}{q^{a\gamma}}\right) = \mathcal{O}\left(\frac{a^{3/2}}{q^{a/4}}\right), \text{ as } a \to \infty,\end{aligned}$$

and hence we have $\mathrm{Avg}(w,a) \to C$, as $a \to \infty$. □

6 Conclusion

Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 5$ with q elements, and write $K := \mathbb{F}_q(t)$. For any integer $a \geq 1$, let $\wp_a(t) = t^{q^a} - t$ and we define the elliptic curve E_a over K by the following Weierstrass model:

$$E_a : y^2 = x^3 + \wp_a(t)x^2 - x. \tag{6.1}$$

Let $\mathcal{N}_a$ be the conductor of E_a, and we define $N_a := q^{\deg \mathcal{N}_a}$. Then by Proposition 2.5, we have $N_a = q^{2(q^a+1)}$.

In section 4.1 we saw that the BSD conjecture holds for E_a, and hence the Tate-Shafarevich group $Ш(E_a)$ of E_a is finite. We can even give a bound on $\big|Ш(E_a)\big|$. First note that with the combination of the upper bound found in Theorem 5.1 and the lower bound found in Corollary 5.7, we have:

$$\left|\frac{\log L^*(E_a)}{\log N_a}\right| \leq o(1), \text{ as } a \to \infty. \tag{6.2}$$

In Proposition 4.7 we found the following relation:

$$\frac{\log L^*(E_a)}{\log N_a} = \frac{\log |Ш(E_a)|}{\log N_a} - \frac{1}{4} + o(1) \text{ as } a \to \infty. \tag{6.3}$$

and combining (6.2) and (6.3) gives:

$$\frac{\log\big|Ш(E_a)\big|}{\log N_a} \to \frac{1}{4}, \text{ as } a \to \infty. \tag{6.4}$$

With this, our main result follows:

Theorem 6.1. *Let $K = \mathbb{F}_q(t)$ be of characteristic at least 5, and for any integer $a \geq 1$, let E_a/K be the elliptic curve defined by (6.1) and set $N_a := q^{\deg \mathcal{N}_a}$, where $\mathcal{N}_a$ is the conductor of E_a. Then for all $\varepsilon > 0$, there exist constants $c_1, c_2 > 0$, depending only on ε and q, such that for all $a \geq 1$, we have:*

$$c_1 \cdot N_a^{1/4-\varepsilon} \leq \big|Ш(E_a)\big| \leq c_2 \cdot N_a^{1/4+\varepsilon}.$$

Let $H(E_a) := q^{(1/12)\deg \Delta_{\min}(E_a)}$. Corollary 2.7 states $\log H(E_a)/\log N_a = 1/4$, hence $H(E_a) = N_a^{1/4}$, from which we now deduce:

Corollary 6.2. *Let $K = \mathbb{F}_q(t)$ be of characteristic at least 5, and for any integer $a \geq 1$, let E_a/K be the elliptic curve defined by (6.1) and consider $H(E_a) := q^{(1/12)\deg \Delta_{\min}(E_a)}$, where $\Delta_{\min}(E_a)$ is the minimal discriminant of E_a. Then for all $\varepsilon > 0$, there exist constants $c_1', c_2' > 0$, depending only on ε and q, such that for all $a \geq 1$, we have:*

$$c_1' \cdot H(E_a)^{1-\varepsilon} \leq \big|Ш(E_a)\big| \leq c_2' \cdot H(E_a)^{1+\varepsilon}.$$

References

[Gri18] Richard Griffon, Bounds on special values of L-functions of elliptic curves in an Artin-Schreier family. (Preprint arXiv:1801.08492), January 2018.

[GS95] Dorian Goldfeld & Lucien Szpiro, Bounds for the order of the Tate-Shafarevich group; pages 71-87, in volume 97, issue no. 1-2, of *Compositio Math.*, Kluwer Academic Publishers, Dordrecht, 1995

[IR90] Kenneth Ireland & Michael Rosen, *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition, 1990.

[LN97] Rudolf Lidl and Harald Niederreiter, *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, second edition, 1997.

[Ser97] Jean-Pierre Serre, *Galois Cohomology*, volume 4 of *Springer Monographs in Mathematics*, Springer-Verlag, Berlin, 1997.

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

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition, 2009.

[SS10] Matthias Schütt & Tetsuji Shioda, Elliptic Surfaces; pages 51-160, in *Algebraic geometry in East Asia-Seoul 2008*, volume 60 of *Adv. Stud. Pure Math.*, Math. Soc. Japan, Tokyo, 2010.

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

[vdGvdV91] Gerard van der Geer and Marcel van der Vlugt, Kloosterman sums and the p-torsion of certain Jacobians; pages 549-563, in volume 290, issue no. 1, of *Math. Ann.*, Springer-Verlag, Berlin, 1991.