Analogue of the Brauer-Siegel theorem for Legendre elliptic curves

Richard Griffon* (Universiteit Leiden)

Abstract – We prove an analogue of the Brauer–Siegel theorem for the Legendre elliptic curves over $\mathbb{F}_q(t)$. Namely, denoting by E_d the elliptic curve with model $y^2 = x(x+1)(x+t^d)$ over $K = \mathbb{F}_q(t)$, we show that, for $d \to \infty$ ranging over the integers, one has

$$\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right) \sim \log H(E_d/K) \sim \frac{\log q}{2} \cdot d.$$

Here, $H(E_d/K)$ denotes the exponential differential height of E_d, $Ш(E_d/K)$ its Tate–Shafarevich group (which is known to be finite), and $\mathrm{Reg}(E_d/K)$ its Néron–Tate regulator.

Keywords: Elliptic curves over function fields, L-functions and BSD conjecture, Estimates on special values.
2010 Math. Subj. Classification: 11G05, 11G40, 11F67, 14G10, 11M99, 11R47.

Introduction

The Brauer–Siegel theorem describes the asymptotic behaviour of the product of the class number by the regulator of units in sequences of number fields. More precisely, when k runs through a sequence of number fields whose degrees over $\mathbb{Q}$ are bounded, and such that the absolute values Δ_k of their discriminants tend to $+\infty$, then one has the asymptotic estimate

$$\log\left(|Cl(k)| \cdot \mathrm{Reg}(k)\right) \sim \log\sqrt{\Delta_k} \qquad (\text{as } \Delta_k \to \infty), \tag{1}$$

where $Cl(k)$ denotes the class-group of k, and $\mathrm{Reg}(k)$ its regulator of units.

In their recent paper [HP16], Hindry and Pacheco proposed to study an analogue of (1) for elliptic curves E over $K = \mathbb{F}_q(t)$, where $\mathbb{F}_q$ is a given finite field. The analogy is as follows: one replaces $\sqrt{\Delta_k}$ by the exponential height of E, the class number $|Cl(k)|$ by the order of the Tate–Shafarevich group $Ш(E/K)$ (assuming it is finite), and the regulator of units $\mathrm{Reg}(k)$ by the Néron-Tate regulator $\mathrm{Reg}(E/K)$. They were thus led to introduce the *Brauer–Siegel ratio* of E/K:

$$\mathfrak{Bs}(E/K) := \frac{\log\left(|Ш(E/K)| \cdot \mathrm{Reg}(E/K)\right)}{\log H(E/K)},$$

and to investigate its asymptotic behaviour as E runs through sequences of elliptic curves over K whose heights tend to $+\infty$. Assuming the finiteness of Tate–Shafarevich groups, they prove that

$$0 \leq \liminf_{H(E/K)\to\infty} \mathfrak{Bs}(E/K) \leq \limsup_{H(E/K)\to\infty} \mathfrak{Bs}(E/K) = 1.$$

Should a perfect analogue of (1) for elliptic curves hold, one would certainly expect that

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

However, not only is the proof of such an asymptotic relation out of reach at the moment, but one can reasonably doubt that it should hold in general. Indeed, Hindry and Pacheco discuss heuristics suggesting the existence of infinite sequences $\{E_n\}_{n\geq 1}$ of elliptic curves for which $\lim_{n\to\infty} \mathfrak{Bs}(E_n/K) = 0$.

The goal of this article is to exhibit a sequence $\{E_d\}_d$ of elliptic curves over K that *does* satisfy unconditionally a complete analogue of the classical Brauer-Siegel theorem (1). Indeed, our main theorem is:

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

Theorem 1.1 – *Let $\mathbb{F}_q$ be a finite field of odd characteristic, and $K = \mathbb{F}_q(t)$. For any integer $d \geq 2$, consider the Legendre elliptic curve E_d/K defined by the affine Weierstrass model:*

$$E_d : \quad y^2 = x(x+1)(x+t^d).$$

Then the Tate–Shafarevich group $Ш(E_d/K)$ is finite and, as $d \to \infty$, one has the asymptotic estimate:

$$\log\big(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\big) \sim \log H(E_d/K), \tag{2}$$

where $\mathrm{Reg}(E_d/K)$ denotes the Néron-Tate regulator of $E_d(K)$, and $H(E_d/K)$ is the (exponential) differential height of E_d/K (see definitions below).

This theorem can be restated as:

$$\forall \varepsilon > 0, \qquad H(E_d/K)^{1-\varepsilon} \ll_{q,\varepsilon} |Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K) \ll_{q,\varepsilon} H(E_d/K)^{1+\varepsilon}.$$

The upper bound essentially proves a conjecture of Lang (originally formulated for elliptic curves over $\mathbb{Q}$ in [Lan83, Conj. 1]), and our lower bound reveals that the exponent 1 is optimal (*i.e.*, no smaller number would do in the upper bound). Furthermore, it follows from the computation of $H(E_d/K)$ (see section 2) that one has

$$\log\big(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\big) \sim \frac{\log q}{2} \cdot d, \qquad (\text{as } d \to \infty),$$

showing that the product $|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)$ grows exponentially fast with d. In the interpretation of [Hin07], this suggests that the Mordell–Weil groups $E_d(K)$ are "exponentially hard to compute".

Note that $\{E_d\}$ is but the second known sequence of elliptic curves satisfying $\lim_{d\to\infty} \mathfrak{Bs}(E_d/K) = 1$ unconditionally (see also [HP16, Thm. 1.4]). Four more examples were constructed in the author's PhD thesis [Gri16a].

To conclude this introduction, let us give the plan of the paper, as well as a rough sketch of the proof of Theorem 1.1. The Legendre elliptic curves E_d have been previously studied by Ulmer, Conceição and Hall in a series of papers ([Ulm14], [CHU14], ...); in particular, they proved that E_d satisfies the Birch and Swinnerton-Dyer conjecture (henceforth abbreviated as BSD). This implies the finiteness of $Ш(E_d/K)$, and is the main reason why our Theorem 1.1 is unconditional (see section 2). Moreover, they have given an explicit expression for the L-function $L(E_d/K, T) \in \mathbb{Z}[T]$ of E_d and of its zeroes (see section 3).

Our first step towards Theorem 1.1 will be to reduce it to an analytic statement: see (3) below. More precisely, denoting by $\rho = \mathrm{ord}_{T=q^{-1}} L(E_d/K, T)$, the BSD conjecture gives the following expression for the special value $L^*(E_d/K, 1)$ of the L-function of E_d:

$$L^*(E_d/K,1) := \left.\frac{L(E_d/K,T)}{(1-qT)^\rho}\right|_{T=q^{-1}} = \frac{|Ш(E_d/K)| \cdot \ \mathrm{Reg}(E_d/K)}{H(E_d/K)} \cdot (\text{ extra terms }).$$

Estimating the size of the "extra terms", we show (see Corollary 2.5) that

$$\frac{\log\big(|Ш(E_d/K) \cdot \mathrm{Reg}(E_d/K)|\big)}{\log H(E_d/K)} = 1 + \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} + o(1) \qquad (\text{as } d \to \infty). \tag{3}$$

The size of these "extra terms" was first controlled in [HP16] for abelian varieties A over K (see Theorems 1.22 and 3.8 there). However, their proof is quite involved. Since the proof in the special case of E_d is elementary and explicit, we thought it was worth giving details here. Given (3), proving Theorem 1.1 boils down to showing that

$$-o(1) \leq \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \leq o(1) \qquad (\text{as } d \to \infty). \tag{4}$$

The upper bound in (4) is relatively easy to prove (see Theorem 3.6), but the proof of the lower bound is much more delicate. We proceed as follows: by definition, the special value $L^*(E_d/K, 1)$ has the following shape:

$$L^*(E_d/K,1) = \frac{(\text{a positive prime-to-}p\text{ integer})}{q^{e_q(d)}}, \qquad \text{for some exponent } e_q(d) \geq 0. \tag{5}$$

A straightforward estimate shows that $e_q(d) \ll d$, but the lower bound in (4) requires to prove the stronger statement that $e_q(d)/d \to 0$, as $d \to \infty$. This improved bound on $e_q(d)$ constitutes our main technical result (Theorem 4.1), the proof of which is given in section 4. There are two main ingredients in the proof of this theorem. First, we rely on the explicit factorization of $L(E_d/K, T)$ in [CHU14] to obtain an expression for $L^*(E_d/K, 1)$ (see Proposition 3.4). Noting that $L^*(E_d/K, 1)$ is given in terms of Jacobi

sums, we use a variant of Stickelberger's theorem to obtain a reasonably explicit expression for $e_q(d)$. Second, we observe that the size of the resulting expression for $e_q(d)$ can be estimated by using an average equidistribution result for subgroups of $(\mathbb{Z}/d\mathbb{Z})^\times$, proved by the author in [Gri16b].

For the purpose of clarity, we have only stated qualitative bounds in this introduction, but note that we will actually prove a quantitative version of Theorem 1.1 (see Theorem 5.3): unlike the (lower bound in the) classical Brauer–Siegel theorem, Theorem 1.1 is entirely effective.

Notations For all integers $d \geq 2$, let μ_d be the group of d-th roots of unity in $\overline{\mathbb{F}_q}$. The cardinality of a finite set X will be denoted by $|X|$. For any prime power q, and any integer $n \geq 1$ coprime to q, $\langle q \rangle_n$ will denote the subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ generated by q, and we let $o_q(n) := |\langle q \rangle_n|$ the multiplicative order of q modulo n. For two functions $f(x), g(x)$ defined on $[0, \infty)$, we make use of the Vinogradov notation $f(x) \ll_a g(x)$ to mean that there exists a constant $C > 0$ (depending at most on the mentioned parameters a) such that $|f(x)| \leq Cg(x)$ for $x \to \infty$. Unless otherwise stated, all constants are effective and could be made explicit.

Acknowledgements This paper contains results from the author's PhD thesis [Gri16a]. The author wishes to thank his advisor Marc Hindry for many illuminating conversations and comments. He also thanks Michael Tsfasman, Douglas Ulmer and the anonymous referees for their careful reading of an earlier version of this text, and their suggestions. He would also like to thank the Universiteit Leiden for providing ideal working conditions during the writing of this article.

2 The Legendre elliptic curves

Throughout the paper, we fix a finite field $\mathbb{F}_q$ of odd characteristic $p \geq 3$ and we denote by $K = \mathbb{F}_q(t)$.

For any integer $d \geq 1$, we consider the *Legendre elliptic curve* E_d/K, given by the affine Weierstrass model

$$E_d : \qquad y^2 = x(x+1)(x+t^d). \tag{2.1}$$

The discriminant of this model of E_d is easily seen to be $\Delta = 16t^{2d}(t^d-1)^2$. Likewise, the j-invariant of E_d is easily computed from (2.1) and we find:

$$j(E_d/K) = \frac{2^8 \cdot (t^{2d} - 16t^d + 1)^3}{t^{2d}(t^d-1)^2} \in K.$$

We note that $j(E_d/K)$ is nonconstant, so that E_d is not isotrivial. Furthermore, $j(E_d/K)$ is visibly not a p-th power in K.

Remark 2.1 We follow [Ulm14] in calling E_d a Legendre curve: see [Ulm14, §2] for more comments on this choice of terminology. We also note the slight change in points of view compared to [Ulm14], [CHU14]: instead of considering a fixed curve E_1 over a varying field $\mathbb{F}_q(t^{1/d})$, we fix the base field $\mathbb{F}_q(t)$ and vary the curve E_d. This is only a matter of convenience, and has no influence on the results.

This section is mainly expository and does not contain new results: we review the definitions of the invariants of E_d and the computations of some of them, we also state the relevant theorems about E_d. In the last subsection, we explain how the problem of bounding $|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)$ can be reduced to studying the size of the special value $L^*(E_d/K, 1)$ of the L-function of E_d/K at $s = 1$.

2.1 Review of the invariants

For any $d \geq 1$, we denote by $|\mu_d|$ the set of places of K that divide $t^d - 1$ *i.e.*, $|\mu_d|$ is the set of closed points of $\mathbb{P}^1$ corresponding to d-th roots of unity in $\overline{\mathbb{F}_q}$. Applying Tate's algorithm (as in §9 of [Sil94, Chap. IV] for example), one can describe the bad reduction of E_d:

Proposition 2.2 – *The elliptic curve E_d/K has good reduction outside the places of K corresponding to $S = \{0\} \cup \mu_d \cup \{\infty\} \subset \mathbb{P}^1$; moreover, the bad reduction of E_d is as follows:*

Place v of K	*Type of E_d at v*	$\mathrm{ord}_v\,\Delta_{\min}(E_d/K)$	$\mathrm{ord}_v\,\mathcal{N}(E_d/K)$	$c_v(E_d/K)$
0	$\mathbf{I}_{2d}$	$2d$	1	$2d$
$v \in \lvert\mu_d\rvert$	$\mathbf{I}_2$	2	1	1 *or* 2
∞	$\mathbf{I}_{2d}$ *if d even*	$2d$	1	$2d$
	$\mathbf{I}^*_{2d}$ *if d odd*	$2d+6$	2	4

In this table, for all places v of K where E_d has bad reduction, we have denoted by $\mathrm{ord}_v(\Delta_{\min})$ (resp. $\mathrm{ord}_v(\mathcal{N})$) the valuation at v of the minimal discriminant of E_d (resp. of the conductor of E_d), and by $c_v(E_d/K)$ the local Tamagawa number (see [Sil94, Chap. IV, §9] for the definitions of these invariants). For $v = \zeta$ dividing $t^d - 1$ (*i.e.*, v corresponds to a closed point of μ_d), note that $c_\zeta(E_d/K) = 2$ if and only if -1 is a square in $\mathbb{F}_q(\zeta)$, and $c_\zeta(E_d/K) = 1$ otherwise.

From this Proposition, one can compute the degrees of the *minimal discriminant* $\Delta_{\min}(E_d/K)$, and of the *conductor* $\mathcal{N}(E_d/K)$ of E_d (both $\Delta_{\min}(E_d/K)$ and $\mathcal{N}(E_d/K)$ are viewed as divisors on $\mathbb{P}^1$). For any $d \geq 2$, we write $d = p^a d'$ where $a \geq 0$ and $d' \geq 1$ is coprime to p. It is then readily seen that

$$\deg \Delta_{\min}(E_d/K) = \begin{cases} 6d & \text{if } d \text{ is even,} \\ 6(d+1) & \text{if } d \text{ is odd,} \end{cases} \quad \text{and} \quad \deg \mathcal{N}(E_d/K) = \begin{cases} d'+2 & \text{if } d' \text{ is even,} \\ d'+3 & \text{if } d' \text{ is odd.} \end{cases} \tag{2.2}$$

By definition, the *exponential differential height of* E_d/K is

$$H(E_d/K) = q^{\frac{1}{12}\deg \Delta_{\min}(E_d/K)} = q^{\left\lfloor \frac{d+1}{2} \right\rfloor}. \tag{2.3}$$

See [Ulm14, Lemma 7.1] for a more geometric computation of $H(E_d/K)$ when d is even and coprime to q.

Finally, the *Tamagawa number* $\tau(E_d/K) := \prod_{v \in S} c_v(E_d/K)$ could be computed exactly from the last column of the table in Proposition 2.2, but we will content ourselves with the estimate:

$$1 \ \leq \tau(E_d/K) \leq (2d)^2 \cdot 2^{\theta_q(d)}, \tag{2.4}$$

where $\theta_q(d)$ denotes the number of closed points of μ_d *i.e.*, $\theta_q(d)$ is the number of monic irreducible polynomials $P \in \mathbb{F}_q[t]$ such that $P \mid t^d - 1$.

2.2 Néron-Tate regulator and Tate–Shafarevich group

By the Mordell–Weil theorem (proved by Lang and Néron in this setting), the group $E_d(K)$ is finitely generated. Moreover, the Mordell–Weil group $E_d(K)$ is endowed with the canonical Néron–Tate height $\widehat{h}_{NT} : E_d(K) \to \mathbb{Q}$. Note that, over $\mathbb{F}_q(t)$, it is indeed possible to normalize $\widehat{h}_{NT}$ to have rational values, because it has an interpretation in terms of intersection theory on the minimal regular model of E_d/K (see [Sil94, Chap. III, §9] for details, more specifically Theorem 9.3 there). The quadratic map $\widehat{h}_{NT}$ induces a $\mathbb{Z}$-bilinear pairing $\langle -, - \rangle_{NT} : E_d(K) \times E_d(K) \to \mathbb{Q}$, which is nondegenerate modulo $E_d(K)_{\mathrm{tors}}$ (*cf.* [Sil94, Chap. III, Thm. 4.3]). The *Néron-Tate regulator* of E_d/K is then defined to be the Gram determinant

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

for any choice of a $\mathbb{Z}$-basis $P_1, \ldots, P_r \in E_d(K)$ of $E_d(K)/E_d(K)_{\mathrm{tors}}$. Let us also recall that the *Tate–Shafarevich group* of E_d/K is defined by

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

where the involved cohomology groups are Galois cohomology groups (see [Sil09, Chap. X, §4] for more details). We will see in Theorem 2.3 below that $Ш(E_d/K)$ is a finite group, which will prove the first assertion of Theorem 1.1.

2.3 BSD conjecture and consequences

The Hasse–Weil L-function of E_d/K is *a priori* defined as a formal Euler product over the places v of K:

$$L(E_d/K,T) = \prod_{v \text{ good}} (1 - a_v(E_d)\cdot T^{\deg v} + q^{\deg v}\cdot T^{2\deg v})^{-1} \cdot \prod_{v \text{ bad}} (1 - a_v(E_d)\cdot T^{\deg v})^{-1},$$

where $a_v(E_d)$ is defined by counting rational points on the reduction of E_d modulo v (see [Sil09, Appendix C, §16] or [Bru92, Appendix] for more details).

Grothendieck's cohomological interpretation of L-functions shows that $L(E_d/K,T)$ is actually a polynomial in T, with integral coefficients, and whose degree is given explicitly in terms of $\mathcal{N}(E_d/K)$. Moreover, by Deligne's proof of the Riemann Hypothesis, the zeroes of $L(E_d/K,T)$ have magnitude q^{-1} in any complex embedding. We can thus study the behaviour of $L(E_d/K,T)$ around the point $T = q^{-1}$ and introduce the *special value* $L^*(E_d/K,1)$ *of* $L(E_d/K,T)$ *at* $T = q^{-1}$:

$$L^*(E_d/K,1) := \left.\frac{L(E_d/K,T)}{(1-qT)^\rho}\right|_{T=q^{-1}} \in \mathbb{Z}[q^{-1}] \smallsetminus \{0\} \quad \text{where } \rho = \operatorname{ord}_{T=q^{-1}} L(E_d/K,T). \tag{2.5}$$

Inspired by the conjecture of Birch and Swinnerton-Dyer for elliptic curves over $\mathbb{Q}$, Tate [Tat66] conjectured that ρ and $L^*(E_d/K,1)$ have an arithmetic interpretation. Their conjecture has been proved for E_d by Ulmer (*cf.* Corollary 11.3 and Remark 12.2 in [Ulm14]), and we state the result as follows:

Theorem 2.3 (Ulmer) – *Let $\mathbb{F}_q$ be a finite field of odd characteristic and $K = \mathbb{F}_q(t)$. For all integers $d \geq 1$, let E_d/K be the Legendre curve (2.1) as above. Then the BSD conjecture is true for E_d/K; that is to say,*

(1) the Tate–Shafarevich group $Ш(E_d/K)$ is finite,

(2) the rank of $E_d(K)$ is equal to $\rho = \operatorname{ord}_{T=q^{-1}} L(E/K,T)$,

(3) and one has

$$L^*(E_d/K,1) = \frac{|Ш(E_d/K)|\cdot \operatorname{Reg}(E_d/K)}{H(E_d/K)} \cdot \frac{\tau(E_d/K)\cdot q}{|E_d(K)_{\text{tors}}|^2}. \tag{2.6}$$

The proof goes roughly as follows (see [Ulm14, §11] and [Ulm13, §7] for more details). Let us write d in the form $d = p^a d'$ with $a \geq 0$ and d' coprime to p. Since E_d and $E_{d'}$ are K-isogenous through the p^a-th power Frobenius morphism, and since the truth of the BSD conjecture is invariant under isogeny, it suffices to treat the case when $d = d'$ is coprime to q (see [Ulm14, Rem. 12.2]). By the main theorem of [KT03], it even suffices to prove that the "weak BSD conjecture" *(2)* holds for E_d. We denote by $\pi : \mathcal{E}_d \to \mathbb{P}^1$ the minimal regular model of E_d. Proving the equality in *(2)* is equivalent, by [Tat66] and [Mil75], to proving that the Tate conjecture holds for the surface $\mathcal{E}_d$. When d is coprime to q, Ulmer [Ulm14, §7] has explicitly constructed the model $\mathcal{E}_d \to \mathbb{P}^1$ and shown that the corresponding surface $\mathcal{E}_d$ is dominated by a product of curves. The Tate conjecture has been proved for products of curves (see [Tat94]), and the existence of a dominant map to $\mathcal{E}_d$ implies the truth of this conjecture for $\mathcal{E}_d$ when d is coprime to q.

The link between the product $|Ш(E_d/K)|\cdot\operatorname{Reg}(E_d/K)$ and the special value $L^*(E_d/K,1)$ is now clear. For any integer $d \geq 2$, reordering terms in (2.6) and taking a log, we obtain that:

$$\frac{\log\big(|Ш(E_d/K)|\cdot\operatorname{Reg}(E_d/K)\big)}{\log H(E_d/K)} = 1 + \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} + \frac{\log|E_d(K)_{\text{tors}}|^2 - \log(\tau(E_d/K)\cdot q)}{\log H(E_d/K)}. \tag{2.7}$$

Let us show that the right-most term is asymptotically negligible:

Lemma 2.4 – *As $d \geq 2$ tends to infinity, one has*

$$|E_d(K)_{\text{tors}}| \ll 1 \qquad \textit{and} \qquad \frac{\log(\tau(E_d/K)\cdot q)}{\log H(E_d/K)} \ll_q \frac{1}{\log d}.$$

Proof: First, Proposition 6.1 in [Ulm14] implies that $|E_{d'}(K)_{\text{tors}}| \leq 8$ for all integers $d' \geq 2$ coprime to p. Now let $d \geq 2$ be any integer and write $d = p^a d'$ with $(d',p) = 1$. Since $j(E_d/K)$ is not a p-th power in K, Proposition 7.3 in [Ulm11, Lect. 1] shows that $E_d(K)_{\text{tors}}$ has trivial p-primary part. Recall that E_d and $E_{d'}$ are related by the p^a-th power Frobenius isogeny, so their torsion subgroups $E_d(K)_{\text{tors}}$ and $E_{d'}(K)_{\text{tors}}$ differ at most by their p-primary parts. Both of these p-parts are trivial, hence $|E_d(K)_{\text{tors}}| \leq 8$ for all integers $d \geq 2$.

Secondly, combining (2.3) and (2.4) leads to

$$\frac{\log(\tau(E_d/K)\cdot q)}{\log H(E_d/K)} \ll_q \frac{\log d}{d} + \frac{\theta_q(d)}{d}.$$

Remember that $\theta_q(d)$ is the number of monic irreducible polynomials in $\mathbb{F}_q[t]$ which divide t^d-1. Again, we write d as $d = p^a d'$ where $a \geq 0$ and d' is coprime to p. By the identity $t^d - 1 = (t^{d'}-1)^{p^a}$, one has $\theta_q(d) = \theta_q(d')$. Since $t^{d'}-1$ factors as a product of cyclotomic polynomials $\Phi_e(t) \in \mathbb{F}_q[t]$ with $e \mid d'$, and since $\Phi_e(t)$ decomposes as a product of $\phi(e)/o_q(e)$ distinct monic irreducible factors in $\mathbb{F}_q[t]$ (see [IR90, Chap. 13, §2]), we have $\theta_q(d') = \sum_{e\mid d'} \frac{\phi(e)}{o_q(e)}$. In the course of the proof of Lemma 3.1(c) below, we will see that $\sum_{e\mid d'} \frac{\phi(e)}{o_q(e)} \ll_q d'/\log d'$. The map $x \mapsto x/\log x$ is increasing on $[3,\infty)$ and $d' \leq d$, hence

$$\frac{\theta_q(d)}{d} = \frac{\theta_q(d')}{d} \ll_q \frac{1}{d}\cdot\frac{d'}{\log d'} \ll_q \frac{1}{\log d}.$$

The desired upper bound on $\tau(E_d/K)$ then follows from the first displayed inequality in this proof. □

Transferring the estimates of Lemma 2.4 into (2.7) immediately yields the following:

Corollary 2.5 – *For all integers $d \geq 2$, we have:*

$$\frac{\log\big(|Ш(E_d/K)|\cdot \mathrm{Reg}(E_d/K)\big)}{\log H(E_d/K)} = 1 + \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} + O_q\left(\frac{1}{\log d}\right) \quad (\text{as } d\to\infty),$$

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

Remark 2.6 This corollary is but an explicit version of a special case of a result in [HP16]. In particular, see the discussion in [HP16, §2] where Corollary 2.5 is proved for abelian varieties over K satisfying BSD. Note that the proof in the general case is much more involved: it requires delicate diophantine estimates on the torsion subgroup ([HP16, Theorem 3.8]) and on Tamagawa numbers ([HP16, Theorem 6.5]).

3 The L-function of E_d and its special value

We have reduced the estimation of $|Ш(E_d/K)\cdot\mathrm{Reg}(E_d/K)|$ to that of $L^*(E_d/K,1)$. As we explained in the introduction, we need to make use of the specific structure of the L-function of E_d to obtain the correct estimate of $L^*(E_d/K,1)$. In this section, we introduce the notations required to state the explicit expression for $L(E_d/K,T)$ when d is coprime to q (obtained in [CHU14]) and we then proceed to express $L^*(E_d/K,1)$ in a suitable form. The proof of the lower bound itself will be the goal of the next section.

Throughout sections 3 and 4 (except in Remarks 3.3 and 3.7), $d \geq 2$ is assumed to be coprime to q.

3.1 Action of q on $\mathbb{Z}/d\mathbb{Z}$

Let $\mathbb{F}_q$ be a finite field of odd characteristic, and let $d \geq 2$ be an integer coprime to q. There is a natural action of q on $\mathbb{Z}/d\mathbb{Z}$ by $n \mapsto q\cdot n$. For any subset $Z \subset \mathbb{Z}/d\mathbb{Z}$ which is stable by multiplication by q, we denote by $\mathcal{O}_q(Z)$ the set of orbits of Z under this action. In what follows, we will be particularly interested in the set

$$Z_d := \begin{cases} \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/2\} & \text{if } d \text{ is even,} \\ \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\} & \text{if } d \text{ is odd,} \end{cases}$$

(which is stable under multiplication by q) and in the corresponding set of orbits $\mathcal{O}_q(Z_d)$. Given an orbit $\mathbf{m} \in \mathcal{O}_q(Z_d)$, we will often have to make a choice of representative $m \in Z_d$ of this orbit: we thus stick to the useful convention that orbits in $\mathcal{O}_q(Z_d)$ are always denoted by a bold letter ($\mathbf{m}$, $\mathbf{n}$, ...) and that the corresponding normal letter (m, n, ...) designates any choice of representative of this orbit in Z_d.

For any orbit $\mathbf{m} \in \mathcal{O}_q(Z_d)$, its length $|\mathbf{m}| = \big|\{m, qm, q^2m, \dots\}\big|$ is clearly equal to

$$|\mathbf{m}| = \min\left\{\nu \in \mathbb{Z}_{\geq 1} \;\middle|\; q^\nu m \equiv m \bmod d\right\},$$

which, in turn, equals $|\mathbf{m}| = o_q(d/\gcd(d,m))$, the multiplicative order of q modulo $d/\gcd(d,m)$, for any $m \in \mathbf{m}$. For any power q^v of v, by construction of the multiplicative order, remark that $q^v m \equiv m \bmod d$ if and only if $|\mathbf{m}|$ divides v *i.e.*, if and only if $\mathbb{F}_{q^v}$ is a finite extension of $\mathbb{F}_{q^{|\mathbf{m}|}}$.

For further use, we record here a few useful facts about the action of q on Z_d in the following lemma:

Lemma 3.1 – *Let $d \geq 2$ be an integer coprime with q. The following upper bounds hold:*

(a) $\displaystyle\sum_{\substack{e|d\\ e\geq 2}} \frac{\phi(e)}{\log e} \ll \frac{d}{\log d}$,

(b) $\displaystyle\sum_{\mathbf{m}\in\mathcal{O}_q(Z_d)} |\mathbf{m}| = |Z_d| \leq d$,

(c) $\displaystyle\sum_{\mathbf{m}\in\mathcal{O}_q(Z_d)} 1 = |\mathcal{O}_q(Z_d)| \ll \log q \cdot \frac{d}{\log d}$,

(d) $\displaystyle\sum_{\mathbf{m}\in\mathcal{O}_q(Z_d)} \log|\mathbf{m}| \ll \log q \cdot \frac{d\cdot\log\log d}{\log d}$.

All the involved constants are absolute and effective.

Proof: We put $x=\sqrt{d}$, cut the sum in (a) into two parts, and bound them separately: this leads to

$$\sum_{\substack{e|d\\ e\geq 2}} \frac{\phi(e)}{\log e} = \sum_{\substack{e|d\\ 2\leq e\leq x}} \frac{\phi(e)}{\log e} + \sum_{\substack{e|d\\ x<e}} \frac{\phi(e)}{\log e} \leq \sum_{\substack{e|d\\ 2\leq e\leq x}} \frac{e}{\log e} + \frac{1}{\log x}\sum_{e|d}\phi(e)$$
$$\leq \frac{x}{\log x}\sum_{2\leq e\leq x} 1 + \frac{1}{\log x}\sum_{e|d}\phi(e) \leq \frac{x^2+d}{\log x} \leq 4\cdot\frac{d}{\log d},$$

because $y\mapsto 1/\log y$ is decreasing on $[3,\infty)$, while $y\mapsto y/\log y$ is increasing on $[3,+\infty)$. This proves (a) with an implicit constant $c_0\leq 4$. Assertion (b) is a direct consequence of the fact that Z_d can be written as the disjoint union of its orbits under the action of q by multiplication.

For any divisor d' of d, let $Y_{d'} := \{n\in Z_d \mid \gcd(n,d)=d/d'\}$ (note that $Y_1=\varnothing$, and that $Y_2=\varnothing$ if d is even). Since $\gcd(d,q)=1$, these sets $Y_{d'}\subset Z_d$ are stable under the action of q, and the decomposition $Z_d=\bigsqcup_{d'|d} Y_{d'}$ of Z_d induces a corresponding decomposition $\mathcal{O}_q(Z_d)=\bigsqcup_{d'|d}\mathcal{O}_q(Y_{d'})$. For all $d'\mid d$ with $d'>2$, elements $n\in Y_{d'}$ are of the form $n=t\cdot d/d'$, where $t\in(\mathbb{Z}/d'\mathbb{Z})^\times$, so that the map $t\mapsto t\cdot d/d'$ induces a bijection between the quotient group $(\mathbb{Z}/d'\mathbb{Z})^\times/\langle q\rangle_{d'}$ and $\mathcal{O}_q(Y_{d'})$. This implies that $|\mathcal{O}_q(Y_{d'})|=\phi(d')/o_q(d')$ (where $o_q(d')=|\langle q\rangle_{d'}|$ denotes the multiplicative order of q modulo d'), but also that all the orbits $\mathbf{m}\in\mathcal{O}_q(Y_{d'})$ have the same cardinality $|\mathbf{m}|=o_q(d')$. By definition of the order, d' divides $q^{o_q(d')}-1$, hence $o_q(d')\geq \log d'/\log q$. We thus deduce from (a) that

$$|\mathcal{O}_q(Z_d)| = \sum_{\substack{d'|d\\ d'>2}} |\mathcal{O}_q(Y_{d'})| = \sum_{\substack{d'|d\\ d'>2}} \frac{\phi(d')}{o_q(d')} \leq \log q\cdot\sum_{\substack{d'|d\\ d'>2}}\frac{\phi(d')}{\log d'} \leq c_0\log q\cdot\frac{d}{\log d}.$$

It remains to prove the last assertion (d): using the remarks in the previous paragraph, we can write

$$\sum_{\mathbf{m}\in\mathcal{O}_q(Z_d)}\log|\mathbf{m}| = \sum_{\substack{d'|d\\ d'>2}}\sum_{\mathbf{m}\in\mathcal{O}_q(Y'_d)}\log|\mathbf{m}| = \sum_{\substack{d'|d\\ d'>2}}\frac{\phi(d')}{o_q(d')}\cdot\log o_q(d').$$

Given a parameter $\theta\in(1,o_q(d))$, we split this last sum according to the size of $o_q(d')$ compared to θ: we then bound from above the two resulting sums, using that $y\mapsto\log y$ is increasing, that $y\mapsto(\log y)/y$ is decreasing, and adding nonnegative terms:

$$\sum_{\substack{d'|d\\ d'>2}}\frac{\phi(d')}{o_q(d')}\cdot\log o_q(d') \leq \log\theta\cdot\sum_{\substack{d' \text{ s.t.}\\ o_q(d')\leq\theta}}\frac{\phi(d')}{o_q(d')} + \frac{\log\theta}{\theta}\cdot\sum_{\substack{d' \text{ s.t.}\\ o_q(d')>\theta}}\phi(d') \leq \log\theta\cdot|\mathcal{O}_q(Z_d)| + \frac{\log\theta}{\theta}\cdot d.$$

Upon choosing $\theta=\log d/(c_0\log q)$ (note that $\theta\leq o_q(d)/c_0<o_q(d)$), we deduce from (c) that

$$\sum_{\mathbf{m}\in\mathcal{O}_q(Z_d)}\log|\mathbf{m}| \leq \log\theta\cdot d\cdot\left(\frac{c_0\log q}{\log d}+\frac{1}{\theta}\right) \leq 2c_0\log q\cdot\frac{d\cdot\log\log d}{\log d},$$

which is inequality (d). □

3.2 Jacobi sums

We fix, once and for all, an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ (of which all number fields are assumed to be subfields) and a prime ideal $\mathfrak{P}$ above p in the ring integers $\overline{\mathbb{Z}}$ of $\overline{\mathbb{Q}}$. The residue field $\overline{\mathbb{Z}}/\mathfrak{P}$ is an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$ (and all finite fields of characteristic p are seen as subfields thereof). The reduction map $\overline{\mathbb{Z}}\to\overline{\mathbb{Z}}/\mathfrak{P}$ induces an isomorphism between the group $\mu_{\infty,p'}\subset\overline{\mathbb{Z}}^\times$ of roots of unity of order prime to p and the

multiplicative group $\overline{\mathbb{F}_p}^\times$. We let $\mathbf{t} : \overline{\mathbb{F}_p}^\times \to \mu_{\infty,p'}$ be the inverse of this isomorphism, and we denote by the same letter the restriction of $\mathbf{t}$ to any finite field $\mathbb{F}_q$.

For any finite extension $\mathbb{F}_Q$ of $\mathbb{F}_p$, we denote by $\lambda_Q : \mathbb{F}_Q^\times \to \{\pm 1\}$ the unique nontrivial character of order 2 of $\mathbb{F}_Q^\times$ (the "Legendre symbol" of $\mathbb{F}_Q$), extended by $\lambda_Q(0) := 0$. For any integer $d \geq 2$ coprime to q and any $m \in Z_d$, we define a character $\mathbf{t}_m : \mathbb{F}_{q^{|\mathbf{m}|}}^\times \to \overline{\mathbb{Q}}^\times$ by

$$\forall x \in \mathbb{F}_{q^{|\mathbf{m}|}}^\times, \quad \mathbf{t}_m(x) = \mathbf{t}(x)^{(q^{|\mathbf{m}|}-1)m/d} \quad \text{and we let } \mathbf{t}_m(0) := 0.$$

By construction, the characters $\mathbf{t}_m$ are nontrivial, have order dividing d (in fact, the order of $\mathbf{t}_m$ is exactly $d/\gcd(d,m)$) and, as such, take values in $\mathbb{Q}(\zeta_d)$, the d-th cyclotomic field.

To $m \in Z_d$, we can now attach a Jacobi sum:

$$\mathbf{J}(m) = \sum_{x \in \mathbb{F}_{q^{|\mathbf{m}|}}} \mathbf{t}_m(x) \cdot \lambda_{q^{|\mathbf{m}|}}(1-x). \tag{3.1}$$

As a sum of d-th roots of unity, $\mathbf{J}(m)$ is an algebraic integer in $\mathbb{Q}(\zeta_d)$. Even though $\mathbf{t}_m$ might differ from $\mathbf{t}_{q\cdot m}$, it turns out that $\mathbf{J}(m) = \mathbf{J}(q \cdot m)$ because $x \mapsto x^q$ is a bijection of $\mathbb{F}_{q^{|\mathbf{m}|}}$ (more generally, $\mathbf{J}(m) = \mathbf{J}(p \cdot m)$). Thus it makes sense to associate a Jacobi sum $\mathbf{J}(\mathbf{m})$ to any orbit $\mathbf{m} \in \mathcal{O}_q(Z_d)$: we let $\mathbf{J}(\mathbf{m}) = \mathbf{J}(m)$ for any choice of $m \in \mathbf{m}$. Since, for all $m \in Z_d$, none of $\mathbf{t}_m, \lambda_{q^{|\mathbf{m}|}}$ and $\mathbf{t}_m \cdot \lambda_{q^{|\mathbf{m}|}}$ is trivial, it is well-known that $|\mathbf{J}(\mathbf{m})| = q^{|\mathbf{m}|/2}$. The reader may consult [IR90] for more details about Jacobi sums.

3.3 L-function and special value

As above, for any integer d, we let

$$Z_d := \begin{cases} \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/2\} & \text{if } d \text{ is even,} \\ \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\} & \text{if } d \text{ is odd ,} \end{cases}$$

and $\mathcal{O}_q(Z_d)$ be the set of orbits of Z_d under the action of q by multiplication. With the notations introduced in the last two subsections (which are essentially the same as those of [CHU14, §3]), we can now state [CHU14, Theorem 3.2.1]:

Theorem 3.2 (Conceição, Hall, Ulmer) – *Let $d \geq 2$ be an integer coprime with q. The L-function of E_d/K is given by*

$$L(E_d/K, T) = \prod_{\mathbf{m} \in \mathcal{O}_q(Z_d)} \left(1 - \mathbf{J}(\mathbf{m})^2 \cdot T^{|\mathbf{m}|}\right), \tag{3.2}$$

where $\mathbf{J}(\mathbf{m})$ is the Jacobi sum defined in (3.1).

The proof of (3.2) in [CHU14, §3] hinges on a clever manipulation of character sums. Since the minimal regular model of E_d/K is explicitly known (see [Ulm14, §7]), the computation can also be done via cohomological methods. Though less elementary, the latter has the advantage of "explaining" the appearance of Jacobi sums in the L-function.

Remark 3.3 From Theorem 3.2, one actually obtains an expression of $L(E_d/K, T)$ for any integer $d \geq 1$: writing d as $d = p^a d'$ with $a \geq 0$ and d' coprime to p, we have $L(E_d/K, T) = L(E_{d'}/K, T)$. Indeed, the p^a-th power Frobenius provides an K-isogeny $E_{d'} \to E_d$ and isogenous elliptic curves have the same L-function. In particular, we note the amusing fact that $L(E_{p^a}/K, T) = L(E_1/K, T) = 1$ for all $a \geq 0$, while $H(E_{p^a}/K) \to \infty$ as $a \to \infty$.

Given (3.2), it is now easy to give an explicit expression for the special value $L^*(E_d/K, 1)$ of the L-function of E_d/K at $s = 1$. We begin by introducing the following two subsets V_d and S_d of Z_d:

$$V_d := \left\{ m \in Z_d \;\middle|\; \mathbf{J}(m)^2 = q^{|\mathbf{m}|} \right\} \quad \text{and} \quad S_d := Z_d \smallsetminus V_d.$$

By their very construction, the sets V_d and S_d are stable under the action of q on Z_d. As we will see in the Proposition below, the orbit set $\mathcal{O}_q(V_d)$ (resp. $\mathcal{O}_q(S_d)$) parametrizes the factors in (3.2) that vanish at $T = q^{-1}$ (resp. those that give a nontrivial contribution to the special value).

With this notation at hand, we prove:

Proposition 3.4 – *For any integer $d \geq 2$ prime to q, the special value $L^*(E_d/K,1)$ admits the following expression:*

$$L^*(E_d/K,1) = \prod_{\mathbf{m}\in\mathcal{O}_q(V_d)} |\mathbf{m}| \cdot \prod_{\mathbf{m}\in\mathcal{O}_q(S_d)} \left(1 - \frac{\mathbf{J}(\mathbf{m})^2}{q^{|\mathbf{m}|}}\right). \tag{3.3}$$

Proof: For any $\mathbf{m} \in \mathcal{O}_q(Z_d)$, let $g_{\mathbf{m}}(T) := 1 - \mathbf{J}(\mathbf{m})^2 \cdot T^{|\mathbf{m}|}$ be the corresponding factor of $L(E_d/K,T)$ (see Theorem 3.2). A straightforward computation shows that we have

$$\rho' = \operatorname{ord}_{T=q^{-1}} g_{\mathbf{m}}(T) = \begin{cases} 1 & \text{if } \mathbf{m} \in \mathcal{O}_q(V_d), \\ 0 & \text{otherwise,} \end{cases} \quad \text{and} \quad \left.\frac{g_{\mathbf{m}}(T)}{(1-qT)^{\rho'}}\right|_{T=q^{-1}} = \begin{cases} |\mathbf{m}| & \text{if } \mathbf{m} \in \mathcal{O}_q(V_d), \\ 1 - \frac{\mathbf{J}(\mathbf{m})^2}{q^{|\mathbf{m}|}} & \text{otherwise.} \end{cases}$$

By definition of $L^*(E_d/K,1)$ (see (2.5)), the desired expression follows by taking the product over all $\mathbf{m} \in \mathcal{O}_q(Z_d) = \mathcal{O}_q(V_d) \sqcup \mathcal{O}_q(S_d)$ of the "special values" at $T = q^{-1}$ of the polynomials $g_{\mathbf{m}}(T)$. □

Remark 3.5 By Theorem 2.3, we know that the rank of $E_d(K)$ is equal to $\rho_d := \operatorname{ord}_{T=q^{-1}} L(E_d/K,T)$. The proof of the above Proposition implies that $\rho_d = \#\mathcal{O}_q(V_d) \leq \#\mathcal{O}_q(Z_d)$. Hence, by Lemma 3.1(c), we have $\rho_d \ll_q d/\log d$ (thus recovering Brumer's bound on the analytic rank [Bru92, Prop. 6.9]).

3.4 Upper bound on the special value

Let us prove an upper bound on $L^*(E_d/K,1)$:

Theorem 3.6 – *Let $\mathbb{F}_q$ be a finite field of odd characteristic and $K = \mathbb{F}_q(t)$. For any integer $d \geq 2$ coprime to q, the special value $L^*(E_d/K,1)$ satisfies the upper bound:*

$$\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \leq A \cdot \frac{\log\log d}{\log d}, \tag{3.4}$$

for some effective absolute constant $A > 0$.

Remark 3.7 The bound (3.4) is not better than the "generic" upper bound of [HP16, Thm. 7.5] on special values of L-functions of abelian varieties over K. The bound in [HP16, Thm. 7.5] is proved with methods from classical complex analysis. We include a proof of (3.4) nonetheless, because our proof is more elementary and gives a very explicit estimate.

We also note that the hypothesis that d be coprime to q is not necessary: one can easily deduce from Theorem 3.6 that (3.4) holds for *all* large enough integers $d \geq 2$ (see Remark 3.3).

Proof: From (3.3) and the fact that $|\mathbf{J}(\mathbf{m})|^2 = q^{|\mathbf{m}|}$ for all $\mathbf{m} \in \mathcal{O}_q(Z_d)$, the triangle inequality leads to

$$\log L^*(E_d/K,1) = \sum_{\mathbf{m}\in\mathcal{O}_q(V_d)} \log|\mathbf{m}| + \sum_{\mathbf{m}\in\mathcal{O}_q(S_d)} \log\left|1 - \frac{\mathbf{J}(\mathbf{m})^2}{q^{|\mathbf{m}|}}\right| \leq \sum_{\mathbf{m}\in\mathcal{O}_q(Z_d)} \log|\mathbf{m}| + \log 2 \cdot |\mathcal{O}_q(Z_d)|.$$

Both the sum on the right-hand side and $|\mathcal{O}_q(Z_d)|$ have already been bounded from above in Lemma 3.1 (items (c) and (d)). We thus infer that

$$\frac{\log L^*(E_d/K,1)}{d\cdot\log q} \ll \frac{\log\log d}{\log d} + \frac{1}{\log d} \ll \frac{\log\log d}{\log d}.$$

And since, by (2.3), one has $\log H(E_d/K) = \left\lfloor \frac{d+1}{2} \right\rfloor \cdot \log q$, we conclude that

$$\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \leq \frac{\log L^*(E_d/K,1)}{d\cdot\log q} \cdot \frac{2d}{d-1} \ll \frac{\log\log d}{\log d}.$$

□

4 Lower bound on the special value

Let $d \geq 2$ be a integer, coprime to q. By construction (see (2.5)), the special value $L^*(E_d/K,1)$ is the value of a certain polynomial $L_d^*(T) \in \mathbb{Z}[T]$ at $T = q^{-1}$. Since $L_d^*(T)$ does not vanish at $T = q^{-1}$, one has $|L^*(E_d/K,1)| \geq q^{-\deg L_d^*(T)}$. Furthermore, by (2.2) and by Remark 3.5 (or by Brumer's bound on the analytic rank [Bru92, Prop. 6.9]), one has

$$\deg L_d^*(T) = \deg L(E_d/K,T) - \operatorname{ord}_{T=q^{-1}} L(E_d/K,T) = d + o(d) \qquad (\text{as } d \to \infty).$$

This quick argument already yields the following lower bound on $L^*(E_d/K,1)$:

$$\frac{\log|L^*(E_d/K,1)|}{d\cdot\log q}\geq -1+o(1)\qquad(\text{as } d\to\infty). \tag{4.1}$$

However, computational evidence suggests that this "trivial" lower bound on $L^*(E_d/K,1)$ is far from the truth. In some special instances, one can improve on (4.1). For example, when d is of the form $d=q^n+1$ (with $n\to\infty$), a theorem of Shafarevich and Tate shows that $\mathbf{J}(m)^2=q^{|\mathbf{m}|}$ for all $m\in Z_d$ (see [ST67], [Ulm02, Prop. 8.1]). In the notations of Proposition 3.4, this means that $V_d=Z_d$ and $S_d=\varnothing$. Thus, for these d's, the special value $L^*(E_d/K,1)$ is actually a positive integer and we obtain an improved lower bound:

$$\frac{\log|L^*(E_d/K,1)|}{d\cdot\log q}\geq 0\qquad(\text{when } d=q^n+1,\text{with } n\to\infty). \tag{4.2}$$

In this section, we prove that the stronger (4.2) holds, up to an error term, for any $d\geq 2$ coprime with q. More precisely, we will show:

Theorem 4.1 – *Let $\mathbb{F}_q$ be a finite field of odd characteristic p and $K=\mathbb{F}_q(t)$. For any integer $d\geq 2$ coprime to q, the special value $L^*(E_d/K,1)$ satisfies the lower bound:*

$$\forall\varepsilon\in(0,1/4),\qquad \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)}\ \geq -B\cdot\left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon}, \tag{4.3}$$

where the constant $B>0$ depends at most on p and ε.

This theorem is our main technical result, from which Theorem 1.1 will follow (see Section 5).

4.1 Proof of Theorem 4.1

Given an integer $d\geq 2$ coprime to q, let us start with the expression for $L^*(E_d/K,1)$ obtained in Proposition 3.4: with the notations introduced there, one has:

$$\log|L^*(E_d/K,1)|=\sum_{\mathbf{m}\in\mathcal{O}_q(V_d)}\log|\mathbf{m}|+\sum_{\mathbf{m}\in\mathcal{O}_q(S_d)}\log\left|1-\frac{\mathbf{J}(\mathbf{m})^2}{q^{|\mathbf{m}|}}\right|.$$

Although the first term here is positive, we know by Lemma 3.1(d) that it is $o(d)$ when $d\to\infty$: consequently, proving Theorem 4.1 requires that we control how negative the second sum can be.

Since $L^*(E_d/K,1)$ is a rational number, the product $\pi_d^*:=\prod_{\mathbf{m}\in\mathcal{O}_q(S_d)}\left(1-\frac{\mathbf{J}(\mathbf{m})^2}{q^{|\mathbf{m}|}}\right)$, *a priori* an element of the cyclotomic field $K:=\mathbb{Q}(\zeta_d)$, is also rational. In particular, one has $\mathbf{N}_{K/\mathbb{Q}}(\pi_d^*)=(\pi_d^*)^{[K:\mathbb{Q}]}$ and the multiplicativity of the norm implies that

$$\begin{aligned}\log|L^*(E_d/K,1)|\geq\log|\pi_d^*|&=\frac{\log\mathbf{N}_{K/\mathbb{Q}}(\pi_d^*)}{[K:\mathbb{Q}]}=\frac{1}{[K:\mathbb{Q}]}\sum_{\mathbf{m}\in\mathcal{O}_q(S_d)}\log\mathbf{N}_{K/\mathbb{Q}}\left(1-\frac{\mathbf{J}(\mathbf{m})^2}{q^{|\mathbf{m}|}}\right)\\&=\frac{1}{\phi(d)}\sum_{m\in S_d}\frac{1}{|\mathbf{m}|}\cdot\log\mathbf{N}_{K/\mathbb{Q}}\left(1-\frac{\mathbf{J}(m)^2}{q^{|\mathbf{m}|}}\right).\end{aligned} \tag{4.4}$$

Indeed, the value of $\mathbf{J}(\mathbf{m})$ does not depend on the representative $m\in\mathbf{m}$ of that orbit (see Section 3.2).

We now try to obtain a more tractable expression for the right-hand side of (4.4). Let us first make use of the following lemma (inspired by [Shi87, Prop. 2.1]):

Lemma A – *Let $d\geq 2$ be an integer prime to q. For $m\in Z_d$, either $\mathbf{J}(m)^2=q^{|\mathbf{m}|}$, or*

$$\log\mathbf{N}_{K/\mathbb{Q}}\left(1-\frac{\mathbf{J}(m)^2}{q^{|\mathbf{m}|}}\right)\geq-(\log q^{|\mathbf{m}|})\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,1-\frac{2\cdot\mathrm{ord}_{\mathfrak{p}}\mathbf{J}(g\cdot m)}{\mathrm{ord}_p(q^{|\mathbf{m}|})}\right\}, \tag{4.5}$$

where $\mathfrak{p}=\mathfrak{P}\cap\mathbb{Q}(\zeta_d)$ is the prime ideal of $K=\mathbb{Q}(\zeta_d)$ which lies below $\mathfrak{P}\subset\overline{\mathbb{Z}}$ (see Section 3.2), and where $\mathrm{ord}_p(.)$ denotes the p-adic valuation on $\mathbb{Z}$.

To avoid interrupting our current computation, we postpone the proof of this Lemma until the next subsection. Plugging (4.5) in (4.4), rearranging terms and dividing throughout by $\log q^d$ leads to:

$$\begin{aligned}\frac{\log|L^*(E_d/K,1)|}{d\cdot\log q} &\geq -\frac{1}{d}\sum_{m\in S_d}\left(\frac{1}{\phi(d)}\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,1-\frac{2\cdot\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(g\cdot m)}{\mathrm{ord}_p(q^{|\mathbf{m}|})}\right\}\right)\\ &\geq -\frac{1}{d}\sum_{m\in Z_d}\left(\frac{1}{\phi(d)}\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,1-\frac{2\cdot\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(g\cdot m)}{\mathrm{ord}_p(q^{|g\cdot\mathbf{m}|})}\right\}\right),\end{aligned}\tag{4.6}$$

because the terms we added are nonnegative, and because $|\mathbf{m}| = |g\cdot\mathbf{m}|$ for $g\in(\mathbb{Z}/d\mathbb{Z})^\times$. To go further, we use the following variation on Stickelberger's theorem:

Lemma B (Stickelberger) – *Let $d\geq 2$ be an integer prime to q, and $\mathfrak{p}$ be as above. For all $n\in Z_d$, the $\mathfrak{p}$-adic valuation of $\mathbf{J}(n)$ is given by*

$$\frac{\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(n)}{\mathrm{ord}_p(q^{|\mathbf{n}|})} = \frac{1}{|\langle p\rangle_d|}\cdot\sum_{\pi\in\langle p\rangle_d}\mathbb{1}\left(\left\{\frac{\pi n}{d}\right\}\right)\tag{4.7}$$

where $\langle p\rangle_d\subset(\mathbb{Z}/d\mathbb{Z})^\times$ is the subgroup generated by p, $\{.\}$ denotes the fractional part, and $\mathbb{1}:[0,1]\to\mathbb{R}$ is the characteristic function of the interval $(0,1/2]$.

The proof of this Lemma will also be given in the next subsection. For now, we use the result with $n = g\cdot m$ and rewrite, for all $m\in Z_d$:

$$\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,1-\frac{2\cdot\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(g\cdot m)}{\mathrm{ord}_p(q^{|g\cdot\mathbf{m}|})}\right\} = 2\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,\frac{1}{2}-\frac{1}{|\langle p\rangle_d|}\sum_{\pi\in\langle p\rangle_d}\mathbb{1}\left(\left\{\frac{\pi g m}{d}\right\}\right)\right\},$$

where $1/2 = \int_{[0,1]}\mathbb{1}$. Summing these identities over all $m\in Z_d$, we rewrite inequality (4.6) under the following form:

$$\frac{\log L^*(E_d/K,1)}{d\cdot\log q}\geq -2\cdot\frac{1}{d}\sum_{m\in Z_d}E_p(m,d),\tag{4.8}$$

where $E_p(m,d)\geq 0$ is defined by

$$E_p(m,d) = \frac{1}{\phi(d)}\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,\int_{[0,1]}\mathbb{1}-\frac{1}{|\langle p\rangle_d|}\sum_{\pi\in\langle p\rangle_d}\mathbb{1}\left(\left\{\frac{\pi g m}{d}\right\}\right)\right\}.$$

The proof of Theorem 4.1 is now reduced to showing that $\frac{1}{d}\sum_{m\in Z_d}E_p(m,d)$ tends to 0 when $d\to\infty$. Since $\mathbb{1}(x)\geq 0$, $E_p(m,d)$ satisfies $E_p(m,d)\leq 1/2$. For most $m\in Z_d$ though, a tighter upper bound holds (the proof of which will be given in subsection 4.3):

Lemma C – *Let $d\geq 2$ be an integer, coprime to q. For $m\in Z_d$, set $d_m = d/\gcd(m,d)$. For all $\varepsilon\in(0,1/4)$, one has*

$$E_p(m,d)\ \ll_{p,\varepsilon}\left(\frac{\log\log d_m}{\log d_m}\right)^{1/4-\varepsilon},\tag{4.9}$$

where the implicit constant is effective and depends only on p and ε.

As suggested by (4.9), we group the terms $m\in Z_d$ of the sum in (4.8) according to the value of $d_m = d/\gcd(d,m)$:

$$\sum_{m\in Z_d}E_p(m,d) = \sum_{\substack{e\mid d\\ e<d}}\sum_{\substack{m\in Z_d\\ d_m=e}}E_p(m,d).$$

For each divisor e of d, note that the set $\{m\in Z_d : d_m = e\}$ contains exactly $|(\mathbb{Z}/e\mathbb{Z})^\times| = \phi(e)$ elements. Since the bound (4.9) is good only when d_m is large enough, we proceed to cut the last displayed sum into two parts, with a parameter $u\in(0,1/2)$. On the one hand, using the trivial bound $E_p(m,d)\leq 1/2$, we obtain that

$$\sum_{\substack{e\mid d\\ e<d^u}}\sum_{\substack{m\in Z_d\\ d_m=e}}E_p(m,d)\leq\sum_{\substack{e\mid d\\ e<d^u}}\frac{1}{2}\cdot|\{m\in Z_d : d_m = e\}|\leq\sum_{\substack{e\mid d\\ e<d^u}}\frac{\phi(e)}{2}\leq\sum_{1\leq e\leq d^u}\frac{e}{2}\ll d^{2u}.$$

On the other hand, using the refined bound (4.9) and the fact that the map $\Psi_\varepsilon : x \mapsto (\log\log x/\log x)^{1/4-\varepsilon}$ is decreasing, we get that

$$\sum_{\substack{e|d\\ e\geq d^u}} \sum_{\substack{m\in Z_d\\ d_m=e}} E_p(m,d) \ll_{p,\varepsilon} \sum_{\substack{e|d\\ e\geq d^u}} \phi(e)\cdot\Psi_\varepsilon(e) \ll_{p,\varepsilon} \Psi_\varepsilon(d^u)\cdot\sum_{e|d}\phi(e) \ll_{p,\varepsilon} \Psi_\varepsilon(d^u)\cdot d \ll_{p,\varepsilon} \frac{\Psi_\varepsilon(d)}{u^{1/4-\varepsilon}}\cdot d,$$

where the last inequality follows from $\frac{\log\log d^u}{\log d^u} \leq \frac{1}{u}\cdot\frac{\log\log d}{\log d}$. Adding the two contributions, we deduce that

$$\frac{1}{d}\sum_{m\in Z_d} E_p(m,d) \ll_{p,\varepsilon} d^{2u-1} + \frac{1}{u^{1/4-\varepsilon}}\cdot\left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon} \ll_{p,\varepsilon,u} \left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon}.$$

Upon choosing a value $u\in(0,1/2)$ and plugging this bound in the right-hand side of (4.8), we arrive at

$$\frac{\log L^*(E_d/K,1)}{d\cdot\log q} \geq -B_0\cdot\left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon},$$

from which it readily follows that

$$\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \geq -B\cdot\left(\frac{\log\log d}{\log d}\right)^{1/4-\varepsilon},$$

for some effective constant $B>0$ depending at most on p,ε. Modulo the proofs of the three Lemmas A, B and C, this last inequality concludes the proof of Theorem 4.1. □

4.2 Proof of the algebraic Lemmas

Let $d\geq 2$ be an integer coprime to q. As above, let $K=\mathbb{Q}(\zeta_d)$ be the d-th cyclotomic field, and $\mathfrak{p}$ be the prime ideal of K which lies below the ideal $\mathfrak{P}\subset\overline{\mathbb{Z}}$ chosen in section 3.2 (thus $\mathfrak{p}$ lies above p). We identify the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ with $(\mathbb{Z}/d\mathbb{Z})^\times$ in the usual manner: to $t\in(\mathbb{Z}/d\mathbb{Z})^\times$ corresponds $\sigma_t\in\mathrm{Gal}(K/\mathbb{Q})$ defined by $\zeta_d\mapsto\zeta_d^t$. We rely on well-known facts on the arithmetic of cyclotomic fields, for which the reader can consult [IR90, Chap. 13].

Proof (of Lemma A): Fix representatives $g_1=1,g_2,\dots,g_s\in(\mathbb{Z}/d\mathbb{Z})^\times$ of the quotient $(\mathbb{Z}/d\mathbb{Z})^\times/\langle p\rangle_d$ of $(\mathbb{Z}/d\mathbb{Z})^\times$ by the subgroup $\langle p\rangle_d$ generated by p. For $i\in\{1,\dots,s\}$, put $\mathfrak{p}_i:=(\sigma_{g_i})^{-1}\mathfrak{p}$, so that p decomposes in K as the product $p\cdot\mathbb{Z}[\zeta_d]=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_s$. We note that $\mathbf{N}\mathfrak{p}_i=\mathbf{N}\mathfrak{p}=p^{\phi(d)/s}$ for all i.

As in the statement of the Lemma, let $m\in Z_d$ such that $\mathbf{J}(m)^2\neq q^{|\mathbf{m}|}$, and define $v_m:=\mathrm{ord}_p(q^{|\mathbf{m}|})$. Since p is unramified in K, $v_m=\mathrm{ord}_{\mathfrak{p}}(q^{|\mathbf{m}|})$ and it is clear that $q^{|\mathbf{m}|}\cdot\mathbb{Z}[\zeta_d]=\prod_{i=1}^s\mathfrak{p}_i^{v_m}$. The integral ideal generated by the Jacobi sum $\mathbf{J}(m)\in\mathbb{Z}[\zeta_d]$ is concentrated above p (because $|\mathbf{J}(m)|=q^{|\mathbf{m}|/2}=p^{v_m/2}$): its decomposition as a product of prime ideals is $\mathbf{J}(m)=\prod_{i=1}^s\mathfrak{p}_i^{\mathrm{ord}_{\mathfrak{p}_i}\mathbf{J}(m)}$. It can be seen that the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\{\mathbf{J}(n)\}_{n\in Z_d}$ is given by $\sigma_g(\mathbf{J}(n))=\mathbf{J}(g\cdot n)$ for all $g\in(\mathbb{Z}/d\mathbb{Z})^\times$. This gives that

$$\mathrm{ord}_{\mathfrak{p}_i}\mathbf{J}(m)=\mathrm{ord}_{\sigma_{g_i}^{-1}\mathfrak{p}}\mathbf{J}(m)=\mathrm{ord}_{\mathfrak{p}}\,\sigma_{g_i}\mathbf{J}(m)=\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(g_i\cdot m).$$

Now, consider the ideal

$$\mathcal{I}_m:=\prod_{i=1}^s\mathfrak{p}_i^{\min\{v_m,2\,\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(g_i\cdot m)\}}=\prod_{g\in(\mathbb{Z}/d\mathbb{Z})^\times/\langle p\rangle_d}(\sigma_g^{-1}\mathfrak{p})^{\min\{v_m,2\,\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(g\cdot m)\}}.$$

By construction, $\mathcal{I}_m$ is an integral ideal in K, which divides the (nonzero) ideal generated by $(q^{|\mathbf{m}|}-\mathbf{J}(m)^2)$ in $\mathbb{Z}[\zeta_d]$. In particular, its norm $\mathbf{N}\mathcal{I}_m$ divides $\mathbf{N}_{K/\mathbb{Q}}(q^{|\mathbf{m}|}-\mathbf{J}(m)^2)$ in $\mathbb{Z}$. We infer that

$$\mathbf{N}_{K/\mathbb{Q}}\left(1-\frac{\mathbf{J}(m)^2}{q^{|\mathbf{m}|}}\right)=\frac{\mathbf{N}_{K/\mathbb{Q}}(q^{|\mathbf{m}|}-\mathbf{J}(m)^2)}{\mathbf{N}_{K/\mathbb{Q}}(q^{|\mathbf{m}|})}\geq\frac{\mathbf{N}\mathcal{I}_m}{\mathbf{N}_{K/\mathbb{Q}}(q^{|\mathbf{m}|})}=\frac{1}{q^{|\mathbf{m}|\cdot\phi(d)}\cdot(\mathbf{N}\mathcal{I}_m)^{-1}}.$$

A straightforward computation from the definition of $\mathcal{I}_m$ implies that

$$q^{|\mathbf{m}|\cdot\phi(d)}\cdot(\mathbf{N}\mathcal{I}_m)^{-1}=q^{|\mathbf{m}|\cdot\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,1-\frac{2\,\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(g\cdot m)}{v_m}\right\}}.$$

This uses our choice of g_i's as representatives of $(\mathbb{Z}/d\mathbb{Z})^\times/\langle p\rangle_d$, and the fact that $\mathbf{J}(p^j\cdot m)=\mathbf{J}(m)$ for all $j\geq 0$. Finally, from the last two displayed relations, we deduce that

$$\log\mathbf{N}_{K/\mathbb{Q}}\left(1-\frac{\mathbf{J}(m)^2}{q^{\mathbf{m}}}\right)\geq-\log(q^{|\mathbf{m}|})\cdot\sum_{g\in(\mathbb{Z}/d\mathbb{Z})^\times}\max\left\{0,1-\frac{2\,\mathrm{ord}_{\mathfrak{p}}\,\mathbf{J}(g\cdot m)}{v_m}\right\},$$

as was to be proved. □

Proof (of Lemma B): Set $Q = q^{o_q(d)}$, $v = [\mathbb{F}_Q : \mathbb{F}_p] = \mathrm{ord}_p\, Q$ and $q' = q^{|\mathbf{n}|}$. The proof of Stickelberger's theorem gives the $\mathfrak{p}$-adic valuations of Jacobi sums (as in [IR90, Chap. 14] for example, see also [CHU14, §4]). The result of that computation is that the Jacobi sum $\mathbf{J}(n)$ has $\mathfrak{p}$-adic valuation:

$$\mathrm{ord}_{\mathfrak{p}}\, \mathbf{J}(n) = \frac{1}{[\mathbb{F}_Q : \mathbb{F}_{q'}]} \sum_{j=0}^{v-1} \left(-1 + 2\left\{ \frac{-np^j}{d} \right\} + \left\{ \frac{2np^j}{d} \right\} \right).$$

One can check that $y \in [0,1] \mapsto -1 + 2\{-y\} + \{2y\}$ is the characteristic function $\mathbb{1} : [0,1] \to \mathbb{R}$ of the interval $(0, 1/2]$, so that

$$\mathrm{ord}_{\mathfrak{p}}\, \mathbf{J}(n) = \frac{1}{[\mathbb{F}_Q : \mathbb{F}_{q'}]} \sum_{j=0}^{v-1} \mathbb{1}\left(\left\{ \frac{np^j}{d} \right\} \right). \tag{4.10}$$

There are repetitions in the sum over j: indeed, since q is a power of p, one has $v = \mathrm{lcm}([\mathbb{F}_q : \mathbb{F}_p], o_p(d))$ and thus, v is a multiple of $o_p(d)$. By construction, d divides $p^{o_p(d)} - 1$ and any multiple thereof: it follows that we may reindex the sum over $j \in [\![0, v-1]\!]$ into a sum over $\pi \in \langle p \rangle_d$ and obtain

$$\sum_{j=0}^{v-1} \mathbb{1}\left(\left\{ \frac{np^j}{d} \right\} \right) = \frac{v}{o_p(d)} \cdot \sum_{\pi \in \langle p \rangle_d} \mathbb{1}\left(\left\{ \frac{n\pi}{d} \right\} \right). \tag{4.11}$$

Secondly, we note that

$$\frac{v}{o_p(d) \cdot [\mathbb{F}_Q : \mathbb{F}_{q'}]} = \frac{[\mathbb{F}_Q : \mathbb{F}_p]}{o_p(d) \cdot [\mathbb{F}_Q : \mathbb{F}_{q'}]} = \frac{[\mathbb{F}_{q'} : \mathbb{F}_p]}{o_p(d)} = \frac{\mathrm{ord}_p(q^{|\mathbf{n}|})}{|\langle p \rangle_d|}. \tag{4.12}$$

Combining (4.11) and (4.12) with (4.10) yields the desired expression for $\mathrm{ord}_{\mathfrak{p}}\, \mathbf{J}(n)$. □

4.3 Proof of the analytic Lemma

Before starting the proof, let us recall the following equidistribution statement:

Theorem 4.2 – *Let $F : [0,1] \to \mathbb{R}$ be a function of bounded total variation, and denote by $\mathscr{V}(F)$ the total variation of F. For an integer $d' \geq 2$, suppose we are given an element $n \in (\mathbb{Z}/d'\mathbb{Z})^\times$ and a subset H of $(\mathbb{Z}/d'\mathbb{Z})^\times$. Then, for all $\varepsilon \in (0, 1/4)$, one has*

$$\frac{1}{\phi(d')} \sum_{g \in (\mathbb{Z}/d'\mathbb{Z})^\times} \left| \int_0^1 F(t)\mathrm{d}t - \frac{1}{|H|} \sum_{h \in H} F\left(\left\{ \frac{hgn}{d'} \right\} \right) \right| \ll_\varepsilon \mathscr{V}(F) \cdot \left(\frac{\log\log d'}{|H|} \right)^{1/4-\varepsilon}. \tag{4.13}$$

We refer to [Gri16b, Theorem 4.1] for the proof of this theorem, and detailed comments.

Let $d \geq 2$ be an integer coprime to q, and $m \in Z_d$, we put $m' := m/\gcd(d,m)$ and $d' := d_m = d/\gcd(d,m)$. As in (4.8), we set

$$E_p(m,d) = \frac{1}{\phi(d)} \sum_{g \in (\mathbb{Z}/d\mathbb{Z})^\times} \max\left\{ 0, \int_{[0,1]} \mathbb{1} - \frac{1}{|\langle p \rangle_d|} \sum_{\pi \in \langle p \rangle_d} \mathbb{1}\left(\left\{ \frac{\pi g m}{d} \right\} \right) \right\}.$$

Proof (of Lemma C): First, we observe that $E_p(m,d) = E_p(m',d')$. Indeed, the subgroup $\langle p \rangle_{d'} \subset (\mathbb{Z}/d'\mathbb{Z})^\times$ is the image of $\langle p \rangle_d$ under the natural surjective morphism $(\mathbb{Z}/d\mathbb{Z})^\times \to (\mathbb{Z}/d'\mathbb{Z})^\times$, and this leads to

$$\forall g \in (\mathbb{Z}/d\mathbb{Z})^\times, \quad \frac{1}{|\langle p \rangle_d|} \sum_{\pi \in \langle p \rangle_d} \mathbb{1}\left(\left\{ \frac{\pi g m}{d} \right\} \right) = \frac{1}{|\langle p \rangle_d|} \sum_{\pi \in \langle p \rangle_d} \mathbb{1}\left(\left\{ \frac{\pi g m'}{d'} \right\} \right) = \frac{1}{|\langle p \rangle_{d'}|} \sum_{\pi' \in \langle p \rangle_{d'}} \mathbb{1}\left(\left\{ \frac{\pi' g m'}{d'} \right\} \right).$$

A similar argument replaces the outer average in $E_p(m,d)$ (over $(\mathbb{Z}/d\mathbb{Z})^\times$) by an average over $(\mathbb{Z}/d'\mathbb{Z})^\times$, thus proving the claim. The upshot of this manipulation is that $\gcd(m',d') = 1$, and we are now in a position to use Theorem 4.2.

Precisely, we apply Theorem 4.2 to the step function $F = \mathbb{1}$ with $n = m'$ and $H = \langle p \rangle_{d'}$. Note that $|\langle p \rangle_{d'}| \geq \log d'/\log p$ because d' divides $p^{o_p(d')} - 1$ by definition of the multiplicative order $o_p(d') = |\langle p \rangle_{d'}|$ of p mod d'. Since $\mathbb{1}$ is a step function on $[0,1]$, it is of bounded total variation; moreover, $\mathbb{1}$ has only one "jump" of height 1, so its total variation is $\mathscr{V}(\mathbb{1}) = 1$.

Noticing that $\max\{0,y\} \leq |y|$ for all $y \in \mathbb{R}$, inequality (4.13) here reads:

$$0 \leq E_p(m,d) = E_p(m',d') \leq \frac{1}{\phi(d')} \sum_{g \in (\mathbb{Z}/d'\mathbb{Z})^\times} \left| \int_{[0,1]} \mathbb{1} - \frac{1}{|\langle p \rangle_{d'}|} \sum_{\pi \in \langle p \rangle_{d'}} \mathbb{1}\left(\left\{ \frac{\pi g m'}{d'} \right\} \right) \right|$$
$$\ll_\varepsilon \left(\frac{\log\log d'}{|H|} \right)^{1/4-\varepsilon} \ll_{p,\varepsilon} \left(\frac{\log\log d'}{\log d'} \right)^{1/4-\varepsilon}.$$

This concludes the proof. □

5 Conclusion

Regrouping the results of Theorems 3.6 and 4.1, we obtain a precise asymptotic estimate of $L^*(E_d/K,1)$ when d is coprime to q:

Corollary 5.1 – *Let $\mathbb{F}_q$ be a finite field of odd characteristic p and $K = \mathbb{F}_q(t)$. For all $\varepsilon \in (0,1/4)$, there are positive constants A, B (depending at most on p and ε) such that: for any integer $d \geq 2$ coprime to q, the special value $L^*(E_d/K,1)$ satisfies*

$$-B \cdot \left(\frac{\log\log d}{\log d} \right)^{1/4-\varepsilon} \leq \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} \leq A \cdot \frac{\log\log d}{\log d}. \tag{5.1}$$

Remark 5.2 By keeping track of constants in the estimates, one can make A and B explicit: it appears that $A = 48$ and $B = 2\left(32 + 4(3\pi)^{-3}\varepsilon^{-2}\right)(4\log p)^{1/4-\varepsilon}$ are suitable choices in (5.1).

We can now state and prove a quantitative form of Theorem 1.1:

Theorem 5.3 – *Let $\mathbb{F}_q$ be a finite field of odd characteristic, and $K = \mathbb{F}_q(t)$. For any integer $d \geq 2$, consider the Legendre elliptic curve E_d/K as defined by (2.1). For all $\varepsilon \in (0,1/4)$, one has*

$$\frac{\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right)}{\log H(E_d/K)} = 1 + O_{q,p,\varepsilon}\left(\left(\frac{\log\log d}{\log d} \right)^{1/4-\varepsilon} \right) \quad (\textit{as } d \to \infty),$$

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

Proof: For conciseness, we denote the ratio $\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)}$ by $\lambda^*(E_d)$ for any integer $d \geq 2$, and we let $\Psi(d) := (\log\log d)/\log d$. Let d be any large enough integer and write $d = p^a d'$ with d' coprime to p. We claim that

$$|\lambda^*(E_d)| \ll_{q,p,\varepsilon} \Psi(d)^{1/4-\varepsilon} \text{ as } d \to \infty \text{ ranges through all integers.} \tag{♯}$$

Assuming that (♯) holds, we deduce from Corollary 2.5 that, for all integers $d \geq 2$,

$$\left| \frac{\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right)}{\log H(E_d/K)} - 1 \right| \ll_q |\lambda^*(E_d)| + \frac{1}{\log d} \ll_{q,p,\varepsilon} \Psi(d)^{1/4-\varepsilon} \quad (\text{as } d \to \infty),$$

which is the desired asymptotic relation. Hence the Theorem will follow once we prove (♯).

As was noted several times, E_d and $E_{d'}$ are K-isogenous *via* the p^a-th power Frobenius morphism: in particular, their L-functions are equal, hence $L^*(E_d/K,1) = L^*(E_{d'}/K,1)$. By construction of d', we know from Corollary 5.1 that $|\lambda^*(E_{d'})| \ll_{q,p,\varepsilon} \Psi(d')^{1/4-\varepsilon}$. With the help of (2.3) we deduce that

$$|\lambda^*(E_d)| = \frac{\log H(E_{d'}/K)}{\log H(E_d/K)} \cdot |\lambda^*(E_{d'})| \ \ll \frac{d'}{d} \cdot |\lambda^*(E_{d'})| \ll_{q,p,\varepsilon} \frac{d'}{d} \cdot \Psi(d')^{1/4-\varepsilon}. \tag{5.2}$$

If we assume that $d'/d \leq \Psi(d)^{1/4-\varepsilon}$, then (5.2) directly implies that $|\lambda^*(E_d)| \ll_{q,p,\varepsilon} \Psi(d)^{1/4-\varepsilon}$ upon noting that $\Psi(d') \leq \mathrm{e}^{-1}$ Indeed, $x \mapsto \Psi(x)$ satisfies $\Psi(x) \leq \mathrm{e}^{-1}$ on $[3,+\infty)$. This proves (♯) for integers d such that d'/d is "small". Let us now assume that $d' > d \cdot \Psi(d)^{1/4-\varepsilon}$, in which case we have $d' \geq d^{1-\eta_\varepsilon}$ with $\eta_\varepsilon = \mathrm{e}^{-1}(1/4-\varepsilon)$ because $\Psi(x) \geq x^{-1/\mathrm{e}}$ for all $x \geq \mathrm{e}^{\mathrm{e}}$. Since $x \mapsto \Psi(x)$ is decreasing on $[\mathrm{e}^{\mathrm{e}},+\infty)$ and since $\Psi(x^{1-\eta}) \leq (1-\eta)^{-1}\Psi(x)$ for all $x \geq 3$ and $\eta \in [0,1)$, we have

$$\frac{d'}{d}\Psi(d')^{1/4-\varepsilon} \leq \Psi(d')^{1/4-\varepsilon} \leq \Psi\left(d^{1-\eta_\varepsilon}\right)^{1/4-\varepsilon} \ll_\varepsilon (1-\eta_\varepsilon)^{\varepsilon-1/4}\Psi(d)^{1/4-\varepsilon} \ll_\varepsilon \Psi(d)^{1/4-\varepsilon}.$$

And (5.2) shows that (♯) also holds for integers $d \geq \mathrm{e}^{\mathrm{e}}$ such that $d' > d \cdot \Psi(d)^{1/4-\varepsilon}$.

Therefore the claim (♯) holds and the proof of Theorem 5.3 is now complete. □

References

[Bru92] Armand Brumer. The average rank of elliptic curves. I. *Invent. Math.*, 109(3):445–472, 1992. ↑ 5, 9

[CHU14] Ricardo P. Conceição, Chris Hall, and Douglas Ulmer. Explicit points on the Legendre curve II. *Math. Res. Lett.*, 21(2):261–280, 2014. ↑ 2, 3, 6, 8, 13

[Gri16a] Richard Griffon. *Analogues du théorème de Brauer-Siegel pour quelques familles de courbes elliptiques.* PhD thesis, Université Paris Diderot, July 2016. (available at math.leidenuniv.nl/~griffonrmm/thesis/Griffon_thesis.pdf). ↑ 2, 3

[Gri16b] Richard Griffon. A Brauer-Siegel theorem for Fermat surfaces over finite fields. (Preprint ArXiv:1612.08721), December 2016. ↑ 3, 13

[Hin07] Marc Hindry. Why is it difficult to compute the Mordell-Weil group? In *Diophantine geometry*, volume 4 of *CRM Series*, pages 197–219. Ed. Norm., Pisa, 2007. ↑ 2

[HP16] Marc Hindry and Amìlcar Pacheco. An analogue of the Brauer–Siegel theorem for abelian varieties in positive characteristic. *Moscow Math. J.*, 16(1):45–93, January–March 2016. ↑ 1, 2, 6, 9

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, 2nd edition, 1990. ↑ 6, 8, 12, 13

[KT03] Kazuya Kato and Fabien Trihan. On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$. *Invent. Math.*, 153(3):537–592, 2003. ↑ 5

[Lan83] Serge Lang. Conjectured Diophantine estimates on elliptic curves. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 155–171. Birkhäuser Boston, Boston, MA, 1983. ↑ 2

[Mil75] James S. Milne. On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975. ↑ 5

[Shi87] Tetsuji Shioda. Some observations on Jacobi sums. In *Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986)*, volume 12 of *Adv. Stud. Pure Math.*, pages 119–135. North-Holland, 1987. ↑ 10

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. ↑ 3, 4

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2nd edition, 2009. ↑ 4, 5

[ST67] Igor R. Shafarevich and John T. Tate. The rank of elliptic curves. *Dokl. Akad. Nauk SSSR*, 175:770–773, 1967. ↑ 10

[Tat94] John T. Tate. Conjectures on algebraic cycles in l-adic cohomology. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 71–83. Amer. Math. Soc., 1994. ↑ 5

[Tat66] John T. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages 415–440 (Exp. No. 306). Soc. Math. France, Paris, 1965/66. ↑ 5

[Ulm02] Douglas Ulmer. Elliptic curves with large rank over function fields. *Ann. of Math. (2)*, 155(1):295–315, 2002. ↑ 10

[Ulm11] Douglas Ulmer. Elliptic curves over function fields. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 211–280. Amer. Math. Soc., Providence, RI, 2011. ↑ 5

[Ulm13] Douglas Ulmer. On Mordell-Weil groups of Jacobians over function fields. *J. Inst. Math. Jussieu*, 12(1):1–29, 2013. ↑ 5

[Ulm14] Douglas Ulmer. Explicit points on the Legendre curve. *J. Number Theory*, 136:165–194, 2014. ↑ 2, 3, 4, 5, 8