PACIFIC JOURNAL OF MATHEMATICS
Vol. 305, No. 2, 2020
dx.doi.org/10.2140/pjm.2020.305.597

ON THE ARITHMETIC OF A FAMILY OF TWISTED CONSTANT ELLIPTIC CURVES

RICHARD GRIFFON AND DOUGLAS ULMER

Let $\mathbb{F}_r$ be a finite field of characteristic $p > 3$. For any power q of p, consider the elliptic curve $E = E_{q,r}$ defined by $y^2 = x^3 + t^q - t$ over $K = \mathbb{F}_r(t)$. We describe several arithmetic invariants of E such as the rank of its Mordell–Weil group $E(K)$, the size of its Néron–Tate regulator $\mathrm{Reg}(E)$, and the order of its Tate–Shafarevich group $Ш(E)$ (which we prove is finite). These invariants have radically different behaviors depending on the congruence class of p modulo 6. For instance $Ш(E)$ either has trivial p-part or is a p-group. On the other hand, we show that the product $|Ш(E)|\,\mathrm{Reg}(E)$ has size comparable to $r^{q/6}$ as $q \to \infty$, regardless of $p \pmod 6$. Our approach relies on the BSD conjecture, an explicit expression for the L-function of E, and a geometric analysis of the Néron model of E.

1. Introduction

For a prime $p > 3$, and powers q and r of p, we study the elliptic curve

$$E: \quad y^2 = x^3 + t^q - t$$

over the rational function field $K = \mathbb{F}_r(t)$. We are interested in the Mordell–Weil group $E(K)$, its regulator $\mathrm{Reg}(E)$, and the Tate–Shafarevich group $Ш(E)$ of E. By old results of Tate [1966] and Milne [1975], $Ш(E)$ is finite and the conjecture of Birch and Swinnerton-Dyer holds for E.

One of our main results says that $\mathrm{Reg}(E)\,|Ш(E)|$ is an integer comparable in archimedean size to $r^{q/6}$ when r is fixed and q tends to ∞. (See Theorem 11.1 for the precise statement.) On the other hand, we will show that if $p \equiv 1 \pmod 6$, then $E(K) = 0$, $\mathrm{Reg}(E) = 1$, and $|Ш(E)|$ is a p-adic unit; and that if $p \equiv -1 \pmod 6$ and $\mathbb{F}_r$ is sufficiently large, then $E(K)$ has rank $2(q-1)$, $\mathrm{Reg}(E)\,|Ш(E)|$ is a power of p, and $Ш(E)$ is a p-group (Propositions 8.3.1 and 8.4.1, and Corollary 9.2). These results show in particular that the archimedean and p-adic sizes of $\mathrm{Reg}(E)\,|Ш(E)|$ are independent — in our examples, $\mathrm{Reg}(E)\,|Ш(E)|$ is

MSC2010: primary 11G05, 14J27; secondary 11G40, 11G99, 14G10, 14G99.
Keywords: elliptic curves over function fields, Mordell–Weil rank, Néron–Tate regulator, Tate–Shafarevich group, L-function and BSD conjecture.

	$p \equiv 1 \pmod 6$	$p \equiv -1 \pmod 6$
$E(K)_{\text{tors}}$	$\cong \{0\}$ (Proposition 2.4(2))	
BSD conjecture	holds for E (Theorem 8.2)	
Rank $E(K)$	$= 0$ (Proposition 8.3.1(3))	$= 2(q-1)$ for $\mathbb{F}_r$ large enough (Proposition 8.4.1(3))
$\operatorname{Reg}(E)$	$= 1$ (Proposition 8.3.1(4))	is a power of p for $\mathbb{F}_r$ large enough (Corollary 9.2(3))
$Ш(E)$	has trivial p-part (Proposition 10.1(1))	is a p-group (Corollary 9.2(3))
$\dim Ш(E)$	$= 0$ (Corollary 9.3(1))	$= \lfloor q/6 \rfloor$ (Corollary 9.3(2))
$\lim_{q\to\infty} \operatorname{BS}(E)$	$= 1$ (Theorem 11.1)	
$\lvert Ш(E)\rvert \operatorname{Reg}(E)$	$\geq r^{\lfloor q/6 \rfloor (1+o(1))}$ as $q \to \infty$ (Corollary 11.9)	$= r^{\lfloor q/6 \rfloor}$ for $\mathbb{F}_r$ large enough (Corollary 9.2(3))

Table 1. A summary of the main results of the paper.

large in the archimedean metric, whereas it may be a p-adic unit or divisible by a large power of p.

To prove these results, we combine an analytic analysis of the special value $L^*(E)$, the Birch and Swinnerton-Dyer (BSD) formula, and an algebraic analysis of $Ш(E)$. We are able to deduce the BSD formula and analyze $Ш(E)$ by using the fact that the Néron model $\mathcal{E} \to \mathbb{P}^1$ of E is birational to the quotient of a product of curves by a finite group. In fact, $\mathcal{E}$ has three distinct such presentations, and each is convenient for some aspect of our study.

The plan of the paper is as follows: In the next section, we gather the basic definitions and present a few preliminary results about E. In Section 3, we recall standard results about Gauss and Jacobi sums and use them in Section 4 to give an elementary calculation of the Hasse–Weil L-function of E. In Section 5, we prove results about the geometry and cohomology of certain curves over $\mathbb{F}_r$ which are used in Section 6 to show that the Néron model of E is dominated by a product of curves (in multiple ways). In Section 7, we use these dominations to give alternate calculations of the L-function. In Section 8, we apply the BSD conjecture to study the rank of $E(K)$, and in Section 9 we study the p-adic size of the special value and the order of $Ш(E)$ using the BSD formula. Section 10 reproves our results about $Ш(E)$ by a direct, algebraic approach, i.e., independently of the BSD formula. In Section 11, we study the archimedean size of the special value and the "Brauer–Siegel ratio" of Hindry.

Table 1 summarizes our main results. There, "for $\mathbb{F}_r$ large enough" means that there is a finite extension $\mathbb{F}_{r_0}$ of $\mathbb{F}_p$ such that the statement holds for all finite extensions $\mathbb{F}_r$ of $\mathbb{F}_{r_0}$ (see Proposition 8.4.1(3) for an explicit definition of r_0).

2. First results

2.1. ***Definitions and notation.*** Notation from this section will be in force throughout the paper. We refer to [Ulmer 2011] for a review of what is known about elliptic curves over function fields, in particular with regard to the conjecture of Birch and Swinnerton-Dyer.

Let $p > 3$ be a prime number, let $\mathbb{F}_p$ be the field of p elements, and fix an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. Let $\mathbb{F}_r \subset \overline{\mathbb{F}}_p$ be the finite extension of $\mathbb{F}_p$ of cardinality $r = p^\nu$, and let $K = \mathbb{F}_r(t)$ be the rational function field over $\mathbb{F}_r$. We write v for a place of K, K_v for the completion of K at v, $\deg(v)$ for the degree of v, $\mathbb{F}_v$ for the residue field at v, and $r_v = r^{\deg(v)}$ for the cardinality of $\mathbb{F}_v$. We identify places of K with closed points of the projective line $\mathbb{P}^1_{\mathbb{F}_r}$ over $\mathbb{F}_r$, and we note that finite places of K are in bijection with monic irreducible polynomials in $\mathbb{F}_r[t]$.

Let $q = p^f$ be a power of p, and let E be the elliptic curve over K defined by

$$E = E_{q,r} : \ y^2 = x^3 + t^q - t. \tag{2-1}$$

Write $E(K)$ for the group of K-rational points on E. By the Lang–Néron theorem, this is a finitely generated abelian group.

Let $\mathcal{E} \to \mathbb{P}^1_{\mathbb{F}_r}$ be the Néron model of E. We write c_v for the number of connected components in the special fiber of $\mathcal{E}$ over v. One also calls c_v the local Tamagawa number of E at v.

We denote the (differential) height of E, as defined in [Ulmer 2011, Lecture 3, §2], by $\deg(\omega_E)$. It follows from [Ulmer 2011, Lecture 3, Exercise 2.2] that for E,

$$\deg(\omega_E) = \lceil q/6 \rceil = \begin{cases} \frac{q+5}{6} & \text{if } q \equiv 1 \pmod 6, \\ \frac{q+1}{6} & \text{if } q \equiv -1 \pmod 6. \end{cases}$$

2.2. ***Reduction types.*** From the Weierstrass equation (2-1), one easily computes

$$\Delta = -2^4 3^3 (t^q - t)^2 \quad \text{and} \quad j(E) = 0.$$

Applying Tate's algorithm (see [Silverman 1994, Chapter IV, §9]), one obtains the following further facts:

- At a finite place dividing $t^q - t$, the curve E has additive reduction of type II.
- At $t = \infty$, the curve E has additive reduction of type II* if $q \equiv 1 \pmod 6$ and of type II if $q \equiv 5 \pmod 6$.
- The curve E has good reduction at all other places of K.

From this collection of local information, one deduces that the conductor $\mathcal{N}_E$ of E has degree $\deg \mathcal{N}_E = 2(q+1)$. One can also recover the fact that $\deg(\omega_E) = \lceil q/6 \rceil$ from this computation.

2.3. ***Isotriviality.*** Consider the finite extension $L = K[u]/(u^6 = t^q - t)$ of K, and let E_0 be the elliptic curve over $\mathbb{F}_r$ defined by

$$E_0 : w^2 = z^3 + 1.$$

Then $E \times_K L$ is isomorphic to the constant curve $E_0 \times_{\mathbb{F}_r} L$ via the substitution $(x, y) = (u^2 z, u^3 w)$. In other words, E is the sextic twist of E_0 (or rather of $E_0 \times_{\mathbb{F}_r} K$) by $t^q - t$.

We record two consequences for later use. Recall that the local Tamagawa number c_v is the number of components in the special fiber of the Néron model at v. Its values in terms of the local reduction type are tabulated in [Silverman 1994, p. 365].

Proposition 2.4. (1) *For every place v of K, the local Tamagawa number c_v is* 1.

(2) $E(K)_{\text{tors}} = 0$.

Proof. Part (1) is immediate from the table cited above. For part (2), suppose that $P \in E(K)$ is a nontrivial torsion point. Let $Q = (\alpha, \beta) \in E_0(L)$ be the image of P under the above isomorphism $E \times_K L \cong E_0 \times_{\mathbb{F}_r} L$. Then Q is again a torsion point, and it is known (e.g., [Ulmer 2011, Proposition I.6.1]) that torsion points on a constant curve have constant coordinates. That is, we have $\alpha, \beta \in \mathbb{F}_r$. The original point P thus has coordinates $(\alpha u^2, \beta u^3)$. However, if $\alpha \in \mathbb{F}_r$, then $\alpha u^2 \in K$ only if $\alpha = 0$, and if $\beta \in \mathbb{F}_r$, then $\beta u^3 \in K$ only if $\beta = 0$. Since $(0, 0) \notin E(K)$, there is no nontrivial torsion point $P \in E(K)$. □

3. Preliminaries on exponential sums

3.1. ***Finite fields.*** Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and a prime ideal $\mathfrak{P}$ above p in the ring of algebraic integers $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$. The quotient $\overline{\mathbb{Z}}/\mathfrak{P}$ is then an algebraic closure of $\mathbb{F}_p$ which we denote by $\overline{\mathbb{F}}_p$. All finite fields in this paper will be viewed as subfields of this $\overline{\mathbb{F}}_p$.

3.2. ***Multiplicative characters.*** Reduction modulo $\mathfrak{P}$ induces an isomorphism between the roots of unity of order prime to p in $\overline{\mathbb{Z}}$ and $\overline{\mathbb{F}}_p^{\times}$. We let $\boldsymbol{t} : \overline{\mathbb{F}}_p^{\times} \to \overline{\mathbb{Q}}^{\times}$ denote the inverse of this isomorphism. The same letter $\boldsymbol{t}$ will be used to denote the restriction of $\boldsymbol{t}$ to the multiplicative group of any finite extension $\mathbb{F}$ of $\mathbb{F}_p$ ($\mathbb{F}$ being viewed as a subextension of $\overline{\mathbb{F}}_p$).

If $\mathbb{F}$ is a finite extension of $\mathbb{F}_p$ and n is a divisor of $|\mathbb{F}^{\times}|$, define

$$\chi_{\mathbb{F},n} := \boldsymbol{t}^{|\mathbb{F}^{\times}|/n}.$$

This is a character of $\mathbb{F}^{\times}$ of order exactly n. In particular, if $n = |\mathbb{F}^{\times}|$, the character $\chi_{\mathbb{F},n}$ is a generator of the group of multiplicative characters of $\mathbb{F}$.

If $\mathbb{F} \subset \mathbb{F}'$ are finite extensions of $\mathbb{F}_p$, if n divides the order of $\mathbb{F}^\times$, and if $\mathrm{N}_{\mathbb{F}'/\mathbb{F}}$ denotes the norm from $\mathbb{F}'$ to $\mathbb{F}$, then an easy calculation shows that $\chi_{\mathbb{F}',n} = \chi_{\mathbb{F},n} \circ \mathrm{N}_{\mathbb{F}'/\mathbb{F}}$.

3.3. ***Additive characters.*** Fix once and for all a nontrivial additive character

$$\psi_p : \mathbb{F}_p \to \mathbb{Q}(\mu_p)^\times \subset \overline{\mathbb{Q}}^\times.$$

If $\mathbb{F}$ is a finite extension of $\mathbb{F}_p$, if $\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}$ denotes the trace from $\mathbb{F}$ to $\mathbb{F}_p$, and if $\alpha \in \mathbb{F}^\times$, then the map $x \mapsto \psi_\alpha(x)$ defined by

$$\psi_\alpha(x) = \psi_p(\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}(\alpha x))$$

for all $x \in \mathbb{F}$ is a nontrivial additive character of $\mathbb{F}$. Moreover, any nontrivial additive character of $\mathbb{F}$ is of the form ψ_α for a unique $\alpha \in \mathbb{F}^\times$. When we need to make the underlying field precise, we write $\psi_{\mathbb{F},\alpha}$ instead of ψ_α.

3.4. ***Gauss sums.*** If $\mathbb{F}$ is a finite extension of $\mathbb{F}_p$, χ is a nontrivial character of $\mathbb{F}^\times$, and ψ is a nontrivial additive character of $\mathbb{F}$, define the Gauss sum $G_{\mathbb{F}}(\chi, \psi)$ by

$$G_{\mathbb{F}}(\chi, \psi) = -\sum_{x \in \mathbb{F}^\times} \chi(x)\psi(x).$$

We recall a few well-known properties of these Gauss sums:

(1) If χ has order n, the sum $G_{\mathbb{F}}(\chi, \psi)$ is an algebraic integer in $\mathbb{Q}(\mu_{np})$.

(2) For any nontrivial characters χ and ψ, one has $|G_{\mathbb{F}}(\chi, \psi)| = |\mathbb{F}|^{1/2}$ in any complex embedding of $\overline{\mathbb{Q}}$.

(3) For all nontrivial multiplicative characters χ on $\mathbb{F}^\times$ and all $\alpha \in \mathbb{F}^\times$, one has

$$G_{\mathbb{F}}(\chi, \psi_\alpha) = \chi^{-1}(\alpha) G_{\mathbb{F}}(\chi, \psi_1).$$

(4) (Hasse–Davenport relation) Let χ be a nontrivial multiplicative character on $\mathbb{F}^\times$ and ψ be a nontrivial additive character on $\mathbb{F}$. Then for any finite extension $\mathbb{F}'/\mathbb{F}$, one has

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

(5) (Stickelberger's theorem) Let ord be the p-adic valuation of $\overline{\mathbb{Q}}$ associated to $\mathfrak{P}$, normalized so that $\mathrm{ord}(p) = 1$. If $\mathbb{F}$ has cardinality p^μ and $0 < s < p^\mu - 1$ has p-adic expansion

$$s = s_0 + s_1 p + \cdots + s_{\mu-1} p^{\mu-1}$$

with $0 \le s_i < p$, then

$$\mathrm{ord}(G_{\mathbb{F}}(\chi_{\mathbb{F},|\mathbb{F}^\times|}^{-s}, \psi)) = \frac{1}{p-1} \sum_{i=0}^{\mu-1} s_i.$$

These results are classical, and the reader may find proofs of them (and the claims in the next two subsections) in [Washington 1997, Chapter VI, §1–§2] for instance.

3.5. ***Explicit Gauss sums.*** Let $\mathbb{F}$ be a finite extension of $\mathbb{F}_p$, and write $|\mathbb{F}| = p^\mu$. An elementary calculation shows that, for any nontrivial additive character ψ of $\mathbb{F}$,

$$G_{\mathbb{F}}(\chi_{\mathbb{F},2}, \psi)^2 = ((-1)^{(p-1)/2} p)^\mu. \tag{3-1}$$

In particular, $\operatorname{ord} G_{\mathbb{F}}(\chi_{\mathbb{F},2}, \psi) = \mu/2$. Here, as above, ord denotes the p-adic valuation on $\overline{\mathbb{Q}}$ associated to $\mathfrak{P}$, normalized to that $\operatorname{ord}(p) = 1$.

If $p \equiv 1 \pmod 3$, then Stickelberger's theorem (see (5) above) shows that, for any nontrivial additive character ψ of $\mathbb{F}$,

$$\operatorname{ord} G_{\mathbb{F}}(\chi_{\mathbb{F},3}, \psi) = \tfrac{2}{3}\mu \quad \text{and} \quad \operatorname{ord} G_{\mathbb{F}}(\chi_{\mathbb{F},3}^{-1}, \psi) = \tfrac{1}{3}\mu. \tag{3-2}$$

On the other hand, if $p \equiv 2 \pmod 3$, then 3 divides $|\mathbb{F}^\times|$ if and only if $\mu = [\mathbb{F} : \mathbb{F}_p]$ is even. If this is the case (i.e., if $|\mathbb{F}| = p^\mu \equiv 1 \pmod 3$), an old result of Tate and Shafarevich (see [Ulmer 2002, Lemma 8.2]) and the Hasse–Davenport relation yield that

$$G_{\mathbb{F}}(\chi_{\mathbb{F},3}, \psi_1) = G_{\mathbb{F}}(\chi_{\mathbb{F},3}^{-1}, \psi_1) = (-p)^{\mu/2},$$

and therefore (see (3) in the previous subsection)

$$G_{\mathbb{F}}(\chi_{\mathbb{F},3}, \psi_\alpha) = \chi_{\mathbb{F},3}^{-1}(\alpha)(-p)^{\mu/2} \quad \text{and} \quad G_{\mathbb{F}}(\chi_{\mathbb{F},3}^{-1}, \psi_\alpha) = \chi_{\mathbb{F},3}(\alpha)(-p)^{\mu/2}. \tag{3-3}$$

In particular, $\operatorname{ord} G_{\mathbb{F}}(\chi_{\mathbb{F},3}^{\pm 1}, \psi_\alpha) = \mu/2$ in this case.

3.6. ***Jacobi sums.*** We require only the simplest case: Let $\mathbb{F}$ be a finite extension of $\mathbb{F}_p$ and let χ_1 and χ_2 be two nontrivial characters of $\mathbb{F}^\times$ such that $\chi_1\chi_2$ is also nontrivial. Define

$$J_{\mathbb{F}}(\chi_1, \chi_2) = -\sum_{x \in \mathbb{F}} \chi_1(x)\chi_2(1-x).$$

An elementary calculation (see [Washington 1997, Chapter VI]) shows that

$$J_{\mathbb{F}}(\chi_1, \chi_2) = \frac{G_{\mathbb{F}}(\chi_1, \psi) G_{\mathbb{F}}(\chi_2, \psi)}{G_{\mathbb{F}}(\chi_1\chi_2, \psi)} \tag{3-4}$$

for any nontrivial additive character ψ of $\mathbb{F}$. One may then deduce the archimedean and p-adic sizes of $J(\chi_1, \chi_2)$ from the results quoted in Section 3.4.

3.7. ***Orbits.*** Recall that $p > 3$ is a prime. Given an integer $n \geq 1$ prime to p, let

$$S = S_{n,q} = (\mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q^\times \quad \text{and} \quad S^\times = S_{n,q}^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times \mathbb{F}_q^\times.$$

Let $r = p^\nu$ for some positive integer ν. Write $\langle r \rangle$ for the subgroup of $\mathbb{Q}^\times$ generated by r, and consider the action of $\langle r \rangle$ on S and $S^\times$ given by the rule

$$r(i, \alpha) := (ri, \alpha^{1/r}) \quad \text{for all } (i, \alpha) \in S.$$

In other words, r acts on $\mathbb{Z}/n\mathbb{Z}$ by multiplication, and on $\mathbb{F}_q^\times$ by the inverse of the r-power Frobenius. Let $O_{r,n,q}$ be the set of orbits of $\langle r\rangle$ on S and $O^\times_{r,n,q}$ the set of orbits on $S^\times$.

If $n = 1$, then $O^\times_{r,n,q}$ is just the set of orbits of $\langle r\rangle$ on $\mathbb{F}_q^\times$, which we denote by $O_{r,q}$. Note that if $o \in O_{r,q}$ is the orbit through α, then the cardinality $|o|$ of o is equal to the degree $[\mathbb{F}_r(\alpha) : \mathbb{F}_r]$ of the field extension $\mathbb{F}_r(\alpha)$ over $\mathbb{F}_r$.

For a general n, if $o \in O^\times_{r,n,q}$ is the orbit through (i, α), then

$$|o| = \operatorname{lcm}(\operatorname{ord}^\times(r \bmod n), [\mathbb{F}_r(\alpha) : \mathbb{F}_r]), \tag{3-5}$$

where $\operatorname{ord}^\times(r \bmod n)$ denotes the order of r in $(\mathbb{Z}/n\mathbb{Z})^\times$. Note that, for any $\alpha \in \mathbb{F}_q$, one has $[\mathbb{F}_r(\alpha) : \mathbb{F}_r] = \operatorname{lcm}(\nu, [\mathbb{F}_p(\alpha) : \mathbb{F}_p])/[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$, and $[\mathbb{F}_p(\alpha) : \mathbb{F}_p]$ divides $f = [\mathbb{F}_q : \mathbb{F}_p]$. It is then clear that $|o|$ divides $\operatorname{lcm}(\operatorname{ord}^\times(r \bmod n), \operatorname{lcm}(f, \nu)/f)$ for any orbit $o \in O^\times_{r,n,q}$.

In what follows, we will only need the cases where n divides 6. If $r \equiv 1 \pmod 6$, then $\langle r\rangle$ acts trivially on $\mathbb{Z}/6\mathbb{Z}$ and the orbits $o \in O_{r,6,q}$ are "vertical" in the sense that they are of the form $o = \{(i, \alpha)\}$ where i is fixed and α runs through an orbit of $\langle r\rangle$ on $\mathbb{F}_q^\times$. In particular, $|o| = [\mathbb{F}_r(\alpha) : \mathbb{F}_r]$.

On the other hand, if $r \equiv 5 \equiv -1 \pmod 6$, then orbits $o \in O_{r,6,q}$ "bounce left and right" in the sense that an orbit o contains elements (i, α) and $r(i, \alpha) = (-i, \alpha^{1/r})$. In this case, if o is the orbit through (i, α), then $|o| = \operatorname{lcm}(2, [\mathbb{F}_r(\alpha) : \mathbb{F}_r])$.

In both cases (that is to say, for $r \equiv \pm 1 \pmod 6$), note that $\nu|o|$ is even for all orbits $o \in O^\times_{r,6,q}$.

For $n \in \{2, 3\}$, the natural projection $(\mathbb{Z}/6\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ induces a map $\pi_n : O^\times_{r,6,q} \to O^\times_{r,n,q}$. We record a few elementary observations about π_n:

- The map π_3 is a bijection, because $(\mathbb{Z}/6\mathbb{Z})^\times \to (\mathbb{Z}/3\mathbb{Z})^\times$ is a bijection.
- If $r \equiv 1 \pmod 6$, then π_2 is two-to-one. (This is essentially the same point as the "vertical" remark above.)
- If $r \equiv -1 \pmod 6$ and if $o' \in O^\times_{r,2,q}$ has $|o'|$ even, then there are two orbits $o \in O^\times_{r,6,q}$ with $\pi_2(o) = o'$. Finally, if $r \equiv -1 \pmod 6$ and if $o' \in O^\times_{r,2,q}$ has $|o'|$ odd, then there is a unique orbit $o \in O^\times_{r,6,q}$ with $\pi_2(o) = o'$ and the underlying map of sets $o \to o'$ is two-to-one.

Motivated by this last remark, for any $o \in O^\times_{r,6,q}$, we define

$$m_2(o) = \frac{|o|}{|\pi_2(o)|}.$$

Thus $m_2(o) = 1$ unless $r \equiv -1 \pmod 6$ and $|\pi_2(o)|$ is odd, in which case $m_2(o) = 2$.

3.8. ***Gauss sums associated to orbits.*** Fix data p, r, q, and n as above, and let $o \in O_{r,n,q}$ be the orbit of $\langle r\rangle$ through $(i, \alpha) \in S_{n,q} = (\mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q^\times$. Let $\mathbb{F} = \mathbb{F}_{r^{|o|}}$,

i.e., $\mathbb{F}$ is the extension of $\mathbb{F}_r$ of degree $|o|$. By formula (3-5) for $|o|$, $\mathbb{F}$ can be interpreted as the smallest extension of $\mathbb{F}_r$ which admits a multiplicative character of order n and contains α. To the orbit o we then associate the Gauss sum

$$G(o) = G_{\mathbb{F}}(\chi_{\mathbb{F},n}^{i}, \psi_\alpha), \tag{3-6}$$

where $\chi_{\mathbb{F},n}$ and ψ_α are the characters on $\mathbb{F}$ defined in Sections 3.2 and 3.3. An elementary computation, as in [Cohen 2007, Lemma 2.5.8], shows that

$$G_{\mathbb{F}}(\chi, \psi_\alpha) = G_{\mathbb{F}}(\chi^p, \psi_{\alpha^{1/p}}),$$

so that $G(o)$ is indeed well defined independently of the choice of element $(i, \alpha) \in o$.

We next record the valuations of Gauss sums associated to orbits for $n = 2$ and 3. These claims follow immediately from the results of Section 3.5.

When $n = 2$, we have $\operatorname{ord}(G(o)) = \frac{1}{2}\nu|o|$ for all orbits $o \in O_{r,2,q}^{\times}$.

When $n = 3$, $p \equiv 1 \pmod 3$, and $o \in O_{r,3,q}^{\times}$, then

$$\operatorname{ord}(G(o)) = \begin{cases} \frac{2}{3}\nu|o| & \text{if } o \text{ contains an element } (1, \alpha), \\ \frac{1}{3}\nu|o| & \text{if } o \text{ contains an element } (-1, \alpha). \end{cases}$$

When $n = 3$ and $p \equiv -1 \pmod 3$, then $\operatorname{ord}(G(o)) = \frac{1}{2}\nu|o|$ for all $o \in O_{r,3,q}^{\times}$.

The following shows that the Gauss sums $G(o)$ "decompose" as roots of unity times powers of Gauss sums of small weight. This will play a key role in our estimation of the archimedean size of $\operatorname{Reg}(E)\,|Ш(E)|$ in Section 11.

Proposition 3.9. *Let $n \geq 1$ be an integer coprime to p, and write*

$$c := \operatorname{ord}^{\times}(p \bmod n)$$

for the order of p modulo n. Then for all $o \in O_{r,n,q}$, one has

$$G(o) = \zeta g^{|o|\nu/c},$$

where ζ is an n-th root of unity, and $g \in \mathbb{Q}(\mu_{np})$ is a Weil integer of size $p^{c/2}$.

Recall that an algebraic number $z \in \overline{\mathbb{Q}}$ is called *a Weil integer of size p^a* (with $a \in \frac{1}{2}\mathbb{Z}_{\geq 0}$) if z is an algebraic integer such that $|z| = p^a$ in any complex embedding $\mathbb{Q}(z) \hookrightarrow \mathbb{C}$. (These numbers are also sometimes called p-Weil integers of weight $2a$.)

Proof. Note that $\mathbb{F}_{p^c}^{\times}$ admits characters of order exactly n. By definition, for any choice of representative $(i, \alpha) \in o$, we have

$$G(o) = G_{\mathbb{F}}(\chi_{\mathbb{F},n}^{i}, \psi_{\mathbb{F},\alpha}),$$

where $\mathbb{F}$ is the extension of $\mathbb{F}_r$ of degree $|o|$, i.e., $|\mathbb{F}| = p^{|o|\nu}$. By construction, c divides $\nu|o|$, so $\mathbb{F}$ is an extension of $\mathbb{F}_{p^c}$. Then the following holds:

$$\begin{aligned} G(o) &= G_{\mathbb{F}}(\chi_{\mathbb{F},n}^{i}, \psi_{\mathbb{F},\alpha}) = \chi_{\mathbb{F},n}^{-i}(\alpha) G_{\mathbb{F}}(\chi_{\mathbb{F},n}^{i}, \psi_{\mathbb{F},1}) && \text{(by (3) in Section 3.4)} \\ &= \chi_{\mathbb{F},n}^{-i}(\alpha) G_{\mathbb{F}_{p^c}}(\chi_{\mathbb{F}_{p^c},n}^{i}, \psi_{\mathbb{F}_{p^c},1})^{|o|\nu/c} && \text{(by the Hasse–Davenport relation).} \end{aligned}$$

We now let $\zeta := \chi_{\mathbb{F},n}^{-i}(\alpha)$ and $g = G_{\mathbb{F}_{p^c}}(\chi_{\mathbb{F}_{p^c},n}, \psi_{\mathbb{F}_{p^c},1})$. Since $\chi_{\mathbb{F},n}$ has order n, ζ is an n-th root of unity. By (1) and (2) in Section 3.4, g is a Weil integer in $\mathbb{Q}(\mu_{np})$ of size $p^{c/2}$. □

3.10. ***Jacobi sums associated to orbits.*** With data p and r as usual, let $\langle r\rangle$ act on $(\mathbb{Z}/6\mathbb{Z})^\times$ by multiplication, and let $N = N_{r,6}$ be the set of orbits of $\langle r\rangle$ on $(\mathbb{Z}/6\mathbb{Z})^\times$. Thus, if $r \equiv 1 \pmod 6$, there are two orbits, both singletons, and if $r \equiv -1 \pmod 6$, there is a unique orbit, $o = \{1, -1\}$. (This is a somewhat trivial situation, but we introduce it for consistency with our treatment of Gauss sums.) Given $o \in N_{r,6}$, write $\mathbb{F} = \mathbb{F}_{r^{|o|}}$ and associate to o the Jacobi sum

$$J(o) := J_{\mathbb{F}}(\chi_{\mathbb{F},2}^{-i}, \chi_{\mathbb{F},3}^{-i}) = J_{\mathbb{F}}(\chi_{\mathbb{F},6}^{-3i}, \chi_{\mathbb{F},6}^{-2i}) \tag{3-7}$$

for any $i \in o$. As a straightforward calculation shows, $J_{\mathbb{F}}(\chi_1^p, \chi_2^p) = J_{\mathbb{F}}(\chi_1, \chi_2)$, so the sum $J(o)$ is well defined independently of the choice of $i \in o$.

We next record the valuations of $J(o)$ for $o \in N_{r,6}$. These claims follow easily from the expression of Jacobi sums in terms of Gauss sums and Stickelberger's theorem (see Sections 3.4 and 3.6). If $p \equiv -1 \pmod 6$, then

$$\operatorname{ord}(J(o)) = \tfrac{1}{2}v|o|$$

for all $o \in N_{r,6}$. On the other hand, if $p \equiv 1 \pmod 6$, then

$$\operatorname{ord}(J(\{1\})) = 0 \quad \text{and} \quad \operatorname{ord}(J(\{-1\})) = v.$$

Finally, we introduce the map $\rho_6 : O_{r,6,q}^\times \to N_{r,6}$ induced by the projection

$$(\mathbb{Z}/6\mathbb{Z})^\times \times \mathbb{F}_q{}^\times \to (\mathbb{Z}/6\mathbb{Z})^\times.$$

This will play a role in our geometric calculation of the L-function in Section 7.

4. Elementary calculation of the L-function

Recall that we have fixed a prime number $p > 3$, a finite field $\mathbb{F}_r$ of characteristic p, a power q of p, and that we have defined $E = E_{q,r}$ as the elliptic curve

$$E : y^2 = x^3 + t^q - t$$

over $K = \mathbb{F}_r(t)$. In this section, we give an elementary calculation of the L-function of E over K. The Hasse–Weil L-function of E is defined as the Euler product

$$L(E, T) = \prod_{\text{good } v} (1 - a_v T^{\deg(v)} + r_v T^{2\deg(v)})^{-1} \prod_{\text{bad } v} (1 - a_v T^{\deg(v)})^{-1},$$

where the products are over places v of K. Here "good v" refers to the places where E has good reduction, "bad v" refers to the places of bad reduction, and for any place v, $\mathbb{F}_v$ is the residue field at v, r_v is its cardinality, and a_v is the integer

such that the number of points on the plane cubic model of E over $\mathbb{F}_v$ is equal to $r_v - a_v + 1$. Note that, since E has additive reduction at all bad places (Section 2.2), the local factors at such places are all 1, so

$$L(E,T) = \prod_{\text{good } v} (1 - a_v T^{\deg(v)} + r_v T^{2\deg(v)})^{-1}. \tag{4-1}$$

One also considers $L(E,s) = L(E,T)$ with $T = r^{-s}$. Since the curve E is nonconstant, it is known (e.g., [Ulmer 2011, Lecture 1, Theorem 9.3]) that $L(E,s)$ is a polynomial in $T = r^{-s}$ and that it satisfies a functional equation relating $L(E,s)$ and $L(E,2-s)$.

Recall from Section 3.7 that $O^{\times}_{r,n,q}$ denotes the set of orbits of $\langle r\rangle$ acting on $(\mathbb{Z}/n\mathbb{Z})^{\times} \times \mathbb{F}_q^{\times}$, that $\pi_n : O^{\times}_{r,6,q} \to O^{\times}_{r,n,q}$ (for $n = 2, 3$) denotes the map induced by the natural projection $(\mathbb{Z}/6\mathbb{Z})^{\times} \to (\mathbb{Z}/n\mathbb{Z})^{\times}$, and that $m_2(o) = |o|/|\pi_2(o)|$. As in Section 3.8, we attach a Gauss sum $G(o)$ to any orbit $o \in O^{\times}_{r,n,q}$.

The main result of this section is the following.

Theorem 4.1. *In the above setting, we have*

$$L(E,s) = \prod_{o \in O^{\times}_{r,6,q}} (1 - G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) r^{-s|o|}).$$

We remark that, as a polynomial in r^{-s}, the L-function has degree $\sum_{o \in O^{\times}_{r,6,q}} |o| = |S^{\times}_{6,r,q}| = 2(q-1)$. This is consistent with what the Grothendieck–Ogg–Shafarevich formula predicts; i.e., that the L-function has degree $\deg(\mathcal{N}_E) - 4$ where $\mathcal{N}_E$ is the conductor of E (recall from Section 2.2 that $\deg \mathcal{N}_E = 2(q+1)$).

The first, elementary, proof of Theorem 4.1 will be given at the end of this section, after proving several lemmas in the next few subsections. In Section 7, we will provide two more conceptual proofs of this statement (see Theorems 7.2 and 7.4, as well as Section 7.5).

Lemma 4.2. *Let $\mathbb{F}$ be a finite field of characteristic p, and let ψ be a nontrivial additive character of $\mathbb{F}$.*

(1) *For any $u \in \mathbb{F}$ and any power q of p, one has*

$$|\{t \in \mathbb{F} : t^q - t = u\}| = \sum_{\alpha \in \mathbb{F} \cap \mathbb{F}_q} \psi(\alpha u).$$

(2) *Denote the nontrivial quadratic character of $\mathbb{F}^{\times}$ by $\lambda = \chi_{\mathbb{F},2}$. Consider the sum*

$$S_{\mathbb{F}}(\lambda, \psi) = \sum_{x,z \in \mathbb{F}} \lambda(x^3 + z)\psi(z). \tag{4-2}$$

Then

$$S_{\mathbb{F}}(\lambda,\psi) = \begin{cases} 0 & \text{if } |\mathbb{F}| \equiv 2 \pmod 3, \\ G_{\mathbb{F}}(\lambda,\psi) \sum_{i \in \{1,2\}} G_{\mathbb{F}}(\chi^i_{\mathbb{F},3}, \psi) & \text{if } |\mathbb{F}| = 1 \pmod 3. \end{cases}$$

Proof. Part (1) is straightforward when $\mathbb{F}$ is an extension of $\mathbb{F}_q$, and the general case is proven in [Griffon 2019, Lemma 4.3]. (The key point is that the kernel and the image of the map $\mathbb{F} \to \mathbb{F}$, $t \mapsto t^q - t$ are orthogonal complements with respect to the $\mathbb{F}_p$-bilinear form $\langle \alpha, \beta \rangle = \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}(\alpha\beta)$.) We now turn to the proof of (2). For any nontrivial additive character ψ on $\mathbb{F}$, consider

$$S_{\mathbb{F}}(\lambda, \psi) = \sum_{x,z \in \mathbb{F}} \lambda(x^3 + z)\psi(z).$$

Let $\mathbf{1}$ denote the trivial multiplicative character of $\mathbb{F}^\times$. It is classical that for any $y \in \mathbb{F}$,

$$|\{x \in \mathbb{F} : y = x^3\}| = \sum_{\theta^3 = \mathbf{1}} \theta(y),$$

where the sum runs over characters on $\mathbb{F}^\times$ whose order divides 3 (see [Cohen 2007, Lemma 2.5.21]). This allows us to rewrite the sum $S_{\mathbb{F}}(\lambda, \psi)$ as

$$\begin{aligned}
S_{\mathbb{F}}(\lambda, \psi) &= \sum_{y \in \mathbb{F}} \sum_{z \in \mathbb{F}} \Bigg(\sum_{\theta^3 = \mathbf{1}} \theta(y) \Bigg) \lambda(y + z)\psi(z) \\
&= \sum_{\theta^3 = \mathbf{1}} \sum_{y \in \mathbb{F}} \theta(y) \Bigg(\sum_{z \in \mathbb{F}} \lambda(y + z)\psi(z) \Bigg) \\
&= \sum_{\theta^3 = \mathbf{1}} \sum_{y \in \mathbb{F}} \theta(y) \Bigg(\sum_{u \in \mathbb{F}} \lambda(u)\psi(u - y) \Bigg) \qquad \text{(by setting } u = z + y\text{)} \\
&= \Bigg(\sum_{\theta^3 = \mathbf{1}} \sum_{y \in \mathbb{F}} \theta(y)\psi(-y) \Bigg) \Bigg(\sum_{u \in \mathbb{F}} \lambda(u)\psi(u) \Bigg) \\
&= \Bigg(\sum_{u \in \mathbb{F}} \lambda(u)\psi(u) \Bigg) \Bigg(\sum_{\theta^3 = \mathbf{1}} \theta(-1) \sum_{v \in \mathbb{F}} \theta(v)\psi(v) \Bigg) \quad \text{(by setting } v = -y\text{)}.
\end{aligned}$$

The first sum equals $-G_{\mathbb{F}}(\lambda, \psi)$ and, for a character θ such that $\theta^3 = \mathbf{1}$, the sum over $v \in \mathbb{F}$ equals $-G_{\mathbb{F}}(\theta, \psi)$. Moreover, $\theta(-1) = 1$ for all θ such that $\theta^3 = \mathbf{1}$, and $G_{\mathbb{F}}(\mathbf{1}, \psi) = 0$, so we have

$$S_{\mathbb{F}}(\lambda, \psi) = G_{\mathbb{F}}(\lambda, \psi) \sum_{\substack{\theta^3 = \mathbf{1} \\ \theta \neq \mathbf{1}}} G_{\mathbb{F}}(\theta, \psi).$$

To conclude the proof, it remains to note that if $|\mathbb{F}| \equiv 2 \pmod 3$, then there are no nontrivial characters of order 3, so that the right-hand side vanishes, while if $|\mathbb{F}| \equiv 1 \pmod 3$, the two nontrivial characters of order 3 are $\chi^i_{\mathbb{F},3}$, $i \in \{1, 2\}$. □

To ease notation, for the rest of this section we write $\mathbb{F}_n$ for $\mathbb{F}_{r^n}$, i.e., $\mathbb{F}_n$ is the extension of $\mathbb{F}_r$ of degree n. Fix a nontrivial additive character $\psi_{\mathbb{F}_n}$ of $\mathbb{F}_n$ and for any $\alpha \in \mathbb{F}_n$, let $\psi_{\mathbb{F}_n,\alpha}$ denote the additive character on $\mathbb{F}_n$ defined by $z \in \mathbb{F}_n \mapsto \psi_{\mathbb{F}_n}(\alpha z)$.

Lemma 4.3. *As Taylor series in T,*

$$-\log L(E,T) = \sum_{n\geq 1} \frac{T^n}{n} \sum_{\alpha \in \mathbb{F}_n \cap \mathbb{F}_q} S_{\mathbb{F}_n}(\lambda_{\mathbb{F}_n}, \psi_{\mathbb{F}_n,\alpha})$$

where $\lambda_{\mathbb{F}_n} = \chi_{\mathbb{F}_n,2}$ is the nontrivial quadratic character of $\mathbb{F}_n^\times$ and $S_{\mathbb{F}_n}(\lambda_{\mathbb{F}_n}, \psi_{\mathbb{F}_n,\alpha})$ is the sum defined by (4-2).

Proof. In the definition of $L(E,T)$, write the Euler factor at a good place v as

$$(1 - a_v T^{\deg(v)} + r_v T^{2\deg(v)}) = (1 - \alpha_v T^{\deg(v)})(1 - \beta_v T^{\deg(v)}).$$

Taking the logarithm of the Euler product (4-1) and reordering terms yields that

$$\log L(E,T) = \sum_{n\geq 1} \frac{T^n}{n} \sum_{\substack{\text{good } v \\ \deg(v)\mid n}} \deg(v)(\alpha_v^{n/\deg(v)} + \beta_v^{n/\deg(v)}).$$

To obtain this expression, we have used the standard identity between Taylor series:

$$\log(1-\alpha T) = -\sum_{n\geq 1} \frac{(\alpha T)^n}{n}. \tag{4-3}$$

If $t \in \mathbb{F}_n$, define $A_E(t,n)$ to be the integer such that $r^n + 1 - A_E(t,n)$ is the number of $\mathbb{F}_n$-rational points on the reduction of E at t. That

$$\alpha_v^{n/\deg(v)} + \beta_v^{n/\deg(v)} = A_E(t,n)$$

for any $t \in \mathbb{F}_n$ lying over v follows from [Silverman 2009, V.2.3.1]. Thus,

$$L(E,T) = \sum_{n\geq 1} \frac{T^n}{n} \sum_{\substack{\text{good } t \\ t\in\mathbb{F}_n}} A_E(t,n).$$

Denote the nontrivial quadratic character of $\mathbb{F}_n^\times$ by $\lambda_{\mathbb{F}_n}$. Then [Silverman 2009, V.1.3] asserts that

$$A_E(t,n) = -\sum_{x\in\mathbb{F}_n} \lambda_{\mathbb{F}_n}(x^3 + t^q - t).$$

Note that if $t \in \mathbb{F}_q$, then $t^q - t = 0$, and the sum on the right-hand side vanishes, so we may drop the restriction "good t" in the last expression for $L(E,T)$, i.e.,

$$-\log L(E,T) = \sum_{n\geq 1} \frac{T^n}{n} \sum_{t\in\mathbb{F}_n} \sum_{x\in\mathbb{F}_n} \lambda_{\mathbb{F}_n}(x^3 + t^q - t).$$

Now applying Lemma 4.2 part (1), we get that

$$\sum_{t\in\mathbb{F}_n}\sum_{x\in\mathbb{F}_n}\lambda_{\mathbb{F}_n}(x^3+t^q-t)=\sum_{x\in\mathbb{F}_n}\sum_{u\in\mathbb{F}_n}\sum_{\alpha\in\mathbb{F}_n\cap\mathbb{F}_q}\psi(\alpha u)\lambda_{\mathbb{F}_n}(x^3+u)$$
$$=\sum_{\alpha\in\mathbb{F}_n\cap\mathbb{F}_q}S_{\mathbb{F}_n}(\lambda_{\mathbb{F}_n},\psi_{\mathbb{F}_n,\alpha}).$$

Therefore, we have proved, as desired, that

$$-\log L(E,T)=\sum_{n\geq 1}\frac{T^n}{n}\sum_{\alpha\in\mathbb{F}_n\cap\mathbb{F}_q}S_{\mathbb{F}_n}(\lambda_{\mathbb{F}_n},\psi_{\mathbb{F}_n,\alpha}).$$ □

Lemma 4.4. *As Taylor series in T,*

$$-\log\prod_{o\in O_{r,6,q}^{\times}}(1-G(\pi_2(o))^{m_2(o)}G(\pi_3(o))T^{|o|})$$
$$=\sum_{\substack{n\geq 1\\ r^n\equiv 1\ (\mathrm{mod}\ 6)}}\frac{T^n}{n}\sum_{\alpha\in\mathbb{F}_n\cap\mathbb{F}_q}\sum_{i\in\{1,2\}}G_{\mathbb{F}_n}(\chi_{\mathbb{F}_n,2},\psi_{\mathbb{F}_n,\alpha})G_{\mathbb{F}_n}(\chi_{\mathbb{F}_n,3}^{i},\psi_{\mathbb{F}_n,\alpha}).$$

Proof. To lighten the notation, we write $\omega(o):=G(\pi_2(o))^{m_2(o)}G(\pi_3(o))$ for any $o\in O_{r,6,q}^{\times}$. By identity (4-3), we have

$$-\log\prod_{o\in O_{r,6,q}^{\times}}(1-\omega(o)T^{|o|})=\sum_{n\geq 1}\frac{T^n}{n}\sum_{\substack{o\in O_{r,6,q}^{\times}\\ |o|\text{ divides }n}}|o|\omega(o)^{n/|o|}.$$

Write $\mathbb{F}_o$ for $\mathbb{F}_{r^{|o|}}$, the extension of $\mathbb{F}_r$ of degree $|o|$. Pick a representative $(i,\alpha)\in o$. By definition, we have $G(\pi_3(o))=G_{\mathbb{F}_o}(\chi_{\mathbb{F}_o,3}^{i},\psi_{\mathbb{F}_o,\alpha})$ and the Hasse–Davenport relation (Section 3.4) yields that

$$G(\pi_3(o))^{n/|o|}=G_{\mathbb{F}_n}(\chi_{\mathbb{F}_n,3}^{i},\psi_{\mathbb{F}_n,\alpha}).$$

Similarly, using the definition and the Hasse–Davenport relation, we have

$$G(\pi_2(o))^{m_2(o)n/|o|}=G_{\mathbb{F}_n}(\chi_{\mathbb{F}_n,2},\psi_{\mathbb{F}_n,\alpha}).$$

Note that $|o|$ divides n if and only if $r^n\equiv 1\ (\mathrm{mod}\ 6)$ and $\alpha\in\mathbb{F}_n$. Thus,

$$-\log\prod_{o\in O_{r,6,q}^{\times}}(1-\omega(o)T^{|o|})$$
$$=\sum_{\substack{n\geq 1\\ r^n\equiv 1\ (\mathrm{mod}\ 6)}}\frac{T^n}{n}\sum_{\alpha\in\mathbb{F}_n\cap\mathbb{F}_q}\sum_{i\in\{1,2\}}G_{\mathbb{F}_n}(\chi_{\mathbb{F}_n,2},\psi_{\mathbb{F}_n,\alpha})G_{\mathbb{F}_n}(\chi_{\mathbb{F}_n,3}^{i},\psi_{\mathbb{F}_n,\alpha}).$$

This completes the proof of the lemma. □

Proof of Theorem 4.1. According to Lemma 4.3,

$$-\log L(E,T)=\sum_{n\geq 1}\frac{T^n}{n}\sum_{\alpha\in\mathbb{F}_n\cap\mathbb{F}_q}S_{\mathbb{F}_n}(\lambda_{\mathbb{F}_n},\psi_{\mathbb{F}_n,\alpha}),$$

and part (2) of Lemma 4.2 says that

$$S_{\mathbb{F}_n}(\lambda_{\mathbb{F}_n},\psi_{\mathbb{F}_n,\alpha})=\begin{cases}0 & \text{if } |\mathbb{F}_n|=r^n\equiv 2 \pmod 3,\\ \sum_{i\in\{1,2\}}G_{\mathbb{F}_n}(\chi_{\mathbb{F}_n,2},\psi_{\mathbb{F}_n,\alpha})G_{\mathbb{F}_n}(\chi^i_{\mathbb{F}_n,3},\psi_{\mathbb{F}_n,\alpha}) & \text{if } |\mathbb{F}_n|=r^n\equiv 1 \pmod 3.\end{cases}$$

Noting that $r^n\equiv 1 \pmod 3$ if and only if $r^n\equiv 1 \pmod 6$, we have

$$-\log L(E,T)=\sum_{\substack{n\geq 1\\ r^n\equiv 1 \pmod 6}}\frac{T^n}{n}\sum_{\alpha\in\mathbb{F}_n\cap\mathbb{F}_q}\sum_{i\in\{1,2\}}G_{\mathbb{F}_n}(\chi_{\mathbb{F}_n,2},\psi_{\mathbb{F}_n,\alpha})G_{\mathbb{F}_n}(\chi^i_{\mathbb{F}_n,3},\psi_{\mathbb{F}_n,\alpha}).$$

By Lemma 4.4, the expression on the right-hand side is

$$-\log\prod_{o\in O^\times_{r,6,q}}(1-G(\pi_2(o))^{m_2(o)}G(\pi_3(o))T^{|o|}).$$ □

5. Auxiliary curves

In this section, we record some well-known facts about the geometry of certain curves to be used in the sequel.

5.1. ***Cohomology.*** Throughout this section and the next, we denote by $H^n(-)$ any rational Weil cohomology theory (with coefficients in an algebraically closed field) for varieties over $\mathbb{F}_r$, for example ℓ-adic cohomology $H^n(-\times_{\mathbb{F}_r}\overline{\mathbb{F}}_r,\overline{\mathbb{Q}}_\ell)$ or crystalline cohomology $H^n(-/W)\otimes_{W(\mathbb{F}_r)}\overline{\mathbb{Q}}_p$. (See, for example, [Kleiman 1968].) Among other things, these groups admit a functorial action of the geometric Frobenius Fr_r.

Here is a well-known lemma about characteristic polynomials in induced representations. See [Gordon 1979, Lemma 1.1] or [Ulmer 2007, Lemma 2.2] for a proof.

Lemma 5.1.1. *Let V be a finite-dimensional vector space with subspaces W_i indexed by $i\in\mathbb{Z}/m\mathbb{Z}$ such that $V=\oplus_{i\in\mathbb{Z}/m\mathbb{Z}}W_i$. Let $\phi:V\to V$ be a linear transformation such that $\phi(W_i)\subset W_{i+1}$ for all $i\in\mathbb{Z}/m\mathbb{Z}$. Then*

$$\det(1-\phi T|V)=\det(1-\phi^m T^m|W_0).$$

5.2. ***An elliptic curve.*** We have already introduced the elliptic curve

$$E_0: w^2=z^3+1$$

over $\mathbb{F}_r$. The displayed equation defines a smooth affine curve, and there is a unique point at infinity on E_0 which we denote by $O\in E_0$.

The curve E_0 carries an action of μ_6 via $\zeta(z, w) = (\zeta^2 z, \zeta^3 w)$. The character group of μ_6 is $\mathbb{Z}/6\mathbb{Z}$. It is well known that $H^1(E_0)$ has dimension 2, and that under the action of μ_6, it decomposes as the direct sum of two lines corresponding to the subspaces where $\zeta \in \mu_6$ acts by ζ and ζ^{-1} (i.e., corresponding to the characters indexed by $\pm 1 \in \mathbb{Z}/6\mathbb{Z}$):

$$H^1(E_0) = H^1(E_0)^{(1)} \oplus H^1(E_0)^{(-1)}. \tag{5-1}$$

Also, powers of Fr_r act on the two subspaces as $\langle r \rangle$ acts on $\{\pm 1\} = (\mathbb{Z}/6\mathbb{Z})^\times \subset \mathbb{Z}/6\mathbb{Z}$.

More explicitly, if $r \equiv 1 \pmod 6$, so that $\langle r \rangle$ has two orbits on $(\mathbb{Z}/6\mathbb{Z})^\times$, then Fr_r preserves the two subspaces, and the corresponding eigenvalues are

$$J(\{1\}) = J_{\mathbb{F}_r}(\chi_{\mathbb{F}_r,6}^{-3}, \chi_{\mathbb{F}_r,6}^{-2}) \quad \text{and} \quad J(\{-1\}) = J_{\mathbb{F}_r}(\chi_{\mathbb{F}_r,6}^{3}, \chi_{\mathbb{F}_r,6}^{2}),$$

where the Jacobi sums are as defined in (3-7).

If $r \equiv 5 \pmod 6$, so that $\langle r \rangle$ has a unique orbit on $(\mathbb{Z}/6\mathbb{Z})^\times$, then Fr_r exchanges the two subspaces, and the eigenvalues of Fr_r^2 are both

$$J(\{1, -1\}) = J_{\mathbb{F}_{r^2}}(\chi_{\mathbb{F}_{r^2},6}^{-3}, \chi_{\mathbb{F}_{r^2},6}^{-2}) = J_{\mathbb{F}_{r^2}}(\chi_{\mathbb{F}_{r^2},6}^{3}, \chi_{\mathbb{F}_{r^2},6}^{2}).$$

Finally, applying Lemma 5.1.1, we find that

$$\det(1 - T\,\mathrm{Fr}_r \mid H^1(E_0)) = \prod_{o \in N_{r,6}} (1 - J(o)T^{|o|}).$$

We remark that this result and the values of $\mathrm{ord}(J(o))$ recorded in Section 3.10 are compatible with the well-known fact that E_0 is ordinary if $p \equiv 1 \pmod 6$ and supersingular if $p \equiv -1 \pmod 6$.

5.3. ***Artin–Schreier curves.*** For a positive integer n relatively prime to p, let $C_{n,q}$ be the smooth projective curve over $\mathbb{F}_r$ defined by the equation

$$C_{n,q} : u^n = t^q - t.$$

(We also use the equation $w^n = z^q - z$ when more than one instance of $C_{n,q}$ is under discussion. Only $n = 2, 3, 6$ will be used later in this paper.) The displayed equation defines a smooth affine curve, and there is a unique point at infinity on $C_{n,q}$ which we denote by $\infty \in C_{n,q}$.

The curve $C_{n,q}$ carries natural actions of μ_n via $\zeta(t, u) = (t, \zeta u)$, and of $\mathbb{F}_q$ via $\alpha(t, u) = (t + \alpha, u)$. (In fact, it carries an action of the larger group $\mathbb{F}_q \rtimes \mu_{n(q-1)}$, where $\zeta \in \mu_{n(q-1)}$ acts via $\zeta(t, u) = (\zeta^n t, \zeta u)$. In this section and the next, we will only need the action of the subgroup $\mu_n \times \mathbb{F}_q$. The action of the larger group will be useful in Section 10.) The character group of $\mu_n \times \mathbb{F}_q$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{F}_q$.

The cohomology group $H^1(C_{n,q})$ has dimension $(q-1)(n-1)$, and under the action of $\mu_n \times \mathbb{F}_q$, it decomposes into lines where μ_n and $\mathbb{F}_q$ act through their

nontrivial characters. (This is proven for $q = p$ in [Katz 1981, Corollary 2.2], and the arguments there generalize straightforwardly to the case $q = p^f$.) In particular, the subspace of $H^1(C_{n,q})$ where μ_n acts via a given nontrivial character has dimension $q-1$, and the subspace where $\mathbb{F}_q$ acts via a given nontrivial character has dimension $n-1$.

Recall from Section 3.7 that $S = S_{n,q} := (\mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q^\times$ and that $O_{r,n,q}$ denotes the set of orbits of the action of $\langle r \rangle$ on S. We index the characters of $\mu_n \times \mathbb{F}_q$ (with values in the coefficient field of our cohomology theory) that are nontrivial on both factors by S. The subspace of $H^1(C_{n,q})$ where $\mu_n \times \mathbb{F}_q$ acts via the character indexed by (i,α) will be denoted by $H^1(C_{n,q})^{(i,\alpha)}$. We thus obtain a direct sum decomposition of $H^1(C_{n,q})$ into lines as follows:

$$H^1(C_{n,q}) = \bigoplus_{(i,\alpha)\in S_{n,q}} H^1(C_{n,q})^{(i,\alpha)}. \tag{5-2}$$

Katz [1981, Corollary 2.2] further gave a description of the action of Frobenius on the cohomology $H^1(C_{n,q})$: the Frobenius Fr_r sends the subspace indexed by (i,α) to the subspace indexed by $(ri, \alpha^{1/r})$. If $o \in O_{r,n,q}$ is the orbit through (i,α), then the $|o|$-th iterate $\mathrm{Fr}_r^{|o|}$ stabilizes the subspace $H^1(C_{n,q})^{(i,\alpha)}$ (which is a line) and the eigenvalue of $\mathrm{Fr}_r^{|o|}$ on $H^1(C_{n,q})^{(i,\alpha)}$ is the Gauss sum

$$G(o) := G_{\mathbb{F}}(\chi_{\mathbb{F},n}^i, \psi_\alpha),$$

where $\mathbb{F} = \mathbb{F}_{r^{|o|}}$. (Again, Katz treated the case $q = p$, but the generalization is straightforward.)

Applying Lemma 5.1.1, we have

$$\det(1 - T\,\mathrm{Fr}_r \mid H^1(C_{n,q})) = \prod_{o\in O_{r,n,q}} (1 - G(o)T^{|o|}).$$

We remark that this result together with the values of $\mathrm{ord}(G(o))$ recorded in Section 3.8 are compatible with the well-known fact that $C_{2,q}$ is supersingular, and they show that $C_{3,q}$ is supersingular when $p \equiv -1 \pmod 6$ and neither supersingular nor ordinary if $p \equiv 1 \pmod 6$. (In this last case, the slopes are $\frac{1}{3}$ and $\frac{2}{3}$, both with multiplicity $q-1$, cf. [Pries and Ulmer 2016, §8.3].)

5.4. ***Fermat curves.*** For a positive integer d prime to p, let F_d be the Fermat curve of degree d over $\mathbb{F}_r$. This is by definition the smooth, projective curve in $\mathbb{P}^2$ given by the homogeneous equation

$$F_d : X_0^d + X_1^d + X_2^d = 0.$$

The genus of F_d is $(d-1)(d-2)/2$, so $H^1(F_d)$ has dimension $(d-1)(d-2)$. The curve F_d carries an action of $(\mu_d)^3/\mu_d$ where the three copies of μ_d in the numerator

act by multiplication on the three coordinates, and the diagonally embedded μ_d acts trivially. Under the action of this group, $H^1(F_d)$ decomposes into lines on which each of the factors μ_d acts nontrivially and the diagonally embedded μ_d acts trivially. There are $(d-1)(d-2)$ such characters. The action of Frobenius on $H^1(F_d)$ is given by Jacobi sums. Since we will not need the cohomology of F_d later in the paper, we omit the details.

6. Domination by a product of curves

In this section we define the Weierstrass and Néron models $\mathcal{W}$ and $\mathcal{E}$ of E and relate them to products of curves. Throughout, unless explicitly indicated otherwise by the notation, products of varieties are over $\mathbb{F}_r$ (i.e., $\times$ means $\times_{\mathbb{F}_r}$).

Our ultimate aim is to compute the relevant part of the cohomology of a model $\mathcal{E}$ of E by showing that $\mathcal{E}$ is birational to the quotient of a product of curves by a finite group.

6.1. ***Models.*** Let $\mathcal{W} \to \mathbb{P}^1_{\mathbb{F}_r}$ be the Weierstrass model of E over K, i.e., the surface fibered over $\mathbb{P}^1$ whose fibers are the plane cubic reductions of E at the places of K. More precisely, let

$$d = \deg(\omega_E) = \lceil q/6 \rceil = \begin{cases} \frac{q+5}{6} & \text{if } q \equiv 1 \pmod 6, \\ \frac{q+1}{6} & \text{if } q \equiv 5 \pmod 6, \end{cases}$$

and define $\mathcal{W}$ by gluing the surfaces

$$y^2 z = x^3 + (t^q - t) z^3 \subset \mathbb{P}^2_{x,y,z} \times \mathbb{A}^1_t$$

and

$$y'^2 z' = x'^3 + (t'^{6d-q} - t'^{6d-1}) z'^3 \subset \mathbb{P}^2_{x',y',z'} \times \mathbb{A}^1_{t'}$$

via the map $([x', y', z'], t') = ([x/t^{2d}, y/t^{3d}, z], 1/t)$. Then $\mathcal{W}$ is an irreducible, normal, projective surface, and projection onto the t and t' coordinates defines a morphism $\mathcal{W} \to \mathbb{P}^1$ whose generic fiber is E.

When $q \equiv 5 \pmod 6$, $\mathcal{W}$ is a regular surface (i.e., is smooth over $\mathbb{F}_r$), and we define $\mathcal{E} = \mathcal{W}$. When $q \equiv 1 \pmod 6$, $\mathcal{W}$ has a singularity at the point $([x', y', z'], t') = ([0, 0, 1], 0)$ and is regular elsewhere. In this case, we define $\mathcal{E}$ as the minimal desingularization of $\mathcal{W}$. (The desingularization introduces eight new components.)

The reduction types of $\mathcal{E}$ at closed points of $\mathbb{P}^1$ (i.e., at places of K) were recorded in Section 2.2.

6.2. ***Sextic twists.*** We saw above that E becomes isomorphic to a constant curve after extension of K to $L = K[u]/(u^6 = t^q - t)$. Geometrically, this means that $\mathcal{E}$

is birational to a quotient of $E_0 \times C_{6,q}$. In this subsection, we make this statement more explicit and deduce a cohomological consequence.

Let μ_6 act on $E_0 \times C_{6,q}$ "antidiagonally," i.e., via

$$\zeta(z, w, t, u) = (\zeta^2 z, \zeta^3 w, t, \zeta^{-1} u).$$

Define a rational map $E_0 \times C_{6,q} \dashrightarrow \mathcal{W}$ by

$$(z, w, t, u) \mapsto ([x, y, z], t) = ([zu^2, wu^3, 1], t).$$

It is obvious that this map factors through the quotient $\mathcal{S} := (E_0 \times C_{6,q})/\mu_6$ and so we have a commutative diagram

$$\begin{array}{ccc} \mathcal{S} & \dashrightarrow & \mathcal{W} \\ \downarrow & & \downarrow \\ C_{6,q}/\mu_6 & = & \mathbb{P}^1_t \end{array}$$

where the bottom horizontal arrow is the canonical isomorphism $C_{6,q}/\mu_6 \cong \mathbb{P}^1_t$ and the left vertical arrow is induced by the projection onto $C_{6,q}$.

Now let $\widetilde{\mathcal{S}} \to \mathcal{S}$ be a blow-up so that $\widetilde{\mathcal{S}}$ is smooth and $\mathcal{S} \dashrightarrow \mathcal{W}$ induces a morphism $\widetilde{\mathcal{S}} \to \mathcal{E}$. (This can be made completely explicit in terms of the fixed points of the action of μ_6 and the formula for the rational map $E_0 \times C_{6,q} \dashrightarrow \mathcal{W}$, but the details will not be important for our analysis.) The diagram above then extends to

$$\begin{array}{ccc} \widetilde{\mathcal{S}} & \longrightarrow & \mathcal{E} \\ \downarrow & & \downarrow \\ \mathcal{S} & \dashrightarrow & \mathcal{W} \\ \downarrow & & \downarrow \\ C_{6,q}/\mu_6 & = & \mathbb{P}^1_t \end{array}$$

The following encapsulates all we need to know about the geometry of $\widetilde{\mathcal{S}} \to \mathcal{E}$.

Proposition 6.2.1. (1) *The strict transform of* $(O \times C_{6,q})/\mu_6$ *in* $\widetilde{\mathcal{S}}$ *maps to the zero section of* $\mathcal{E}$.

(2) *The strict transform of* $(E_0 \times \infty)/\mu_6$ *in* $\widetilde{\mathcal{S}}$ *maps to a fiber of* $\mathcal{E} \to \mathbb{P}^1$.

(3) *Every component of the exceptional divisor of* $\widetilde{\mathcal{S}} \to \mathcal{S}$ *maps into a fiber of* $\mathcal{E} \to \mathbb{P}^1$.

Proof. The first two points are obvious from the formula defining $E_0 \times C_{6,q} \dashrightarrow \mathcal{W}$. The third point follows by examining the outer rectangle of the last displayed diagram. Indeed, if D is a component of the exceptional divisor of $\widetilde{\mathcal{S}} \to \mathcal{S}$, then D lies over a single point of $C_{6,q}/\mu_6 \cong \mathbb{P}^1_t$ and thus maps to a fiber of $\mathcal{E} \to \mathbb{P}^1_t$. □

Let $T \subset H^2(\mathcal{E})$ be the subspace spanned by the classes of the zero section and components of fibers of $\mathcal{E} \to \mathbb{P}^1$. This is the subspace Shioda [1992] calls the "trivial lattice".

Corollary 6.2.2. *There is a canonical isomorphism*

$$H^2(\mathcal{E})/T \cong (H^1(E_0) \otimes H^1(C_{6,q}))^{\mu_6}.$$

Here the exponent μ_6 indicates the subspace invariant under the antidiagonal action of μ_6.

Proof. The dominant morphism $\widetilde{\mathcal{S}} \to \mathcal{E}$ induces a surjection $H^2(\widetilde{\mathcal{S}}) \to H^2(\mathcal{E})$. Using the Künneth formula, taking invariants, and using the blow-up formula, we obtain a canonical isomorphism

$$\begin{aligned} H^2(\widetilde{\mathcal{S}}) &\cong H^2(\mathcal{S}) \oplus B \cong H^2(E_0 \times C_{6,q}/\mu_6) \oplus B \cong H^2(E_0 \times C_{6,q})^{\mu_6} \oplus B \\ &\cong \big(H^1(E_0) \otimes H^1(C_{6,q})\big)^{\mu_6} \oplus \big(H^0(E_0) \otimes H^2(C_{6,q})\big) \oplus \big(H^2(E_0) \otimes H^0(C_{6,q})\big) \oplus B \end{aligned}$$

where B denotes the subspace spanned by the classes of components of the exceptional divisor of $\widetilde{\mathcal{S}} \to \mathcal{S}$.

The proposition shows that $H^0(E_0) \otimes H^2(C_{6,q})$, $H^2(E_0) \otimes H^0(C_{6,q})$, and B all map to T. Thus we have a well-defined and canonical surjection

$$(H^1(E_0) \otimes H^1(C_{6,q}))^{\mu_6} \to H^2(\mathcal{E})/T.$$

To finish, we compare dimensions. We recalled in Section 5 that μ_6 acts on $H^1(E_0)$ through the characters $\zeta \mapsto \zeta^{\pm 1}$, each with multiplicity one (see (5-1)). Similarly, μ_6 acts on $H^1(C_{6,q})$ through characters $\zeta \mapsto \zeta^i$ with $i \not\equiv 0 \pmod 6$, each with multiplicity $q-1$ (see (5-2)). Thus

$$\dim(H^1(E_0) \otimes H^1(C_{6,q}))^{\mu_6} = 2(q-1).$$

On the other hand, the Grothendieck–Ogg–Shafarevich formula says that the quotient $H^2(\mathcal{E})/T$ has dimension $\deg(\mathcal{N}_E) - 4$ where $\mathcal{N}_E$ denotes the conductor of E. We noted above that $\deg(\mathcal{N}_E) = 2(q+1)$, so $H^2(\mathcal{E})/T$ has dimension $2(q-1)$. Therefore the surjection

$$(H^1(E_0) \otimes H^1(C_{6,q}))^{\mu_6} \to H^2(\mathcal{E})/T$$

is in fact a bijection. □

6.3. ***Artin–Schreier quotients.*** In this subsection, we show that $\mathcal{E}$ is birational to a quotient of a product of Artin–Schreier curves, in the style of [Pries and Ulmer 2016]. Let

$$\mathcal{C} = C_{2,q} : w_1^2 = z_1^q - z_1 \quad \text{and} \quad \mathcal{D} = C_{3,q} : w_2^3 = z_2^q - z_2.$$

Write $\infty_{\mathcal{C}}$ and $\infty_{\mathcal{D}}$ for the points at infinity on $\mathcal{C}$ and $\mathcal{D}$, respectively. Let $\mathbb{F}_q$ act on $\mathcal{C} \times \mathcal{D}$ "diagonally," i.e., via $\alpha(z_1, w_1, z_2, w_2) = (z_1 + \alpha, w_1, z_2 + \alpha, w_2)$. It is easily seen that the sole fixed point of this action is $(\infty_{\mathcal{C}}, \infty_{\mathcal{D}})$.

Define a rational map $\mathcal{C} \times \mathcal{D} \dashrightarrow \mathbb{P}^1_t$ by $(z_1, w_1, z_2, w_2) \mapsto t = z_1 - z_2$, and a rational map $\mathcal{C} \times \mathcal{D} \dashrightarrow \mathcal{W}$ by

$$(z_1, w_1, z_2, w_2) \mapsto ([x, y, z], t) = ([w_2, w_1, 1], z_1 - z_2).$$

Both of these maps are morphisms away from $(\infty_{\mathcal{C}}, \infty_{\mathcal{D}})$, and they clearly factor through the quotient $(\mathcal{C} \times \mathcal{D})/\mathbb{F}_q$.

Proposition 6.3.1. *There is a proper birational morphism $\mathcal{S}' \to \mathcal{C} \times \mathcal{D}$ resolving the indeterminacy of $\mathcal{C} \times \mathcal{D} \dashrightarrow \mathcal{W}$ such that the components of the exceptional divisor of $\mathcal{S}' \to \mathcal{C} \times \mathcal{D}$ map either to the fiber of $\mathcal{W}$ over $t = \infty$ or to the zero section of $\mathcal{W}$.*

Proof. The proof of [Pries and Ulmer 2016, Proposition 3.1.5] gives an explicit recipe for a morphism $\mathcal{S}' \to \mathcal{C} \times \mathcal{D}$ resolving the indeterminacy of $\mathcal{C} \times \mathcal{D} \dashrightarrow \mathbb{P}^1_t$. It is a sequence of four blow-ups of closed points. Straightforward calculation, which we omit, shows that the induced map $\mathcal{S}' \to \mathcal{C} \times \mathcal{D} \dashrightarrow \mathcal{W}$ is in fact a morphism, and that it behaves as stated in the proposition on the components of the exceptional divisor. Indeed, the first three blow-ups map to the fiber over $t = \infty$ and the last maps to the zero section. □

The diagonal action of $\mathbb{F}_q$ on $\mathcal{C} \times \mathcal{D}$ lifts uniquely to $\mathcal{S}'$ and fixes the exceptional divisor pointwise. It is clear that the morphism $\mathcal{S}' \to \mathcal{W}$ factors through the quotient $\mathcal{S}'/\mathbb{F}_q$, so we have the following commutative diagram:

$$\begin{array}{ccc} \mathcal{S}'/\mathbb{F}_q & \longrightarrow & \mathcal{W} \\ \downarrow & & \downarrow \\ \mathbb{P}^1_t & = & \mathbb{P}^1_t \end{array}$$

Now let $\widetilde{\mathcal{S}} \to \mathcal{S}'/\mathbb{F}_q$ be a proper birational morphism so that $\widetilde{\mathcal{S}}$ is a smooth projective surface and the induced rational map $\widetilde{\mathcal{S}} \dashrightarrow \mathcal{E}$ is a morphism. The diagram above then extends to

$$\begin{array}{ccc} \widetilde{\mathcal{S}} & \longrightarrow & \mathcal{E} \\ \downarrow & & \downarrow \\ \mathcal{S}'/\mathbb{F}_q & \longrightarrow & \mathcal{W} \\ \downarrow & & \downarrow \\ \mathbb{P}^1_t & = & \mathbb{P}^1_t \end{array}$$

The following summarizes the relevant aspects of the geometry of this picture.

Proposition 6.3.2. (1) *The strict transforms of $\infty_{\mathcal{C}} \times \mathcal{D}$ and $\mathcal{C} \times \infty_{\mathcal{D}}$ in $\widetilde{\mathcal{S}}$ map to the fiber of $\mathcal{E} \to \mathbb{P}^1$ over $t = \infty$.*

(2) *The strict transforms in $\widetilde{\mathcal{S}}$ of the images in $\mathcal{S}'/\mathbb{F}_q$ of the components of the exceptional fiber of $\mathcal{S}' \to \mathcal{C} \times \mathcal{D}$ map to the fiber of $\mathcal{E} \to \mathbb{P}^1$ over $t = \infty$ or to the zero section of $\mathcal{E}$.*

(3) *Every component of the exceptional divisor of $\widetilde{\mathcal{S}} \to \mathcal{S}'/\mathbb{F}_q$ maps to a fiber of $\mathcal{E} \to \mathbb{P}^1$.*

Proof. The first point is obvious from the formula defining $\mathcal{C} \times \mathcal{D} \dashrightarrow \mathcal{W}$. The second point follows from the previous proposition. The third point follows by examining the last displayed diagram. Indeed, if D is a component of the exceptional divisor of $\widetilde{\mathcal{S}} \to \mathcal{S}/\mathbb{F}_q$, then D lies over a single point of $\mathbb{P}^1_t$ and so maps to a fiber of $\mathcal{E} \to \mathbb{P}^1_t$. □

Corollary 6.3.3. *Let $T \subset H^2(\mathcal{E})$ be the trivial lattice, i.e., the subspace spanned by the classes of the zero section and components of fibers of $\mathcal{E} \to \mathbb{P}^1$. There is a canonical isomorphism*

$$H^2(\mathcal{E})/T \cong (H^1(\mathcal{C}) \otimes H^1(\mathcal{D}))^{\mathbb{F}_q}.$$

The exponent $\mathbb{F}_q$ indicates the subspace invariant under the diagonal action of $\mathbb{F}_q$.

Proof. The proof is completely parallel to that of Corollary 6.2.2, so we just sketch the argument. The dominant morphism $\widetilde{\mathcal{S}} \to \mathcal{E}$ induces a surjection $H^2(\widetilde{\mathcal{S}}) \to H^2(\mathcal{E})$. Using the Künneth formula, taking invariants, using the blow-up formula, and applying the proposition, we obtain a canonical surjection

$$(H^1(\mathcal{C}) \otimes H^1(\mathcal{D}))^{\mathbb{F}_q} \to H^2(\mathcal{E})/T.$$

We conclude by using Section 5 and the proof of Corollary 6.2.2 to check that $H^2(\mathcal{E})/T$ and $(H^1(\mathcal{C}) \otimes H^1(\mathcal{D}))^{\mathbb{F}_q}$ both have dimension $2(q-1)$. Thus the displayed surjection is a bijection. □

6.4. ***Fermat quotients.*** The surfaces $\mathcal{W}$ and $\mathcal{E}$ have affine open subsets defined by an equation with four monomials in three variables, namely,

$$y^2 = x^3 + t^q - t.$$

In Shioda's terminology, these are "Delsarte surfaces." This allows one to show that (over a sufficiently large ground field) $\mathcal{E}$ is birational to a quotient of a Fermat surface by a finite group. The Fermat surface is itself birational to the quotient of a product of two Fermat curves by a finite group. Thus we arrive at a birational presentation of $\mathcal{E}$ as a quotient of a product of Fermat curves. It turns out that this presentation factors through the sextic twist presentation given in Section 6.2, in a sense to be explained below. Thus, the Fermat quotient presentation does not give essential new information, and we will only sketch the main points, omitting most details.

Let $d = 6q - 6$. Applying the method of Shioda (see [Shioda 1986] and [Ulmer 2007, §6] or [Ulmer 2011, Lecture 2, §10]) yields a dominant rational map from F_d^2 to $\mathcal{E}$. Explicitly, take two copies of F_d with homogeneous coordinates $[X_0, X_1, X_2]$ and $[Y_0, Y_1, Y_2]$, and assume that $\mathbb{F}_r$ is large enough to contain a primitive $2d$-th root of unity ϵ. Consider the rational map $\phi : F_d^2 \dashrightarrow \mathcal{E}$ given by

$$\begin{aligned}([X_0, X_1, X_2], [Y_0, Y_1, Y_2]) &\mapsto (x, y, t)\\ &= \left(\epsilon^2 \frac{X_1^{2q-2}}{X_2^{2q-2}} \frac{Y_0^{2q-2} Y_1^2}{Y_2^{2q}}, \epsilon^{3q} \frac{X_0^{3q-3}}{X_2^{3q-3}} \frac{Y_0^{3q-3} Y_1^3}{Y_2^{3q}}, \epsilon^6 \frac{Y_1^6}{Y_2^6}\right).\end{aligned}$$

Then it is not hard to check that ϕ is dominant of generic degree d^3 and that it induces a birational isomorphism $F_d^2/G \dashrightarrow \mathcal{E}$ where $G \subset (\mu_d^3/\mu_d)^2$ is the group generated by

$$([1, 1, \zeta], [\zeta, 1, 1]), \quad ([\zeta^2, \zeta^3, 1], [1, 1, 1]), \quad \text{and} \quad ([\zeta, \zeta^2, 1], [1, \zeta^{q-1}, 1]),$$

where $\zeta = \epsilon^2$ is a primitive d-th root of unity in $\mathbb{F}_r$.

Analyzing the geometry of ϕ would allow us to show that $H^2(\mathcal{E})/T$ is isomorphic to a certain subspace of $H^2(F_d^2)$. We omit the details, because, as we explain next, ϕ factors through the rational map $E_0 \times C_{6,q} \dashrightarrow \mathcal{W}$ given in Section 6.2.

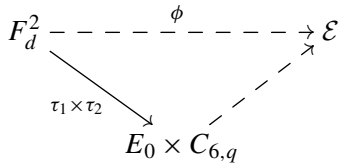
Indeed, consider the morphism $\tau_1 : F_d \to E_0$ given by

$$[X_0, X_1, X_2] \mapsto (z, w) = \left(\left(\frac{X_1}{X_2}\right)^{2q-2}, \left(\frac{\epsilon X_0}{X_2}\right)^{3q-3}\right)$$

and the morphism $\tau_2 : F_d \to C_{6,q}$ given by

$$[Y_0, Y_1, Y_2] \mapsto (t, u) = \left(\left(\frac{\epsilon Y_1}{Y_2}\right)^6, \frac{\epsilon Y_0^{q-1} Y_1}{Y_2^q}\right).$$

Then it is straightforward to check that the diagram



commutes, where the right diagonal rational map is that given in Section 6.2. This implies that $H^2(\mathcal{E})/T$ already appears in the cohomology of $E_0 \times C_{6,q}$, and that, moreover, the relevant map is defined without requiring an extension of $\mathbb{F}_r$. We will thus omit any further consideration of Fermat curves.

7. Geometric calculation of the L-function

In this section, we use the presentation of $\mathcal{E}$ as a quotient of a product of curves to give another calculation of $L(E, s)$ via the cohomological formula for it proved in [Shioda 1992]. As in the previous section, let $T \subset H^2(\mathcal{E})$ be the subspace spanned by the classes of the zero section and all components of all fibers of $\mathcal{E} \to \mathbb{P}^1$. Shioda proved that

$$L(E, s) = \det(1 - \mathrm{Fr}_r\, r^{-s} \mid H^2(\mathcal{E})/T).$$

7.1. ***Via sextic twists.*** Recall from Section 3.7 that $\langle r \rangle$ acts on $S^\times = (\mathbb{Z}/6\mathbb{Z})^\times \times \mathbb{F}_q^\times$, the set of orbits being denoted $O^\times_{r,6,q}$. As in Section 3.10, let $N_{r,6}$ denote the set of orbits of $\langle r \rangle$ on $(\mathbb{Z}/6\mathbb{Z})^\times$, and let $\rho_6 : O^\times_{r,6,q} \to N_{r,6}$ be the map induced by the projection $(\mathbb{Z}/6\mathbb{Z})^\times \times \mathbb{F}_q^\times \to (\mathbb{Z}/6\mathbb{Z})^\times$. Define

$$n_6(o) = \frac{|o|}{|\rho_6(o)|}.$$

Note that $n_6(o)$ is either $|o|$ (if $r \equiv 1 \pmod 6$) or $|o|/2$ (if $r \equiv -1 \pmod 6$). To each orbit $o \in O^\times_{r,6,q}$ we attach the Jacobi sum $J(\rho_6(o))$ (see (3-7)) and the Gauss sum $G(o)$ (see (3-6)).

Theorem 7.2. $$L(E, s) = \prod_{o \in O^\times_{r,6,q}} (1 - J(\rho_6(o))^{n_6(o)} G(o) r^{-s|o|}).$$

Proof. By Corollary 6.2.2, we know that

$$H^2(\mathcal{E})/T \cong (H^1(E_0) \otimes H^1(C_{6,q}))^{\mu_6},$$

where μ_6 acts antidiagonally. Combining (5-1) and (5-2), the right-hand side decomposes as the direct sum

$$\bigoplus_{(i,\alpha) \in S^\times} H^1(E_0)^{(i)} \otimes H^1(C_{6,q})^{(i,\alpha)},$$

where the summands are one-dimensional. If $o \in O^\times_{r,6,q}$, then the subspace

$$\bigoplus_{(i,\alpha) \in o} H^1(E_0)^{(i)} \otimes H^1(C_{6,q})^{(i,\alpha)}$$

is preserved by the r-power Frobenius Fr_r, and by what was recalled in Sections 5.2 and 5.3, the eigenvalue of $\mathrm{Fr}_r^{|o|}$ on $H^1(E_0)^{(i)} \otimes H^1(C_{6,q})^{(i,\alpha)}$ is $J(\rho_6(o))^{n_6(o)} G(o)$. By Lemma 5.1.1, the characteristic polynomial of $\mathrm{Fr}_r\, r^{-s|o|}$ on the displayed subspace is $(1 - J(\rho_6(o))^{n_6(o)} G(o) r^{-s|o|})$. Taking the product over all orbits yields the theorem. □

7.3. ***Via Artin–Schreier quotients.*** Let $\langle r\rangle$ act on $S^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times \mathbb{F}_q^\times$ with orbits $O^\times_{r,n,q}$, as in Section 3.7. For $n = 2, 3$, the natural projection $(\mathbb{Z}/6\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ induces a map $\pi_n : O^\times_{r,6,q} \to O^\times_{r,n,q}$. Recall that we write

$$m_2(o) = \frac{|o|}{|\pi_2(o)|}.$$

(There is no need for an analogous $m_3(o)$ since $|\pi_3(o)| = |o|$ for all $o \in O^\times_{r,6,q}$.) To each orbit $o \in O^\times_{r,6,q}$ we associate Gauss sums $G(\pi_2(o))$ and $G(\pi_3(o))$ (see Section 3.8).

Theorem 7.4. $$L(E, s) = \prod_{o\in O^\times_{r,6,q}} (1 - G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) r^{-s|o|}).$$

Proof. By Corollary 6.3.3, we have

$$H^2(\mathcal{E})/T \cong (H^1(C_{2,q}) \otimes H^1(C_{3,q}))^{\mathbb{F}_q},$$

where $\mathbb{F}_q$ acts diagonally. Using (5-2) twice, we get a direct sum decomposition of the right-hand side:

$$\bigoplus_{(i,\alpha)\in S^\times} H^1(C_{2,q})^{(i \bmod 2,\alpha)} \otimes H^1(C_{3,q})^{(i \bmod 3,-\alpha)},$$

where all the summands are one-dimensional. For any orbit $o \in O^\times_{r,6,q}$, the subspace

$$\bigoplus_{(i,\alpha)\in o} H^1(C_{2,q})^{(i \bmod 2,\alpha)} \otimes H^1(C_{3,q})^{(i \bmod 3,-\alpha)}$$

is preserved by the r-power Frobenius. The results recalled in Section 5.3 show that the eigenvalue of $\mathrm{Fr}_r^{|o|}$ acting on the line $H^1(C_{2,q})^{(i \bmod 2,\alpha)} \otimes H^1(C_{3,q})^{(i \bmod 3,-\alpha)}$ is $G(\pi_2(o))^{m_2(o)} G(\pi_3(o))$. (Here we use that $G_{\mathbb{F}}(\chi^i_{\mathbb{F},3}, \psi_{-\alpha}) = G_{\mathbb{F}}(\chi^i_{\mathbb{F},3}, \psi_\alpha)$, a consequence of the fact that -1 is a cube in any finite field $\mathbb{F}$.) Lemma 5.1.1 now implies that the characteristic polynomial of $\mathrm{Fr}_r\, r^{-s|o|}$ on the displayed subspace is $(1 - G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) r^{-s|o|})$. Taking the product over orbits then yields the theorem. □

7.5. ***Comparison of L-functions.*** As a check, we verify that the three expressions for $L(E, s)$ are in fact equal.

The "Artin–Schreier" expression for the L-function in Theorem 7.4 is visibly equal to the "elementary" expression in Theorem 4.1.

The index sets for the products in the "Artin–Schreier" and "sextic twist" expressions for the L-function (Theorems 7.4 and 7.2, respectively) are the same, namely, $O^\times_{r,6,q}$. If $o \in O^\times_{r,6,q}$ is the orbit through (i, α), let o' be the orbit through $(-i, \alpha)$. The map $o \mapsto o'$ gives a bijection $O^\times_{r,6,q} \to O^\times_{r,6,q}$ with $n_6(o) = n_6(o')$.

Let $o \in O^{\times}_{r,6,q}$ and choose $(i, \alpha) \in o$. Write $\mathbb{F} = \mathbb{F}_{r^{|o|}}$, $\mathbb{F}' = \mathbb{F}_{r^{|\pi_2(o)|}}$, and $\mathbb{F}'' = \mathbb{F}_{r^{|\rho_6(o)|}}$, so that $\mathbb{F}/\mathbb{F}'$ is an extension of degree $m_2(o)$, and $\mathbb{F}/\mathbb{F}''$ is an extension of degree $n_6(o)$. Then

$$\begin{aligned}
&G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) \\
&\quad = G_{\mathbb{F}'}(\chi^i_{\mathbb{F}',2}, \psi_\alpha)^{m_2(o)} G_{\mathbb{F}}(\chi^i_{\mathbb{F},3}, \psi_\alpha) && \text{(definition of } G(\pi_n(o))) \\
&\quad = G_{\mathbb{F}}(\chi^i_{\mathbb{F},2}, \psi_\alpha) G_{\mathbb{F}}(\chi^i_{\mathbb{F},3}, \psi_\alpha) && \text{(Hasse–Davenport relation)} \\
&\quad = J_{\mathbb{F}}(\chi^i_{\mathbb{F},2}, \chi^i_{\mathbb{F},3}) G_{\mathbb{F}}(\chi^i_{\mathbb{F},2}\chi^i_{\mathbb{F},3}, \psi_\alpha) && \text{(equation (3-4))} \\
&\quad = J_{\mathbb{F}''}(\chi^i_{\mathbb{F}'',2}, \chi^i_{\mathbb{F}'',3})^{n_6(o)} G_{\mathbb{F}}(\chi^i_{\mathbb{F},2}\chi^i_{\mathbb{F},3}, \psi_\alpha) && \text{(Hasse–Davenport relation)} \\
&\quad = J(\rho_6(o'))^{n_6(o')} G_{\mathbb{F}}(\chi^i_{\mathbb{F},2}\chi^i_{\mathbb{F},3}, \psi_\alpha) && \big(\text{definition of } J(\rho_6(o')) \\
&&& \quad \text{and } n_6(o) = n_6(o')\big) \\
&\quad = J(\rho_6(o'))^{n_6(o')} G_{\mathbb{F}}(\chi^{-i}_{\mathbb{F},6}, \psi_\alpha) && (2+3 = -1 \pmod 6) \\
&\quad = J(\rho_6(o'))^{n_6(o')} G(o') && \text{(definition of } G(o')).
\end{aligned}$$

Thus the o factor in the "Artin–Schreier" product for $L(E, s)$ equals the o' factor in the "sextic twist" product for $L(E, s)$.

8. First application of the BSD conjecture

In this section, we show that the conjecture of Birch and Swinnerton-Dyer (BSD) holds for E, and we deduce consequences for the Mordell–Weil group $E(K)$.

8.1. ***Notation and definitions.*** We recall the remaining definitions needed to state our BSD result. There is a canonical $\mathbb{Z}$-bilinear pairing

$$\langle \cdot, \cdot \rangle : E(K) \times E(K) \to \mathbb{Q}$$

which is nondegenerate modulo torsion. (This is the canonical Néron–Tate height pairing divided by $\log r$. See [Néron 1965] for the definition and [Hindry and Silverman 2000, B.5] for a friendly introduction.) Choosing a $\mathbb{Z}$-basis $P_1, \ldots, P_R$ for $E(K)$ modulo torsion, we define the *regulator* of E as

$$\mathrm{Reg}(E) := |\det\langle P_i, P_j\rangle_{1 \le i,j \le R}|.$$

The regulator is a positive rational number, well defined independently of the choice of bases, and by convention, it is 1 when the rank of $E(K)$ is 0.

We write $H^1(K, E)$ for the étale cohomology of K with coefficients in E and similarly for $H^1(K_v, E)$ for any place v of K. The *Tate–Shafarevich group* of E is

defined as

$$Ш(E) := \ker\left(H^1(K, E) \to \prod_v H^1(K_v, E) \right),$$

where the product is over the places of K and the map is the product of the restriction maps.

The leading coefficient of the L-function (also called its *special value* at $s = 1$ or $T = r^{-1}$) is defined by

$$L^*(E) := \frac{1}{\rho!}\left(\frac{d}{dT}\right)^\rho L(E, T)\Big|_{T=r^{-1}} = \frac{1}{(\log r)^\rho}\frac{1}{\rho!}\left(\frac{d}{ds}\right)^\rho L(E, s)\Big|_{s=1}$$

where ρ is the order of vanishing $\rho := \operatorname{ord}_{s=1} L(E, s)$. The point of the normalization by $(\log r)^{-\rho}$ is to ensure that $L^*(E)$ is a rational number (recall indeed that $L(E, s)$ is a polynomial with integral coefficients in $T = r^{-s}$). Note that the above definition directly implies the two relations

$$L^*(E) = \frac{L(E, T)}{(1 - rT)^\rho}\Big|_{T=r^{-1}} \quad \text{and} \quad L^*(E) = \lim_{s\to 1} \frac{L(E, s)}{(1 - r^{1-s})^\rho}.$$

We refer to Section 2.1 for the definition of the local Tamagawa numbers c_v.

Here is our main result connecting all these invariants.

Theorem 8.2. *The BSD conjecture holds for E. More precisely,*

(1) $\operatorname{ord}_{s=1} L(E, s) = \operatorname{Rank} E(K)$,

(2) $Ш(E)$ *is finite,*

(3) *we have an equality*

$$L^*(E) = \frac{\operatorname{Reg}(E)\,|Ш(E)| \prod_v c_v}{r^{\deg(\omega_E)-1}|E(K)_{\mathrm{tors}}|^2}.$$

Proof. This follows from the fact (see Sections 6.2 and 6.3) that the Néron model of E is dominated by a product of curves, and earlier work of Tate [1966] and Milne [1975]. See [Ulmer 2011, Theorem 9.1] for more details. □

As we have shown, the L-function $L(E, s)$ is a polynomial of degree $2(q - 1)$ in r^{-s}. In particular, $\rho = \operatorname{ord}_{s=1} L(E, s)$ cannot exceed $2(q - 1)$. By part (1) of the BSD result, this proves that $0 \le \operatorname{Rank} E(K) \le 2(q - 1)$. In what follows, we will describe more precisely the value of $\operatorname{Rank} E(K)$, depending on $p \bmod 6$.

We proved in Proposition 2.4 that $|E(K)_{\mathrm{tors}}| = 1$ and that $\prod_v c_v = 1$, and we noted in Section 2.2 that $\deg(\omega_E) = \lceil q/6 \rceil$. Thus the BSD formula simplifies to

$$L^*(E) = \frac{\operatorname{Reg}(E)\,|Ш(E)|}{r^{\lfloor q/6 \rfloor}}. \tag{8-1}$$

In the rest of this section, we will deduce consequences from part (1) of the theorem, and in the following section we will use parts (2) and (3).

8.3. ***Explicit L-function for*** $p \equiv 1 \pmod 6$**.** Recall that we have shown that

$$L(E,T) = \prod_{o \in O^{\times}_{r,6,q}} (1 - G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) T^{|o|}),$$

where we substitute T for r^{-s}. We will make this more explicit using results from Section 3.5.

First, note that when $p \equiv 1 \pmod 6$, the action of $\langle r \rangle$ on $(\mathbb{Z}/6\mathbb{Z})^{\times}$ is trivial, so an orbit $o \in O^{\times}_{r,6,q}$ consists of pairs (i, α) where $i \in (\mathbb{Z}/6\mathbb{Z})^{\times}$ is constant and $\alpha \in \mathbb{F}_q^{\times}$ runs through an orbit $\bar{o} \in O_{r,q}$ (recall that $O_{r,q}$ denotes the set of orbits of the action of $\langle r \rangle$ on $\mathbb{F}_q^{\times}$). In particular, we have $|\pi_2(o)| = |o|$ so that $m_2(o) = 1$.

For a given orbit $\bar{o} \in O_{r,q}$, let us consider the two orbits in $O^{\times}_{r,6,q}$,

$$o = \{(1, \alpha) : \alpha \in \bar{o}\} \quad \text{and} \quad o' = \{(-1, \alpha) : \alpha \in \bar{o}\},$$

"lying over $\bar{o}$" and the two corresponding factors in the product for the L-function. Set $\mathbb{F} = \mathbb{F}_r(\alpha)$ and note that $\mathbb{F}$ is an extension of $\mathbb{F}_r = \mathbb{F}_{p^{\nu}}$ of degree $|o| = |o'| = |\bar{o}|$. By definition we have

$$\begin{aligned} (8\text{-}2)\quad & \big(1 - G(\pi_2(o))G(\pi_3(o))T^{|o|}\big)\big(1 - G(\pi_2(o'))G(\pi_3(o'))T^{|o'|}\big) \\ &= \big(1 - G_{\mathbb{F}}(\chi_{\mathbb{F},2}, \psi_\alpha) G_{\mathbb{F}}(\chi_{\mathbb{F},3}, \psi_\alpha) T^{|o|}\big)\big(1 - G_{\mathbb{F}}(\chi_{\mathbb{F},2}, \psi_\alpha) G_{\mathbb{F}}(\chi_{\mathbb{F},3}^{-1}, \psi_\alpha) T^{|o|}\big) \\ &=: L_{\bar{o}}(T). \end{aligned}$$

Since $|\mathbb{F}| = p^{\nu|o|}$, it follows from (3-1) that

$$\operatorname{ord}(G_{\mathbb{F}}(\chi_{\mathbb{F},2}, \psi_\alpha)) = \tfrac{1}{2}\nu|o|.$$

On the other hand, (3-2) yields that

$$\operatorname{ord}(G_{\mathbb{F}}(\chi_{\mathbb{F},3}, \psi_\alpha)) = \tfrac{2}{3}\nu|o| \quad \text{and} \quad \operatorname{ord}(G_{\mathbb{F}}(\chi_{\mathbb{F},3}^{-1}, \psi_\alpha)) = \tfrac{1}{3}\nu|o|.$$

In particular, the inverse roots of the product $L_{\bar{o}}(T)$ have valuation $\frac{7}{6}\nu$ and $\frac{5}{6}\nu$. We deduce that $T = r^{-1}$, which satisfies $\operatorname{ord}(r^{-1}) = -\nu$, cannot be a root of $L_{\bar{o}}(T)$.

Since this holds for any orbit $\bar{o} \in O_{r,q}$ and since $L(E,T) = \prod_{\bar{o} \in O_{r,q}} L_{\bar{o}}(T)$, we obtain that $L(E,T)$ does not vanish at $T = r^{-1}$. This establishes the first two points of the following result.

Proposition 8.3.1. *Assume that* $p \equiv 1 \pmod 6$.

(1) *The inverse roots on the right-hand side of* (8-2) *have valuations* $\frac{7}{6}\nu$ *and* $\frac{5}{6}\nu$.

(2) $\operatorname{ord}_{s=1} L(E,s) = 0$.

(3) $E(K) = 0$.

(4) $\operatorname{Reg}(E) = 1$.

Proof. Points (1) and (2) follow immediately from the above discussion. It then follows from our BSD result (Theorem 8.2) that Rank $E(K) = 0$ so that $E(K)$ is torsion. But we showed in Proposition 2.4 that $E(K)_{\text{tors}} = 0$, so $E(K) = 0$. Finally, since $E(K)$ has rank 0, the regulator is 1. □

We remark that point (1) of the proposition leads to another proof of BSD in this case. Indeed, the inequality $0 \le \text{Rank } E(K) \le \text{ord}_{s=1} L(E, s)$ is known in general (see [Tate 1966]), so if $\text{ord}_{s=1} L(E, s) = 0$, then $\text{Rank } E(K) = \text{ord}_{s=1} L(E, s) = 0$, and this equality between algebraic and analytic ranks implies the rest of the BSD conjecture (by the main result of [Kato and Trihan 2003]).

8.4. ***Explicit L-function for*** $p \equiv -1 \pmod 6$**.** As in the preceding subsection, we start from the expression

$$L(E, T) = \prod_{o \in O^{\times}_{r,6,q}} (1 - G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) T^{|o|}),$$

which we make more explicit, in the case when $p \equiv -1 \pmod 6$, using results from Section 3.5.

Let $o \in O^{\times}_{r,6,q}$ be an orbit, pick $(i, \alpha) \in o$ and write $\mathbb{F} = \mathbb{F}_{r^{|o|}}$. If $m_2(o) = 1$ then, by definition of the Gauss sums, we have

$$\big(1 - G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) T^{|o|}\big) = \big(1 - G_{\mathbb{F}}(\chi_{\mathbb{F},2}, \psi_\alpha) G_{\mathbb{F}}(\chi^i_{\mathbb{F},3}, \psi_\alpha) T^{|o|}\big).$$

On the other hand, if $m_2(o) = 2$ (i.e., if $|o| = 2|\pi_2(o)|$), setting $\mathbb{F}' = \mathbb{F}_r(\alpha) = \mathbb{F}_{r^{|\pi_2(o)|}}$ (which is a quadratic extension of $\mathbb{F}$), the Hasse–Davenport relation yields

$$G(\pi_2(o))^{m_2(o)} = G_{\mathbb{F}'}(\chi_{\mathbb{F}',2}, \psi_\alpha)^2 = G_{\mathbb{F}}(\chi_{\mathbb{F},2}, \psi_\alpha).$$

Thus, in both cases, we can rewrite the factor of $L(E, T)$ indexed by $o \in O^{\times}_{r,6,q}$ as

$$\big(1 - G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) T^{|o|}\big) = \big(1 - G_{\mathbb{F}}(\chi_{\mathbb{F},2}, \psi_\alpha) G_{\mathbb{F}}(\chi^i_{\mathbb{F},3}, \psi_\alpha) T^{|o|}\big),$$

where $\mathbb{F} = \mathbb{F}_{r^{|o|}}$ and $(i, \alpha) \in o$. Now using (3-1) and (3-3) and recalling that $\mathbb{F}_r = \mathbb{F}_{p^\nu}$, we remark that

$$G_{\mathbb{F}}(\chi_{\mathbb{F},2}, \psi_\alpha) G_{\mathbb{F}}(\chi^i_{\mathbb{F},3}, \psi_\alpha) = p^{*\nu|o|/2} \chi^{-i}_{\mathbb{F},3}(\alpha)(-p)^{\nu|o|/2} = \epsilon_o r^{|o|},$$

where ϵ_o is a sixth root of unity, namely,

$$\epsilon_o = (-1)^{(p+1)\nu|o|/4} \chi^{-i}_{\mathbb{F},3}(\alpha). \tag{8-3}$$

Note that, p being odd and $\nu|o|$ being even, the exponent $(p+1)\nu|o|/4$ of -1 is an integer. Therefore, for any orbit $o \in O^{\times}_{r,6,q}$, the factor of $L(E, T)$ indexed by o can be rewritten as

$$(1 - G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) T^{|o|}) = (1 - \epsilon_o r^{|o|} T^{|o|}). \tag{8-4}$$

We can now prove the following result, analogous to Proposition 8.3.1.

Proposition 8.4.1. *Assume that* $p \equiv -1 \pmod 6$. *Let*

$$\rho = \rho_{r,q} := \left|\left\{o \in O_{r,6,q}^{\times} : (p+1)v|o| \equiv 0 \pmod 8 \text{ and } \alpha \text{ is a cube in } \mathbb{F}_{r^{|o|}}^{\times} \text{ for any } (i,\alpha) \in o\right\}\right|.$$

Then

(1) $\operatorname{ord}_{s=1} L(E,s) = \rho$.

(2) $E(K)$ *is free abelian of rank* ρ.

(3) *For a given* q, $\operatorname{Rank} E(K) = 2(q-1)$ *for* $\mathbb{F}_r$ *sufficiently large. More precisely, if* $r = p^v$ *is a power of* q, $(p+1)v \equiv 0 \pmod 8$, *and* $3(q-1) \mid (r-1)$, *then*

$$\operatorname{Rank} E(K) = 2(q-1).$$

(4) *For a given* r, $\operatorname{Rank} E(K)$ *is unbounded as* q *varies. Indeed, for every* $\epsilon > 0$, *if* $q = p^f$ *and* f *is a sufficiently large multiple of* 4, *then*

$$\operatorname{Rank} E(K) > 2(1-\epsilon)p^f/f.$$

Proof. By our formula for $L(E,s)$ and (8-4), the order of vanishing of $L(E,s)$ at $s=1$ equals the number of orbits $o \in O_{r,6,q}$ such that $G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) = r^{|o|}$, i.e., the number of orbits such that $\epsilon_o = 1$. Part (1) then follows easily from (8-3). For (2), it follows from the BSD theorem (Theorem 8.2) that $\operatorname{Rank} E(K) = \rho$, and we showed in Proposition 2.4 that $E(K)_{\text{tors}} = 0$, so that $E(K)$ is indeed free abelian of rank ρ. The conditions in (3) guarantee that all orbits o have size 1 and satisfy $\epsilon_o = 1$. In this case, there are $2(q-1)$ orbits, all contributing to ρ, and this yields the claim. (Under these assumptions, the L-function of E therefore admits a very simple expression: $L(E,s) = (1-r^{1-s})^{2(q-1)}$).

To prove (4), we first note that it suffices to treat the case $r = p$, i.e., $v = 1$. Next, we note that "most" elements $\alpha \in \mathbb{F}_{p^f}$ satisfy $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^f}$. Indeed, it is elementary that the number of elements in $\mathbb{F}_{p^f}$ that do not lie in a smaller field is at least $p^f - (\log_2 f)p^{f/2}$. It follows that for every $\epsilon > 0$, there is a constant f_0 such that

$$|\{\alpha \in \mathbb{F}_{p^f} \mid \mathbb{F}_p(\alpha) = \mathbb{F}_{p^f}\}| \geq (1-\epsilon)p^f$$

for all $f > f_0$. On the other hand, at least $\frac{1}{3}(p^f - 1)$ elements of $\mathbb{F}_{p^f}^{\times}$ are cubes. Thus, if $\epsilon < \frac{1}{3}$, then for all sufficiently large f, the number of elements of $\mathbb{F}_{p^f}$ that are cubes and that generate $\mathbb{F}_{p^f}$ is at least $\left(\frac{1}{3} - \epsilon\right)p^f$. If f is even and α has these properties, then the orbit through (i,α) has size f, and if f is a multiple of 4, then these orbits all contribute to ρ. This shows that for f divisible by 4 and sufficiently large, ρ is bounded below by $2(1-\epsilon)p^f/f$, and this completes the proof of part (4). □

We note that although the rank is always unbounded for varying q, it does not go to infinity with $q = p^f$, i.e., the rank of $E(K)$ may be small even when f is large. For example, when $p \equiv 5 \pmod{12}$ and $v = 1$, it follows from part (1) of the proposition that the rank is 0 for all odd f.

9. p-adic size of $L^*(E)$ and $Ш(E)$

The special value $L^*(E)$ was defined in the previous section. Since $L(E,T)$ is a polynomial in T with integer coefficients, $L^*(E)$ actually lies in $\mathbb{Z}[1/p]$. In this section, we use the explicit presentation of the L-function in terms of exponential sums to estimate the p-adic valuation of $L^*(E)$, and then use the BSD formula to deduce consequences for $\mathrm{Reg}(E)\,|Ш(E)|$.

Recall from Section 3.1 that we fixed a prime ideal $\mathfrak{P}$ of $\overline{\mathbb{Z}}$ that lies over p. As before, we denote by ord the p-adic valuation of $\overline{\mathbb{Q}}$ associated to $\mathfrak{P}$ normalized so that $\mathrm{ord}(p)=1$.

Proposition 9.1. *Given data p, q and $r=p^\nu$ as before, we have*:

(1) *If* $p\equiv 1 \pmod 6$,
$$\mathrm{ord}(L^*(E)) = -\frac{q-1}{6}\nu.$$

(2) *If* $p\equiv -1 \pmod 6$, *then* $L^*(E)$ *is an integer, so* $\mathrm{ord}(L^*(E))\geq 0$.

(3) *If* $p\equiv -1 \pmod 6$ *and* r *is sufficiently large* (*in the sense of part* (3) *of Proposition 8.4.1*), $L^*(E)=1$.

Proof. First assume that $p\equiv 1 \pmod 6$. As we saw in Section 8.3, $L^*(E)$ is simply the value of $L(E,T)$ at $T=r^{-1}$. We further showed that $L(E,T)$ is the product over orbits $\bar{o}$ of $\langle r\rangle$ acting on $\mathbb{F}_q^\times$ of factors of the form
$$(1-\gamma_1 T^{|\bar{o}|})(1-\gamma_2 T^{|\bar{o}|}),$$
where $\mathrm{ord}(\gamma_1)=\frac{5}{6}\nu|\bar{o}|$ and $\mathrm{ord}(\gamma_2)=\frac{7}{6}\nu|\bar{o}|$. (See Proposition 8.3.1 (1) and the discussion above that result.) Substituting $T=r^{-1}=p^{-\nu}$, we see that the contribution to $\mathrm{ord}\,L^*(E)$ from the pair of factors associated to $\bar{o}$ has valuation $-\frac{1}{6}\nu|\bar{o}|$. Taking the product over all orbits shows that
$$\mathrm{ord}(L^*(E)) = \sum_{\bar{o}\in O_{r,q}} -\frac{\nu|\bar{o}|}{6} = -\frac{\nu}{6}\sum_{\bar{o}\in O_{r,q}}|\bar{o}| = -\frac{(q-1)\nu}{6},$$
and this establishes part (1) of the proposition.

Now assume that $p\equiv -1 \pmod 6$. In Section 8.4, we showed that $L(E,T)$ is the product over orbits $o\in O_{r,6,q}^\times$ of factors of the form $(1-\epsilon_o r^{|o|}T^{|o|})$ where ϵ_o is a sixth root of unity. If $\epsilon_o\neq 1$, then the contribution of this factor to the special value is $(1-\epsilon_o)$, an algebraic integer. If $\epsilon_o=1$, then the contribution is
$$\left.\frac{(1-r^{|o|}T^{|o|})}{1-rT}\right|_{T=r^{-1}} = \left.(1+rT+\cdots+(rT)^{|o|-1})\right|_{T=r^{-1}} = |o|,$$
an integer. This shows that $L^*(E)$ is an algebraic integer, and since it also lies in

$\mathbb{Z}[1/p] \subset \mathbb{Q}$, $L^*(E)$ is an integer. This establishes part (2) of the proposition. For part (3), we note that if r is sufficiently large, all orbits o are singletons and all the ϵ_o are 1 (see Proposition 8.4.1(3)). The analysis above shows that $L^*(E) = 1$. □

Now we apply the BSD formula, as simplified in (8-1):

$$L^*(E) = \frac{\mathrm{Reg}(E)\,|Ш(E)|}{r^{\lfloor q/6 \rfloor}}.$$

Corollary 9.2. (1) *If* $p \equiv 1 \pmod 6$, *then*

$$\mathrm{Reg}(E) = 1 \quad \textit{and} \quad \mathrm{ord}(|Ш(E)|) = 0.$$

In particular, the p*-primary part of* $Ш(E)$ *is trivial.*

(2) *If* $p \equiv -1 \pmod 6$, *then*

$$\mathrm{ord}(\mathrm{Reg}(E)\,|Ш(E)|) \geq \lfloor q/6 \rfloor \nu.$$

(3) *If* $p \equiv -1 \pmod 6$ *and* r *is sufficiently large* (*in the sense of part* (4) *of Proposition 8.3.1*), *then*

$$\mathrm{Reg}(E)\,|Ш(E)| = r^{\lfloor q/6 \rfloor} = p^{\nu \lfloor q/6 \rfloor}.$$

In particular, $Ш(E)$ *is a* p*-group.*

Proof. If $p \equiv 1 \pmod 6$, then combining Proposition 9.1 with the BSD formula (8-1) yields that

$$\mathrm{ord}(\mathrm{Reg}(E)\,|Ш(E)|) = 0.$$

We showed in Proposition 8.3.1 that $\mathrm{Reg}(E) = 1$, so that $\mathrm{ord}(|Ш(E)|) = 0$. This proves part (1).

If $p \equiv -1 \pmod 6$, then Proposition 9.1 says that $L^*(E)$ is an integer, and it follows immediately from (8-1) that $\mathrm{ord}(\mathrm{Reg}(E)\,|Ш(E)|) \geq \lfloor q/6 \rfloor \nu$. This yields part (2).

For part (3), we know from Proposition 9.1 that $L^*(E) = 1$, so (8-1) implies that $\mathrm{Reg}(E)\,|Ш(E)| = r^{\lfloor q/6 \rfloor}$. By [Ulmer 2019, Proposition 3.1.1], $\mathrm{Reg}(E)$ is an integer, so both it and $|Ш(E)|$ are powers of p. This establishes part (3). □

Following [Ulmer 2019, §4], let us consider the limit

$$\dim Ш(E) := \lim_{n \to \infty} \frac{\log |Ш(E \times \mathbb{F}_{r^n}(t))[p^\infty]|}{\log(r^n)},$$

where $Ш(-)[p^\infty]$ denotes the p-primary part of $Ш(-)$. As is shown in [loc. cit.], the limit exists and is a nonnegative integer, called the "dimension of Ш" of E. The value of $\dim Ш(E)$ is expressed in terms of the valuations of the inverse roots of $L(E, T)$ in [Ulmer 2019, Proposition 4.2].

In the situation at hand, the mentioned expression and the results of Sections 8.3 and 8.4 directly yield the following values for $\dim Ш(E)$:

Corollary 9.3. (1) *If* $p \equiv 1 \pmod 6$, *then* $\dim Ш(E) = 0$.

(2) *If* $p \equiv -1 \pmod 6$, *then* $\dim Ш(E) = \lfloor q/6 \rfloor$.

10. Algebraic analysis of $Ш(E)[p^\infty]$

In this section we recover the results of Corollaries 9.2 and 9.3 regarding the p-torsion in $Ш(E)$ by algebraic means, more specifically via crystalline cohomology. Here is the statement.

Proposition 10.1. (1) *If* $p \equiv 1 \pmod 6$, *then* $Ш(E)[p] = 0$.

(2) *If* $p \equiv -1 \pmod 6$, *then* $\dim Ш(E) = \lfloor q/6 \rfloor$.

The proof will use that the Néron model $\mathcal{E}$ is dominated by the product of curves $E_0 \times C_{6,q}$, knowledge of the crystalline cohomology of the curves, and p-adic semilinear algebra, as in [Ulmer 2019, §6–8]. We collect the needed background results in the next subsection and treat the cases $p \equiv 1 \pmod 6$ and $p \equiv -1 \pmod 6$ separately in the following two subsections.

10.2. ***Preliminaries.*** Let $W = W(\mathbb{F}_r)$ denote the ring of Witt vectors over $\mathbb{F}_r$ and σ denote its Frobenius morphism. We denote the Dieudonné ring by $A = W\{F, V\}$: this is the noncommutative polynomial ring over W with indeterminates F, V modulo the relations $FV = VF = p \in W$, $Fw = \sigma(w)F$, and $\sigma(w)V = Vw$ for all $w \in W$.

Throughout this section, we write $H^1(C)$ for the integral crystalline cohomology $H^1_{\mathrm{crys}}(C/W)$ of a curve C over $\mathbb{F}_r$. The space $H^1(C)$ is a finitely generated, free $W = W(\mathbb{F}_r)$-module equipped with semilinear actions of F and V such that $FV = VF =$ multiplication by p. In other words, $H^1(C)$ is a module over the Dieudonné ring A. We will apply this for $C = E_0$ and $C = C_{6,q}$ and make it much more explicit below.

We saw in Section 6.2 that the Néron model $\mathcal{E}$ of E, is birational to the quotient of $E_0 \times C_{6,q}$ by the antidiagonal action of μ_6. Then [Ulmer 2019, Proposition 6.2] says that

$$Ш(E)[p^\infty] \cong \mathrm{Br}(\mathcal{E})[p^\infty] \cong \mathrm{Br}((E_0 \times C_{6,q})/\mu_6)[p^\infty] \cong \mathrm{Br}(E_0 \times C_{6,q})[p^\infty]^{\mu_6} \tag{10-1}$$

where the exponent indicates the invariant subgroup. Moreover, by [Ulmer 2019, Proposition 6.4], for all $n \geq 1$ we have

$$\mathrm{Br}(E_0 \times C_{6,q})[p^n] \cong \frac{\mathrm{Hom}_A(H^1(E_0)/p^n, H^1(C_{6,q})/p^n)}{\mathrm{Hom}_A(H^1(E_0), H^1(C_{6,q}))/p^n} \tag{10-2}$$

compatibly with the action of μ_6.

To prove part (1) of the proposition, we will show that the μ_6-invariant part of the numerator in the last expression is 0 whenever $p \equiv 1 \pmod 6$. For part (2), we will recall from [Ulmer 2019, §8] that the growth of $Ш(E \times \mathbb{F}_{r^m}(t))[p^\infty]$ as a function of m is controlled by the numerator in the previous display, and this is in turn computable in terms of the action of $\langle p \rangle$ on a finite set indexing the cohomology of E_0 and $C_{6,q}$.

10.3. ***Explicit A-module structure of $H^1(E_0)$ and $H^1(C_{6,q})$.*** We now make explicit the results on the cohomology groups $H^1(E_0)$ and $H^1(C_{6,q})$ (viewed as A-modules) that will be needed below. All results stated in this subsection follow from well-known results about Fermat curves and their quotients, as recalled in [Ulmer 2019, §7] and in [Katz 1981].

Let $I = \{\pm 1\} \subset (\mathbb{Z}/6\mathbb{Z})^\times = I_0 \cup I_1$ where $I_0 = \{1\}$ and $I_1 = \{-1\}$. As a W-module, $H^1(E_0)$ has rank 2 and is generated by classes e_i with $i \in I$, where e_{-1} is the class of the regular differential dx/y and e_1 is associated to the meromorphic differential $x\,dx/y$. (This can be taken to mean that the restriction of e_1 to $E_0 \smallsetminus \{O\}$ is the class of the regular differential $x\,dx/y$.) The indexing is motivated by the fact that over an extension of $\mathbb{F}_r$ large enough to contain the sixth roots of unity, one has

$$\zeta^*(e_1) = \zeta e_1 \quad \text{and} \quad \zeta^*(e_{-1}) = \zeta^{-1} e_{-1}$$

for all $\zeta \in \mu_6$, where the ζs on the left of each equation are in the finite field $\mathbb{F}_r$ and those on the right are their Teichmüller lifts to the Witt vectors W. The action of A satisfies $F(e_i) = c_i e_{pi}$ for some $c_i \in W$ with

$$\operatorname{ord}(c_i) = \begin{cases} 0 & \text{if } i \in I_0, \\ 1 & \text{if } i \in I_1. \end{cases} \tag{10-3}$$

Since $FV = p$, we deduce that $V(e_i) = p/\sigma^{-1}(c_{i/p}) e_{i/p}$.

Let $J \subset \mathbb{Z}/6(q-1)\mathbb{Z}$ be the set of classes that are nonzero modulo 6. Given $j \in J$, there is a unique pair of integers (a, b) with $1 \le a \le q-1$, $1 \le b \le 5$, and $j \equiv 6a - b \pmod{6(q-1)}$. Then $H^1(C_{6,q})$ is a free W-module of rank $5(q-1)$ with basis elements f_j, $j \in J$, where f_j is associated to the differential $t^{a-1}dt/u^b$ in the following sense: Let $J_1 \subset J$ be the set of classes j whose associated (a, b) satisfy $a < qb/6$. For these j, the differential $t^{a-1}dt/u^b$ is everywhere regular on $C_{6,q}$ and f_j is its class. Let $J_0 = J \smallsetminus J_1$. If $j \in J_0$, the differential $t^{a-1}dt/u^b$ is regular on $C_{6,q} \smallsetminus \{\infty\}$, and the restriction of f_j to the open curve is the class of this differential. Over an extension of $\mathbb{F}_r$ large enough to contain the roots of unity of order $6(q-1)$, we have $\zeta^* f_j = \zeta^j f_j$ for all $\zeta \in \mu_{6(q-1)}$ (with the same convention as before). The action of A on $H^1(C_{6,q})$ is given by $F(f_j) = d_j f_{pj}$, for some $d_j \in W$ satisfying

$$\operatorname{ord}(d_j) = \begin{cases} 0 & \text{if } j \in J_0, \\ 1 & \text{if } j \in J_1. \end{cases}$$

Since $FV = p$, we obtain that $V(f_j) = p/\sigma^{-1}(c_{j/p}) f_{j/p}$.

Fix $j \in J$ with $j \not\equiv 0 \pmod 3$. Let $\mathbb{F} = \mathbb{F}_r(\mu_{6(q-1)})$ and let $m = [\mathbb{F} : \mathbb{F}_p]$, so that $p^m j \equiv j \pmod{6(q-1)}$. Then the m-th power F^m of the Frobenius acts on f_j by multiplication by a Gauss sum. More precisely, let $\chi = \chi_{\mathbb{F},6(q-1)}$ be the character defined in Section 3.2, viewed as a W-valued character. Then $F^m f_j = G_j f_j$ where $G_j = G_{\mathbb{F}}(\chi^j, \psi_1)$. When $p \equiv 1 \pmod 6$, it follows from Stickelberger's theorem that

$$\operatorname{ord}(G_j) = \begin{cases} \frac{2}{3}m & \text{if } j \equiv 1 \pmod 3, \\ \frac{1}{3}m & \text{if } j \equiv 2 \pmod 3. \end{cases} \tag{10-4}$$

(This is essentially the same calculation as that in Section 3.5.)

When $p \equiv 1 \pmod 6$, we will calculate $\operatorname{Hom}_A(H^1(E_0)/p, H^1(C_{6,q})/p)$ explicitly in the next subsection and see that it vanishes. In the following subsection, we will assume $p \equiv -1 \pmod 6$ and use the action of $\langle p \rangle$ on $I \times J$ to compute $\dim Ш(E)$ as in [Ulmer 2019, §8].

10.4. ***Proof of Proposition 10.1(1).*** In light of the isomorphisms (10-1) and (10-2), we remark that it suffices to show that

$$\operatorname{Hom}_A(H^1(E_0)/p, H^1(C_{6,q})/p)^{\mu_6} = 0,$$

to show that $Ш(E)[p] = 0$ in the case when $p \equiv 1 \pmod 6$. To that end, let $\varphi \in \operatorname{Hom}_A(H^1(E_0)/p, H^1(C_{6,q})/p)^{\mu_6}$. Since φ is, in particular, a W-linear map, we can write

$$\varphi(e_i) = \sum_j \alpha_{i,j} f_j$$

for all $i \in I = (\mathbb{Z}/6\mathbb{Z})^\times$, where the sum runs over $j \in J \subset \mathbb{Z}/6(q-1)\mathbb{Z}$, and where $\alpha_{i,j} \in W/p = \mathbb{F}_r$. For φ to commute with the antidiagonal μ_6 action, it is necessary that $\alpha_{i,j} = 0$ unless $i \equiv -j \pmod 6$. Further, φ being an A-module homomorphism means that $\varphi F = F\varphi$ and $\varphi V = V\varphi$. Let us now write down what these conditions mean in terms of the "matrix" $(\alpha_{i,j})_{i,j}$ of φ. Let $m = [\mathbb{F}_r(\mu_{6(q-1)}) : \mathbb{F}_p]$, so that $p^m i \equiv i \pmod 6$ and $p^m j \equiv j \pmod{6(q-1)}$ for all $i \in I$ and $j \in J$. Then, by the results in the previous subsection, we have

$$F^m \varphi(e_1) = F^m \Bigg(\sum_{j \equiv -1 \pmod 6} \alpha_{1,j} f_j \Bigg) = \sum_{j \equiv -1 \pmod 6} \sigma^m(\alpha_{1,j}) G_j f_j$$

and

$$\varphi F^m(e_1) = \varphi(ue_1) = u \sum_{j \equiv -1 \pmod 6} \alpha_{1,j} f_j$$

for a certain $u \in W^\times$ (by (10-3)). Equating coefficients of f_j then yields that $u\alpha_{1,j} = \sigma^m(\alpha_{1,j}) G_j$. However, we know from (10-4) that $\operatorname{ord}(G_j) = \frac{1}{3}m > 0$.

Hence $\alpha_{1,j} = 0$ for all $j \in J$. Similarly, we have

$$V^m\varphi(e_{-1}) = V^m\left(\sum_{j\equiv 1 \pmod 6} \alpha_{-1,j} f_j\right) = \sum_{j\equiv 1 \pmod 6} \sigma^{-m}(\alpha_{-1,j})(p^m/G_j) f_j$$

and

$$\varphi V^m(e_{-1}) = \varphi(ve_{-1}) = v \sum_{j\equiv 1 \pmod 6} \alpha_{-1,j} f_j$$

for some $v \in W^\times$ (by (10-3)). Equating coefficients of f_j then shows that

$$v\alpha_{-1,j} = \sigma^{-m}(\alpha_{-1,j})(p^m/G_j).$$

On the other hand, (10-4) tells us that $\operatorname{ord}(p^m/G_j) = \frac{1}{3}m > 0$. This implies that $\alpha_{-1,j} = 0$ for all $j \in J$.

Thus every $\varphi \in \operatorname{Hom}_A(H^1(E_0)/p, H^1(C_{6,q})/p)^{\mu_6}$ satisfies $\varphi(e_1) = \varphi(e_{-1}) = 0$. This proves that $\operatorname{Hom}_A(H^1(E_0)/p, H^1(C_{6,q})/p)^{\mu_6} = 0$ which completes the proof of part (1) of the proposition. □

10.5. ***Proof of Proposition 10.1 (2).*** We now turn to part (2) of the proposition and assume that $p \equiv -1 \pmod 6$. For any $n \geq 1$, the set $I \times J$ indexes the eigenspaces of $\mu_6 \times \mu_{6(q-1)}$ acting on $\operatorname{Hom}(H^1(E_0)/p^n, H^1(C_{6,q})/p^n)$, and the subset (which we denote by $(I \times J)^{\mu_6}$) indexing invariants under the antidiagonal action of μ_6 consists of pairs (i, j) with $i \equiv -j \pmod 6$.

Define a bijection

$$(I \times J)^{\mu_6} \to S := \{1, 5\} \times \{1, \ldots, q-1\} \tag{10-5}$$

by $(i, j) \mapsto (b, a)$ where $6a - b \equiv j \pmod{6(q-1)}$ (so that $b \equiv i \pmod 6$). Under this bijection, $(I_0 \times J_1)^{\mu_6}$ corresponds to pairs $(1, a)$ where $0 < a < q/6$, and $(I_1 \times J_0)^{\mu_6}$ corresponds to pairs $(5, a)$ where $5q/6 < a < q$. (See the definitions of I_0, I_1, J_0, and J_1 in Section 10.2.) We thus define

$$S_0 = \{(1, a) : 0 < a < q/6\}$$

and

$$S_1 = \{(5, a) : 5q/6 < a < q\}.$$

The action of $\langle p\rangle$ on $I \times J$ preserves $(I \times J)^{\mu_6}$ and so, by transport of structure, we get a (nonstandard) action on S which we will make explicit below. Let O be the set of orbits of $\langle p\rangle$ on S. Given an orbit $o \in O$, define

$$d(o) := \min(|o \cap S_0|, |o \cap S_1|).$$

Part (2) of the proposition will be a consequence of the following "equidistribution" result.

Proposition 10.6. *For every $o \in O$, $|o \cap S_0| = |o \cap S_1|$.*

Indeed, this proposition implies that

$$\sum_{o\in O} d(o) = \sum_{o\in O} |o \cap S_0| = |S_0| = \lfloor q/6 \rfloor.$$

On the other hand, by (10-1), (10-2), and [Ulmer 2019, Theorem 8.3], recall that

$$\dim Ш(E) = \sum_{o\in O} d(o).$$

Hence we have $\dim Ш(E) = \lfloor q/6 \rfloor$, so that proving Proposition 10.6 will complete the proof of part (2) of Proposition 10.1.

Proof of Proposition 10.6. We begin the proof by making the action of $\langle p \rangle$ on S more explicit. Suppose that $(i, j) \in (I \times J)^{\mu_6}$ corresponds to $(b, a) \in S$ through the bijection (10-5) and that $p \cdot (i, j) = (pi, pj)$ corresponds to (b', a'). Then $b' = 6 - b$ and $6a' - b' \equiv p(6a - b) \pmod{6(q-1)}$, so that

$$a' \equiv pa - \frac{p+1}{6} b + 1 \pmod{q-1} \equiv \begin{cases} pa - \frac{p-5}{6} \pmod{q-1} & \text{if } b = 1, \\ pa - \frac{5p-1}{6} \pmod{q-1} & \text{if } b = 5. \end{cases}$$

We now divide the proof into two cases according to $q \pmod 6$. Suppose first that $q \equiv 1 \pmod 6$, so that $q = p^f$ with f even. Then using the last displayed formula, one finds that q acts on S by $(b, a) \mapsto (b', a')$ where $b' = b$ and

$$a' \equiv \begin{cases} a - \frac{q-1}{6} \pmod{q-1} & \text{if } b = 1, \\ a - \frac{5p-5}{6} \pmod{q-1} & \text{if } b = 5. \end{cases}$$

It follows that the orbits of $\langle q \rangle$ have size exactly 6, all elements of an orbit have the same value of b, and each orbit meets either S_0 or S_1 in exactly one point and does not meet the other. (If the constant value of b is 1, the orbit meets S_0 and if it is 5, the orbit meets S_1.) The orbits of $\langle p \rangle$ are unions of an even number of orbits of $\langle q \rangle$, half of them meeting S_0 and half of them meeting S_1. It follows that $|o \cap S_0| = |o \cap S_1|$ for all orbits o of $\langle p \rangle$. This completes the proof in the case when $q \equiv 1 \pmod 6$.

Now assume that $q \equiv -1 \pmod 6$, so that $q = p^f$ with f odd. In this case, q acts on S by $(b, a) \mapsto (b', a')$ where $b' = 6 - b$ and

$$a' \equiv \begin{cases} a - \frac{q-5}{6} \pmod{q-1} & \text{if } b = 1, \\ a - \frac{5q-1}{6} \pmod{q-1} & \text{if } b = 5. \end{cases}$$

Note that q interchanges the subsets S_0 and S_1, so every orbit of $\langle q \rangle$ on S meets S_0 and S_1 in the same number of points. Since the orbits of $\langle p \rangle$ are unions of orbits of $\langle q \rangle$, it follows that the orbits o of $\langle p \rangle$ satisfy $|o \cap S_0| = |o \cap S_1|$. This completes the proof in the case $q \equiv -1 \pmod 6$, and thus in general. □

11. Archimedean size of $L^*(E)$ and the Brauer–Siegel ratio

Define the exponential differential height of $E = E_{q,r}$ by $H(E) := r^{\deg(\omega_E)}$. As we have seen in Section 2.1, one has $H(E) = r^{\lceil q/6 \rceil}$. Following Hindry and Pacheco [2016], consider the Brauer–Siegel ratio $\mathrm{BS}(E)$ of E:

$$\mathrm{BS}(E) := \frac{\log(\mathrm{Reg}(E)\,|Ш(E)|)}{\log H(E)}.$$

(By Theorem 8.2, $Ш(E)$ is finite so this quantity makes sense). Our goal in this section is to estimate the size of the Brauer–Siegel ratio of $E_{q,r}$ for a fixed r as $q \to \infty$. Here is the statement.

Theorem 11.1. *For a fixed r, as $q \to \infty$ runs through powers of p, one has*

$$\lim_{q\to\infty} \mathrm{BS}(E_{q,r}) = 1.$$

We will actually prove a slightly more precise estimate; namely,

$$\frac{\log(\mathrm{Reg}(E)\,|Ш(E)|)}{\log r} = \frac{q}{6}\left(1 + O\left(\frac{\log\log q}{\log q}\right)\right).$$

Thus for large q, the product $\mathrm{Reg}(E)\,|Ш(E)|$ is of size comparable to $r^{q/6}$. In the case when $p \equiv -1 \pmod 6$ we already know this fact, at least for large enough r (see Corollary 9.2(3)). On the other hand, in the case when $p \equiv 1 \pmod 6$, we know from Proposition 8.3.1(4) that $\mathrm{Reg}(E) = 1$, so we deduce that $|Ш(E)|$ is "large" (of size comparable to $r^{q/6}$).

We saw in (8-1) that

$$L^*(E) = \frac{\mathrm{Reg}(E)\,|Ш(E)|}{H(E)r^{-1}} = \frac{\mathrm{Reg}(E)\,|Ш(E)|}{r^{\lfloor q/6 \rfloor}},$$

so, given the definition of $\mathrm{BS}(E)$, the above theorem will be an immediate consequence of the following one, which is the main result of this section.

Theorem 11.2. *For a fixed r, as $q \to \infty$ runs through powers of p, one has*

$$\lim_{q\to\infty} \frac{\log L^*(E_{q,r})}{q} = 0.$$

To prove this we estimate $\log L^*(E_{q,r})$ from above and from below. While the upper bound is relatively easy to show, proving the required lower bound is more demanding. Before we prove the theorem at the end of this section, we first collect various intermediate results in the next few subsections.

11.3. ***Explicit special value.*** Recall from Theorem 4.1 that

$$L(E,s) = \prod_{o \in O^\times_{r,6,q}} (1 - G(\pi_2(o))^{m_2(o)} G(\pi_3(o)) r^{-s|o|}),$$

where $O^\times_{r,6,q}$ denotes the set of orbits of $\langle r \rangle$ acting on $(\mathbb{Z}/6\mathbb{Z})^\times \times {\mathbb{F}_q}^\times$. To lighten notation we write

$$\omega(o) := G(\pi_2(o))^{m_2(o)} G(\pi_3(o))$$

for the remainder of the article. Note that $\omega(o)$ is a Weil integer of size $p^{v|o|} = r^{|o|}$, where a "Weil integer of size p^c" is an algebraic integer whose absolute value in every complex embedding is p^c.

We partition $O^\times := O^\times_{r,6,q}$ as $O^\times = O_1^\times \cup O_2^\times$ where $O_1^\times$ consists of those orbits o such that $\omega(o) = r^{|o|}$. Thus the orbits in $O_1^\times$ are the ones contributing zeroes at $T = r^{-1}$ to the L-function. In particular, we have $\left|O_1^\times\right| = \operatorname{Rank} E(K)$ by our BSD result (Theorem 8.2). From the definition of special value (see Section 8.1), it is a simple exercise to see that

$$L^*(E) = \prod_{o \in O_1^\times} |o| \prod_{o \in O_2^\times} \left(1 - \frac{\omega(o)}{r^{|o|}}\right). \tag{11-1}$$

11.4. ***Estimates for orbits.*** Let us gather here a few estimates to be used below. Although we only need the case $n = 6$ in this paper, we work in more generality for future use.

Lemma 11.4.1. *Let p be a prime number, let q and r be powers of p, and let n be an integer prime to p. Let $S^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times \mathbb{F}_q^\times$ and let $O^\times$ denote the set of orbits of $\langle r \rangle$ on $S^\times$. Then*

(1) $\sum_{o \in O^\times} |o| = \left|S^\times\right| = \phi(n)(q-1)$,

(2) $\sum_{o \in O^\times} 1 = \left|O^\times\right| \ll q/\log q$,

(3) $\sum_{o \in O^\times} \log|o| \ll q \log\log q / \log q$.

The implied constants depend only on r and n.

Proof. By general properties of group actions, $S^\times$ decomposes as the disjoint union of orbits $o \in O^\times$; this yields (1). To prove (2), we study "long" orbits and "short" orbits separately. Let $x \geq 1$ be a parameter to be chosen later. Then

$$\left|\{o \in O^\times : |o| > x\}\right| = \sum_{\substack{o \in O^\times \\ |o| > x}} 1 \leq \sum_{\substack{o \in O^\times \\ |o| > x}} \frac{|o|}{x} \leq \frac{1}{x} \sum_{o \in O^\times} |o| = \frac{\left|S^\times\right|}{x}.$$

Let $o \in O^\times$ be the orbit through (i, α). As was noted in Section 3.7, $|o| \geq [\mathbb{F}_r(\alpha) : \mathbb{F}_r]$. In particular, $\left|\{o \in O^\times : |o| \leq x\}\right|$ is at most $\left|\{\alpha \in \overline{\mathbb{F}}_p : [\mathbb{F}_r(\alpha) : \mathbb{F}_r] \leq x\}\right|$. An element $\alpha \in \overline{\mathbb{F}}_p$ has degree $\leq x$ over $\mathbb{F}_r$ if and only if its monic minimal polynomial

has degree $\leq x$. The prime number theorem for $\mathbb{F}_r[t]$ implies that there are at most $c_r r^x/x$ monic irreducible polynomials of degree $\leq x$ in $\mathbb{F}_r[t]$ (see [Rosen 2002, Theorem 2.2]) for some constant $c_r > 0$ depending at most on r. This argument yields that $|\{o \in O^\times : |o| \leq x\}| \leq c_r r^x/x$. Adding the two contributions, and choosing $x = \log q/\log r$, we find that $|O^\times| \leq c'q/\log q$ where c' depends only on r and n.

Let us finally turn to the proof of (3): given a parameter $y \geq 1$, we have

$$\sum_{o\in O^\times} \log|o| = \sum_{|o|\leq y} \log|o| + \sum_{|o|>y} \log|o| \leq \log y \sum_{|o|\leq y} 1 + \sum_{|o|>y} \frac{\log|o|}{|o|}|o|$$
$$\leq \log y \sum_{o\in O^\times} 1 + \frac{\log y}{y} \sum_{|o|>y} |o| \leq \log y|O^\times| + \frac{\log y}{y}|S^\times|,$$

because $x \mapsto (\log x)/x$ is decreasing on (e, ∞). Upon using (2) and choosing $y = \log q$, one finds that $\sum_{o\in O^\times} \log|o| \leq c''q \log\log q/\log q$, where c'' depends only on r and n. This is the desired estimate. □

11.5. ***Linear forms in logarithms.*** For the convenience of the reader, we quote a special case of the main result of [Baker and Wüstholz 1993] about $\mathbb{Z}$-linear forms in logarithms of algebraic numbers. Choose once and for all an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and fix the branch of the complex logarithm $\log : \mathbb{C} \to \mathbb{C}$ with the imaginary part of $\log z$ in $(-\pi, \pi]$ for all $z \in \mathbb{C}$. In particular, if $|z| = 1$, then $|\log(z)| \leq \pi$ and $\log(-1) = i\pi$. Define the modified height ht'_F as follows: For a number field F and $\alpha \in F$, put

$$ht'_F(\alpha) := \frac{1}{[F : \mathbb{Q}]} \max\{ht_F(\alpha), |\log\alpha|, 1\},$$

where $ht_F(\alpha)$ denotes the usual logarithmic Weil height of α (relative to F); see [Hindry and Silverman 2000, B.2].

Let α_1, α_2 be two algebraic numbers (not 0 or 1) and denote by $\log\alpha_1$, $\log\alpha_2$ their logarithms. Let $F \subset \overline{\mathbb{Q}}$ be the number field generated by α_1, α_2 over $\mathbb{Q}$, and let $d := [F : \mathbb{Q}]$. Let $B = (b_1, b_2)$ with $b_1, b_2 \in \mathbb{Z}$ not both zero and set $ht'(B) := \max\{ht_{\mathbb{Q}}(b_1 : b_2), 1\}$, where $ht_{\mathbb{Q}}$ here denotes the logarithmic Weil height on $\mathbb{P}^1_{\mathbb{Q}}$ (relative to $\mathbb{Q}$). Note that $ht'(B) \leq \log\max\{|b_1|, |b_2|, e\}$.

With notation as above, let $\Lambda := b_1 \log\alpha_1 + b_2 \log\alpha_2 \in \mathbb{C}$. Then the Baker–Wüstholz theorem states that either $\Lambda = 0$ or

$$\log|\Lambda| > -c_d ht'_F(\alpha_1) ht'_F(\alpha_2) ht'(B), \tag{11-2}$$

where $c_d > 0$ is an explicit constant depending only on d.

We make use of the Baker–Wüstholz theorem to prove the following:

Theorem 11.6. *Let p be an odd prime number. Let $z \in \overline{\mathbb{Q}}$ be a Weil integer of size p^a, and let $\zeta \in \overline{\mathbb{Q}}$ be a root of unity. For any integer $L \neq 0$, either $\zeta(zp^{-a})^L = 1$ or*

$$\log\left|1 - \zeta(zp^{-a})^L\right| \geq -c_0 - c_1 \log|L|, \tag{11-3}$$

for some effective constants $c_0, c_1 > 0$ depending at most on p, a, the degree of z over $\mathbb{Q}$, and the order of ζ.

Proof. Let $F := \mathbb{Q}(\zeta, z)$ be the number field generated by ζ and z (viewed as a subfield of $\overline{\mathbb{Q}}$), and d be its degree over $\mathbb{Q}$. We begin by estimating the modified height of zp^{-a}. By assumption z is a Weil integer of size p^a. Straightforward estimates imply that the absolute logarithmic Weil height of zp^{-a} is at most $\log p^a$. Therefore,

$$ht'_F(zp^{-a}) \leq \max\left\{\log p^a, \frac{|\log(zp^{-a})|}{d}, \frac{1}{d}\right\} \leq \max\left\{\log p^a, \frac{\pi}{d}\right\},$$

We have used here that $|zp^{-a}| = 1$ in the chosen complex embedding.

For all $|x| \leq \pi/2$, we have $|\sin x| \geq \frac{2}{\pi}|x|$ and thus, for all $|\theta| \leq \pi$, we have

$$|1 - e^{i\theta}| = 2\left|\sin\frac{\theta}{2}\right| \geq \frac{2}{\pi}|\theta|.$$

If $0 < |\theta| < \pi$, this leads to $\log|1 - e^{i\theta}| \geq \log(2/\pi) + \log|\theta|$.

In the given complex embedding $F \subset \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, one can write $\zeta = e^{2\pi ik/n}$ for some $n \in \mathbb{Z}_{\geq 1}$ and $k \in \{1, \ldots, n-1\}$ coprime to n (so that ζ is a primitive n-th root of unity). There is also a unique angle $\phi \in (-\pi, \pi]$ such that $zp^{-a} = e^{i\phi}$. Let $L \neq 0$ be an integer. To prove the theorem, we may assume that $\zeta(zp^{-a})^L \neq 1$. Write

$$\zeta(zp^{-a})^L = e^{i(2\pi k/n + L\phi)} = e^{i\tilde{\theta}},$$

where $\tilde{\theta} \in (-\pi, \pi]$, and let m be the integer such that $2\pi k/n + L\phi = 2\pi m + \tilde{\theta}$. Note that $|m| \leq (|L| + 3)/2$. The trigonometric considerations above show that

$$\begin{aligned}\log\left|1 - \zeta(zp^{-a})^L\right| &= \log\left|1 - e^{i\tilde{\theta}}\right| \\ &\geq \log(2/\pi) + \log|\tilde{\theta}| \\ &= \log(2/\pi) + \log|2\pi k/n + L\phi - 2\pi m| \\ &= \log(2/(n\pi)) + \log|2\pi(k - nm) + Ln\phi|.\end{aligned}$$

Let us now consider the $\mathbb{Z}$-linear combination of logarithms of algebraic numbers

$$\Lambda := b_1 \log(-1) + b_2 \log(zp^{-a}),$$

where $B = (b_1, b_2) := (2(k - mn), nL) \neq (0, 0)$. Note that $\log(-1) = i\pi$ and $\log(zp^{-a}) = i\phi$, so that $\Lambda = i(2\pi(k - nm) + Ln\phi)$. By assumption, $\Lambda \neq 0$ so the

Baker–Wüstholz theorem (11-2) yields that

$$\log|\Lambda| \geq -c_d ht'_F(-1) ht'_F(zp^{-a}) ht'(B).$$

As was shown above,

$$ht'_F(zp^{-a}) \leq \max\{\log p^a, \pi/d\},$$

and one can easily see that $ht'_F(-1) = \pi/d$. Also, $ht'(B) \leq \log\max\{|b_1|, |b_2|, e\}$, where

$$|b_1| = |2(k - mn)| \leq 2n(1 + |m|) \leq (3 + |L|) \leq 3n|L|,$$

and $|b_2| = n|L|$, so that $ht'(B) \leq \log(3n|L|)$.

Putting these estimates together, we arrive at

$$\begin{aligned}\log\left|1 - \zeta(zp^{-a})^L\right| &\geq \log\frac{2}{n\pi} - c_d\frac{\pi}{d}\max\left\{\log p^a, \frac{\pi}{d}\right\}\log(3n|L|)\\ &\geq -c_0 - c_1\log|L|,\end{aligned}$$

where c_0 and c_1 are certain positive constants depending only on p, a, n, and d. This completes the proof of the theorem. □

We now apply this result to the situation at hand. For any orbit $o \in O^{\times}_{r,6,q}$, we deduce from Proposition 3.9 that we can write $G(\pi_2(o)) = \zeta_2 g_2^{|\pi_2(o)|\nu}$ where $\zeta_2 = \pm 1$, and $g_2 \in \mathbb{Q}(\mu_{2p})$ is a Weil integer of size $p^{1/2}$. Similarly, letting c be the order of p modulo 3, Proposition 3.9 implies that $G(\pi_3(o)) = \zeta_3 g_3^{|\pi_3(o)|\nu/c}$ where ζ_3 is a third root of unity and $g_3 \in \mathbb{Q}(\mu_{3p})$ is a Weil integer of size $p^{c/2}$. Since $m_2(o)|\pi_2(o)| = |o|$ and $|\pi_3(o)| = |o|$, and since $c \in \{1, 2\}$, we find that

$$\omega(o) = \zeta_2^{m_2(o)}\zeta_3(g_2^2 g_3^{2/c})^{|o|\nu/2}.$$

For any orbit $o \in O^{\times}$, it follows that $\omega(o)$ is of the form $\omega(o) = \zeta_o g_o^{|o|\nu/2}$ where $\zeta_o = \zeta_2^{m_2(o)}\zeta_3$ is a sixth root of unity and $g_o = g_2^2 g_3^{2/c} \in \mathbb{Q}(\mu_{6p})$ is a Weil integer of size p^2.

Using the previous theorem for $\zeta = \zeta_o$, $z = g_o$ (with $a = 2$) and $L = |o|\nu/2$, and setting $c_2 = c_0 + c_1\log(\nu/2)$, one obtains the following corollary:

Corollary 11.7. *For any orbit $o \in O^{\times}_{r,6,q}$, either $\omega(o)/r^{|o|} = 1$ (i.e., $o \in O_1^{\times}$) or*

$$\log\left|1 - \frac{\omega(o)}{r^{|o|}}\right| \geq -c_2 - c_1\log|o|.$$

11.8. ***Proof of Theorem 11.2.*** Recall that the theorem asserts that

$$\lim_{q\to\infty}\frac{\log L^*(E_{q,r})}{q} = 0.$$

We saw in (11-1) that

$$L^*(E_{q,r}) = \prod_{o\in O_1^\times} |o| \prod_{o\in O_2^\times} \left(1 - \frac{\omega(o)}{r^{|o|}}\right),$$

where $O_1^\times \subset O_{r,6,q}^\times$ consists of those orbits o such that $\omega(o) = r^{|o|}$ and $O_2^\times = O_{r,6,q}^\times \smallsetminus O_1^\times$.

It is clear that $|1 - \omega(o)/r^{|o|}| \le 2$ for all $o \in O^\times$. We can thus bound $\log L^*(E)$ from above as follows:

$$\log L^*(E_{q,r}) = \log\left(\prod_{o\in O_1^\times} |o| \prod_{o\in O_2^\times} \left(1 - \frac{\omega(o)}{r^{|o|}}\right)\right) \le \sum_{o\in O_1^\times} \log|o| + \sum_{o\in O_2^\times} \log 2$$
$$\ll \frac{q\log\log q}{\log q} + \frac{q}{\log q}\log 2 \ll \frac{q\log\log q}{\log q},$$

where we made use of Lemma 11.4.1 in the last step. Thus

$$\limsup_{q\to\infty} \frac{\log L^*(E_{q,r})}{q} \ll \limsup_{q\to\infty}\left(\frac{\log\log q}{\log q}\right) = 0.$$

We now turn to a lower bound. We obtain from Corollary 11.7 that

$$\log L^*(E_{q,r}) = \log\left(\prod_{o\in O_1^\times} |o| \prod_{o\in O_2^\times} \left(1 - \frac{\omega(o)}{r^{|o|}}\right)\right)$$
$$\ge \sum_{o\in O_1^\times} \log|o| + \sum_{o\in O_2^\times} (-c_2 - c_1\log|o|)$$
$$\gg -\frac{q}{\log q} - \frac{q\log\log q}{\log q} \gg -\frac{q\log\log q}{\log q},$$

using Lemma 11.4.1 again for the penultimate inequality. Therefore

$$\liminf_{q\to\infty} \frac{\log L^*(E_{q,r})}{q} \gg \liminf_{q\to\infty}\left(-\frac{\log\log q}{\log q}\right) = 0.$$

Combining the upper and lower bounds, we finally obtain that

$$\lim_{q\to\infty} \frac{\log L^*(E_{q,r})}{q} = 0,$$

and this completes the proof of Theorem 11.2. □

As a direct consequence of Corollary 9.2(1) and Theorem 11.1, we obtain the following.

Corollary 11.9. *Assume that* $p \equiv 1 \pmod 6$. *As* $q \to \infty$, *we have* $|Ш(E)[p^\infty]| = 1$ *and*

$$|Ш(E)| \ge H(E)^{1+o(1)} = r^{\frac{q}{6}(1+o(1))}.$$

Acknowledgements

Griffon is supported by the Swiss National Science Foundation (SNSF Professorship #170565 awarded to Pierre Le Boudec), and received additional funding from ANR grant ANR-17-CE40-0012 (FLAIR). Ulmer is partially supported by grant 359573 from the Simons Foundation. Both authors thank the anonymous referee for a very careful reading of the paper and several valuable suggestions.

References

[Baker and Wüstholz 1993] A. Baker and G. Wüstholz, "Logarithmic forms and group varieties", *J. Reine Angew. Math.* **442** (1993), 19–62. MR Zbl

[Cohen 2007] H. Cohen, *Number theory*, vol. I: Tools and Diophantine equations, Graduate Texts in Mathematics **239**, Springer, 2007. MR Zbl

[Gordon 1979] W. J. Gordon, "Linking the conjectures of Artin–Tate and Birch–Swinnerton-Dyer", *Compositio Math.* **38**:2 (1979), 163–199. MR Zbl

[Griffon 2019] R. Griffon, "Bounds on special values of L-functions of elliptic curves in an Artin–Schreier family", *Eur. J. Math.* **5**:2 (2019), 476–517. MR Zbl

[Hindry and Pacheco 2016] M. Hindry and A. Pacheco, "An analogue of the Brauer–Siegel theorem for abelian varieties in positive characteristic", *Mosc. Math. J.* **16**:1 (2016), 45–93. MR Zbl

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Graduate Texts in Mathematics **201**, Springer, 2000. MR Zbl

[Kato and Trihan 2003] K. Kato and F. Trihan, "On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$", *Invent. Math.* **153**:3 (2003), 537–592. MR Zbl

[Katz 1981] N. M. Katz, "Crystalline cohomology, Dieudonné modules, and Jacobi sums", pp. 165–246 in *Automorphic forms, representation theory and arithmetic* (Bombay, 1979), Tata Inst. Fund. Res. Studies in Math. **10**, Tata Inst. Fundamental Res., Bombay, 1981. MR Zbl

[Kleiman 1968] S. L. Kleiman, "Algebraic cycles and the Weil conjectures", pp. 359–386 in *Dix exposés sur la cohomologie des schémas*, Adv. Stud. Pure Math. **3**, North-Holland, Amsterdam, 1968. MR Zbl

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

[Néron 1965] A. Néron, "Quasi-fonctions et hauteurs sur les variétés abéliennes", *Ann. of Math.* (2) **82** (1965), 249–331. MR Zbl

[Pries and Ulmer 2016] R. Pries and D. Ulmer, "Arithmetic of abelian varieties in Artin–Schreier extensions", *Trans. Amer. Math. Soc.* **368**:12 (2016), 8553–8595. MR Zbl

[Rosen 2002] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics **210**, Springer, 2002. MR Zbl

[Shioda 1986] T. Shioda, "An explicit algorithm for computing the Picard number of certain algebraic surfaces", *Amer. J. Math.* **108**:2 (1986), 415–432. MR Zbl

[Shioda 1992] T. Shioda, "Some remarks on elliptic curves over function fields", pp. 99–114 in *Journées Arithmétiques* (Geneva, 1991), Astérisque **209**, Soc. Math. France, Paris, 1992. MR Zbl

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994. MR Zbl

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, 2009. MR Zbl

[Tate 1966] J. Tate, "On the conjectures of Birch and Swinnerton-Dyer and a geometric analog", exposé 306 in *Séminaire Bourbaki* 1965/1966, W. A. Benjamin, Amsterdam, 1966. Reprinted as pp. 415–440 in *Séminaire Bourbaki* **9**, Soc. Math. France, Paris, 1995. MR Zbl

[Ulmer 2002] D. Ulmer, "Elliptic curves with large rank over function fields", *Ann. of Math.* (2) **155**:1 (2002), 295–315. MR Zbl

[Ulmer 2007] D. Ulmer, "L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields", *Invent. Math.* **167**:2 (2007), 379–408. MR Zbl

[Ulmer 2011] D. Ulmer, "Elliptic curves over function fields", pp. 211–280 in *Arithmetic of L-functions*, edited by C. Popescu et al., IAS/Park City Math. Ser. **18**, Amer. Math. Soc., Providence, RI, 2011. MR Zbl

[Ulmer 2019] D. Ulmer, "On the Brauer–Siegel ratio for abelian varieties over function fields", *Algebra Number Theory* **13**:5 (2019), 1069–1120. MR Zbl

[Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, 1997. MR Zbl

Received May 29, 2019. Revised November 11, 2019.

RICHARD GRIFFON
DEPARTEMENT MATHEMATIK UND INFORMATIK UNIVERSITÄT BASEL
SPIEGELGASSE
BASEL
SWITZERLAND
richard.griffon@unibas.ch

DOUGLAS ULMER
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ARIZONA
TUCSON, AZ 85721-0089
UNITED STATES
ulmer@math.arizona.edu