On the arithmetic of a family of superelliptic curves

Sarah Arpin, Richard Griffon, Libby Taylor, and Nicholas Triantafillou

May 7, 2021

Abstract

Let p be a prime, let r and q be powers of p, and let a and b be relatively prime integers not divisible by p. Let $C/\mathbb{F}_r(t)$ be the superelliptic curve with affine equation $y^b + x^a = t^q - t$. Let J be the Jacobian of C. By work of Pries–Ulmer [PU16], J satisfies the Birch and Swinnerton-Dyer conjecture (BSD). Generalizing work of Griffon–Ulmer [GU20], we compute the L-function of J in terms of certain Gauss sums. In addition, we estimate several arithmetic invariants of J appearing in BSD, including the rank of the Mordell–Weil group $J(\mathbb{F}_r(t))$, the Faltings height of J, and the Tamagawa numbers of J in terms of the parameters a, b, q. For any p and r, we show that for certain a and b depending only on p and r, these Jacobians provide new examples of families of simple abelian varieties of fixed dimension and with unbounded analytic and algebraic rank as q varies through powers of p. Under a different set of criteria on a and b, we prove that the order of the Tate–Shafarevich group $Ш(J)$ is "large" as $q \to \infty$.

1 Introduction

Let p be a prime number, let r be a power of p, let $\mathbb{F}_r$ denote the finite field with r elements, and let $K = \mathbb{F}_r(t)$. Let J/K be a principally polarized abelian variety of dimension g.

The Birch and Swinnerton-Dyer conjecture (abbreviated as BSD in what follows) is a sweeping statement that predicts a relationship between several important analytic and arithmetic quantities associated to J. On the analytic side, the central object of study is the L-function $L(J, T)$, a meromorphic function on the complex plane which encodes the action of Frobenius elements.

The order of vanishing $\operatorname{ord}_{T=r^{-1}} L(J, T)$ of $L(J, T)$ at the 'central point' and the leading coefficient $L^*(J)$ of $L(J, T)$ expanded as a power series at $T = r^{-1}$ are of particular interest. On the arithmetic side, $J(K)$ is a finitely-generated abelian group by the Mordell–Weil theorem. Its rank, $\operatorname{rank} J(K) := \dim_{\mathbb{Q}} J(K) \otimes \mathbb{Q}$ is conjectured to equal $\operatorname{ord}_{T=r^{-1}} L(J, T)$. Other terms include the size of the torsion subgroup $J(K)_{\mathrm{tors}}$, the regulator $\operatorname{Reg}(J)$, the Tate–Shafarevich group $Ш(J)$, the local Tamagawa numbers $c_v(J)$, and the exponential Faltings height $H(J)$. In this article, we study the BSD invariants for a family of abelian varieties J/K, which we now describe.

Let q be a power of p and let $a, b \geq 1$ be coprime integers which are both coprime to p. Let C/K be the unique (up to isomorphism) smooth projective curve containing the affine curve defined by

$$y^b + x^a = t^q - t \tag{1.1}$$

as a dense open subset. The curve C is a cyclic Galois cover of $\mathbb{P}^1$, i.e. a *superelliptic* curve. Let J be the Jacobian of C. Since J satisfies BSD by [PU16, Corollary 3.1.4], it is particularly interesting to study its L-function and BSD invariants.

Our main results include: an explicit formula for $L(J, T)$ in terms of Gauss sums, an analogue of the Brauer–Siegel theorem relating the asymptotic growth of $Ш(J), \operatorname{Reg}(J)$, and $H(J)$ for J, and a criterion on a and b depending only on r so that $\operatorname{rank} J(K)$ grows quasi-linearly in q. This

last result provides new explicit examples of families of simple abelian varieties of fixed dimension, but unbounded rank. Under different criteria on a and b, we prove that $\operatorname{rank} J(K) = 0$ and (via our Brauer–Siegel analogue for J) that the order of the Tate–Shafarevich group $Ш(J)$ is unbounded as $q \to \infty$. In fact, by computing the Faltings height $H(J)$, we are able to provide explicit asymptotics for $Ш(J) \cdot \operatorname{Reg}(J)$ more generally.

We also study a number of other arithmetic and geometric properties of J. For instance, we show that J is simple if and only if a and b are both primes. We also compute the minimal proper regular simple normal crossings model of J (using the method described in [Dok20]) and apply it to show that at any place v of bad reduction, J has totally unipotent reduction, to determine the Tamagawa numbers c_v of J are all equal to 1, to compute the conductor $N(J)$, and to give an explicit formula for the the Faltings height of J.

In the interest of giving a self-contained treatment, we also include a proof of the Birch and Swinnerton-Dyer conjecture for J using work of Shioda [Shi86]. In that article, Shioda introduces a powerful way of producing abelian varieties that satisfy the Birch and Swinnerton-Dyer conjecture; he proves that if C is a curve over a function field $\mathbb{F}_q(t)$ whose associated surface over $\mathbb{F}_q$ is dominated by a product of curves, then $\operatorname{Jac}(C)$ satisfies BSD. Using this method, we conclude:

Theorem 1.1. *The Jacobian J of C satisfies the Birch and Swinnerton-Dyer conjecture. That is:*

- *The algebraic and analytic ranks of J coincide:* $\operatorname{ord}_{T=r^{-1}} L(J,T) = \operatorname{rank} J(K)$.
- *The Tate–Shafarevich group $Ш(J)$ is finite.*
- *The BSD formula holds:*

$$L^*(J) = \frac{|Ш(J)| \operatorname{Reg}(J) \prod_v c_v(J)}{H(J)\, r^{-g}\, |J(K)_{\mathrm{tors}}|^2}, \tag{1.2}$$

where the $c_v(J)$ are the local Tamagawa numbers of J and $\operatorname{Reg}(J)$ is the regulator.

The statement of BSD opens up a powerful analytic approach to computing $\operatorname{rank} J(K)$. The strategy is to determine the L-function sufficiently explicitly so that one can compute/bound $\operatorname{ord}_{T=r^{-1}} L(J,T)$. In several cases, this strategy has led to new families of abelian varieties of fixed dimension but with unbounded rank. In [Ulm02], Ulmer used this strategy to produce the first non-isotrival families of elliptic curves over $\mathbb{F}_p(t)$ satisfying BSD and with arbitrarily large analytic rank. (Isotrivial families of elliptic curves over $\mathbb{F}_p(t)$ with unbounded rank had previously been constructed by more algebraic methods in [TS67].) In [Ulm06], Ulmer proves an analogue of the previous results for abelian varieties of larger dimension; in particular, he proves that for every $g > 0$ and for ever prime p, there is an absolutely simple, non-isotrivial abelian variety of dimension g over $\mathbb{F}_p(t)$ satisfying BSD and of arbitrarily large analytic rank. These two papers use Kummer towers of field extensions to produce the abelian varieties. In [BHP+15], the authors prove similar results for another family of curves over function fields. They develop new algebro-geometric techniques involving explicit subgroups of divisors on the Jacobian over towers of function fields, expanding the tools used to study curves of arbitrary genus over function fields.

Other work has studied ranks of Jacobians of curves when the field varies in Artin–Schreier towers, which corresponds to varying q in our setup. For instance, given rational functions $f, g \in \mathbb{F}_r(t)$, [PU16] includes a study of curves with affine model $f(x) - g(y) = t^q - t$. Under genericity conditions on f and g, including critical points having multiplicity 1 and restrictions on the order of poles, they prove that the rank of the Jacobian is unbounded as q varies through powers of p. The case $f(x) = x^2$ satisfies their genericity assumptions, so their work applies to generic hyperelliptic curves. However, the critical points of $f(x) = x^a$ are not generic when $a > 2$, so their work does

not apply to most superelliptic curves. In fact, [PU16] shows that many families of superelliptic curves over $\mathbb{F}_r(t)$ have Jacobians with bounded rank as q varies. More recently, [GU20] studied the family of elliptic (and superelliptic) curves with affine model $y^2 = x^3 + t^q - t$. In this case, they show that the behavior of the rank is either 0 or unbounded as q varies, depending only on the congruence class of p modulo 6.

In this article, we generalize the work of [GU20], showing that the rank of J is sometimes 0 and sometimes unbounded as q varies, depending on r, a and b. To state our results, we define $o_p(n)$ to be the order of p in $\mathbb{Z}/n\mathbb{Z}$ and recall that an integer n is said to be *supersingular* for p if some power of p is congruent to -1 modulo n. Note that if n is supersingular for p, then $o_p(n)$ is automatically even.

In Section 6.4, we prove:

Theorem 1.2. *Suppose that the pair (a, b) satisfies one of the following:*

(1) $a\, o_p(a)$ and $b\, o_p(b)$ are relatively prime,

(2) $a\, o_p(a)$ is odd, and b is supersingular for p,

(3) a is supersingular for p, and $b\, o_p(b)$ is odd.

Then, for any power q of p, we have $\operatorname{ord}_{T=r^{-1}} L(J, T) = \operatorname{rank} J(K) = 0$.

For any prime p, the hypotheses of Theorem 1.2 are satisfied for infinitely many pairs of primes a, b, as we show in Lemma 6.14. In Section 6.5, we prove:

Theorem 1.3. *Let $p \neq 2$ be an odd prime. Let a and b be relatively prime positive integers which are both supersingular for p. Let $\nu_a, \nu_b \geq 1$ be the least positive integers such that $p^{\nu_a} \equiv -1 \pmod{a}$ and $p^{\nu_b} \equiv -1 \pmod{b}$. Suppose also that $[\mathbb{F}_r : \mathbb{F}_p]$ is a multiple of both $4\nu_a$ and $4\nu_b$.*

Then, we have

$$(a-1)(b-1)\left\lceil \frac{1}{\log_p(q)} \left(\frac{q-1}{ab} - \frac{p\sqrt{q}-1}{p-1} \right) \right\rceil \leq \operatorname{rank} J(K)\,.$$

For any p, there are infinitely many pairs of primes a, b satisfying the hypotheses of Theorem 1.3. Fixing such a pair, as q varies among powers of p, Theorem 1.3 gives a family of Jacobians of fixed dimension satisfying BSD with unbounded rank. When a and b are both prime, Theorem 1.3 actually gives a family of *simple* abelian varieties with these properties, which we prove in Section 2.6:

Theorem 1.4. *The Jacobian of $y^b + x^a = t^q - t$ is simple over $\mathbb{F}_r(t)$ if and only if both a and b are prime.*

Our other major results focus on understanding the BSD invariants and other properties of C and J via their geometry. Most notably, we show that many of these Jacobians are simple abelian varieties with Tate–Shafarevich group unbounded as q varies. Recall that $H(J)$ is the exponential Faltings height of J. In Section 8, we prove that for infinitely many a, b, the size of $Ш(J)$ is asymptotic to $H(J)$.

Theorem 1.5. *Fix parameters a, b which satisfy the hypotheses of Theorem 1.2. Then, as q runs through powers of p, we have*

$$|Ш(J)| = H(J)^{1+o(1)}.$$

Moreover, in Lemma 2.7 we show that there is a positive constant D depending only on a and b and a positive constant E depending only on a, b, and $q \mod ab$ such that $H(J) = r^{Dq+E}$. In particular, the order of $Ш(J)$ grows exponentially in q as q varies.

This result generalizes [GdW21], which exhibits sequences of elliptic curves over $\mathbb{F}_q(t)$ with arbitrarily large Tate–Shafarevich group, to simple abelian varieties of dimension greater than 1.

We remark briefly that in contrast to our results in the function field setting, much less is known over number fields, and especially over $\mathbb{Q}$. Work of Clark and Sharif [CS10] (in the elliptic curve case) and of Creutz [Cre11] (in the higher-dimensional case, building on previous work of Clark) shows that all principally polarized abelian varieties satisfying a certain technical hypothesis have arbitrarily large Ш after a suitable extension of the base field. If one restricts the ground field to $\mathbb{Q}$, work of Cassels in the 1960s [Cas64] showed that when $A/\mathbb{Q}$ is an elliptic curve, $Ш(A/\mathbb{Q})$ can be arbitrarily large. Recent work of Flynn [Fly18] extends this to abelian surfaces, but it is not known whether $Ш(A/\mathbb{Q})$ can be arbitrarily large when A is a simple abelian variety of dimension greater than 2.

In contrast, in the function field setting, our results give new examples of simple, principally polarized abelian varieties A of arbitrarily large dimension over $\mathbb{F}_p(t)$ and with $Ш(A/\mathbb{F}_p(t))$ arbitrarily large. Previously, the only known examples of such abelian varieties appeared in work of Ulmer [Ulm19].

The proof of Theorem 1.5 contains several statements which are of interest in their own right. For instance, in Section 7, we describe the asymptotics of the special value of the L-function as $q \to \infty$ via analytic methods, generalizing results from [GU20] in the elliptic curve case. We prove:

Theorem 1.6. *For fixed a, b, as $q \to \infty$ runs through powers of p,*

$$\frac{\log L^*(J)}{\log H(J)} = o(1).$$

In particular, note that this theorem does not require special assumptions on a and b.

On the algebraic side, we are able to compute many BSD invariants of J by studying the geometry of C. To begin, we use recent machinery from [Dok20] to compute the minimal regular proper simple normal crossings model of our curves at any place of bad reduction. In our case, the special fibers of these models have a very simple structure — all irreducible components have genus 0 and the dual graph is a tree. From this information, we are able to conclude that J has unipotent reduction at all bad places and that the local Tamagawa numbers $c_v(J)$ of J are all equal to 1, and to compute the conductor divisor of J. We also leverage the recipe from [Dok20] to compute a formula for the Faltings height $H(J)$ in Lemma 2.7.

Combining these computations with Theorem 1.6, we deduce an analogue of the Brauer–Siegel theorem for the family of Jacobians $(J_{a,b,q})_q$. (See [HP16] for a nice explanation of the connection with Brauer–Siegel.) In Section 7.3 we prove:

Corollary 1.7. *For fixed a, b, as $q \to \infty$ runs through powers of p,*

$$\log\big(|Ш(J)|\operatorname{Reg}(J)\big) \sim \log H(J).$$

Theorem 1.5 follows since $\operatorname{Reg}(J) = 1$ when $\operatorname{rank} J(K) = 0$.

Several sequences of elliptic curves are known to satisfy a similar asymptotic description of $|Ш(A)|\operatorname{Reg}(A)$ in terms of the height $H(A)$ as in Corollary 1.7. (For instance, see [HP16, Gri16, Gri18, Gri19, GU20].) However, similar results for simple abelian varieties of higher dimension are much rarer. The only previous examples we are aware of appear in [Ulm19, §10.4, §11.4].

1.1 Roadmap to this article.

The paper is organized as follows. In Section 2, we study the geometry of C and use work in [Dok20] to compute the minimal regular proper simple normal crossings model of our curves. This model is used to compute the reduction types, Tamagawa numbers, and Faltings height of these curves. We also prove Theorem 1.4 on the simplicity of J in Section 2. In Section 3, we recall classical results on Gauss sums which will be used in the computation of the L-function. In Section 4, we give an explicit computation for the L-function of the Jacobian in terms of the valuations of some associated Gauss sums. In Section 5, we prove that our Jacobians satisfy BSD. In Section 6, we use p-adic valuations of Gauss sums to prove estimates on rank $J(K)$ in Theorems 1.2 and 1.3. In Section 7 we prove our asymptotic formula for $L^*(J)$ in Theorem 1.6 and our analogue of Brauer–Siegel in Corollary 1.7. Finally, in Section 8, we prove Theorem 1.5 giving infinitely many families of simple abelian varieties with unbounded Ш(J) as q varies.

General notation and conventions For two functions f, g of a variable x on $[0, \infty)$, we use Vinogradov's notation $f(x) \ll_a g(x)$ to mean that there is a constant $C > 0$ (depending at most on the mentioned parameter(s) a) such that $|f(x)| \leq Cg(x)$ for $x \to \infty$.

There is a list of notation provided in Appendix A.

Acknowledgements

We thank the AMS and the organizers of the 2019 Mathematics Research Communities workshop on *Explicit Methods in Characteristic p* for creating a productive working environment in which this project was started. We thank Douglas Ulmer for his guidance and support during the realization of this project, and for his helpful comments on a previous draft. Thanks are also due to Daniel Litt for providing help with the proof in Appendix B.

The second author was funded by the Swiss National Science Foundation through the SNSF Professorship #170565 awarded to Pierre Le Boudec, and received additional funding from ANR project ANR-17-CE40-0012 (FLAIR). The third author was supported by an NSF graduate research fellowship. The fourth author thanks the National Science Foundation Research Training Group in Algebra, Algebraic Geometry, and Number Theory at the University of Georgia [grant DMS-1344994] for funding this research.

2 Geometry of C and its Jacobian

Fix a prime p, and let r be a power of p. Let $\mathbb{F}_r$ be the finite field with r elements, and let $K := \mathbb{F}_r(t)$ denote the function field of the projective line $\mathbb{P}^1_{\mathbb{F}_r}$. When the field of definition is understood, we write $\mathbb{P}^1$ for $\mathbb{P}^1_{\mathbb{F}_r}$. For any power q of p, and any pair of relatively prime integers a, b which are both coprime to p, consider the superelliptic curve $C_{a,b,q}$ over K given by the affine model

$$C_{a,b,q}: \qquad y^b + x^a = t^q - t.$$

In other words, $C_{a,b,q}$ is the unique (up to a birational morphism) smooth projective curve over K which contains the affine curve $y^b + x^a = t^q - t$ as a dense open subset. Let $J_{a,b,q}$ denote the Jacobian variety of $C_{a,b,q}$, which is an abelian variety over K.

Throughout the paper, the curve $C_{a,b,q}$ is denoted by C, and its Jacobian $J_{a,b,q}$ by J. We suppress the "$/K$" in the notation for invariants of C and J, since both of these objects will only be studied over K.

Proposition 2.1. *The genus of the curve $C = C_{a,b,q}$ is $g = (a-1)(b-1)/2$.*

Proof. The result follows from a direct computation using the Hurwitz genus formula and the assumption that a and b are coprime. □

We prove various geometric properties about C and J in this section. In particular, we use the minimal proper regular SNC model of C to prove that J has totally unipotent reduction at each place of bad reduction. For more specific information about the reduction type in the elliptic curve case, see [GU20]. We also compute the height of J, and prove that it is K-simple for when both a and b are prime.

2.1 The minimal proper regular SNC model of C

In this section, we give a brief description of the minimal proper regular simple normal crossings model $\pi : \mathcal{S} \to \mathbb{P}^1$ of C using the recipe provided in [Dok20]. This description allows us to read off the reduction of the Jacobian of J at the places of bad reduction, which will in turn be necessary for the computation of the L-function. It is also useful for computing the Tamagawa numbers, exponential Faltings height, and conductor of J.

We will use notation from [Dok20] freely throughout this section. The results presented here could alternately be recovered via a toric resolution of singularities.

Recall the definition of a simple normal crossing model.

Definition 2.2. Let W be a variety with irreducible components $\{W_i : i \in I\}$. We say that W is a simple normal crossing variety if both

1. The W_i are all smooth, and
2. For every point $w \in W$ there are independent étale local parameters $x_1, x_2, \ldots, x_r \in \mathcal{O}_w$ such that $\prod_{i=1}^{r} x_i$ cuts out an étale open neighborhood $U_w \subset W$ containing w.

A simple normal crossing model of $C/\mathbb{P}^1$ is a model of C such that every fiber above every point $v \in \mathbb{P}^1$ is a simple normal crossing variety.

For $v \in \mathbb{P}^1$ a closed point, we now study the fiber $\mathcal{S}_v$ of $\pi : \mathcal{S} \to \mathbb{P}^1$. We will abuse notation slightly and say that $v \in \mathbb{F}_q \cup \{\infty\}$ if v decomposes into degree one points over the compositum $\mathbb{F}_r\mathbb{F}_q$. Equivalently, $v \in \mathbb{F}_q \cup \{\infty\}$ if v is fixed by the action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, on $\mathbb{P}^1$.

When $v \notin \mathbb{F}_q \cup \{\infty\} \subset \mathbb{P}^1$, the curve C has good reduction, so $\mathcal{S}_v$ is a smooth curve of genus g.

When $v \in \mathbb{F}_q \cup \{\infty\} \subset \mathbb{P}^1$, the curve C has bad reduction at v. Set $Q = 1$ if $v \in \mathbb{F}_q$ and $Q = -q$ if $v = \infty$. In the notation of [Dok20], the Newton polytopes associated to C at v are

$$\Delta = \text{convex hull}(\{(0,0),(a,0),(0,b)\}) \subset \mathbb{R}^2$$

and

$$\Delta_v = \text{lower convex hull}(\{(0,0,Q),(a,0,0),(0,b,0)\}) \subset \mathbb{R}^2 \times \mathbb{R}\,.$$

The polytope Δ_v consists of three 0-dimensional vertices $(a,0,0),(0,b,0)$, and $(0,0,Q)$; three 1-dimensional (open) edges

- L_3 connecting $(a,0,0)$ to $(0,b,0)$ with denominator $\delta_{L_3} = 1$,
- L_2 connecting $(0,b,0)$ to $(0,0,Q)$ with denominator $\delta_{L_2} = b$, and
- L_1 connecting $(a,0,0)$ to $(0,0,Q)$ with denominator $\delta_{L_1} = a$; and

a single 2-dimensional (open) face F with denominator $\delta_F = ab$. Moreover, $F(\mathbb{Z})_{\mathbb{Z}} \subset F \cap \mathbb{Z}^3 = \emptyset$, so $|F(\mathbb{Z})_{\mathbb{Z}}| = 0$. The face-polynomial X_F and the side polynomials X_{L_i} are all smooth, so C is Δ_v-regular, as defined in [Dok20, Definition 3.9]. As a result, we can read off the structure of $\mathcal{S}_v$ using [Dok20, Theorem 3.13].

We find that $\mathcal{S}_v$ consists of three chains of $\mathbb{P}^1$s (corresponding to the edges L_1, L_2, and L_3) branching off of a central curve corresponding to the face F. Since the interior of F contains no lattice points, $|F(\mathbb{Z})_{\mathbb{Z}}| = 0$. Moreover, $\delta_F = ab$, so the central curve has genus 0 and multiplicity ab. For $i = 1, 2, 3$, every curve in the chain of $\mathbb{P}^1$s corresponding to L_i has multiplicity a multiple of δ_i. The final curve in the chain has multiplicity exactly δ_i. For a more precise description of the multiplicities of the components, see [Dok20]. We give an examples of the resulting special fiber $\mathcal{S}_v$ when v is a finite place of bad reduction or $v = \infty$ in the case $a = 7, b = 5, q = 67$ in Figure 1.

For later use, we note that the final component in $\mathcal{S}_v$ of the chain corresponding to L_3 always has multiplicity 1. In particular, the gcd of the multiplicities of the components of $\mathcal{S}_v$ is 1. Writing K_v for the completion of K at v, this means that $\mathcal{S}_{K_v}$ is a Spec $\mathcal{O}_{K_v}$-curve (or S-curve) in the notation of [Lor90].

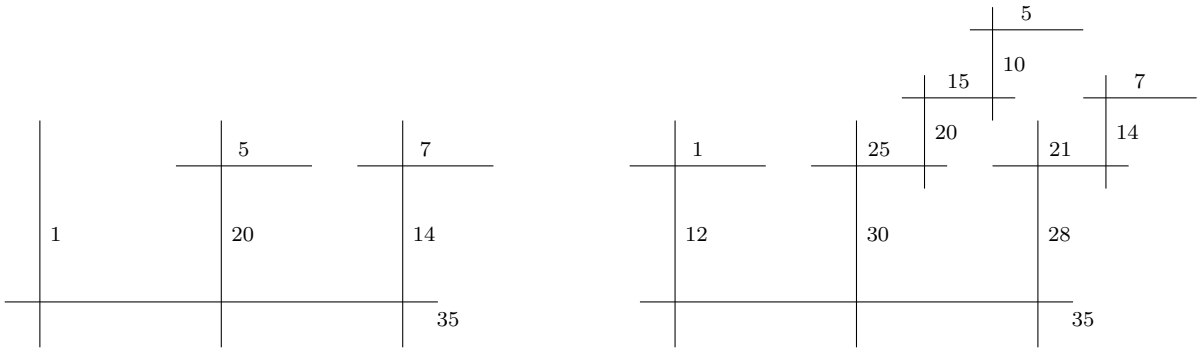

Figure 1: Fibers of the minimal proper regular SNC model of $y^5 + x^7 = t^{67} - t$ over $\mathbb{P}^1_{\mathbb{F}_{67}}$ at finite places of bad reduction (left) and at infinity (right)

2.2 Unipotent reduction of J at bad places.

We give an analysis of the reduction types of J at the finite places and the infinite place.

Proposition 2.3. *The Jacobian J has potentially good, totally unipotent reduction above any $t_0 \in \mathbb{F}_q \cup \{\infty\} \subset \mathbb{P}^1$, and it has good reduction elsewhere.*

Proof. The roots of $t^q - t$ lie in $\mathbb{F}_q$, so C has good reduction away from $\mathbb{F}_q \cup \{\infty\}$. Moreover, C is isotrivial and becomes isomorphic to $y^b + x^a = 1$ over $\mathbb{F}_r(\sqrt[ab]{t^q - t})$ so C has potentially good reduction everywhere.

In the remaining cases, we can read off the reduction of the Jacobian from the special fiber of the simple normal crossings model $\mathcal{S}$. Write $\mathcal{J}$ for the Néron model of J. Given a point $v \in \mathbb{P}^1$, let $\mathcal{J}_v^0$ denote the connected component of the identity of the fiber of $\mathcal{J}$ above v. We recall some facts on the structure of the fibers of $\mathcal{J}$ from Section 1 of [Lor90].

Above any point $v \in \mathbb{P}^1$, there is a unipotent group scheme U, a torus T and an abelian variety A fitting into the following exact sequence of group schemes over t_0:

$$0 \to U \times T \to \mathcal{J}_v^0 \to A \to 0\,.$$

Let $\mathcal{O}_v$ be the discrete valuation ring in the completion of $K = \mathbb{F}_r(t)$ at v. The fiber $\mathcal{S}_v$ of $\mathcal{S}$ above $\mathcal{O}_v$ is then a simple normal crossings model of a curve over $\mathrm{Frac}(\mathcal{O}_v)$.

In this situation, Corollary 1.4 of [Lor90] states that $\dim(T)$ is equal to the first Betti number of the dual graph of $\mathcal{S}_v$. The dual graph of $\mathcal{S}_v$ is a tree, so it has trivial homology. Hence, T is trivial.

Also, if $\mathcal{S}_v$ has irreducible components $C_1, \ldots, C_r$, then $\dim A = \sum_{i=1}^{r} \mathrm{genus}(C_i)$. For $v \in \mathbb{F}_q \cup \{\infty\}$, all of the components of $\mathcal{S}_v$ have genus 0, so $\dim A = 0$ as well.

In summary, for any place v of bad reduction for C, J_v is a unipotent group scheme, since both the toric and abelian parts are trivial. □

2.3 Tamagawa numbers of J.

From our description of the type of reduction of J at bad places, we now deduce an explicit expression for another important invariant of J — its Tamagawa number. First, recall the definition:

Definition 2.4 (Tamagawa Number)**.** For any place v of K, the *local Tamagawa number* $c_v(J)$ is defined to be the number of components of the minimal Néron model of J at v which are rational over the residue field of K at v. The *Tamagawa number* $\mathcal{T}(J/K)$ of J is defined as the product $\prod_v c_v(J)$ over all places of K.

Proposition 2.5. *For $J = J_{a,b,q}$, the Tamagawa number $\mathcal{T}(J/K)$ is equal to* 1.

This fact is used in Section 7.3.

Proof. If v is a place of good reduction for J, then $c_v(J) = 1$. Corollary 1.5 of [Lor90] allows us to compute the local Tamagawa numbers from the simple normal crossings models at the places of bad reduction. We recall this result here for convenience: If the special fiber of the SNC model is given by $\sum_{i=1}^{n} r_i C_i$, let $d_i := \sum_{i \neq j} C_i \cdot C_j$. If the associated Jacobian has toric dimension 0, the local Tamagawa number is given by

$$c_v(J) = \prod_{i=1}^{n} r_i^{d_i - 2}.$$

Proposition 2.3 says that $\mathcal{J}_v$ has toric dimension 0, so we may apply this result. We recall the relevant intersection numbers and multiplicities from Section 2.1. At each place of bad reduction, there is one fiber of multiplicity ab with 3 intersections, and three fibers of multiplicities a, b, and 1 with 1 intersection. All other fibers have 2 intersections, so the local Tamagawa number is $(ab)^1 a^{-1} b^{-1} 1^{-1} = 1$.

Since all of the local Tamagawa numbers are equal to 1, we conclude $\mathcal{T}(J/K) = 1$. □

2.4 Conductor of J

We also use the reduction type of J to compute the conductor divisor $N_J \in \mathrm{Div}(\mathbb{P}^1)$ of J/K in Proposition 2.6. In Section 4, we use this computation to verify the degree of $L(J, T)$.

We refer the reader to [Ser70] for the construction of N_J. Fix, once and for all, a prime $\ell \neq p$ and let $V = V_\ell(J)$ be the ℓ-adic Tate module of J viewed as a representation of $\mathrm{Gal}(\overline{K}/K)$. Given a place $v \in \mathbb{P}^1$, let I_v be the inertia subgroup and denote by V^{I_v} the subspace fixed by I_v.

Proposition 2.6. *The conductor N_J is an effective divisor on $\mathbb{P}^1$, supported on $\mathbb{F}_q \cup \{\infty\}$, with*

$$\deg N_J = (a-1)(b-1)(q+1) = 2g(q+1).$$

Proof. From the definition of N_J, we see that

$$\deg(N_J) = \sum_{v \text{ bad reduction}} (2g - \dim(V^{I_v})) \deg v \,.$$

By Proposition 2.3, the places of bad reduction of J are exactly those closed points v of $\mathbb{P}^1$ with $v \in \mathbb{F}_q \cup \{\infty\}$. At each of those places, the Jacobian J has unipotent reduction, hence V^{I_v} is trivial by [ST68, §3]. Therefore, $2g - \dim(V^{I_v}) = 2g$ at every such place v. So,

$$\sum_{v \text{ bad reduction}} (2g - \dim(V^{I_v})) \deg v = 2g \sum_{v \in \mathbb{F}_q \cup \{\infty\}} \deg v = 2g(q+1) \,.$$

□

2.5 Height of J

In this section, we compute the Faltings height of J. Let $\mathcal{J} \to \mathbb{P}^1$ be the (global) Néron model of $J/\mathbb{F}_r(t)$. Let $z : \mathbb{P}^1 \to \mathcal{J}$ be the identity section. Let $\Omega^g_{\mathcal{J}/\mathbb{P}^1}$ be the relative dualizing sheaf on $\mathcal{J}$. This sheaf pulls back to a line bundle $\omega_J := z^*\Omega^g_{\mathcal{J}/\mathbb{P}^1}$ on $\mathbb{P}^1$. The Faltings height of J is defined as

$$h(J) := \deg(\omega_J)$$

and the exponential Faltings height of J is defined as $H(J) := r^{h(J)}$.

Lemma 2.7. *There is a positive $D \in \mathbb{Q}$ depending only on a and b and a positive $E \in \mathbb{Q}$ depending only on a, b, and the congruence class of q mod ab such that the Faltings height of J is*

$$h(J) = Dq + E \,.$$

The values D and E satisfy

$$\frac{(ab-a-b)^3}{6a^2b^2} < D < \frac{ab}{6} \qquad \text{and} \qquad 0 < E < g_C \,.$$

Proof. Since J is a Jacobian, the Faltings height can be reinterpreted in terms of our regular model $\mathcal{S}$ for C and the map $\pi : \mathcal{S} \to \mathbb{P}^1$. There is a section $s : \mathbb{P}^1 \to \mathcal{S}$ which maps $\mathbb{P}^1$ isomorphically onto the Zariski closure in $\mathcal{S}$ of the point at infinity on the generic fiber C. So, we may apply Proposition 7.4 of [BHP+15], which gives

$$\omega_J \cong \bigwedge^g \pi_* \Omega^1_{\mathcal{S}/\mathbb{P}^1}.$$

For any integers $i, j \geq 1$, consider the meromorphic differential $\omega_{i,j} := x^{i-1}y^{j-b}dx \in \Omega^1_{\mathcal{S}/\mathbb{P}^1}$. The set of differentials restricted to the generic fiber C of $\mathcal{S} \to \mathbb{P}^1$

$$\left\{\omega_{i,j}|_C : i > 0, j > 0, \text{ and } ab > bi + aj\right\}$$

forms a K-basis for Ω^1_C. We may thus compute $\deg \omega_J$ in terms of the orders of poles/zeros of the relative differential g-form on $\mathcal{S}$ defined by

$$\eta := \bigwedge_{\substack{(i,j): i,j>0 \\ ab > bi+aj \,.}} \omega_{i,j} \,.$$

More precisely, we have

$$\deg(\omega_J) = \sum_{v \in \mathbb{P}^1} \operatorname{ord}_v(\pi_*\eta) \deg v \,.$$

Since $\pi_*\eta$ has finitely many zeros and poles, the sum is finite. Given a point v of $\mathbb{P}^1$, let $\mathcal{O}_v$ denote the local ring at v and let $\mathcal{S}_v$ be the base change of $\mathcal{S}$ to $\mathcal{O}_v$. We use [Dok20, Theorem 8.12] to understand the $\operatorname{ord}_v(\pi_*\eta)$. For $v \in \mathbb{A}^1 \subset \mathbb{P}^1$, set

$$V_{i,j,v} = \begin{cases} (ab - bi - aj)/ab & \text{if} \quad v \in \mathbb{F}_q \,, \\ 0 & \text{otherwise.} \end{cases}$$

In all cases, $\lfloor V_{i,j,v} \rfloor = 0$. So, by [Dok20, Theorem 8.12] the $\omega_{i,j}|_{\mathcal{S}_f}$ form a R_f basis for the relative canonical sheaf on $\mathcal{S}_f$. Hence, the g-form η is regular and non-vanishing on $\mathcal{S}_f$. In other words, $\operatorname{ord}_f(\pi_*\eta) = 0$. It follows that $\deg(\omega_J) = \operatorname{ord}_\infty(\eta)$.

Set

$$V_{i,j,\infty} := (bi + aj - ab)\frac{q}{ab} \,.$$

Taking local parameter $s = t^{-1}$ on the fiber $\mathcal{S}_\infty$ above infinity, Theorem 8.12 of [Dok20] says that an $\mathbb{F}_q[[s]]$-basis for the relative dualizing sheaf is given by

$$\{ s^{\lfloor V_{i,j,\infty} \rfloor} \omega_{i,j} : i > 0, j > 0, ab > bi + aj \} \,.$$

Hence,

$$\operatorname{ord}_\infty(\eta) = \sum_{\substack{(i,j):i,j>0 \\ ab>bi+aj \,.}} - \lfloor V_{i,j,\infty} \rfloor = \sum_{\substack{(i,j):i,j>0 \\ ab>bi+aj \,.}} - \left\lfloor (bi + aj - ab)\frac{q}{ab} \right\rfloor = \sum_{\substack{(i,j):i,j>0 \\ ab>bi+aj}} \left\lceil q\frac{ab - (bi+aj)}{ab} \right\rceil \,.$$

If we set

$$D := \sum_{\substack{(i,j):i,j>0 \\ ab>bi+aj}} \frac{ab - (bi+aj)}{ab}$$

and

$$E := \sum_{\substack{(i,j):i,j>0 \\ ab>bi+aj}} \left\lceil q\frac{ab - (bi+aj)}{ab} \right\rceil - q\frac{ab - (bi+aj)}{ab} \,,$$

then $h(J) = \deg(\omega_J) = Dq + E$. The definition of D depends only on a and b, while E only depends on the residue class of $q \pmod{ab}$.

To bound E, we note that

$$E = \sum_{\substack{(i,j):i,j>0 \\ ab>bi+aj}} \left\lceil q\frac{ab - (bi+aj)}{ab} \right\rceil - q\frac{ab - (bi+aj)}{ab} < \sum_{\substack{(i,j):i,j>0 \\ ab>bi+aj}} 1 = g \,.$$

To bound D, we interpret each term $(ab - bi - aj)/ab$ as the volume of a rectangular prism with height $(ab - bi - aj)/ab$ and base a square of side length 1. If we take as the base the square $[i, i+1] \times [j, j+1]$, then the tops of these prisms lie above the hyperplane $z = (ab - bx - ay)/ab$. If we take as base the square $[i-1, i] \times [j-1, j]$, the tops of these prisms lie below this hyperplane.

Hence, we may bound D between the areas of two right triangular pyramids, or equivalently the integrals

$$\frac{(ab-a-b)^3}{6a^2b^2} = \iint\limits_{\left\{\substack{(x,y):x,y>1,\\ ab>bx+ay}\right\}} \frac{ab-(bx+ay)}{ab}dxdy < D < \iint\limits_{\left\{\substack{(x,y):x,y>0,\\ ab>bx+ay}\right\}} \frac{ab-(bx+ay)}{ab}dxdy = \frac{ab}{6}\,.$$

□

Remark 2.8. When $a=2$, we can compute that $D=(b-1)^2/8b$, since

$$D = \frac{1}{2b}\sum_{j:0<ja<b}(b-ja) = \frac{1}{2b}\left(\frac{b-1}{2}\right)^2 = \frac{(b-1)^2}{8b}\,.$$

Remark 2.9. For a fixed pair a,b, note that the ratio $h(J)/q$ is bounded from above and from below by positive constants depending only on a and b as q tends to $+\infty$ through powers of p.

2.6 Decomposition of the Jacobian

In this section, we prove Theorem 1.4 on the simplicity of J. In Sections 6.5, 7.3, and 8 we will produce examples of abelian varieties with large rank, satisfying a Brauer–Siegel ratio, and with large order of Tate–Shafarevich, respectively. Theorem 1.4 shows that our examples can be constructed as simple abelian varieties, and are not built as isogeny products of elliptic curves over K.

Theorem 1.4. *The Jacobian J is K-simple if and only if a and b are both prime.*

Proof. For clarity, we will use the following notation in this proof. For any $\alpha,\beta\in\mathbb{Z}_{\geq 1}$, let $C_{\alpha,\beta}$ denote the smooth projective curve over K admitting a dense affine open subset defined by the equation

$$y^\beta + x^\alpha = t^q - t,$$

so that $C_{a,b}$ will denote our usual curve C. We then let $J_{\alpha,\beta}$ denote the Jacobian of $C_{\alpha,\beta}$.

We begin by proving the "only if" direction of the statement: Assume that at least one of a and b is composite. By symmetry, assume that a is composite, and let d be one of its nontrivial divisors. The map $(x,y)\mapsto(x^{a/d},y)$ extends to a non-constant K-morphism $C_{a,b}\to C_{d,b}$. The curve $C_{d,b}$ has positive genus since $d>1$. On the other hand, the genus of $C_{d,b}$ is strictly smaller than that of $C_{a,b}$ since $d<a$. The contravariant functoriality of the Jacobian then implies the existence of a morphism of abelian varieties $J_{d,b}\hookrightarrow J_{a,b}$, whose image is a positive-dimensional strict abelian subvariety of $J_{a,b}$ defined over K. Hence $J_{a,b}$ is not simple.

Conversely, assume that both a and b are prime, and pick a prime $\ell\neq p$ such that $\ell\not\equiv 1 \pmod a$ and $\ell\not\equiv 1 \pmod b$. Recall $K=\mathbb{F}_r(t)$ and let $k:=\mathbb{F}_r$.

Let

$$L = K[u]/(u^{ab}-(t^q-t)) = k(\sqrt[ab]{t^q-t})\,,$$

let $K'=K\overline{k}$, and let $L'=L\overline{k}$. Then $\mathrm{Gal}(L'/K)\cong\hat{\mathbb{Z}}\times\mu_{ab}$. The $\hat{\mathbb{Z}}$ is topologically generated by the Frobenius and $\zeta\in\mu_{ab}$ acts by $u\mapsto\zeta u$. Let C_0 be the curve defined by

$$y^b + x^a = 1$$

and let J_0 be its Jacobian. After base change to L, the curves C and C_0 become isomorphic: that is, $C_0 \times_k L \cong C \times_K L$ via the morphism

$$(x, y) \mapsto (u^{-b}x, u^{-a}y)\,.$$

In particular, C becomes constant over L. Similarly, J and J_0 become isomorphic after base change to L, so J becomes constant over L. We wish to use this property to understand the action of the absolute Galois group G_K on the ℓ-adic Tate modules $V_\ell(J)$. We begin with 2 lemmas.

Lemma 2.10. *Let G be a finite group, let X be a curve equipped with a G action, let $Y = X/G$, and let $f : X \to Y$ be the quotient map. Then, $J_X^G \sim J_Y$. That is, the subabelian variety of G-invariants of J_X is isogenous to J_Y.*

Proof. Suppose that $P \in J_X(\overline{K})^G$ is G-invariant. Then, P is represented by some divisor D on X, and $\#G \cdot P$ is represented by the G-invariant divisor $\sum_{g\in G} g \cdot D$ on X, which is the pullback of some divisor on Y. In particular, $\#G \cdot P$ is in the image of the finite map $f^* : J_Y \to J_X$. The image of f^* is contained in J_X^G. So, the image of f^* is finite index in J_X^G. It follows that $J_X^G \sim J_Y$. □

As a consequence of Lemma 2.10, we see that $V_\ell(J_X)^G = V_\ell(J_Y)$.

Lemma 2.11. *$V_\ell(J_0) \otimes \overline{\mathbb{Q}}_\ell$ is the direct sum of $2g$ one-dimensional $\overline{\mathbb{Q}}_\ell$-vector spaces indexed by the characters $\mu_a \times \mu_b \cong \mu_{ab} \to \overline{\mathbb{Q}}_\ell^\times$ which are nontrivial on both μ_a and μ_b. There are $(a-1)(b-1) = 2g$ such characters.*

Proof. The assumption that $\ell \not\equiv 1 \pmod a$ and $\ell \not\equiv 1 \pmod b$, together with the assumption that a and b are prime, implies that $\mathbb{Q}_\ell$ does not contain any nontrivial a-th or b-th roots of unity.

The action of μ_{ab} on $V_\ell(J_0) \otimes \overline{\mathbb{Q}}_\ell$ is diagonal with respect to a well-chosen basis, so $V_\ell(J_0) \otimes \overline{\mathbb{Q}}_\ell$ is a direct sum of $2g$ one-dimensional $\overline{\mathbb{Q}}_\ell$-representations of μ_{ab}. (Over $\mathbb{Q}_\ell$, the action gives an irreducible representation of μ_{ab}, which splits completely over $\overline{\mathbb{Q}}_\ell$.) We now consider the multiplicities of these one-dimensional representations.

Suppose that for some $P \in V_\ell(J_0)$ and some character $\chi : \mu_{ab} \to \mathbb{Q}_\ell^\times$ we have $\zeta \cdot P = \chi(\zeta)P$ for all $\zeta \in \mu_{ab}$. Suppose $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$.

There is a unique $c \in (\mathbb{Z}/ab\mathbb{Z})^\times$ such that $\sigma(\zeta)^c = \zeta$ for all $\zeta \in \mu_{ab}$. Then,

$$\zeta \cdot \sigma(P) = \sigma(\zeta)^c \cdot \sigma(P) = \sigma(\zeta^c \cdot P) = \sigma(\chi(\zeta)^c P) = \chi(\zeta)^c \sigma(P)\,.$$

So, if the action of μ_{ab} on $\mathbb{Q}_\ell P$ is by χ, then the action of μ_{ab} on $\mathbb{Q}_\ell$ is by χ^c. Since $\mathbb{Q}_\ell$ does not contain any nontrivial (ab)-th roots of unity, all characters of the same order are Galois conjugate. Hence, each character of μ_{ab} of a given order has the same multiplicity in the representation $V_\ell(J_0)$.

Next, we prove that each of the primitive characters appears with positive multiplicity.

Applying Lemma 2.10 in our situation, any non-primitive character of μ_{ab} factors through some proper subgroup G of μ_{ab}. In particular, since each primitive character appears with the same multiplicity n, we have

$$V_\ell(J_0) = \bigoplus_{\substack{\chi:\mu_{ab}\to\mathbb{Q}_\ell^\times \\ \text{primitive}}} \chi^{\oplus n}$$

as a representation of μ_{ab}. Comparing $\dim V_\ell(J_0)$ and the number of primitive characters of μ_{ab}, we see that $n = 1$. Therefore,

$$V_\ell(J_0) \cong \bigoplus_{\substack{\chi:\mu_a\times\mu_b\to\mathbb{Q}_\ell^\times: \\ \chi(\cdot,1) \text{ nontrivial and} \\ \chi(1,\cdot) \text{ nontrivial.}}} \chi\,,$$

as claimed. □

On the line indexed by the pair of characters (χ_a, χ_b), the Frobenius generating $\mathrm{Gal}(\overline{k}/k) \cong \hat{\mathbb{Z}}$ acts by some exponential sum attached to the pair of characters. There is also an action of μ_{ab} on J_0 induced by the action of μ_{ab} on C_0 defined by $(x, y) \mapsto (\zeta^b x, \zeta^a y)$. This action preserves the decomposition into lines, and on the line indexed by a pair of characters (χ_a, χ_b), ζ acts by $\chi_a(\zeta^b)\chi_b(\zeta^a) \in \mathbb{Q}_\ell^\times$. In particular, if $V \subset V_\ell(J_0)$ is a nonzero subspace preserved by the action of μ_{ab}, then μ_{ab} acts faithfully on V. There is an isomorphism of $\mathbb{Q}_\ell$-vector spaces:

$$V_\ell(J_0) = V_\ell(J_0 \times_k K) \cong V_\ell(J).$$

This isomorphism is not equivariant for the actions of G_K on both sides, because the isomorphism between J_0 and J is defined only over L, and cannot be defined over K. We wish to describe the Galois action on $V_\ell(J)$ in terms of the actions of $\mathrm{Gal}(\overline{k}/k)$ and μ_{ab} on $V_\ell(J_0)$ which are described above.

A point $(x, y) \in C_0(\overline{k})$ maps to $(u^{-b}x, u^{-a}y) \in C(L')$ under the action by $\mathrm{Gal}(L'/K) \cong \hat{\mathbb{Z}} \times \mu_{ab}$ as follows The Frobenius acts as usual on x and y, since these are elements of $\overline{k}$, and μ_{ab} acts by the inverse of the geometric action

$$(u^{-b}x, u^{-a}y) \mapsto (\zeta^{-b}u^{-b}x, \zeta^{-a}u^{-a}y).$$

Transporting back to $C_0(\overline{k})$ gives

$$(x, y) \mapsto (u^{-b}x, u^{-a}y) \mapsto (\zeta^{-b}u^{-b}x, \zeta^{-a}u^{-a}y) \mapsto (\zeta^{-b}x, \zeta^{-a}y).$$

In summary: there is in injection $C_0(\overline{k}) \hookrightarrow C(L')$, $\mathrm{Gal}(L'/K)$ preserves the image of the injection, and the action of $(\mathrm{Fr}_q^m, \zeta) \in \mathrm{Gal}(L'/K)$ on $C(L')$ carries over to

$$(x, y) \mapsto (\zeta^{-b} \mathrm{Fr}_q^m(x), \zeta^{-a} \mathrm{Fr}_q^m(y)).$$

Similarly, on the level of Tate modules: the torsion points of J_0 are defined over $\overline{k}$, and they are represented by divisors on C_0 supported on points defined over $\overline{k}$. This means that the action of G_K on $V_\ell(J)$ factors through $\mathrm{Gal}(L'/K)$. Under the isomorphism $V_\ell(J_0) \cong V_\ell(J)$, the action of

$$\mathrm{Gal}(L'/K) \cong \mathrm{Gal}(\overline{k}/k) \times \mathrm{Gal}(L/K) \cong \hat{\mathbb{Z}} \times \mu_{ab}$$

carries over to the product of the usual action of $\mathrm{Gal}(\overline{k}/k)$ on $V_\ell(J_0)$ times the inverse of the action of μ_{ab} on $V_\ell(J_0)$ induced by the natural action of μ_{ab} on C_0.

In summary, $V_\ell(J)$ is a sum of 1-dimensional $\mathbb{Q}_\ell$-vector spaces indexed by characters $(\chi_a, \chi_b) : \mu_a \times \mu_b \to \mathbb{Q}_\ell^\times$, with both χ_a and χ_b nontrivial. On the subspace indexed by (χ_a, χ_b), Frobenius acts by some exponential sum, and $\zeta \in \mathrm{Gal}(L/K) \cong \mu_{ab}$ acts as $\chi_a^{-1}(\zeta)\chi_b^{-1}(\zeta)$. J also carries a geometric action of μ_{ab} induced from the action of μ_{ab} on C defined by

$$(x, y) \mapsto (\zeta^b x, \zeta^a y).$$

Now we prove that J is simple. Suppose $A \subset J$ is a positive-dimensional abelian subvariety. Then, $V = V_\ell(A) \subset V_\ell(J)$ is a nonzero $\mathrm{Gal}(L'/K)$-invariant subspace. We have $\mathrm{Gal}(L'/K) \cong \mathrm{Gal}(\overline{k}/k) \times \mathrm{Gal}(L/K) \cong \hat{\mathbb{Z}} \times \mu_{ab}$, and the action of $\mathrm{Gal}(L/K) \cong \mu_{ab}$ is the inverse of the geometric action. This implies that V is stable under the geometric action, which implies that $A \subset J$ is preserved by this action. Since the action of μ_{ab} on $V_\ell(J)$ is faithful, we may conclude that the geometric action of μ_{ab} on A induces an inclusion $\mathbb{Q}(\mu_{ab}) \hookrightarrow \mathrm{End}_K(A) \otimes \mathbb{Q}$. If A has dimension d, the dimension of a semi-simple commutative subalgebra of $\mathrm{End}_K(A) \otimes \mathbb{Q}$ is bounded above by $2d$. Since $[\mathbb{Q}(\mu_{ab}) : \mathbb{Q}] = (a-1)(b-1) = 2g$, A must have dimension g, so it is equal to J. Therefore J is K-simple. □

3 Background on Gauss sums

In this section, we gather some facts about Gauss sums which will be useful in future sections.

3.1 Multiplicative and additive characters on extensions of $\mathbb{F}_p$

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and denote by $\overline{\mathbb{Z}}$ the ring of algebraic integers. We choose, once and for all, a prime ideal $\mathfrak{p}$ of $\overline{\mathbb{Z}}$ which lies over the rational prime p. We then write $\nu_{\mathfrak{p}} : \overline{\mathbb{Q}} \to \mathbb{Q}$ for the $\mathfrak{p}$-adic valuation on $\overline{\mathbb{Q}}$, normalised so that $\nu_{\mathfrak{p}}(r) = 1$.

The quotient $\overline{\mathbb{Z}}/\mathfrak{p}$ is an algebraic closure of $\mathbb{F}_p$, denoted by $\overline{\mathbb{F}_p}$. All finite extensions of $\mathbb{F}_p$ will be viewed as subfields of $\overline{\mathbb{F}_p}$. The quotient map $\overline{\mathbb{Z}} \to \overline{\mathbb{Z}}/\mathfrak{p} = \overline{\mathbb{F}_p}$ further induces an isomorphism between the group of roots of unity in $\overline{\mathbb{Q}}$ whose order is prime to p, and $\overline{\mathbb{F}_p}^\times$. Let $\boldsymbol{\chi} : \overline{\mathbb{F}_p}^\times \to \overline{\mathbb{Q}}^\times$ denote the inverse of this isomorphism. The isomorphism $\boldsymbol{\chi}$ is sometimes called the Teichmüller character of $\overline{\mathbb{F}_p}$.

Definition 3.1. Let $\mathbb{F}$ be a finite field extension of $\mathbb{F}_p$, and n be a positive integer dividing $|\mathbb{F}^\times|$. We let

$$\chi_{\mathbb{F},n} : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times, \quad x \mapsto \boldsymbol{\chi}(x)^{|\mathbb{F}^\times|/n}.$$

This defines a multiplicative character on $\mathbb{F}$ which, as a straightforward computation shows, has exact order n.

We fix a nontrivial additive character ψ_0 on $\mathbb{F}_p$. We may, and will, assume that ψ_0 takes values in the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$. For any finite extension $\mathbb{F}/\mathbb{F}_p$, we denote the relative trace map by $\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p} : \mathbb{F} \to \mathbb{F}_p$. The composition $\psi_0 \circ \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p}$ is then a nontrivial additive character on $\mathbb{F}$. More generally:

Definition 3.2. Let $\mathbb{F}$ be any finite field extension of $\mathbb{F}_p$, and let $\alpha \in \mathbb{F}$. We let

$$\psi_{\mathbb{F},\alpha} : \mathbb{F} \to \mathbb{Q}(\zeta_p)^\times, \quad x \mapsto (\psi_0 \circ \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_p})(\alpha x)\,.$$

This defines an additive character on $\mathbb{F}$, which is nontrivial for any $\alpha \neq 0$.

To lighten expressions, we suppress $\mathbb{F}$ from the notation when it is clear from context.

3.2 Classical properties of Gauss Sums

We begin by recalling the definition of Gauss sums and some of their classical properties.

Definition 3.3. Let $\mathbb{F}$ be a finite field of characteristic p. Given an additive character ψ and a multiplicative character χ on $\mathbb{F}$, we define the Gauss sum $\mathrm{G}_{\mathbb{F}}(\chi, \psi)$ by

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

Let $\mathbb{F}$ be a finite field of characteristic p. For any additive character ψ and any multiplicative character χ on $\mathbb{F}$, we have the following facts.

1. If χ has order n, then $\mathrm{G}_{\mathbb{F}}(\chi, \psi)$ is an algebraic integer in the cyclotomic field $\mathbb{Q}(\mu_{np})$.
2. If χ is nontrivial, orthogonality of characters implies that in any complex embedding,

$$|\mathrm{G}_{\mathbb{F}}(\chi, \psi)| = |\mathbb{F}|^{1/2}\,. \tag{3.1}$$

3. For $\alpha \in \mathbb{F}^\times$, in the notation introduced in the previous subsection,

$$\mathrm{G}_{\mathbb{F}}(\chi, \psi_{\mathbb{F},\alpha}) = \chi(\alpha)^{-1}\mathrm{G}_{\mathbb{F}}(\chi, \psi_{\mathbb{F},1})\,. \tag{3.2}$$

4. (Hasse-Davenport relation) For any finite extension $\mathbb{F}'/\mathbb{F}$,

$$\mathrm{G}_{\mathbb{F}'}\big(\chi \circ \mathrm{N}_{\mathbb{F}'/\mathbb{F}}, \psi \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}}\big) = \mathrm{G}_{\mathbb{F}}(\chi, \psi)^{[\mathbb{F}':\mathbb{F}]}. \tag{3.3}$$

3.3 Orbits

Let p be a prime number and r be a fixed power of p. For any integers a, b which are relatively prime to each other and coprime to p, and for any power q of p, define

$$S := S_{a,b,q} = (\mathbb{Z}/a\mathbb{Z} \smallsetminus \{0\}) \times (\mathbb{Z}/b\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q^\times.$$

The subgroup $\langle r \rangle$ of $\mathbb{Q}^\times$ generated by r acts on S via the rule

$$\forall (i,j,\alpha) \in S, \qquad r \cdot (i,j,\alpha) := (ri, rj, \alpha^{1/r}).$$

In other words, r acts on $(\mathbb{Z}/a\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z}/b\mathbb{Z} \setminus \{0\})$ by component-wise multiplication, and on $\mathbb{F}_q^\times$ by the inverse of the r-power Frobenius.

We denote by $O := O_{r,a,b,q}$ the set of orbits of $\langle r \rangle$ on S. Recall that for $n \geq 1$ coprime to p, we have defined $o_p(n)$ (resp. $o_r(n)$) to be the multiplicative order of p (resp. r) modulo n. For $n \geq 1$ coprime to p and $i \in \mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}$, we write $\kappa_{r,n}(i)$ for the multiplicative order of r modulo $n/\gcd(n,i)$ *i.e.*,

$$\kappa_{r,n}(i) := o_r\big(n/\gcd(n,i)\big)\,.$$

If $o \in O$ is the orbit of $(i,j,\alpha) \in S$, then a computation shows that

$$|o| = \mathrm{lcm}\left(\kappa_{r,a}(i), \kappa_{r,b}(j), [\mathbb{F}_r(\alpha), \mathbb{F}_r]\right). \tag{3.4}$$

For any integer n coprime to p, let

$$S'_n := (\mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q^\times,$$

and endow it with an action of $\langle r \rangle$ *via* the rule $r \cdot (i,\alpha) = (ri, \alpha^{1/r})$. Write O'_n for the set of orbits of S'_n under this action.

If $(i,\alpha) \in S'_n$, then the length $|o'|$ of its orbit $o' \in O'_n$ is the smallest integer $f \geq 1$ such that $\mathbb{F}_{r^f}$ contains α and for which n divides $i(r^f - 1)$. In other words,

$$|o'| = \mathrm{lcm}\left(\kappa_{r,a}(i), [\mathbb{F}_r(\alpha) : \mathbb{F}_r]\right). \tag{3.5}$$

With S'_n and O as above, the natural projection maps $S_{a,b,q} \to S'_a$ and $S_{a,b,q} \to S'_b$ commute with the actions of $\langle r \rangle$ on these sets. These projections therefore induce surjective maps $\pi_a : O \to O'_a$ and $\pi_b : O \to O'_b$. For any $o \in O$, we let

$$\nu_a(o) := |o|/|\pi_a(o)| \qquad \text{and} \qquad \nu_b(o) := |o|/|\pi_b(o)|.$$

If o is the orbit of (i,j,α), we have

$$\nu_a(o) = \frac{\mathrm{lcm}\left(\kappa_{r,a}(i), \kappa_{r,b}(j), [\mathbb{F}_r(\alpha) : \mathbb{F}_r]\right)}{\mathrm{lcm}\left(\kappa_{r,a}(i), [\mathbb{F}_r(\alpha) : \mathbb{F}_r]\right)} = \frac{\mathrm{lcm}\left(|\pi_a(o)|, \kappa_{r,b}(j)\right)}{|\pi_a(o)|} = \frac{\kappa_{r,b}(j)}{\gcd\left(|\pi_a(o)|, \kappa_{r,b}(j)\right)}.$$

In particular, $\nu_a(o)$ and $\nu_b(o)$ are integers, and $\nu_a(o) = 1$ if and only if $\kappa_{r,b}(j)$ divides $|\pi_a(o)|$.

Since a and b are relatively prime, the Chinese remainder theorem gives a natural isomorphism $\phi : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \simeq \mathbb{Z}/ab\mathbb{Z}$. The set $\phi((\mathbb{Z}/a\mathbb{Z} \smallsetminus \{0\}) \times (\mathbb{Z}/b\mathbb{Z} \smallsetminus \{0\}))$ is clearly stable under the action of $\langle r \rangle$ by component-wise multiplication on $\mathbb{Z}/ab\mathbb{Z} \smallsetminus \{0\}$, so the orbit set $O_{r,a,b,q}$ may be viewed as a subset of O'_{ab}.

3.4 Gauss sums associated to orbits

Recall that we have fixed a non-trivial additive character ψ_0 on $\mathbb{F}_p$. Let n be an integer which is coprime to p. Consider the set S'_n as above, with its action of $\langle r\rangle$. Let $(i,\alpha) \in S'_n$, and write $o' \in O'_n$ for its orbit under the action $\langle r\rangle$ on S'_n. Let $\mathbb{F}'$ be the extension of $\mathbb{F}_r$ of degree $|o'|$. By construction, $\alpha^{r^{|o'|}} = \alpha$ so that $\alpha \in \mathbb{F}'$. Hence we may consider the non-trivial additive character $\Psi_{(i,\alpha)}$ on $\mathbb{F}'$ defined by

$$\forall x \in \mathbb{F}', \qquad \Psi_{(i,\alpha)}(x) := \psi_{\mathbb{F}',\alpha}(x) = (\psi_0 \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_p})(\alpha x).$$

By construction, n divides $i\,(r^{|o|}-1) = i\,|\mathbb{F}'^{\times}|$ and we introduce a non-trivial multiplicative character $\boldsymbol{\lambda}_{(i,\alpha)}$ on $\mathbb{F}'$ defined by

$$\forall x \in \mathbb{F}', \qquad \boldsymbol{\lambda}_{(i,\alpha)}(x) := \boldsymbol{\chi}(x)^{i(r^{|o|}-1)/n}.$$

This leads us to consider the Gauss sum $\mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(i,\alpha)}, \Psi_{(i,\alpha)}\big)$.

Lemma 3.4. *For all $(i,\alpha) \in S'_n$, we have*

$$\mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(i,\alpha)}, \Psi_{(i,\alpha)}\big) = \mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{r\cdot(i,\alpha)}, \Psi_{r\cdot(i,\alpha)}\big).$$

In other words, the value of $\mathrm{G}_{\mathbb{F}}\big(\boldsymbol{\lambda}_{(i,\alpha)}, \Psi_{(i,\alpha)}\big)$ is constant along the $\langle r\rangle$-orbit o' of (i,α).

Proof. By definition,

$$-\mathrm{G}_{\mathbb{F}}\big(\boldsymbol{\lambda}_{r\cdot(i,\alpha)}, \Psi_{r\cdot(i,\alpha)}\big) = \sum_{x\in(\mathbb{F}')^{\times}} \boldsymbol{\chi}(x)^{ri(r^{|o|}-1)/n}\,(\psi_0 \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_p})(\alpha^{1/r}x)$$

Since $x \mapsto x^r$ defines a bijection $(\mathbb{F}')^{\times} \to (\mathbb{F}')^{\times}$, we may set $y = x^r$ and reindex. This yields

$$\begin{aligned}-\mathrm{G}_{\mathbb{F}}\big(\boldsymbol{\lambda}_{r\cdot(i,\alpha)}, \Psi_{r\cdot(i,\alpha)}\big) &= \sum_{y\in(\mathbb{F}')^{\times}} \boldsymbol{\chi}(y)^{i(r^{|o|}-1)/n}\,(\psi_0 \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_p})(\alpha^{1/r}y^{1/r}) \\ &= \sum_{y\in(\mathbb{F}')^{\times}} \boldsymbol{\lambda}_{(i,\alpha)}(y)\,(\psi_0 \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_p})((\alpha y)^{1/r})\,.\end{aligned}$$

Since $\mathbb{F}_r \subset \mathbb{F}'$, if $z \in \mathbb{F}'$, then z is conjugate to z^r over $\mathbb{F}_r$. So, $\mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_p}(z) = \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_p}(z^r)$. Hence,

$$\begin{aligned}-\mathrm{G}_{\mathbb{F}}\big(\boldsymbol{\lambda}_{r\cdot(i,\alpha)}, \Psi_{r\cdot(i,\alpha)}\big) &= \sum_{y\in(\mathbb{F}')^{\times}} \boldsymbol{\lambda}_{(i,\alpha)}(y)\,(\psi_0 \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_p})(\alpha y) \\ &= -\mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(i,\alpha)}, \Psi_{(i,\alpha)}\big).\end{aligned}$$

□

Lemma 3.4 allows us to define Gauss sums associated to $\langle r\rangle$-orbits:

Definition 3.5. In the above setting, for an orbit $o' \in O'_n$, we write $\mathbb{F}'$ for the extension of $\mathbb{F}_r$ of degree $|o'|$ and we set

$$\mathbf{G}\left(o'\right) := \mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(i,\alpha)}, \Psi_{(i,\alpha)}\big),$$

for one/any representative $(i,\alpha) \in S'_n$ of o'.

Since $\boldsymbol{\lambda}_{(i,\alpha)}$ is nontrivial, by (3.1) we have

$$|\mathbf{G}\left(o'\right)| = |\mathbb{F}'|^{1/2} = r^{|o'|/2}$$

in any complex embedding of $\overline{\mathbb{Q}}$.

Now let a and b be relatively prime integers which are coprime to p, and consider the set O of orbits of $\langle r\rangle$ acting on the set $S_{a,b,q}$ introduced in §3.3. Recall that there are surjective maps $\pi_a : O \to O'_a$ and $\pi_b : O \to O'_b$. We may finally introduce:

Definition 3.6. In the above setting, for any orbit $o \in O$, we let

$$\boldsymbol{\omega}(o) := \mathbf{G}\left(\pi_a(o)\right)^{\nu_a(o)} \mathbf{G}\left(\pi_b(o)\right)^{\nu_b(o)},$$

where $\nu_a(o) = |o|/|\pi_a(o)|$ and $\nu_b(o) = |o|/|\pi_b(o)|$.

For any orbit $o \in O$, we have $|\boldsymbol{\omega}(o)| = r^{|o|}$ in any complex embedding of $\overline{\mathbb{Q}}$.

For any a, b, we let $\theta_{a,b} := \operatorname{lcm}(o_p(a), o_p(b))$. Recall that an algebraic integer g is called a Weil integer of size p^θ (with $\theta \in \frac{1}{2}\mathbb{Z}$) if and only if g has magnitude p^θ in any complex embedding of $\overline{\mathbb{Q}}$. We record the following proposition for future use.

Proposition 3.7. *For any orbit $o \in O$, there exist an ab-th root of unity ζ_o and a Weil integer g_o of size $p^{\theta_{a,b}}$ such that*

$$\boldsymbol{\omega}(o) = \zeta_o g_o^{[\mathbb{F}_r:\mathbb{F}_p]\cdot|o|/\theta_{a,b}}.$$

Proof. Let $(i,j,\alpha) \in S$ have orbit $o \in O$. Then, $(i,\alpha) \in S'_a$ is a representative of $o' := \pi_a(o) \in O'_a$ and $(j,\alpha) \in S'_b$ is a representative of $\pi_b(o) \in O'_b$. Let $\mathbb{F}'$ be the extension of $\mathbb{F}_r$ of degree $|o'|$. By definition of $\mathbf{G}\left(o'\right)$ and equation (3.2), we have

$$\mathbf{G}\left(o'\right) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}\mathrm{G}_{\mathbb{F}'}\left(\boldsymbol{\lambda}_{(i,\alpha)}, \psi_{\mathbb{F}',1}\right).$$

Observe that $\zeta_{o'} := \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}$ is an a-th root of unity because $\boldsymbol{\lambda}_{(i,\alpha)}$ has order dividing a. Let $\mathbb{F}$ be the extension of $\mathbb{F}_p$ of degree $\kappa_{p,a}(i) = o_p(a/\gcd(i,a))$. We note that $[\mathbb{F}' : \mathbb{F}] = [\mathbb{F}_r : \mathbb{F}_p]\cdot|o'|/\kappa_{p,a}(i)$. Moreover, the character $\boldsymbol{\lambda}_{(i,\alpha)}$ is none other than $\chi_{\mathbb{F},|\mathbb{F}^\times|}^{i|\mathbb{F}^\times|/a} \circ \mathrm{N}_{\mathbb{F}'/\mathbb{F}}$.

Define $g_{o'} := \mathrm{G}_{\mathbb{F}}\left(\chi_{\mathbb{F},|\mathbb{F}|}^{i|\mathbb{F}^\times|/a}, \psi_{\mathbb{F},1}\right)$. Then, $g_{o'}$ is a Weil integer of size $p^{\kappa_{p,a}(i)/2}$. Applying the Hasse–Davenport relation (3.3) for Gauss sums, we deduce that

$$\mathbf{G}\left(o'\right) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}\left(\mathrm{G}_{\mathbb{F}}\left(\chi_{\mathbb{F},|\mathbb{F}^\times|}^{i|\mathbb{F}^\times|/a}, \psi_{\mathbb{F},1}\right)\right)^{[\mathbb{F}':\mathbb{F}]} = \zeta_{o'}\, g_{o'}^{[\mathbb{F}_r:\mathbb{F}_p]|o'|/\kappa_{p,a}(i)}.$$

A similar argument shows that if we define $\zeta_{\pi_b(o)} := \boldsymbol{\lambda}_{(j,\alpha)}(\alpha)^{-1}$ and $g_{\pi_b(o)} := \mathrm{G}_{\mathbb{F}}\left(\chi_{\mathbb{F},|\mathbb{F}|}^{j|\mathbb{F}^\times|/b}, \psi_{\mathbb{F},1}\right)$, then $\mathbf{G}\left(\pi_b(b)\right) = \zeta_{\pi_b(o)} g_{\pi_b(o)}^{[\mathbb{F}_r:\mathbb{F}_p]|\pi_b(o)|/\kappa_{p,b}(j)}$.

By the definition of $\boldsymbol{\omega}(o)$, we may write

$$\begin{aligned}\boldsymbol{\omega}(o) &= \zeta_{\pi_a(o)}^{\nu_a(o)}\zeta_{\pi_b(o)}^{\nu_b(o)} g_{\pi_a(o)}^{[\mathbb{F}_r:\mathbb{F}_p]|o|/\kappa_{p,a}(i)} g_{\pi_b(o)}^{[\mathbb{F}_r:\mathbb{F}_p]|o|/\kappa_{p,b}(j)} \\ &= \left(\zeta_{\pi_a(o)}^{\nu_a(o)}\zeta_{\pi_b(o)}^{\nu_b(o)}\right)\left(g_{\pi_a(o)}^{\theta_{a,b}/\kappa_{p,a}(i)} g_{\pi_b(o)}^{\theta_{a,b}/\kappa_{p,b}(j)}\right)^{[\mathbb{F}_r:\mathbb{F}_p]\cdot|o|/\theta_{a,b}}.\end{aligned}$$

Note that both $\kappa_{p,a}(i)$ and $\kappa_{p,b}(j)$ divide $\theta_{a,b}$. In this expression, $\zeta_o := \zeta_{\pi_a(o)}^{\nu_a(o)}\zeta_{\pi_b(o)}^{\nu_b(o)}$ is a root of unity of order dividing ab, and the term

$$g_o := g_{\pi_a(o)}^{\theta_{a,b}/\kappa_{p,a}(i)} g_{\pi_b(o)}^{\theta_{a,b}/\kappa_{p,b}(j)}$$

is a Weil integer of size $p^{\theta_{a,b}}$. Therefore, $\boldsymbol{\omega}(o)$ may be written in the desired form. □

4 Explicit expression for the L-function

In this section, we provide an explicit formula for the L-function of the Jacobian J of the curve C. Our proof is based on a computation with character sums.

4.1 Definition of the L-function

Fix a prime number $\ell \neq p$, and let $H^1(J)$ denote the first ℓ-adic étale cohomology group of J/K. It is well-known that $H^1(J)$ is a $\overline{\mathbb{Q}_\ell}$-vector space of dimension $2g$ which is equipped with a natural action of the absolute Galois group of K. For any place v of K, we let Fr_v denote the geometric Frobenius at v, let I_v denote the inertia group at v, and let $V_\ell(J)$ denote the ℓ-adic Tate module of J. As a Galois module, $H^1(J)$ is isomorphic to the dual of $V_\ell(J)$. (This duality follows by using the short exact sequence $0 \to \mu_{\ell^n} \to \mathbb{G}_m \to \mathbb{G}_m \to 0$ of sheaves on J and taking an inverse limit over n.)

The Hasse–Weil L-function of J may be defined by the Euler product:

$$L(J,T) = \prod_v \det\left(1 - T^{\deg v}\,\mathrm{Fr}_v \mid H^1(J)^{I_v}\right)^{-1}, \tag{4.1}$$

where the product runs over all places v of K. Here, $H^1(J)^{I_v}$ designates the I_v-invariant subspace of $H^1(J)$.

The abelian variety J has good reduction at a place v if and only if I_v acts trivially on $H^1(J)$, or equivalently, if and only if $H^1(J)^{I_v}$ has dimension $2g$ [ST68].

The power series in T resulting from the formal expansion of the product (4.1) is known, by the Hasse–Weil bound on the eigenvalues of Fr acting on $H^1(J)$, to converge on the complex open disc $\{T \in \mathbb{C} : |T| < r^{-3/2}\}$. But actually, much more is true! We summarize deep results of Grothendieck, Deligne, and others in the following theorem.

Theorem 4.1. *Let J/K be as above. Write $g = \dim J$ for its dimension, and $N_J \in \mathrm{Div}(\mathbb{P}^1)$ for its conductor divisor.*

(1. Rationality) The L-function $L(J,T)$ is a rational function in T with integral coefficients. The global degree of $L(J,T)$ as a rational function in T is denoted by $b(J)$. The degree $b(J)$ is related to $\deg N_J$ by $b(J) = \deg N_J - 4g$.

(2. Functional equation) There is some $w(J) \in \{\pm 1\}$ such that $L(J,T)$ satisfies

$$L(J,T) = w(J)\,(rT)^{b(J)} L\left(J, (r^2T)^{-1}\right).$$

(3. Riemann Hypothesis) If $z \in \mathbb{C}$ is such that $L(J,z) = 0$, then $|z| = r^{-1}$.

Proof. For the proofs of rationality, the functional equation, and the Riemann hypothesis, we refer the reader to [Del80]. We provide a proof of the formula for the degree $b(J)$ of $L(J,T)$ in Proposition A.1. □

Once we compute the L-function of our Jacobian in Theorem 4.2, we check the degree in Remark 4.9 using the formula $b(J) = \deg N_J - 4g$.

4.2 Explicit expression for the L-function

We let p, r, a, b, q have the same meaning as in the introduction. With the notation introduced in Section 3, we state our formula for the L-function of J.

Theorem 4.2. *Let O be the orbit set defined in §3.3 and, for any $o \in O$, define $\boldsymbol{\omega}(o)$ as in Definition 3.6. The L-function $L(J,T) \in \mathbb{Z}[T]$ of J/K admits the following expression:*

$$L(J,T) = \prod_{o \in O} \left(1 - \boldsymbol{\omega}(o)\, T^{|o|}\right) . \tag{4.2}$$

The proof of Theorem 4.2 occupies the rest of Section 4.2. We start by proving a number of elementary lemmas in Section 4.3, before gathering our results to conclude the proof in Section 4.4.

4.3 Preliminary lemmas

We first recall an expression for the logarithm of $L(J,T)$. For any $\beta \in \overline{\mathbb{F}_r}^{\times}$, let X_β denote the smooth projective curve over $\mathbb{F}_r(\beta)$ which is birational to the curve defined by the affine model $x^a + y^b = \beta^q - \beta$.

Lemma 4.3. *For $m \in \mathbb{Z}_{\geq 1}$ and $\beta \in \mathbb{F}_{r^m}$, set $A_J(\beta, m) = r^m + 1 - |X_\beta(\mathbb{F}_{r^m})|$. Then,*

$$\log L(J,T) = \sum_{m \geq 1} \left(\sum_{\beta \in \mathbb{F}_{r^m}^{\times}} A_J(\beta, m) \right) \frac{T^m}{m}.$$

Proof. We have shown in Proposition 2.3 that J has totally unipotent reduction at all of its places of bad reduction. At a place v of totally unipotent reduction for J, $\dim_{\mathbb{Q}_\ell} H^1(J)^{I_v} = 0$. (See [ST68].) Hence, the associated Euler factor $\det(1 - T^{\deg v} \operatorname{Fr}_v \mid H^1(J)^{I_v})$ in $L(J,T)$ is equal to 1.

Hence, in the Euler product (4.1) defining $L(J,T)$, we may ignore the factors corresponding to places of bad reduction. We thus have

$$L(J,T) = \prod_{\text{good } v} \det(1 - T^{\deg v} \operatorname{Fr}_v \mid H^1(J)^{I_v})^{-1} .$$

At a place v of good reduction, the inertia group I_v acts trivially on $H^1(J)$ (see [ST68] again), so that $H^1(J)^{I_v}$ has dimension $2g$. We write $\alpha_{v,1}, \ldots, \alpha_{v,2g} \in \overline{\mathbb{Q}_\ell}$ for the eigenvalues of Fr_v acting on $H^1(J)$. Formally expanding the power series $\log L(J,T) \in \overline{\mathbb{Q}_\ell}[[T]]$, we obtain that

$$\begin{aligned}
\log L(J,T) &= - \sum_{\text{good } v} \sum_{i=1}^{2g} \log(1 - \alpha_{v,i}\, T^{\deg v}) \\
&= \sum_{\text{good } v} \sum_{i=1}^{2g} \sum_{k=1}^{\infty} \frac{(\alpha_{v,i}\, T^{\deg v})^k}{k} \\
&= \sum_{k=1}^{\infty} \left(\sum_{\text{good } v} \left(\sum_{i=1}^{2g} \alpha_{v,i}^k \right) \frac{T^{k \deg v}}{k} \right) .
\end{aligned}$$

We now now write $m = k \deg v$ and reindex the sums. Since

$$\operatorname{Tr}(\operatorname{Fr}_{v_\beta}^{m/\deg v_\beta} | H^1(J)) = \sum_{i=1}^{2g} \alpha_{v,i}^{m/\deg v} , \tag{4.3}$$

this yields

$$\log L(J,T) = \sum_{m=1}^{\infty} \left(\sum_{\substack{\text{good } v \\ \deg v | m}} \operatorname{Tr}(\operatorname{Fr}_v^{m/\deg v} | H^1(J)) \deg v \, \frac{T^m}{m} \right). \tag{4.4}$$

Since K is the function field of $\mathbb{P}^1$, a place v of K may be viewed as the $\operatorname{Gal}(\overline{\mathbb{F}_r}/\mathbb{F}_r)$-orbit of an $\overline{\mathbb{F}_r}$-rational point on $\mathbb{P}^1$. The degree of v is the number of elements in the associated orbit.

Let $\beta \in \mathbb{P}^1(\overline{\mathbb{F}_r})$ and v_β be the corresponding place of K. The orbit of β under the action of $\operatorname{Gal}(\overline{\mathbb{F}_r}/\mathbb{F}_r)$ has exactly $[\mathbb{F}_r(\beta) : \mathbb{F}_r]$ elements. So, $\deg(v_\beta) = [\mathbb{F}_r(\beta) : \mathbb{F}_r]$. By construction, the numbers $\operatorname{Tr}(\operatorname{Fr}_{v_\beta}^{m/\deg v_\beta} | H^1(J))$ do not depend on the choice of a representative $\beta \in \mathbb{P}^1(\overline{\mathbb{F}_r})$ of the orbit v.

Let U be the largest subscheme of $\mathbb{P}^1$ such that J_v has good reduction at all places $v \in U$. By Proposition 2.3, we have $U = \mathbb{A}^1 \smallsetminus \{z : z^q - z = 0\}$. We may thus rewrite identity (4.4) as

$$\log L(J,T) = \sum_{m=1}^{\infty} \left(\sum_{\beta \in U(\mathbb{F}_{r^m})} \operatorname{Tr}(\operatorname{Fr}_{v_\beta}^{m/\deg v_\beta} | H^1(J)) \right) \frac{T^m}{m}. \tag{4.5}$$

By flat base change, we have $H^1(J) \cong H^1_{\text{et.}}(J_v), \mathbb{Q}_\ell)$. From [Poo06, 5.3.5], we have $H^1_{\text{et.}}(J_v, \mathbb{Q}_\ell) \cong H^1_{\text{et.}}(X_v, \mathbb{Q}_\ell)$. Together, we see

$$H^1(J)^{I_v} = H^1(J) \cong H^1_{\text{et.}}(J_v, \mathbb{Q}_\ell) \cong H^1_{\text{et.}}(X_v, \mathbb{Q}_\ell).$$

So, the Grothendieck–Lefschetz trace formula gives $\operatorname{Tr}(\operatorname{Fr}_{v_\beta}^{m/\deg v_\beta} | H^1(J)) = |\mathbb{F}_{r^m}| + 1 - |X_\beta(\mathbb{F}_{r^m})| = A_J(\beta, m)$. □

We now interpret the quantities $A_J(\beta, m)$ appearing in Lemma 4.3 as character sums. Write $\mathbf{1}$ for the trivial multiplicative character. For any $m \geq 1$ and $c \geq 2$ we set

$$\begin{aligned} M_c(r^m) &:= \{ \quad \text{characters } \lambda : \mathbb{F}_{r^m}^\times \to \mathbb{C}^\times \text{ such that } \lambda^c = \mathbf{1}\}, \\ M'_c(r^m) &:= \{\text{nontrivial characters } \lambda : \mathbb{F}_{r^m}^\times \to \mathbb{C}^\times \text{ such that } \lambda^c = \mathbf{1}\}. \end{aligned}$$

We further define $M'_{a,b}(r^m) = M'_a(r^m) \times M'_b(r^m)$ and extend all multiplicative characters λ by $\lambda(0) = 0$. For any pair (λ_2, λ_2) of multiplicative characters on $\mathbb{F}_{r^m}$, any additive character ψ on $\mathbb{F}_{r^m}$ and any $\alpha \in \mathbb{F}_{r^m}$, we set

$$S_{r^m}(\lambda_1, \lambda_2, \psi, \alpha) := \sum_{(w,z) \in (\mathbb{F}_{r^m})^2} \lambda_1(z) \lambda_2(w - z) \psi(\alpha w).$$

With this new notation at hand, we may now state:

Lemma 4.4. *For any non-trivial additive character ψ_r on $\mathbb{F}_r$, and any $m \geq 1$, we have*

$$\sum_{\beta \in \mathbb{F}_{r^m}^\times} A_J(\beta, m) = - \sum_{\substack{\alpha \in \mathbb{F}_{r^m} \cap \mathbb{F}_q, \\ (\lambda_1, \lambda_2) \in M'_{a,b}(r^m)}} S_{r^m}(\lambda_1, \lambda_2, \psi_r \circ \operatorname{Tr}_{\mathbb{F}_{r^m}/\mathbb{F}_r}, \alpha).$$

Remark 4.5. It may seem odd that the right-hand side depends on the choice of a non-trivial additive character ψ_r while, a priori, the left-hand side does not. However, as should be clear after the proof, a different choice of ψ_r merely permutes the terms $S_{r^m}(\lambda_1, \lambda_2, \psi, \alpha)$.

Proof. For a given $\beta \in \mathbb{F}_{r^m}^\times$, we begin by giving an expression of $|X_\beta(\mathbb{F}_{r^m})|$ as a character sum. Recall that the curve X_β has a unique point at infinity. This point is rational over $\mathbb{F}_{r^m}$. We have $|X_\beta(\mathbb{F}_{r^m})| = 1 + \left|\left\{(x,y) \in (\mathbb{F}_{r^m})^2 : x^a + y^b = \beta^q - \beta\right\}\right|$, so that

$$|X_\beta(\mathbb{F}_{r^m})| - 1 = \sum_{x \in \mathbb{F}_{r^m}} \left|\left\{y \in \mathbb{F}_{r^n} : x^a + y^b = \beta^q - \beta\right\}\right|. \tag{4.6}$$

It is classical (see [Coh07, Lemma 2.5.21]) that, given an integer N, for any $z \in \mathbb{F}_{r^m}$, we have

$$\left|\left\{y \in \mathbb{F}_{r^m} : y^N = z\right\}\right| = \sum_{\lambda \in M_N(r^m)} \lambda(z), \tag{4.7}$$

The term corresponding to $\lambda = \mathbf{1}$ contributes 1. Plugging in (4.7) with $N = b$ and $z = -x^a + \beta^q - \beta$ into (4.6) and swapping the sums yields

$$|X_\beta(\mathbb{F}_{r^m})| - 1 = \sum_{\lambda \in M_b(r^m)} \sum_{x \in \mathbb{F}_{r^m}} \lambda(-x^a + \beta^q - \beta) = r^m + \sum_{\lambda \in M_b'(r^m)} \sum_{x \in \mathbb{F}_{r^m}} \lambda(-x^a + \beta^q - \beta).$$

It follows that, for all $\beta \in \mathbb{F}_{r^m}$, we have

$$A_J(\beta, m) = -\sum_{\lambda \in M_b'(r^m)} \sum_{x \in \mathbb{F}_{r^m}} \lambda(-x^a + \beta^q - \beta)\,.$$

For each $\lambda \in M_b'(r^m)$, we use (4.7) once more, this time with $N = a$, to reindex the sum over x in the above display. This yields

$$\begin{aligned}\sum_{x \in \mathbb{F}_{r^m}} \lambda(-x^a + \beta^q - \beta) &= \sum_{z \in \mathbb{F}_{r^m}} \left|\left\{x \in \mathbb{F}_{r^m} : x^a = z\right\}\right| \lambda(-z + \beta^q - \beta) \\ &= \sum_{\theta \in M_a(r^m)} \sum_{z \in \mathbb{F}_{r^m}} \theta(z)\lambda(-z + \beta^q - \beta) = \sum_{\theta \in M_a'(r^m)} \sum_{z \in \mathbb{F}_{r^m}} \theta(z)\lambda(-z + \beta^q - \beta).\end{aligned}$$

To justify the last equality, we note that the term corresponding to $\theta = \mathbf{1}$ does not contribute by orthogonality of characters for $\mathbb{F}_{r^m}$. We have thus proved that

$$A_J(\beta, m) = \sum_{\lambda \in M_b'(r^m)} \sum_{\theta \in M_a'(r^m)} \sum_{z \in \mathbb{F}_{r^m}} \theta(z)\lambda(-z + \beta^q - \beta)\,.$$

Applying orthogonality of characters for $\mathbb{F}_{r^m}^\times$ once again, we also note that if θ and λ are multiplicative characters such that $\theta \neq \lambda^{-1}$, the sum $\sum_{z \in \mathbb{F}_{r^m}} \theta(z)\lambda(-z + \beta^q - \beta)$ vanishes if $\beta^q - \beta = 0$. It follows that from the previous paragraph that, for all $m \geq 1$, we have

$$\begin{aligned}\sum_{\beta \in \mathbb{F}_{r^m}^\times} A_J(\beta, m) &= -\sum_{\beta \in \mathbb{F}_{r^m}^\times} \sum_{\theta \in M_a'(r^m)} \sum_{\lambda \in M_b'(r^m)} \sum_{z \in \mathbb{F}_{r^m}} \theta(z)\lambda(-z + \beta^q - \beta) \\ &= -\sum_{\theta \in M_a'(r^m)} \sum_{\lambda \in M_b'(r^m)} \left(\sum_{\beta \in \mathbb{F}_{r^m}} \sum_{z \in \mathbb{F}_{r^m}} \theta(z)\lambda(-z + \beta^q - \beta)\right). \end{aligned} \tag{4.8}$$

For fixed $(\theta, \lambda) \in M_{a,b}'(r^m)$, we now reindex the inner sum:

$$\sum_{\beta \in \mathbb{F}_{r^m}} \sum_{z \in \mathbb{F}_{r^m}} \theta(z)\lambda(-z + \beta^q - \beta) = \sum_{w \in \mathbb{F}_{r^m}} \left|\left\{\beta \in \mathbb{F}_{r^m} : w = \beta^q - \beta\right\}\right| \left(\sum_{z \in \mathbb{F}_{r^m}} \theta(z)\lambda(-z + w)\right).$$

We now appeal to [Gri19, Lemma 4.5], which states that for any $z \in \mathbb{F}_{r^m}$ and any nontrivial additive character ψ on $\mathbb{F}_{r^m}$ we have

$$\left|\left\{\beta \in \mathbb{F}_{r^m} : w = \beta^q - \beta\right\}\right| = \sum_{\alpha \in (\mathbb{F}_{r^m} \cap \mathbb{F}_q)} \psi(\alpha w)\,. \tag{4.9}$$

Plugging (4.9) into (4.8) and reordering the sums, for any nontrivial additive character ψ on $\mathbb{F}_{r^m}$ we obtain

$$\sum_{\beta \in U(\mathbb{F}_{r^m})} A_J(\beta, m) = - \sum_{\theta \in M'_a(r^m)} \sum_{\lambda \in M'_b(r^m)} \sum_{\alpha \in (\mathbb{F}_{r^m} \cap \mathbb{F}_q)} \left(\sum_{(w,z) \in (\mathbb{F}_{r^m})^2} \theta(z)\lambda(w-z)\psi(\alpha w) \right).$$

Note that the sum between brackets is equal to $S_{r^m}(\theta, \lambda, \psi, \alpha)$.

To conclude, recall that we have fixed a non-trivial additive character ψ_r on $\mathbb{F}_r$. For any integer $m \geq 1$, we write the last display for $\psi = \psi_r \circ \mathrm{Tr}_{\mathbb{F}_{r^m}/\mathbb{F}_r}$, which is indeed a non-trivial additive character on $\mathbb{F}_{r^m}$. This yields that, for any $m \geq 1$,

$$\sum_{\beta \in U(\mathbb{F}_{r^m})} A_J(\beta, m) = - \sum_{(\lambda_1, \lambda_2) \in M'_{a,b}(r^m)} \sum_{\alpha \in (\mathbb{F}_{r^m} \cap \mathbb{F}_q)} S_{r^m}(\lambda_1, \lambda_2, \psi_r \circ \mathrm{Tr}_{\mathbb{F}_{r^m}/\mathbb{F}_r}, \alpha).$$

This identity together with (4.5) yields the lemma. □

Our next step towards proving Theorem 4.2 is to give a more recognizable form to the inner sums which appear in Lemma 4.4.

Lemma 4.6. *Let $m \geq 1$. Given a pair (λ_1, λ_2) of non-trivial multiplicative characters on $\mathbb{F} = \mathbb{F}_{r^m}$, a non-trivial additive character ψ on $\mathbb{F}_{r^m}$ and an element $\alpha \in \mathbb{F}_{r^m}$, we have*

$$S_{r^m}(\lambda_1, \lambda_2, \psi, \alpha) = \mathrm{G}_{\mathbb{F}}(\lambda_1, \psi_\alpha)\mathrm{G}_{\mathbb{F}}(\lambda_2, \psi_\alpha)\,,$$

where ψ_α is the additive character on $\mathbb{F}_{r^m}$ defined by $x \mapsto \psi(\alpha x)$.

Proof. By definition of $S_{r^m}(\lambda_1, \lambda_2, \psi, \alpha)$, we have

$$S_{r^m}(\lambda_1, \lambda_2, \psi, \alpha) = \sum_{z \in \mathbb{F}} \sum_{w \in \mathbb{F}} \lambda_1(z)\lambda_2(w-z)\psi(\alpha w)\,.$$

Re-indexing the inner sum by setting $y = w - z$, we obtain

$$\begin{aligned} S_{r^m}(\lambda_1, \lambda_2, \psi, \alpha) &= \sum_{y \in \mathbb{F}} \sum_{z \in \mathbb{F}} \lambda_1(z)\lambda_2(y)\psi(\alpha y + \alpha z) \\ &= \left(\sum_{y \in \mathbb{F}} \lambda_1(z)\psi(\alpha y) \right) \left(\sum_{z \in \mathbb{F}} \lambda_2(z)\psi(\alpha z) \right) \\ &= \mathrm{G}_{\mathbb{F}_{r^m}}(\lambda_1, \psi_\alpha)\mathrm{G}_{\mathbb{F}_{r^m}}(\lambda_2, \psi_\alpha)\,. \end{aligned}$$

This concludes the proof. Note that both sides vanish if $\alpha = 0$. □

Recall that $o_r(n)$ denotes the multiplicative order of r modulo n and that $\boldsymbol{\chi} : \overline{\mathbb{F}_p}^\times \to \overline{\mathbb{Q}}^\times$ is the Teichmüller character defined in Section 3.1

Lemma 4.7. *Fix an integer $c \geq 1$ which is coprime to p. For $i \in \mathbb{Z}/c\mathbb{Z} \smallsetminus \{0\}$, let $\kappa = o_r\big(c/\gcd(c,i)\big)$. Then, the map*

$$\begin{aligned}\big\{i \in \mathbb{Z}/c\mathbb{Z} \smallsetminus \{0\} : \kappa \mid m\big\} &\to M'_c(r^m)\\ i &\mapsto \Big[x \mapsto \big(\boldsymbol{\chi} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r^\kappa}}\big)(x)^{i(r^\kappa-1)/c}\Big]\end{aligned}$$

is a bijection.

Proof. Choose any $i \in \mathbb{Z}/c\mathbb{Z} \smallsetminus \{0\}$ such that κ divides m. The multiplicative character $\lambda : \mathbb{F}_{r^m}^\times \to \mathbb{C}^\times$ defined by $\lambda(x) = (\boldsymbol{\chi} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r^\kappa}})(x)^{i(r^\kappa-1)/c}$ for all $x \in \mathbb{F}_{r^m}^\times$ has exact order $c/\gcd(i,c)$. In particular, λ is non-trivial and has order dividing c, so $\lambda \in M'_c(r^m)$.

Conversely, let λ be a non-trivial multiplicative character on $\mathbb{F}_{r^m}$ whose c-th power is trivial. The Teichmüller character $\boldsymbol{\chi}$ generates the group of multiplicative characters on $\mathbb{F}_{r^m}$, so $\lambda = \boldsymbol{\chi}^\ell$ for some integer $\ell \in \{1, \dots, r^m - 2\}$. Since λ^c is trivial on $\mathbb{F}_{r^m}^\times$ and since $\boldsymbol{\chi}$ has order exactly $r^m - 1$, there exists an integer $i \geq 1$ such that $\ell c = i(r^m - 1)$. Since $1 \leq \ell \leq r^m - 2$, we have $1 \leq i \leq c - 1$. Letting $c' = c/\gcd(c,i)$ and $i' = i/\gcd(c,i)$, we find that $\ell c' = i'(r^m - 1)$. By construction, $\gcd(c', i') = 1$ and so c' divides $r^m - 1$. In particular the order κ of r modulo c' divides m and so $i'(r^\kappa - 1)/c'$ is an integer. We have $\ell = i(r^m - 1)/c$. So, for all $x \in \mathbb{F}_{r^m}^\times$,

$$\begin{aligned}\lambda(x) = \boldsymbol{\chi}(x)^{i(r^m-1)/c} &= \boldsymbol{\chi}(x)^{\frac{i'(r^\kappa-1)}{c'}(1+r^\kappa+\cdots+r^{m-\kappa})} = \boldsymbol{\chi}\left(x^{1+r^\kappa+\cdots+r^{m-\kappa}}\right)^{\frac{i'(r^\kappa-1)}{c'}}\\ &= \big(\boldsymbol{\chi} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r^\kappa}}\big)(x)^{i(r^\kappa-1)/c}.\end{aligned}$$

Hence λ has the desired form. □

We now connect our last results with the discussion in §3.3– §3.4. We previously introduced the set O of orbits of the action of r on $(\mathbb{Z}/a\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z}/b\mathbb{Z} \setminus \{0\}) \times \mathbb{F}_q^\times$, and denoted the size of an orbit o by $|o|$. We also defined the natural projection maps

$$\begin{aligned}\pi_a &: (\mathbb{Z}/a\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z}/b\mathbb{Z} \setminus \{0\}) \times \mathbb{F}_q^\times \to (\mathbb{Z}/a\mathbb{Z} \setminus \{0\}) \times \mathbb{F}_q^\times \text{ and}\\ \pi_b &: (\mathbb{Z}/a\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z}/b\mathbb{Z} \setminus \{0\}) \times \mathbb{F}_q^\times \to (\mathbb{Z}/b\mathbb{Z} \setminus \{0\}) \times \mathbb{F}_q^\times,\end{aligned}$$

and fixed an additive character ψ_0 on $\mathbb{F}_p$.

For any $m \geq 1$ and $\alpha \in \mathbb{F}_{r^m} \cap \mathbb{F}_q$, write $\psi_{m,\alpha} : \mathbb{F}_{r^m} \to \overline{\mathbb{Q}}$ for the additive character $x \mapsto (\psi_0 \circ \mathrm{Tr}_{\mathbb{F}_{r^m}/\mathbb{F}_p})(\alpha x)$.

Lemma 4.8. *For any $m \geq 1$, we have*

$$\sum_{\substack{o \in O \text{ s.t.}\\ |o| \text{ divides } m}} |o|\, \boldsymbol{\omega}(o)^{m/|o|} = \sum_{\substack{\alpha \in (\mathbb{F}_{r^m} \cap \mathbb{F}_q)^\times,\\ (\lambda_1,\lambda_2) \in M'_{a,b}(r^m)}} \mathrm{G}_{r^m}(\lambda_1, \psi_{m,\alpha}) \mathrm{G}_{r^m}(\lambda_2, \psi_{m,\alpha}).$$

Proof. For any integer $m \geq 1$ and any orbit $o \in O$ we note that $|\pi_a(o)|$ and $|\pi_b(o)|$ both divide $|o|$. If $|o|$ divides m, then $|\pi_a(o)|$ and $|\pi_b(o)|$ must also divide m. Since $\nu_a(o) = |o|/|\pi_a(o)|$, we have

$$\boldsymbol{\omega}(o)^{m/|o|} = \mathbf{G}\left(\pi_a(o)\right)^{m/|\pi_a(o)|} \mathbf{G}\left(\pi_b(o)\right)^{m/|\pi_b(o)|}. \tag{4.10}$$

Pick a representative $(i,j,\alpha) \in S$ of $o \in O$. Then, $(i,\alpha) \in S'_a$ is a representative of $\pi_a(o)$ and $(j,\alpha) \in S'_b$ is a representative of $\pi_b(o)$. We write $r_a = r^{|\pi_a(o)|}$. Using the Hasse–Davenport relation for Gauss sums and noting that $\Psi_{(i,\alpha)} \circ \mathrm{Tr}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_a}} = \psi_{m,\alpha}$ yields

$$\begin{aligned}\mathbf{G}\left(\pi_a(o)\right)^{m/|\pi_a(o)|} &= \mathrm{G}_{r_a}\big(\boldsymbol{\lambda}_{(i,\alpha)}, \Psi_{(i,\alpha)}\big)^{m/\pi_a(o)} = \mathrm{G}_{r^m}\big(\boldsymbol{\lambda}_{(i,\alpha)} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_a}}, \Psi_{(i,\alpha)} \circ \mathrm{Tr}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_a}}\big)\\ &= \mathrm{G}_{r^m}\big(\boldsymbol{\lambda}_{(i,\alpha)} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_a}}, \psi_{m,\alpha}\big).\end{aligned}$$

A similar computation shows

$$\mathbf{G}\left(\pi_b(o)\right)^{m/|\pi_b(o)|} = \mathrm{G}_{r^m}\left(\boldsymbol{\lambda}_{(j,\alpha)} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_b}}, \psi_{m,\alpha}\right).$$

If o is the orbit of $(i,j,\alpha) \in S$, then $|o|$ divides m if and only if (i) $\alpha \in \mathbb{F}_{r^m}$, (ii) the order of r modulo $a/\gcd(a,i)$ divides m (which happens if and only if a divides $i(r^m-1)$) and (iii) the order of r modulo $b/\gcd(b,j)$ divides m (which happens if and only if b divides $j(r^m-1)$).

Recall that we have set $\kappa_{r,a}(i) = o_r(a/\gcd(a,i))$. We have

$$\sum_{\substack{o\in O\\ |o| \text{ divides } m}} |o|\,\boldsymbol{\omega}(o)^{m/|o|} = \sum_{\substack{(i,j,\alpha)\in S\\ \alpha\in\mathbb{F}_{r^m}^\times\\ \kappa_{r,a}(i)|m\\ \kappa_{r,b}(j)|m}} \mathrm{G}_{r^m}\left(\boldsymbol{\lambda}_{(i,\alpha)} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_a}}, \psi_{m,\alpha}\right)\mathrm{G}_{r^m}\left(\boldsymbol{\lambda}_{(j,\alpha)} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_b}}, \psi_{m,\alpha}\right). \tag{4.11}$$

Set $\kappa = \kappa_{r,a}(i)$. Then, κ divides $o_r(a)$ which divides $\pi_a(o)$. Also, note that for any finite field $\mathbb{F}$ of characteristic p and any extension $\mathbb{F}'$ of $\mathbb{F}$, we have $\boldsymbol{\chi}|_{\mathbb{F}} \circ N_{\mathbb{F}'/\mathbb{F}} = (\boldsymbol{\chi}|_{\mathbb{F}'})^{|\mathbb{F}'^\times|/|\mathbb{F}^\times|}$. Together, these imply that

$$\boldsymbol{\lambda}_{(i,\alpha)} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_a}} = (\boldsymbol{\chi} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_a}})^{\frac{i(r_a^\kappa-1)}{a}} = (\boldsymbol{\chi} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_a}} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r^\kappa}})^{\frac{i(r^\kappa-1)}{a}} = (\boldsymbol{\chi} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r^\kappa}})^{\frac{i(r^\kappa-1)}{a}}.$$

So, for any $m \geq 1$, Lemma 4.7 says that as i varies over all elements of $(\mathbb{Z}/a\mathbb{Z} \smallsetminus \{0\})$ satisfying $\kappa_{r,a}(i) \mid m$, the character $\boldsymbol{\lambda}_{(i,\alpha)} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_a}}$ varies over all characters $\lambda_1 \in M_a'(r^m)$. Similarly, as j varies over all elements of $(\mathbb{Z}/b\mathbb{Z} \smallsetminus \{0\})$ satisfying $\kappa_{r,b}(j) \mid m$, the character $\boldsymbol{\lambda}_{(j,\alpha)} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_b}}$ varies over all characters $\lambda_2 \in M_b'(r^m)$. Finally, recall that $S = (\mathbb{Z}/a\mathbb{Z} \setminus \{0\}) \times (\mathbb{Z}/b\mathbb{Z} \setminus \{0\}) \times \mathbb{F}_q^\times$, we see that if $(i,j,\alpha) \in S$, then $\alpha \in \mathbb{F}_q^\times$. Altogether, we conclude that re-indexing the sum on the right-hand side of (4.11) gives the desired result. □

4.4 Proof of Theorem 4.2

We make use of the notation introduced in the previous subsection. By Lemma 4.3, we have

$$\log L(J,T) = \sum_{m\geq 1}\left(\sum_{\beta\in\mathbb{F}_{r^m}^\times} A_J(\beta,m)\right)\frac{T^m}{m}.$$

Combining Lemmas 4.4 and 4.6 yields that, for all $m \geq 1$,

$$\sum_{\beta\in\mathbb{F}_{r^m}^\times} A_J(\beta,m) = -\sum_{\substack{\alpha\in\mathbb{F}_{r^m}\cap\mathbb{F}_q,\\ (\lambda_1,\lambda_2)\in M_{a,b}'(r^m)}} \mathrm{G}_{\mathbb{F}}(\lambda_1,\psi_{m,\alpha})\mathrm{G}_{\mathbb{F}}(\lambda_2,\psi_{m,\alpha}).$$

Here, we may ignore the term $\alpha = 0$ because $\mathrm{G}_{\mathbb{F}}(\lambda_1,\psi_{m,0})\cdot\mathrm{G}_{\mathbb{F}}(\lambda_2,\psi_{m,0})$ vanishes. We combine this identity with Lemma 4.8 to obtain

$$-\log L(J,T) = \sum_{m\geq 1}\left(\sum_{\substack{o\in O \text{ s.t.}\\ |o| \text{ divides } m}} |o|\,\boldsymbol{\omega}(o)^{m/|o|}\right)\frac{T^m}{m}.$$

On the other hand, expanding the logarithm, we see that

$$-\log\prod_{o\in O}(1-\boldsymbol{\omega}(o)T^{|o|}) = \sum_{o\in O}\log\left(1-\boldsymbol{\omega}(o)T^{|o|}\right) = \sum_{o\in O}\sum_{n\geq 1}\frac{\left(\boldsymbol{\omega}(o)T^{|o|}\right)^n}{n}$$
$$= \sum_{m\geq 1}\left(\sum_{\substack{o\in O\\ |o| \text{ divides } m}} |o|\,\boldsymbol{\omega}(o)^{m/|o|}\right)\cdot\frac{T^m}{m}.$$

Therefore,

$$\log L(J,T) = \log\prod_{o\in O}(1-\boldsymbol{\omega}(o)T^{|o|}).$$

Exponentiating this identity concludes the proof of Theorem 4.2.

□

Remark 4.9. We verify the degree of this $L(J,T)$ using Theorem 4.1:

$$\deg L(J,T) = b(J) = \deg N_J - 4g.$$

From this formula and the computation of $\deg N_J$ in Proposition 2.6, we find

$$\deg(L(J,T)) = (a-1)(b-1)(q+1) - 4\frac{(a-1)(b-1)}{2} = (a-1)(b-1)(q-1)\,.$$

Alternately, from our computations in Theorem 4.2, the degree of the $L(J,T)$ is $\sum_{o\in O}|o|$, where O is the set of orbits $\langle r\rangle$ on $S = (\mathbb{Z}/a\mathbb{Z}\setminus\{0\})\times(\mathbb{Z}/b\mathbb{Z}\setminus\{0\})\times\mathbb{F}_q^\times$, where r acts on $(i,j,\alpha)\in S$ via $r\cdot(i,j,\alpha) = (ri, rj, \alpha^{1/r})$, as defined in Section 3.3. The sum of the sizes of these orbits is equal to the size of S, namely $(a-1)(b-1)(q-1)$.

5 The BSD conjecture for J

The special value $L^*(J)$ of the L-function of J at $T = r^{-1}$ is defined as

$$L^*(J) := \left.\frac{L(J,T)}{(1-rT)^v}\right|_{T=r^{-1}}, \quad \text{where } v = \operatorname{ord}_{T=r^{-1}} L(J,T).$$

This definition makes sense since the L-function is a rational function of T (see Theorem 4.1). By definition of $L(J,T)$, the function $\mathcal{L} : s\mapsto L(J,r^{-s})$ is positive on $[3/2,\infty)$ and, by the Riemann Hypothesis for L-functions of abelian varieties over K, the function $\mathcal{L}$ does not vanish on $(1,3/2]$. The special value $L^*(J)$ is thus non-negative. Since $L^*(J)$ is by definition a non-zero rational number, we conclude that $L^*(J)\in\mathbb{Q}_{>0}$.

Let $\widehat{J}$ denote the dual abelian variety to K and let

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

denote the canonical Néron–Tate height divided by $\log r$. Then, $\langle\cdot,\cdot\rangle$ is a bilinear pairing which is nondegenerate modulo torsion. Choosing a basis $P_1,\dots,P_r$ for $J(K)$ modulo torsion and a basis $\widehat{P_1},\dots,\widehat{P_r}$ for $\widehat{J}(K)$ modulo torsion, the regulator of J is defined to be

$$\operatorname{Reg}(J) := |\det\langle P_i,\widehat{P_j}\rangle_{1\leq i,j\leq r}|.$$

In this section, we prove Theorem 1.1, which we restate for convenience:

Theorem 1.1. *Let C and J be as above. The abelian variety J satisfies the Birch and Swinnerton-Dyer conjecture. This means that*

- *The algebraic and analytic ranks of J coincide:* $\operatorname{ord}_{T=r^{-1}} L(J,T) = \operatorname{rank} J(K)$.
- *The Tate–Shafarevich group $Ш(J)$ is finite.*
- *The BSD formula holds:*

$$L^*(J) = \frac{|Ш(J)| \operatorname{Reg}(J) \prod_v c_v(J)}{H(J)\, r^{-g}\, |J(K)_{\mathrm{tors}}|^2}, \tag{5.1}$$

where the $c_v(J)$ are the local Tamagawa numbers of J and $\operatorname{Reg}(J)$ *is the regulator.*

We refer the reader to [Ulm14, §6.2.3] for more details about the Birch and Swinnerton-Dyer conjecture for Jacobians over function fields.

Proof. [Ulm14] proves that any curve over a function field whose associated surface is dominated by a product of curves has a Jacobian which satisfies BSD. We briefly summarize the argument. Any such surface $\mathcal{X}$ satisfies Tate's T_2 conjecture. Namely, $\operatorname{rank} NS(\mathcal{X}) = -\operatorname{ord}_{s=1} \zeta(\mathcal{X}, s)$. Now [Ulm14, Thm. 6.3.1] states that there is an equality

$$\operatorname{ord}_{s=1} L(J,s) - \operatorname{rank} J(K) = -\operatorname{ord}_{s=1} \zeta(\mathcal{X}, s) - \operatorname{rank} NS(\mathcal{X}) \geq 0.$$

Therefore J satisfies the rank part of BSD. $T_2(\mathcal{X})$ implies that $\operatorname{Br}(\mathcal{X})[\ell^\infty]$ is finite for all ℓ, which again by [Ulm14, Thm. 6.3.1] implies the BSD formula for J.

It remains to show that our model $\mathcal{S}$ of C constructed in Section 2.1 is dominated by a product of curves. The curve C becomes constant over a finite extension of K, namely the extension $L := K(u)$ for $u^{ab} = t^q - t$. Let C_0 be the constant curve C_L. Let Y be the curve over the residue field of L corresponding to C_0. Then, $C_0 \times Y$ dominates $\mathcal{S}$. □

Remark 5.1. The more typical statement of the BSD formula is

$$L^*(J) = \frac{|Ш(J)| \operatorname{Reg}(J) \prod_v c_v(J)}{H(J)\, r^{-g}\, |J(K)_{\mathrm{tors}}|\, |J^\vee(K)_{\mathrm{tors}}|}. \tag{5.2}$$

In our case, J is principally polarized since J is the Jacobian of a curve. So, $J \cong J^\vee$. In particular, we have $|J(K)_{\mathrm{tors}}|\, |J^\vee(K)_{\mathrm{tors}}| = |J(K)_{\mathrm{tors}}|^2$. So, our statement agrees with the typical one.

6 Rank and $\mathfrak{p}$-adic valuation of Gauss sums

By the BSD conjecture (Theorem 1.1):

$$\operatorname{rank} J(K) = \operatorname{ord}_{T=r^{-1}} L(J,T)\,. \tag{6.1}$$

In this section, we use our explicit expression for $L(J,T)$ from Theorem 4.2 to study $\operatorname{rank} J(K)$ in terms of the parameters a, b, and q.

Lemma 6.1. *The rank of $J(K)$ is given by*

$$\operatorname{rank} J(K) = \left| \left\{ o \in O : \boldsymbol{\omega}(o) = r^{|o|} \right\} \right|. \tag{6.2}$$

Proof. Using (6.1) for the first equality and Theorem 4.2 for the second, we have

$$\operatorname{rank} J(K) = \operatorname{ord}_{T=r^{-1}} L(J,T) = \operatorname{ord}_{T=r^{-1}} \prod_{o\in O}(1-\boldsymbol{\omega}(o)T^{|o|}) = \sum_{o\in O} \operatorname{ord}_{T=r^{-1}}(1-\boldsymbol{\omega}(o)T^{|o|}).$$

The result follows immediately from the observation that

$$\operatorname{ord}_{T=r^{-1}}(1-\boldsymbol{\omega}(o)T^{|o|}) = \begin{cases} 1 & \text{if } \boldsymbol{\omega}(o) = r^{|o|}, \\ 0 & \text{otherwise.} \end{cases}$$

□

Theorem 6.2. *We have*

$$0 \le \operatorname{rank} J(K) \le (a-1)(b-1)(q-1) = 2g(q-1).$$

Proof. From (6.2), we see that $\operatorname{rank} J(K) \le |O|$. Since O is a set of orbits on a set of cardinality $(a-1)(b-1)(q-1)$, we have $|O| \le (a-1)(b-1)(q-1)$. □

In the remainder of this section, we estimate the rank of $J(K)$ more precisely than in Theorem 6.2 under various assumptions on a, b, and q. In §6.4, we provide conditions on a, b, q so that $\operatorname{rank} J(K) = 0$. In §6.5, we provide conditions so that $\operatorname{rank} J(K)$ is "large," that is, such that the upper bound in Theorem 6.2 is tight.

In order to refine our bounds on $\operatorname{rank} J(K)$, we estimate the right-hand side of (6.2) using explicit results about the Gauss sums appearing in $\boldsymbol{\omega}(o)$. We gather the necessary results in subsections 6.1 and 6.2.

6.1 Explicit Gauss sums

Let $n \ge 2$ be a prime-to-p integer. As in §3.3, we consider the set $S'_n := (\mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q^\times$ equipped with its action of $\langle r \rangle$. We write O'_n for the set of orbits of this action. In this subsection, we describe situations where the values of the Gauss sums $\mathbf{G}(o')$ (for $o' \in O'_n$) may be explicitly determined. We refer to §3.4 for the definition of $\mathbf{G}(o')$.

Recall that for any prime-to-p integer $n \ge 1$, we denote by $o_p(n)$ the multiplicative order of p modulo n *i.e.*, $o_p(n)$ is the least integer $e \ge 1$ such that $p^e \equiv 1 \bmod n$.

Definition 6.3 (Supersingular Integer)**.** A positive prime-to-p integer n is called *supersingular (for p)* if there exists a positive integer $\nu \ge 1$ such that $p^\nu \equiv -1 \pmod{n}$.

Lemma 6.4. *Suppose that n is supersingular for p and $[\mathbb{F}_r : \mathbb{F}_p]$ is odd. Let $o' \in O'_n$ be an orbit with representative (i, α). If $2i \ne n$, then the cardinality of o' is even.*

Proof. Note that if $p^\nu \equiv -1 \pmod{n}$ and $d|n$, then $p^\nu \equiv -1 \pmod{d}$. So, if n is supersingular for p, then any divisor of n is supersingular for p.

If $d > 2$ is a divisor of n and ν_0 is the least positive integer such that $p^{\nu_0} \equiv -1 \pmod{d}$, we have $o_p(d) = 2\nu_0$. In particular, the order $o_p(d)$ is even. Since r is an odd power of p, the multiplicative order of r modulo d is also even.

Given $o' \in O'_n$, choose a representative $(i, \alpha) \in S'_n$. Since $2i \ne n$, we have $n/\gcd(n,i) > 2$. In particular, the previous paragraph implies that $o_r(n/\gcd(n,i))$ is even. On the other hand, we know from equation (3.5) that

$$|o'| = \operatorname{lcm}\left(o_r\left(\frac{n}{\gcd(n,i)}\right), [\mathbb{F}_r(\alpha) : \mathbb{F}_r] \right),$$

whence we conclude that $|o'|$ is even. □

We now describe situations where one can compute $\mathbf{G}(o')$ explicitly.

Lemma 6.5. *Let $p \neq 2$ be an odd prime. Let $n \geq 2$ be an even integer and let $o' \in O'_n$ be an orbit with representative $(n/2, \alpha) \in S'_n$. Then,*

$$\mathbf{G}(o')^2 = (-1)^{(p-1)|o'|\,[\mathbb{F}_r:\mathbb{F}_p]}\, r^{|o'|}\,.$$

If $[\mathbb{F}_r : \mathbb{F}_p]$ is a multiple of 4, then

$$\mathbf{G}(o') = \boldsymbol{\lambda}_{(n/2,\alpha)}(\alpha)^{-1} r^{|o'|/2}\,. \tag{6.3}$$

If $[\mathbb{F}_r : \mathbb{F}_p]$ is a multiple of 4 and α is an square in $(\mathbb{F}')^\times$, then

$$\mathbf{G}(o') = r^{|o'|/2}\,. \tag{6.4}$$

Proof. Write $\mathbb{F}'$ for the extension of $\mathbb{F}_r$ of degree $|o'|$. By Definition 3.5, $\mathbf{G}(o') = \mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(n/2,\alpha)}, \Psi_{(n/2,\alpha)}\big)$. Now, $\boldsymbol{\lambda}_{(n/2,\alpha)} = \boldsymbol{\chi}^{(r^{|o'|}-1)/2}$ is a quadratic character on $(\mathbb{F}')^\times$. The first claim then follows from a short computation on Gauss sums for quadratic characters dating back to Gauss. See [Was97, Lemma 6.1] for a proof.

For the second claim, we not that if $[\mathbb{F}_r : \mathbb{F}_p]$ is a multiple of 4, then $[\mathbb{F}' : \mathbb{F}_p]$ is a multiple of 4. Let $\mathbb{F}$ denote the subextension of $\mathbb{F}'/\mathbb{F}_p$ with $[\mathbb{F}' : \mathbb{F}] = 4$. We deduce from equation (3.2) in §3.2 that

$$\mathbf{G}(o') = \boldsymbol{\lambda}_{(n/2,\alpha)}(\alpha)^{-1}\mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(n/2,\alpha)}, \psi_{\mathbb{F}',1}\big)\,. \tag{6.5}$$

Then, the Hasse–Davenport relation ((3.3) in §3.2) implies that

$$\mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(n/2,\alpha)}, \psi_{\mathbb{F}',1}\big) = \mathrm{G}_{\mathbb{F}'}\Big(\boldsymbol{\chi}|_{\mathbb{F}}^{(|\mathbb{F}|-1)/2} \circ \mathrm{N}_{\mathbb{F}'/\mathbb{F}}, \psi_{\mathbb{F},1} \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}}\Big) = \mathrm{G}_{\mathbb{F}}\Big(\boldsymbol{\chi}^{n(|\mathbb{F}|-1)/2}, \psi_{\mathbb{F},1}\Big)^4\,. \tag{6.6}$$

Since $\boldsymbol{\chi}^{n(|\mathbb{F}|-1)/2}$ is a quadratic character on $\mathbb{F}$, the same computation of Gauss as in the first claim yields that

$$\mathrm{G}_{\mathbb{F}}\Big(\boldsymbol{\chi}^{n(|\mathbb{F}|-1)/2}, \psi_{\mathbb{F},1}\Big)^4 = |\mathbb{F}|^2 = |\mathbb{F}'|^{1/2}\,.$$

The second claim follows by combining the previous three equations.

The third claim is immediate from the fact that $\boldsymbol{\lambda}_{(n/2,\alpha)}$ is a quadratic character on $\mathbb{F}'$. □

Let us recall the following result of Shafarevich and Tate, as stated in [Ulm02, Lemma 8.3].

Lemma 6.6 (Shafarevich–Tate)**.** *Let $\mathbb{F}_0$ be a finite field extension of $\mathbb{F}_p$, and $\mathbb{F}/\mathbb{F}_0$ be a quadratic extension. Let $\psi = \psi_{\mathbb{F},1}$ be the standard nontrivial additive character on $\mathbb{F}$. Let χ be a nontrivial multiplicative character on $\mathbb{F}$ which is trivial upon restriction to $\mathbb{F}_0$. For any element $x \in (\mathbb{F})^\times$ with $\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_0}(x) = 0$, we have*

$$\mathrm{G}_{\mathbb{F}}(\chi, \psi) = -\chi(x)\,|\mathbb{F}_0|\,.$$

We use Lemma 6.6 to prove the following:

Lemma 6.7. *Let $p \neq 2$ be an odd prime. Let $n \geq 2$ be a supersingular integer, and let $o' \in O'_n$ be an orbit with representative $(i, \alpha) \in S'_n$ such that $2i \neq n$. Let ν_i be the smallest positive integer such that $p^{\nu_i} \equiv -1$ modulo $n/\gcd(n, i)$. Then,*

$$\mathbf{G}(o') = (-1)^{\left(1+\frac{i(p^{\nu_i}+1)}{n}\right)\frac{|o'|\,[\mathbb{F}_r:\mathbb{F}_p]}{2\nu_i}}\boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1} r^{|o'|/2}\,. \tag{6.7}$$

In particular, if $[\mathbb{F}_r : \mathbb{F}_p]$ *is a multiple of* $4\nu_i$*, then*

$$\mathbf{G}\left(o'\right) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1} r^{|o'|/2}\,. \tag{6.8}$$

If $[\mathbb{F}_r : \mathbb{F}_p]$ *is a multiple of* $4\nu_i$ *and* α *is an* n*-th power in* $(\mathbb{F}')^\times$*, then*

$$\mathbf{G}\left(o'\right) = r^{|o'|/2}\,. \tag{6.9}$$

Before the proof, we remark that by construction, the exponent of -1 in (6.7) is an integer.

Proof. Let $\mathbb{F}'$ denote the extension of $\mathbb{F}_r$ of degree $|o'|$. By Definition 3.5, we have $\mathbf{G}\left(o'\right) = \mathrm{G}_{\mathbb{F}'}\left(\boldsymbol{\lambda}_{(i,\alpha)}, \Psi_{(i,\alpha)}\right)$. We deduce from equation (3.2) in §3.2 that

$$\mathbf{G}\left(o'\right) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}\mathrm{G}_{\mathbb{F}'}\left(\boldsymbol{\lambda}_{(i,\alpha)}, \psi_{\mathbb{F}',1}\right). \tag{6.10}$$

Set $n' = n/\gcd(n,i)$. Recall that the character $\boldsymbol{\lambda}_{(i,\alpha)} = \boldsymbol{\chi}^{i(r^{|o'|}-1)/n}$ has exact order n'. We now focus on providing an explicit expression for the Gauss sum $\mathrm{G}_{\mathbb{F}'}\left(\boldsymbol{\lambda}_{(i,\alpha)}, \psi_{\mathbb{F}',1}\right)$.

Since n' divides n and n is supersingular for p, we see that n' is also supersingular for p. As in the statement of Lemma 6.7, let ν_i denote the smallest positive integer such that $p^{\nu_i} \equiv -1 \bmod n'$. Since $2i \neq n$, we have $n' > 2$. Hence, the order of p modulo n' is $o_p(n') = 2\nu_i$.

Let $\mathbb{F}_0$ denote the extension of $\mathbb{F}_p$ of degree ν_i and let $\mathbb{F}$ denote its quadratic extension. We claim that $\mathbb{F}$ is a subextension of $\mathbb{F}'/\mathbb{F}_p$. Indeed, $[\mathbb{F}' : \mathbb{F}_p] = [\mathbb{F}_r : \mathbb{F}_p]|o'|$ is a multiple of $[\mathbb{F}_r : \mathbb{F}_p]o_r(n')$ and

$$[\mathbb{F}_r : \mathbb{F}_p]o_r(n') = \frac{[\mathbb{F}_r : \mathbb{F}_p]}{\gcd([\mathbb{F}_r : \mathbb{F}_p], o_p(n'))} o_p(n') = \frac{[\mathbb{F}_r : \mathbb{F}_p]}{\gcd([\mathbb{F}_r : \mathbb{F}_p], o_p(n'))} [\mathbb{F} : \mathbb{F}_p]$$

is in turn an integer multiple of $[\mathbb{F} : \mathbb{F}_p]$.

By construction, n' divides $|\mathbb{F}| - 1$. So, n divides $i(|\mathbb{F}| - 1)$. In particular, we deduce that

$$\boldsymbol{\lambda}_{(i,\alpha)} = \boldsymbol{\chi}|_{\mathbb{F}'}{}^{i(|\mathbb{F}'|-1)/n} = (\boldsymbol{\chi}|_{\mathbb{F}} \circ \mathrm{N}_{\mathbb{F}'/\mathbb{F}})^{i(|\mathbb{F}|-1)/n}.$$

By the Hasse–Davenport relation ((3.3) in §3.2), we have

$$\mathrm{G}_{\mathbb{F}'}\left(\boldsymbol{\lambda}_{(i,\alpha)}, \psi_{\mathbb{F}',1}\right) = \mathrm{G}_{\mathbb{F}'}\left(\boldsymbol{\chi}|_{\mathbb{F}}{}^{i(|\mathbb{F}|-1)/n} \circ \mathrm{N}_{\mathbb{F}'/\mathbb{F}}, \psi_{\mathbb{F},1} \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}}\right) = \mathrm{G}_{\mathbb{F}}\left(\boldsymbol{\chi}^{i(|\mathbb{F}|-1)/n}, \psi_{\mathbb{F},1}\right)^{[\mathbb{F}':\mathbb{F}]}. \tag{6.11}$$

Consider the multiplicative character $\chi = \boldsymbol{\chi}^{i(|\mathbb{F}|-1)/n}$ on $\mathbb{F}$. The character χ has exact order n'. In particular, the order of χ is greater than 2. Since n' divides $p^{\nu_i} + 1$, the restriction of χ to the quadratic subextension $\mathbb{F}_0$ of $\mathbb{F}$ is trivial.

Now, let g be a generator of the cyclic group $\mathbb{F}^\times$. Set $x = g^{(p^{\nu_i}+1)/2}$. Since $|\mathbb{F}^\times|/|\mathbb{F}_0^\times| = p^{\nu_i} + 1$, we have $x \in \mathbb{F}^\times \smallsetminus \mathbb{F}_0^\times$ and $x^2 \in \mathbb{F}_0^\times$. So, $\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_0}(x) = 0$.

With this choice of x, Lemma 6.6 gives $\mathrm{G}_{\mathbb{F}}(\chi, \psi_{\mathbb{F},1}) = -\chi(x)|\mathbb{F}|^{1/2}$. Moreover,

$$\chi(x) = \boldsymbol{\chi}\left(g^{\frac{p^{\nu_i}+1}{2}}\right)^{i(|\mathbb{F}|-1))/n} = \boldsymbol{\chi}\left(g^{\frac{|\mathbb{F}|-1}{2}}\right)^{i(p^{\nu_i}+1)/n} = \boldsymbol{\chi}\,(-1)^{i(p^{\nu_i}+1)/n} = (-1)^{i(p^{\nu_i}+1)/n}.$$

It follows that

$$\mathrm{G}_{\mathbb{F}}(\chi, \psi_{\mathbb{F},1}) = (-1)^{1+i(p^{\nu_i}+1)/n}|\mathbb{F}|^{1/2}. \tag{6.12}$$

We now put (6.10), (6.11), and (6.12) together to deduce that

$$\mathbf{G}\left(o'\right) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}(-1)^{[\mathbb{F}':\mathbb{F}]\,(1+i(p^{\nu_i}+1)/n)}\,|\mathbb{F}'|^{1/2}\,.$$

Finally, we note that

$$[\mathbb{F}' : \mathbb{F}] = \frac{[\mathbb{F}' : \mathbb{F}_r][\mathbb{F}_r : \mathbb{F}_p]}{[\mathbb{F} : \mathbb{F}_p]} = \frac{|o'|\,[\mathbb{F}_r : \mathbb{F}_p]}{2\nu_i}.$$

This completes the proof of (6.7).

If $[\mathbb{F}_r : \mathbb{F}_p]$ is a multiple of $4\nu_i$, then

$$\frac{|o'|\,[\mathbb{F}_r : \mathbb{F}_p]}{2\nu_i}\left(1 + \frac{i(p^{\nu_i}+1)}{n}\right)$$

is even and $\mathbf{G}(o') = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}|\mathbb{F}'|^{1/2}$. On the other hand, if $\alpha \in \mathbb{F}_q^\times$ is a n-th power in $(\mathbb{F}')^\times$, we have $\boldsymbol{\lambda}_{(i,\alpha)}(\alpha) = 1$ because the order of $\boldsymbol{\lambda}_{(i,\alpha)}$ divides n. □

6.2 Denominators of $\mathfrak{p}$-adic valuation of Gauss sums

We work with the same notation as in the previous subsection. Recall that we have fixed a prime ideal $\mathfrak{p}$ of $\overline{\mathbb{Q}}$ above p. This choice allowed us to define the Teichmüller character $\boldsymbol{\chi} : \overline{\mathbb{F}_p}^\times \to \overline{\mathbb{Q}}^\times$, in §3.1. Recall also that $\nu_\mathfrak{p}$ denotes the valuation on $\overline{\mathbb{Q}}$ associated to $\mathfrak{p}$, normalised so that $\nu_\mathfrak{p}(r) = 1$. Throughout this section, given $x \in \mathbb{R}$, we let $\{x\}$ denote the fractional part of x.

Let $n \geq 2$ be an integer coprime to p. For any orbit $o' \in O'_n$, the $\mathfrak{p}$-adic valuation of the Gauss sum $\mathbf{G}(o')$ is a non-negative rational number.

For any orbit $o' \in O'_n$, we write $\nu_\mathfrak{p}(\mathbf{G}(o'))/|o'|$ as a reduced fraction:

$$\frac{\nu_\mathfrak{p}(\mathbf{G}(o'))}{|o'|} = \frac{\mathrm{H}(o')}{Д(o')},$$

for integers $\mathrm{H}(o') \geq 0$, $Д(o') \geq 1$ such that $\gcd(\mathrm{H}(o'), Д(o')) = 1$.

Our goal in this section is to control $Д(o')$ under various hypotheses on p, r, and n. We begin with an immediate consequence of Lemmas 6.5 and 6.7.

Lemma 6.8. *Suppose $n \geq 2$ is supersingular for p. Then, for all $o' \in O'_n$, $\mathrm{H}(o')/Д(o') = 1/2$.*

When n is not supersingular for p, we need to do more work to control $Д(o')$. Our main tool is the following lemma, which gives an explicit formula for $\nu_\mathfrak{p}(\mathbf{G}(o'))/|o'|$.

For $x \in \mathbb{R}$, let

Lemma 6.9. *Let $n \geq 2$ be an integer coprime to p. Let $o' \in O'_n$ be an orbit and pick a representative $(i,\alpha) \in S'_n$ of o'. Let $\mu = [\mathbb{F}_r : \mathbb{F}_p]\,|o'|$. Write $i \in \mathbb{Z}$ for any lift of $i \in \mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}$. Then,*

$$\frac{\nu_\mathfrak{p}(\mathbf{G}(o'))}{|o'|} = \frac{1}{\mu}\sum_{k=0}^{\mu-1}\left\{\frac{-ip^k}{n}\right\}, \tag{6.13}$$

where $\{x\}$ denote the fractional part of $x \in \mathbb{R}$.

The proof of Lemma 6.9 relies on a version of Stickelberger's Theorem. We use Lemma 6.14 from [Was97], which we restate here in our notation for the reader's convenience. The extra factor $[\mathbb{F}_r : \mathbb{F}_p]$ appearing in our statement comes from our different choice of normalization for $\nu_\mathfrak{p}$.

Theorem 6.10 (Stickelberger's Theorem)**.** *Let $\mathbb{F}$ be a finite extension of $\mathbb{F}_p$ with degree $\mu = [\mathbb{F} : \mathbb{F}_p]$. Fix an integer s such that $0 < s < p^\mu - 1$. For any nontrivial additive character ψ on $\mathbb{F}$, we have*

$$\nu_\mathfrak{p}\left(\mathrm{G}_\mathbb{F}\left((\boldsymbol{\chi}|_{\mathbb{F}^\times})^{-s}, \psi\right)\right) = \frac{1}{[\mathbb{F}_r : \mathbb{F}_p]}\sum_{k=0}^{\mu-1}\left\{\frac{sp^k}{p^\mu - 1}\right\},$$

where $\{x\}$ denote the fractional part of $x \in \mathbb{R}$. Here, as above, $\boldsymbol{\chi}$ denotes the Teichmüller character.

Proof of Lemma 6.9. Let $(i,\alpha) \in S'_n$ be a representative of the orbit $o' \in O'_n$. Let $\mathbb{F}'$ denote the finite field extension of $\mathbb{F}_r$ of degree $|o'|$. By Definition 3.5 in §3.4,

$$\mathbf{G}\left(o'\right) = \mathrm{G}_{\mathbb{F}'}\left(\boldsymbol{\lambda}_{(i,\alpha)}, \Psi_{(i,\alpha)}\right) = \mathrm{G}_{\mathbb{F}'}\left(\left(\boldsymbol{\chi}|_{(\mathbb{F}')^\times}\right)^{i(r^{|o'|}-1)/n}, \Psi_{(i,\alpha)}\right).$$

Since $\alpha \neq 0$, the additive character $\Psi_{(i,\alpha)}$ on $\mathbb{F}'$ is non-trivial.

Note that $[\mathbb{F}' : \mathbb{F}_p] = |o'| \cdot [\mathbb{F}_r : \mathbb{F}_p] = \mu$ and $r^{|o'|} = p^\mu$. Moreover, $r^{|o'|}$ acts trivially on $(\mathbb{Z}/n\mathbb{Z})^\times$, so $i(r^{|o'|}-1)/n$ is an integer. Applying Stickelberger's Theorem (Theorem 6.10) gives

$$\frac{\nu_{\mathfrak{p}}(\mathbf{G}\left(o'\right))}{|o'|} = \frac{1}{[\mathbb{F}_r : \mathbb{F}_p]\,|o'|} \sum_{k=0}^{\mu-1} \left\{ \frac{-i(r^{|o'|}-1)}{n} \frac{p^k}{p^\mu - 1} \right\} = \frac{1}{\mu} \sum_{k=0}^{\mu-1} \left\{ \frac{-ip^k}{n} \right\}.$$

□

Corollary 6.11. *Let $n \geq 1$ be a prime-to-p integer. For any orbit $o' \in O'_n$, we have*

$$\frac{1}{n} \leq \frac{\nu_{\mathfrak{p}}(\mathbf{G}\left(o'\right))}{|o'|} = \frac{\mathrm{H}(o')}{Д(o')} \leq 1 - \frac{1}{n}.$$

In particular, $1 \leq \mathrm{H}(o') < Д(o')$.

Proof. Let $(i,\alpha) \in S'_n$ be a representative of o'. We lift $i \in \mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}$ to $i \in \mathbb{Z}$.

In the notation of Lemma 6.9, for any $k \in \{0,\dots,\mu-1\}$, we have $1/n \leq \left\{-ip^k/n\right\} \leq (n-1)/n$ because i is not a multiple of n, and p is relatively prime to n. To conclude, sum these inequalities over all k from 0 to $\mu - 1$ and apply (6.13) from Lemma 6.9. □

We now prove a more precise estimate on the denominator of $\nu_{\mathfrak{p}}(\mathbf{G}\left(o'\right))/|o'|$. The following may be viewed as a bound on the denominators of slopes of the $\mathfrak{p}$-adic Newton polygon of the L-function of the projective curve defined over $\mathbb{F}_r$ by $y^n = t^q - t$.

Proposition 6.12. *Let $n \geq 2$ be an integer coprime to p. Let $o' \in O'_n$ be an orbit with representative $(i,\alpha) \in S'_n$. Then,*

$$Д(o') \text{ divides } \frac{n}{\gcd(n,i)} o_p\left(\frac{n}{\gcd(n,i)}\right)$$

In particular, $Д(o')$ divides $n\, o_p(n)$.

Proof. In this proof, we use the same notation as in that of Lemma 6.9. With $\mu = |o'|[\mathbb{F}_r : \mathbb{F}_p]$, we know from Lemma 6.9 that

$$\frac{\mathrm{H}(o')}{Д(o')} = \frac{\nu_{\mathfrak{p}}(\mathbf{G}\left(o'\right))}{|o'|} = \frac{1}{\mu} \sum_{k=0}^{\mu-1} \left\{ \frac{-ip^k}{n} \right\}. \tag{6.14}$$

To lighten notation, set $\kappa = o_p(n/\gcd(n,i))$. We remark that κ divides $o_p(n)$, which divides $o_r(n)[\mathbb{F}_r : \mathbb{F}_p]$, which in turn divides $|o'|[\mathbb{F}_r : \mathbb{F}_p]$. In particular, κ divides μ.

In the sum on the right-hand side of (6.14), write the Euclidean division of any index $k \in \{0,\dots,\mu-1\}$ by κ as $k = x\kappa + y$ with $y \in \{0,\dots,\kappa-1\}$ and $x \in \{0,\dots,\mu/\kappa\}$. One may then rewrite the sum in the following form:

$$\frac{1}{\mu} \sum_{k=0}^{\mu-1} \left\{ \frac{-ip^k}{n} \right\} = \frac{1}{\mu} \sum_{y=0}^{\kappa-1} \sum_{x=0}^{\mu/\kappa-1} \left\{ \frac{-ip^y p^{x\kappa}}{n} \right\}.$$

Since $\kappa = o_p(n/\gcd(n,i))$, we have $ip^\kappa \equiv i \pmod n$, so the inner sums (over x) are equal as y varies. More precisely,

$$\sum_{x=0}^{\mu/\kappa-1} \left\{\frac{-ip^y p^{x\kappa}}{n}\right\} = \sum_{x=0}^{\mu/\kappa-1} \left\{\frac{-ip^y}{n}\right\} = \frac{\mu}{\kappa}\left\{\frac{-ip^y}{n}\right\}.$$

Summing this equality over all $y \in \{0,\dots,\kappa-1\}$, we deduce that

$$\frac{\mathrm{H}(o')}{Д(o')} = \frac{1}{\mu}\sum_{y=0}^{\kappa-1}\frac{\mu}{\kappa}\left\{\frac{-ip^y}{n}\right\} = \frac{1}{\kappa}\sum_{y=0}^{\kappa-1}\left\{\frac{-ip^y}{n}\right\}. \tag{6.15}$$

Each term $\{-ip^y/n\}$ in the right-most sum in (6.15) is a rational number with denominator $n/\gcd(n,ip^y) = n/\gcd(n,i)$. So, the right-most sum in (6.15) is a rational number with denominator dividing $n/\gcd(n,i)$. After division by $\kappa = o_p(n/\gcd(n,i))$, we conclude that $Д(o')$ divides $o_p(n/\gcd(n,i)) \cdot n/\gcd(n,i)$.

The order of p modulo any divisor of n divides the order of p modulo n, so $o_p(n/\gcd(n,i))$ divides $o_p(n)$. This proves the second assertion of the proposition. □

6.3 Explicit $\mathfrak{p}$-adic valuations of $\omega(o)$

We now come back to the general setting of this paper. We fix a finite extension $\mathbb{F}_r$ of $\mathbb{F}_p$. For any pair (a,b) of relatively prime integers which are both coprime to p, and for any power q of p, we consider the Jacobian J of the curve C over $K = \mathbb{F}_r(t)$.

As was shown in Section 4.2, the L-function of J involves certain character sums $\boldsymbol{\omega}(o)$, indexed by orbits $o \in O = O_{a,b,q,r}$. By Definition 3.6, we have

$$\forall o \in O, \qquad \boldsymbol{\omega}(o) = \mathbf{G}\left(\pi_a(o)\right)^{|o|/|\pi_a(o)|}\mathbf{G}\left(\pi_b(o)\right)^{|o|/|\pi_b(o)|},$$

where $\pi_a : O \to O'_a$ and $\pi_b : O \to O'_b$ are the maps introduced in Section 3.3. For any orbit $o \in O$, in the notation introduced in §6.2, we thus have

$$\frac{\nu_{\mathfrak{p}}(\boldsymbol{\omega}(o))}{|o|} = \frac{\mathrm{H}(\pi_a(o))}{Д(\pi_a(o))} + \frac{\mathrm{H}(\pi_b(o))}{Д(\pi_b(o))}. \tag{6.16}$$

In the upcoming subsection, it will be useful to know of situations in which $\nu_{\mathfrak{p}}(\boldsymbol{\omega}(o)) \neq |o|$.

From the previous subsection, we deduce the following:

Lemma 6.13. *Let a,b,q,r be as above. Assume that one of the following holds:*

(1) $ao_p(a)$ and $bo_p(b)$ are relatively prime,

(2) $ao_p(a)$ is odd, and b is supersingular for p,

(3) a is supersingular for p, and $bo_p(b)$ is odd.

Then, for any orbit $o \in O = O_{a,b,q,r}$, we have $\nu_{\mathfrak{p}}(\boldsymbol{\omega}(o)) \neq |o|$.

Proof. Let $o \in O$ be an orbit. If condition *(1)* is satisfied, then $\gcd(Д(\pi_a(o)), Д(\pi_b(o))) = 1$ by Proposition 6.12. Hence, $Д(\pi_a(o)) \neq Д(\pi_b(o))$ unless both $Д(\pi_a(o)) = 1$ and $Д(\pi_b(o)) = 1$. This situation does not occur, by Corollary 6.11.

If a is supersingular for p, then $Д(\pi_a(o)) = 2$ by Lemma 6.8. By Proposition 6.12, $Д(\pi_b(o))$ divides $bo_r(b)$. Hence, if $bo_r(b)$ is odd, so is $Д(\pi_b(o))$. In particular, if *(2)* is satisfied, then

$Д(\pi_a(o)) \neq Д(\pi_b(o))$. The case where *(3)* holds is treated in a similar way, by switching the roles of a and b.

In all three situations, we have shown that $Д(\pi_a(o)) \neq Д(\pi_b(o))$. Since two reduced fractions with different denominators cannot sum to 1, the result now immediately follows from (6.16). □

Lemma 6.14 shows that there are infinitely many choices for a and b satisfying each of the hypotheses of Lemma 6.13.

Lemma 6.14. *For any fixed p, each of the following conditions:*

(1) $ao_p(a)$ and $bo_p(b)$ are relatively prime,

(2) $ao_p(a)$ is odd, and b is supersingular for p,

(3) a is supersingular for p, and $bo_p(b)$ is odd.

is satisfied for infinitely many a and b. Moreover, each condition is satisfied for infinitely many primes *a and b.*

Proof. First, consider condition *(2)*. If k is an odd positive integer and a is any odd divisor of $p^k - 1$, then $o_p(a)$ divides k. So, $ao_p(a)$ is odd too. We claim that there are infinitely many such integers a. Indeed, for any odd integer k, the integer $a = (p^k - 1)/(p - 1)$ is odd. On the other hand, there are infinitely many supersingular prime numbers b, all but finitely many of which are coprime to any particular choice of a. Condition *(3)* can be satisfied by exchanging the role of a and b.

We now consider condition *(1)*. Choose any odd prime $k \geq 3$ so that $p \not\equiv 1 \pmod{k}$ and take $a = (p^k - 1)/(p - 1)$. Choose any odd prime ℓ which is relatively prime to both k and a and which does not divide $o_p(k)$. There are infinitely many such ℓ. If we set $b = (p^\ell - 1)/(p - 1)$, then $b \not\equiv 0 \pmod{k}$. We have $ao_p(a) = ak$ and $bo_p(b) = b\ell$. By construction, $\gcd(a, \ell) = \gcd(k, \ell) = 1$, and $\gcd(b, k) = 1$. Finally,

$$\gcd(a, b) = \frac{\gcd(p^k - 1, p^\ell - 1)}{p - 1} = \frac{p^{\gcd(k,\ell)} - 1}{p - 1} = \frac{p - 1}{p - 1} = 1\,.$$

Modifying these constructions slightly and still keeping p fixed, we may arrange that a and b are both primes, as we now explain.

Let T be the set of primes k so that $p^k - 1$ is a product of primes dividing $p - 1$. We first show that T is finite. By work of Siegel, given any set S of primes, the set of solutions to $x - y = 1$ in S-units x and y is finite. Let S be the set of primes dividing $p(p - 1)$. Then, for each $k \in T$, the pair $x = p^k$, $y = p^k - 1$, is a solution to the S-unit equation. Hence, by Siegel's Theorem, T is finite. In particular, if we choose distinct odd primes $k, \ell \notin T$ in the preceding constructions, we may choose a and b to be odd prime factors of $p^k - 1$ and $p^\ell - 1$ respectively, and which do not divide $p - 1$. We conclude that $ao_p(a)$ and $bo_p(b)$ will still be relatively prime odd integers.

A similar argument shows that there are infinitely many supersingular primes b for p. So, conditions *(2)* and *(3)* are also satisfied for infinitely many primes a and b. □

6.4 Rank 0

It follows from (6.2) that

$$\operatorname{rank} J(K) = \operatorname{ord}_{T=r^{-1}} L(J, T) \leq \left|\left\{o \in O : \nu_{\mathfrak{p}}(\boldsymbol{\omega}(o)) = |o|\right\}\right|.$$

Hence, to show that the rank is "small" it suffices to give conditions on a, b, q that ensure that "many" orbits $o \in O$ satisfy $\nu_{\mathfrak{p}}(\boldsymbol{\omega}(o)) \neq |o|$. We prove:

Theorem 1.2. *Suppose that the pair (a, b) satisfies one of the following:*

(1) $ao_p(a)$ and $bo_p(b)$ are relatively prime,

(2) $ao_p(a)$ is odd, and b is supersingular for p,

(3) a is supersingular for p, and $bo_p(b)$ is odd.

Then, for any power q of p, we have $\operatorname{ord}_{T=r^{-1}} L(J,T) = \operatorname{rank} J(K) = 0$.

Proof. The conditions here are the same as in Lemma 6.13. That Lemma asserts that, for all orbits $o \in O = O_{r,a,b,q}$, the $\mathfrak{p}$-adic valuation of $\boldsymbol{\omega}(o)$ does not match that of $r^{|o|}$ (which equals $|o|$).

The assertion is then immediate from (6.2). □

Example 6.15. Let $\mathbb{F}_r = \mathbb{F}_{67^n}$ for some $n \geq 1$. For $p = 67$, the pair $a = 5$ and $b = 7$ satisfies condition *(3)* of Theorem 1.2. So, if q is any power of 67, the Jacobian $J = J_{a,b,q}$ satisfies $\operatorname{rank} J(\mathbb{F}_r(t)) = 0$.

For a fixed odd prime p, the set of parameters a, b for which the conditions of Theorem 1.2 hold is infinite, as shown in Lemma 6.14.

6.5 Large ranks

We now provide a sufficient condition on a, b and q for the rank of $J(K)$ to be "large". We actually prove a more precise result, estimating the rank of $J(K)$ under certain assumptions. First, we prove a lemma to calculate $\boldsymbol{\omega}(o)$ for $o \in O$.

Lemma 6.16. *Assume that $p \neq 2$ is an odd prime. Let a and b be relatively prime positive integers which are both supersingular for p. Let $\nu_a, \nu_b \geq 1$ be the least positive integers such that $p^{\nu_a} \equiv -1 \pmod{a}$ and $p^{\nu_b} \equiv -1 \pmod{b}$. Suppose also that $[\mathbb{F}_r : \mathbb{F}_p]$ is a multiple of both $4\nu_a$ and $4\nu_b$.*

If (i, j, α) is any representative of the orbit $o \in O$, then

$$\boldsymbol{\omega}(o) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}\boldsymbol{\lambda}_{(j,\alpha)}(\alpha)^{-1} r^{|o|}\,. \tag{6.17}$$

In particular, $\boldsymbol{\omega}(o) = r^{|o|}$ if and only if $\alpha \in \mathbb{F}_q$ is an $(ab)^{th}$ power in $\mathbb{F}_r(\alpha)$ for any representative (i, j, α) of o (equivalently for all representatives (i, j, α) of o).

Proof. Since $4\nu_a$ divides $[\mathbb{F}_r : \mathbb{F}_p]$ and $p^{\nu_a} \equiv -1 \pmod{a}$, we see that $r \equiv 1 \pmod{a}$. Hence $\langle r \rangle$ acts trivially by multiplication on $\mathbb{Z}/a\mathbb{Z} \smallsetminus \{0\}$. Similarly, $r \equiv 1 \pmod{b}$, so $\langle r \rangle$ acts trivially by multiplication on $\mathbb{Z}/b\mathbb{Z} \smallsetminus \{0\}$. Hence, the orbit o is of the form $\{(i, j, \alpha(o)^{1/r^t}) : t \in \mathbb{Z}\}$ for some $(i, j, \alpha) \in S$ depending on o. We then have $|o| = |\pi_a(o)| = |\pi_b(o)|$.

In particular,

$$\boldsymbol{\omega}(o) = \mathbf{G}\left(\pi_a(o)\right)\mathbf{G}\left(\pi_b(o)\right).$$

We may now apply Lemma 6.5 (resp. Lemma 6.7) to compute $\mathbf{G}\left(\pi_a(o)\right)$ when $2i = n$ (resp. $2i \neq n$). Since $4\nu_a$ divides $[\mathbb{F}_r : \mathbb{F}_p]$ and the ν_i's appearing in Lemmas 6.5 and 6.7 applied to $\mathbf{G}\left(\pi_a(o)\right)$ are divisors of ν_a, we have $4\nu_i | [\mathbb{F}_r : \mathbb{F}_p]$. So, equations (6.3) and (6.8) hold. We find that $\mathbf{G}\left(\pi_a(o)\right) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1} \cdot r^{|o'|/2}$. Computing $\mathbf{G}\left(\pi_b(o)\right)$ in the same way yields that

$$\boldsymbol{\omega}(o) = \mathbf{G}\left(\pi_a(o)\right)\mathbf{G}\left(\pi_b(o)\right) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}\boldsymbol{\lambda}_{(j,\alpha)}(\alpha)^{-1} r^{|o|}\,.$$

Now, $\boldsymbol{\lambda}_{(i,\alpha)}$ and $\boldsymbol{\lambda}_{(j,\alpha)}$ are characters of relatively prime orders a and b, so $\boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}\boldsymbol{\lambda}_{(j,\alpha)}(\alpha)^{-1} = 1$ if and only if both $\boldsymbol{\lambda}_{(i,\alpha)}(\alpha) = 1$ and $\boldsymbol{\lambda}_{(j,\alpha)}(\alpha) = 1$.

Since $|\pi_a(o)|$ and $|\pi_b(o)|$ are both equal to the size of the orbit of r acting on $\mathbb{F}_q^\times$, the extensions of $\mathbb{F}_r$ of degree $|\pi_a(o)|$ and $|\pi_b(o)|$ are both $\mathbb{F}_r(\alpha)$. This is the extension over which both $\boldsymbol{\lambda}_{(i,\alpha)}$ and $\boldsymbol{\lambda}_{(j,\alpha)}$ are defined. To conclude, observe that $\boldsymbol{\lambda}_{(i,\alpha)}(\alpha) = \boldsymbol{\lambda}_{(j,\alpha)}(\alpha) = 1$ if and only if α is an $(ab)^{\text{th}}$ power in $\mathbb{F}_r(\alpha)$. □

Theorem 1.3. *Let $p \neq 2$ be an odd prime. Let a and b be relatively prime positive integers which are both supersingular for p. Let $\nu_a, \nu_b \geq 1$ be the least positive integers such that $p^{\nu_a} \equiv -1 \pmod{a}$ and $p^{\nu_b} \equiv -1 \pmod{b}$. Suppose also that $[\mathbb{F}_r : \mathbb{F}_p]$ is a multiple of both $4\nu_a$ and $4\nu_b$.*

Then, we have

$$(a-1)(b-1)\left\lceil \frac{1}{\log_p(q)} \left(\frac{q-1}{ab} - \frac{p\sqrt{q}-1}{p-1} \right) \right\rceil \leq \operatorname{rank} J(K) .$$

Proof of Theorem 1.3. Combining Lemma 6.1 and Lemma 6.16 gives that $\operatorname{rank} J(K)$ is equal to the number of orbits $o \in O$ such that a representative (i, j, α) satisfies the property that α is an $(ab)^{\text{th}}$ power in $\mathbb{F}_r(\alpha)$.

We first bound the number of $\alpha \in \mathbb{F}_q^\times$ such that α is an $(ab)^{\text{th}}$ power in $\mathbb{F}_p(\alpha)$. We remark that $\mathbb{F}_q^\times$ contains at least $(q-1)/ab$ distinct values which are ab^{th} powers. Indeed the image of the map $x \in \mathbb{F}_q^\times \mapsto x^{ab} \in \mathbb{F}_q^\times$ has order $|\mathbb{F}_q^\times| / \gcd(ab, |\mathbb{F}_q^\times|) = (q-1)/\gcd(ab, q-1)$. Note that $\gcd(ab, q-1) \leq ab$. Now, at most $q^{1/2} + q^{1/2}p^{-1} + \cdots + 1 = (p\sqrt{q}-1)(p-1)$ elements of $\mathbb{F}_q$ lie in a proper subfield, since each proper subfield has order a distinct power of p which is at most $\sqrt{q}$. Hence, there are at least

$$\frac{q-1}{ab} - \frac{p\sqrt{q}-1}{p-1}$$

distinct values $\alpha \in \mathbb{F}_q$ such that $\mathbb{F}_p(\alpha) = \mathbb{F}_q$ and α is an $(ab)^{\text{th}}$ power in $\mathbb{F}_p(\alpha)$. Moreover, each orbit of $\langle r \rangle$ on $\mathbb{F}_q^\times$ contains at most $[\mathbb{F}_q : \mathbb{F}_p] = \log_p(q)$ many such α.

Since $\langle r \rangle$ acts trivially on both $\mathbb{Z}/a\mathbb{Z}$ and $\mathbb{Z}/b\mathbb{Z}$ under the hypotheses, the number of orbits $o \in O$ such that a representative (i, j, α) satisfies the property that α is an $(ab)^{\text{th}}$ power in $\mathbb{F}_r(\alpha)$ is at least

$$(a-1)(b-1)\left\lceil \frac{1}{\log_p(q)} \left(\frac{q-1}{ab} - \frac{p\sqrt{q}-1}{p-1} \right) \right\rceil .$$

□

Theorem 6.17. *Let $p \neq 2$ be an odd prime. Let a and b be relatively prime positive integers which are both supersingular for p. Let $\nu_a, \nu_b \geq 1$ be the least positive integers such that $p^{\nu_a} \equiv -1 \pmod{a}$ and $p^{\nu_b} \equiv -1 \pmod{b}$. Suppose that $[\mathbb{F}_r : \mathbb{F}_p]$ is a multiple of $4\nu_a, 4\nu_b$, and $ab(q-1)$. Then,*

$$\operatorname{rank} J(K) = (a-1)(b-1)(q-1) = 2g(q-1) .$$

In other words, the upper bound in Theorem 6.2 is met.

Proof. Under these assumptions, the product $ab(q-1)$ divides $r-1$, hence $\langle r \rangle$ acts trivially on S. Hence each orbit $o \in O$ has $|o| = 1$. Moreover, each $\alpha \in \mathbb{F}_q$ is an $(ab)^{\text{th}}$ power in $\mathbb{F}_r$ (and therefore also in $\mathbb{F}_r(\alpha)$.) Then, Lemma 6.1 and Lemma 6.16 together imply

$$\operatorname{rank} J(K) = |O| = (a-1)(b-1)(q-1) .$$

□

Remark 6.18. [Hypotheses of Theorems 1.3 and 6.17] For any fixed p, there are infinitely many choices of a, b, r satisfying the hypotheses of Theorem 1.3 and Theorem 6.17, as we now explain.

For instance, for any choice of a and b, a positive density of primes p satisfy $p \equiv -1 \pmod{ab}$. In that case we may take $\nu_a = \nu_b = 1$. Let $\mathbb{F}$ be the smallest extension of $\mathbb{F}_p$ such that 4 divides $[\mathbb{F} : \mathbb{F}_p]$. The hypotheses of Theorem 1.3 hold whenever $\mathbb{F}_r \supset \mathbb{F}$. Let t be the order of p in $\mathbb{Z}/ab(q-1)\mathbb{Z}$. Let $\mathbb{F}'$ be the smallest extension of of $\mathbb{F}_p$ such that both 4 and t divide $[\mathbb{F}' : \mathbb{F}_p]$. The hypotheses of Theorem 6.17 are satisfied whenever $\mathbb{F}_r \supset \mathbb{F}'$.

In fact, if a and b are prime, the required ν_a and ν_b exist whenever p has even order in both $(\mathbb{Z}/a\mathbb{Z})^\times$ and $(\mathbb{Z}/b\mathbb{Z})^\times$. Again, Theorem 1.3 holds whenever $\mathbb{F}_r$ contains an appropriate finite extension of $\mathbb{F}_p$. The same is true for Theorem 6.17.

Remark 6.19. Theorem 1.3 implies that when both a and b are supersingular for p and $[\mathbb{F}_r : \mathbb{F}_p]$ is a fixed multiple of some number depending only on a, b, and p, the analytic rank of J is unbounded as $q \to \infty$. This means that if we take a and b to be distinct primes, the Jacobians of the curves $y^b + x^a = t^q - t$ as q varies give a family of simple abelian varieties of dimension $(a-1)(b-1)/2$ which satisfy BSD and which have unbounded algebraic and analytic rank. The dimension can be made arbitrarily large by increasing a and b.

7 Size of the special value

Recall that the special value $L^*(J)$ is defined as

$$L^*(J) := \left.\frac{L(J,T)}{(1-rT)^v}\right|_{T=r^{-1}}, \quad \text{where } v = \operatorname{ord}_{T=r^{-1}} L(J,T).$$

As discussed in Section 5, the Riemann Hypothesis for $L(J,T)$ implies that $L^*(J)$ is a positive rational number. The goal of this section is to prove the following estimate on $L^*(J)$:

Theorem 1.6. *For fixed a, b as above, as $q \to \infty$ through powers of p, we have*

$$\frac{\log L^*(J)}{\log H(J)} = o(1),$$

where the implicit constants depend only on a, b and p.

7.1 Preliminary estimates

The proof of Theorem 1.6 requires two preliminary estimates that we now state.

We choose, once and for all, an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. We write $\log : \mathbb{C} \to \mathbb{C}$ for the branch of the complex logarithm such that the imaginary part of $\log z$ belongs to $(-\pi, \pi]$ for all $z \in \mathbb{C}$. For a given $\theta \in \frac{1}{2}\mathbb{Z}_{\geq 0}$, an algebraic integer will be called a *Weil integer of size p^θ* if its absolute value in any complex embedding of $\overline{\mathbb{Q}}$ is p^θ. (These are sometimes called Weil integers of weight 2θ).

Theorem 7.1. *Let p be a prime number, and $\theta \in \frac{1}{2}\mathbb{Z}_{\geq 0}$. Let $z \in \overline{\mathbb{Q}}$ be a Weil integer of size p^θ, and $\zeta \in \overline{\mathbb{Q}}$ be a root of unity. For any integer $L \neq 0$, either $\zeta(zp^{-\theta})^L = 1$ or, in any complex embedding $|\cdot|$ of $\overline{\mathbb{Q}}$ in $\mathbb{C}$, we have*

$$\log \left|1 - \zeta(zp^{-\theta})^L\right| \geq -c_0 - c_1 \log |L|, \tag{7.1}$$

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

We refer the reader to [GU20, Thm 11.6] for a proof of Theorem 7.1. The main ingredient in the proof is a lower bound for linear forms in logarithms of algebraic numbers due to Baker–Wüstholz in [BW93].

We also need some estimates on the orbits in O. As before, p is a prime number and r is a fixed power of p. For any relatively prime integers a, b which are coprime to p, and any power q of p, we let $S := (\mathbb{Z}/a\mathbb{Z}) \smallsetminus \{0\} \times (\mathbb{Z}/b\mathbb{Z}) \smallsetminus \{0\} \times \mathbb{F}_q^\times$. As in §3.3, let O denote the set of orbits for the action of $\langle r \rangle$ on S.

Lemma 7.2. *For fixed a, b as above, the following bounds hold as $q \to \infty$ through powers of p.*

(1) $\sum_{o \in O} |o| = |S| = (a-1)(b-1)(q-1) \ll q$,

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

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

The implied constants depend at most on the product ab.

Proof. As defined in Section 3.3, the set S is a subset of $S'_{ab} = (\mathbb{Z}/ab\mathbb{Z}) \smallsetminus \{0\} \times \mathbb{F}_q^\times$. Hence O may be viewed as a subset of the set O'_{ab} of orbits for the action of $\langle r \rangle$ on S'_{ab}. Lemma 11.4.1 of [GU20] directly gives the required bounds. □

7.2 Size of the special value

For any a, b, q as above, for any orbit $o \in O$, recall that we have defined

$$\boldsymbol{\omega}(o) = \mathbf{G}\left(\pi_a(o)\right)^{\nu_a(o)} \mathbf{G}\left(\pi_b(o)\right)^{\nu_b(o)}.$$

Let O_0 denote the set of orbits $o \in O$ such that $\boldsymbol{\omega}(o) = r^{|o|}$, and $O_* := O \smallsetminus O_0$ denote its complement. We require the following special case of Theorem 7.1:

Proposition 7.3. *There exist constants $c_2, c_3 > 0$ depending only on a, b, and p such that for any orbit $o \in O$, either $\boldsymbol{\omega}(o) = r^{|o|}$ or*

$$\log \left| 1 - \frac{\boldsymbol{\omega}(o)}{r^{|o|}} \right| \geq -c_2 - c_3 \log |o|.$$

Proof. It suffices to treat the case when $o \in O_*$, since otherwise $\boldsymbol{\omega}(o) = r^{|o|}$. Recall from §3.4 that we may write $\boldsymbol{\omega}(o) = \zeta_o \cdot g_o^{L_o}$, where ζ_o is an ab-th root of unity, g_o is a Weil integer of size $p^{\theta_{a,b}/2}$, and $L_o = [\mathbb{F}_r : \mathbb{F}_p]|o|/\theta_{a,b}$, with $\theta_{a,b} = \operatorname{lcm}(o_p(a), o_p(b))$. We thus have

$$\log \left| 1 - \frac{\boldsymbol{\omega}(o)}{r^{|o|}} \right| = \log \left| 1 - \zeta_o \big(g_o p^{-\theta_{a,b}}\big)^{L_o} \right|.$$

Applying Theorem 7.1 yields that

$$\log \left| 1 - \zeta_o \big(g_o p^{-\theta_{a,b}}\big)^{L_o} \right| \geq -c_0 - c_1 \log |L_o|,$$

for some constants c_0 and c_1 depending on at most p, the integer $\theta_{a,b}$, the degree of g_o over $\mathbb{Q}$ and the order of ζ_o. These three quantities can be bounded solely in terms of a, b, and p, as we now explain. The root of unity ζ_o has order at most ab, the Gauss sum g_o has degree at most $[\mathbb{Q}(g_o) : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_a, \zeta_b, \zeta_p) : \mathbb{Q}] \leq abp$, and $\theta_{a,b} \leq o_p(a) o_p(b) \leq \phi(a)\phi(b) \leq ab$.

The result follows from the observation that L_o divides $|o|$, so that $L_o \leq |o|$. □

We are now ready to prove Theorem 1.6.

Proof of Theorem 1.6. Combining the definition of $L^*(J)$ with the explicit expression for the L-function from Theorem 4.2 yields that

$$L^*(J) = \prod_{o \in O_0} |o| \prod_{o \in O_*} \left(1 - \frac{\boldsymbol{\omega}(o)}{r^{|o|}}\right).$$

From this, we deduce that

$$\frac{\log L^*(J)}{q} = \frac{1}{q} \sum_{o \in O_0} \log |o| + \frac{1}{q} \sum_{o \in O_*} \log \left|1 - \frac{\boldsymbol{\omega}(o)}{r^{|o|}}\right|. \tag{7.2}$$

We now estimate the two terms on the right-hand side separately. Lemma 7.2*(3)* gives

$$0 \leq \frac{1}{q} \sum_{o \in O_0} \log |o| \leq \frac{1}{q} \sum_{o \in O^\times} \log |o| \ll \frac{q}{q} \frac{\log \log q}{\log q} \ll \frac{\log \log q}{\log q}. \tag{7.3}$$

As q tends to infinity through powers of p, this term is $o(1)$.

We estimate the second term on the right-hand side of (7.2) in two steps. We begin by proving a suitable upper bound. Since $|\boldsymbol{\omega}(o)| = r^{|o|}$ for all $o \in O$, the triangle inequality implies that

$$\frac{1}{q} \sum_{o \in O_*} \log \left|1 - \frac{\boldsymbol{\omega}(o)}{r^{|o|}}\right| \leq \frac{|O_*|}{q} \log 2 \leq \cdot \frac{|O|}{q} \log 2\,.$$

We know from Lemma 7.2*(2)* that $|O|/q \ll (\log q)^{-1}$ as q tends to infinity.

We now prove the required lower bound. By Proposition 7.3, we have

$$-\frac{1}{q} \sum_{o \in O_*} \log \left|1 - \frac{\boldsymbol{\omega}(o)}{r^{|o|}}\right| \leq \frac{1}{q} \sum_{o \in O_*} c_2 + c_3 \log |o| \leq c_2 \frac{|O|}{q} + c_3 \frac{1}{q} \sum_{o \in O_*} \log |o|\,.$$

By Lemma 7.2*(2)*, we have $|O|/q \ll (\log q)^{-1}$. Lemma 7.2*(3)* implies that $\sum_{o \in O_*} \log |o|$ is $o(q)$ as $q \to \infty$. Thus, the second terms on the right-hand side of (7.2) satisfies

$$-\frac{\log \log q}{\log q} \ll \frac{1}{q} \sum_{o \in O_*} \log \left|1 - \frac{\boldsymbol{\omega}(o)}{r^{|o|}}\right| \ll \frac{1}{\log q} \tag{7.4}$$

as $q \to \infty$ through powers of p. Summing the inequalities (7.3) and (7.4) yields that

$$-\frac{\log \log q}{\log q} \ll \frac{\log L^*(J)}{q} \ll \frac{1}{\log q},$$

as $q \to \infty$ through powers of p. We conclude that

$$\frac{|\log L^*(J)|}{q} = O\left(\frac{\log \log q}{\log q}\right) \qquad \text{as } q \to \infty\,.$$

Our estimate from the height $H(J)$ in Lemma 2.7 shows that the ratio $q/\log H(J)$ remains bounded (in terms of constants depending only on a and b) as q varies. We conclude that

$$\frac{|\log L^*(J)|}{\log H(J)} = \frac{|\log L^*(J)|}{q} \frac{q}{\log H(J)} = o(1)\,.$$

The implicit constants depend at most on a, b and p. This concludes the proof of Theorem 1.6. □

7.3 Analogue of the Brauer–Siegel theorem

Combining Theorem 1.6 and the Birch and Swinnerton-Dyer conjecture (Theorem 1.1), we arrive at the following estimate.

Corollary 1.7. *For given a, b, as $q \to \infty$ runs through powers of p, we have*

$$\log\big(|Ш(J)|\operatorname{Reg}(J)\big) \sim \log H(J).$$

In the interpretation suggested by [HP16], this result provides an analogue of the Brauer–Siegel theorem for the family $(J_{a,b,q})_q$ of Jacobians.

Note that, except for a few examples in [Ulm19, §10.4, §11.4], the relationship between the asymptotic growth rate of the product $|Ш(A)|\operatorname{Reg}(A)$ and the asymptotic growth rate of the height $H(A)$ has not previously been elucidated in any sequence of abelian varieties A of dimension greater than 1. We note that there are several sequences of elliptic curves for which similar behaviour has been described. See [HP16, Gri16, Gri18, Gri19, GU20] for examples.

Proof. By the BSD formula (see (1.2) in Theorem 1.1), we have

$$\frac{\log\big(|Ш(J)|\operatorname{Reg}(J)\big)}{\log H(J)} = 1 - \frac{\log r^g}{\log H(J)} + \frac{2\log|J(K)_{\mathrm{tors}}|}{\log H(J)} - \frac{\log\prod_v c_v}{\log H(J)} + \frac{\log L^*(J)}{\log H(J)}.$$

For a fixed pair (a, b), the genus g of $C = C_{a,b,q}$ is constant as q varies. Hence the term $\log r^g/\log H(J)$ is $o(1)$ as $q \to \infty$. By Theorem 3.8 in [HP16], we have

$$\log|J(K)_{\mathrm{tors}}| = o\big(\log H(J)\big),$$

as $q \to \infty$ for a fixed a, b. Furthermore, since the local Tamagawa numbers c_v are all equal to 1 (see Proposition 2.5), we have $\log\prod_v c_v = 0$.

Now, Theorem 1.6 shows that the term $\log L^*(J)/\log H(J)$ is also $o(1)$ as $q \to \infty$. All in all, we obtain

$$\frac{\log\big(|Ш(J)|\operatorname{Reg}(J)\big)}{\log H(J)} = 1 + o(1),$$

ce qu'il fallait démontrer. □

8 Large Tate–Shafarevich Groups

In this section we prove Theorem 1.5, which we recall for convenience:

Theorem 1.5. *Fix parameters a, b which satisfy the hypotheses of Theorem 1.2. Then, as q runs through powers of p, we have*

$$|Ш(J)| = H(J)^{1+o(1)}.$$

Proof. By Corollary 1.7, we have

$$\frac{\log\big(|Ш(J)|\operatorname{Reg}(J)\big)}{\log H(J)} = 1 + o(1).$$

Theorem 1.2 shows that given the hypotheses made on (a, b), the analytic rank of J is 0 and so $\operatorname{Reg}(J) = 1$. Hence, we have

$$\frac{\log|Ш(J)|}{\log H(J)} = 1 + o(1),$$

as $q \to \infty$ through powers of p. □

Corollary 8.1. *There are arbitrarily large integers $d \geq 1$ such that there exists an infinite sequence of K-simple Abelian varieties A over K of dimension d satisfying*

$$|Ш(A)| = H(A)^{1+o(1)} \qquad \text{as } H(A) \to \infty\,.$$

Proof. Let $d_0 \geq 1$ be any integer. By Lemma 6.14, we may choose a pair of coprime integers (a, b) such that a and b are both prime, $(a-1)(b-1) \geq 2d_0$, and one of the conditions of Theorem 1.2 is satisfied. For such a pair (a, b), consider the sequence $(J_{a,b,q})_q$ of Jacobian varieties of dimension $d = (a-1)(b-2)/2$ indexed by powers q of p. Since both a and b are prime, Theorem 1.4 says that for any power q of p, the Jacobian $J_{a,b,q}$ is K-simple. By Theorem 1.5, the sequence $(J_{a,b,q})_q$ satisfies $|Ш(J_{a,b,q})| = H(J_{a,b,q})^{1+o(1)}$ as q grows. □

References

[BHP+15] L. Berger, C. Hall, R. Pannekoek, J. Park, R. Pries, S. Sharif, A. Silverberg, and D. Ulmer. Explicit arithmetic of Jacobians of generalized Legendre curves over global function fields. *Mem. Amer. Math. Soc.*, 266(1295), 2015.

[BW93] A. Baker and G. Wüstholz. Logarithmic forms and group varieties. *J. Reine Angew. Math.*, 442(12):19–62, 1993.

[Cas64] J.W.S. Cassels. Arithmetic on curves of genus 1. vi. the Tate–Safarevic group can be arbitrarily large. *J. Reine Angew. Math.*, 1964(214-215):65–70, 1964.

[Cas16] P. Casillejo. Grothendieck–Ogg–Shafarevich formula for ℓ-adic sheaves. Master's thesis, Freie Universitat Berlin, 2016.

[Coh07] H. Cohen. *Number Theory. Volume I: Tools and Diophantine Equations.* Springer, New York, N.Y., 2007.

[Cre11] B. Creutz. Potential Sha for abelian varieties. *J. Number Theory*, 131(11):2162–2174, 2011.

[CS10] P. Clark and S. Sharif. Period, index and potential Sha. *Algebra Number Theory*, 4(2):151–174, 2010.

[Del80] P. Deligne. La conjecture de Weil : II. *Publ. Math. Inst. Hautes Études Sci.*, 52, 1980.

[Dok20] T. Dokchitser. Models of curves over DVRs. *Duke Math. J.*, 2020.

[Fly18] E.V. Flynn. Arbitrarily large Tate–Shafarevich group on Abelian surfaces. *J. Number Theory*, 186:248–258, 2018.

[GdW21] R. Griffon and G. de Wit. Elliptic curves with large Tate–Shafarevich groups over $\mathbb{F}_q(t)$. *to appear in Contemp. Math. (preprint ArXiv:1907.13038)*, 2021.

[Gri16] R. Griffon. *Analogues du théorème de Brauer-Siegel pour quelques familles de courbes elliptiques.* PhD thesis, Université Paris Diderot (Paris 7), 2016.

[Gri18] R. Griffon. Analogue of the Brauer–Siegel theorem for Legendre elliptic curves. *J. Number Theory*, 193:189–212, December 2018.

[Gri19] R. Griffon. Bounds on special values of L-functions of elliptic curves in an Artin-Schreier family. *Eur. J. Math.*, 5(2):476–517, 2019.

[GU20] R. Griffon and D. Ulmer. On the arithmetic of a family of twisted constant elliptic curves. *Pacific J. Math.*, 305(2):597–640, April 2020. `https://arxiv.org/abs/1903.03901`.

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

[Lor90] D. Lorenzini. Groups of components of Néron models of Jacobians. *Compos. Math.*, 73(2):145–160, 1990.

[Poo06] B. Poonen. Lectures on rational points on curves. `https://math.mit.edu/~poonen/papers/curves.pdf`, 2006.

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

[Ser70] J.P. Serre. Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, 11(19):1–15, 1969–1970.

[Shi86] T. Shioda. An explicit algorithm for computing the Picard number of certain algebraic surfaces. *Amer. J. Math.*, 108:415–432, 1986.

[ST68] J.P. Serre and T. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492 – 517, Nov. 1968.

[TS67] J. Tate and I.R. Shafarevich. The rank of elliptic curves. *Doklady Akademii Nauk*, 175(4):770–773, 1967.

[Ulm02] D. Ulmer. Elliptic curves with large rank over function fields. *Ann. of Math.*, 155:295–315, 2002.

[Ulm06] D. Ulmer. L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields. *Invent. Math.*, 167:379–408, 2006.

[Ulm14] D. Ulmer. CRM lectures on curves and Jacobians over function fields. In *Arithmetic geometry over global function fields*, pages 281–337. Springer, 2014.

[Ulm19] D. Ulmer. On the Brauer–Siegel ratio for abelian varieties over function fields. *Algebra Number Theory*, 13(5):1069–1120, 2019.

[Was97] L. Washington. *Introduction to Cyclotomic Fields*. Springer, New York, N.Y., 2nd edition, 1997.

Sarah Arpin (*sarah.arpin@colorado.edu*) – University of Colorado Boulder, Boulder, CO 80309 (USA).

Richard Griffon (*richard.griffon@uca.fr*) – Université Clermont–Auvergne, Campus des Cézeaux, 3 place Vasarely, TSA 60026 CS 60026, 63178 Aubière Cedex (France).

Libby Taylor (*lt691@stanford.edu*) – Stanford University, 380 Serra Mall, Stanford, CA 94305 (USA).

Nicholas Triantafillou (*nicholas.triantafillou@gmail.com*) – University of Georgia, Boyd Graduate Research Center, Athens, GA 30602 (USA).

A Conductor Computations

Recall that $N_J \in \mathrm{Div}(\mathbb{P}^1)$ is the conductor divisor of J/K.

Proposition A.1. *We prove the statement from Theorem 4.1 regarding the degree $b(J)$ of the L-function $L(J,T)$:*

$$b(J) = \deg(N_J) - 4g.$$

Proof. We begin by defining the conductor divisor N_J as a divisor on the base $\mathbb{P}^1$. The action of inertia I_v on the ℓ-adic Tate module V_ℓ is tame[1]. For any place v of K, define

$$f(v) := \dim(V_\ell) - \dim(V_\ell^{I_v}),$$

and let the conductor of J be the divisor $N_J := \sum_v f(v)v$ on $\mathbb{P}^1$. By [Ser70], $f(v) = 0$ whenever v is a place of good reduction for J. Plugging in $\dim(V_\ell) = 2g$ gives

$$\deg(N_J) = \sum_{v \text{ bad reduction}} (2g - \dim(V_\ell^{I_v})) \deg v,$$

where the sum is over places v of K where J has bad reduction. Now, we investigate the L-function and see how its degree relates to $\deg N_J$. Begin with the definition:

$$L(J,T) := \prod_v \det(1 - T\mathrm{Fr}_v^{-1} | V_\ell^{I_v})^{-1}.$$

This product can be split up into products over good and bad places of C:

$$L(J,T) := \prod_{\text{good } v} \det(1 - T\mathrm{Fr}_v^{-1} | V_\ell^{I_v})^{-1} \prod_{\text{bad } v} \det(1 - T\mathrm{Fr}_v^{-1} | V_\ell^{I_v})^{-1}.$$

Let $\tilde{L}(J,T) := \prod_{\text{good } v} \det(1 - T\mathrm{Fr}_v^{-1} | V_\ell^{I_v})^{-1}$. This gives a decomposition of the degree:

$$\deg(L(J,T)) = \deg(\tilde{L}(J,T)) - \sum_{\text{bad } v} \dim(V_\ell^{I_v}).$$

Since $L(J,T)$ is rational, and since the sum $\sum_{\text{bad } v} \dim(V_\ell^{I_v})$ is finite, the "complement" $\tilde{L}(J,T)$ is also rational. From here, we need a more precise formula for $\deg(\tilde{L}(J,T))$. Let U denote the affine open subset of $\mathbb{P}^1$ above which J has good reduction. Since U is a punctured $\mathbb{P}^1$, by the étale-singular cohomology comparison theorem, we have $\chi(U, \overline{\mathbb{Q}_\ell}) := \dim H^0(U, \overline{\mathbb{Q}}_\ell) - \dim H^1(U, \overline{\mathbb{Q}}_\ell) + \dim H^2(U, \overline{\mathbb{Q}}_\ell) = 2 - 2g(\mathbb{P}^1) - r$, where $g(\mathbb{P}^1)$ is the genus of $\mathbb{P}^1$ and r is the number of geometric points over which J has bad reduction. That is, r is the sum of the degrees of places of bad reduction for J: $r = \sum_{\text{bad } v} \deg v$. Therefore $\chi(U, \overline{\mathbb{Q}_\ell}) = 2 - r$.

The Grothendieck–Ogg–Shafarevich formula (see [Cas16]) yields that

$$\chi(U, \mathcal{F}) = \chi(U, \overline{\mathbb{Q}_\ell}) \cdot \mathrm{rank}(\mathcal{F}) - \sum_{x \in \mathbb{P}^1 \setminus U} (\mathrm{rank}(\mathcal{F}) + Sw_x(\mathcal{F})),$$

[1] [ST68] proves this when $p > 2g+1$. In our case, we can remove the hypothesis on p as follows. J becomes trivial after a degree ab field extension. Over this extension, the action of inertia is trivial, so descending back to K gives that the ramification degree must divide ab. But ab is prime to p, so the ramification must be tame.

where in our case $\mathcal{F} = V_\ell$, which is a lisse ℓ-adic sheaf of rank $\dim V_\ell = 2g$ on U. Since the action of inertia on V_ℓ is tame (see [ST68, Corollary 2, p. 497]), this implies that

$$\chi(U, \mathcal{F}) = \chi(U, \overline{\mathbb{Q}_\ell}) \cdot \operatorname{rank}(\mathcal{F}) = 2g(2-r).$$

Now, since $\deg \tilde{L}(J,T) = -\chi(U,\mathcal{F})$, we deduce that $\det \tilde{L}(J,T) = -2g(2-r)$. Putting this back into the equation for $\deg L(J,T)$ gives

$$\begin{aligned}\deg(L(J,T)) &= \deg(\tilde{L}(J,T)) - \sum_{\text{bad } v} \dim(V_\ell^{I_v}) = -4g + \sum_{\text{bad } v} 2g - \sum_{\text{bad } v} \dim(V_\ell^{I_v}) \\ &= \sum_{\text{bad } v} (2g - \dim(V_\ell^{I_v})) - 4g = \deg(N_J) - 4g.\end{aligned}$$

□