On the arithmetic of a family of superelliptic curves

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

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 $y^b + x^a = t^q - t$, and 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 $Ш(J)$ grows exponentially fast in q 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 $a, b > 1$ 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 unipotent reduction, to determine that 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, in Section 4.5, 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.*

Theorem 1.1 follows from [PU16, Theorem 3.1.2]. In our setting, 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 [Ulm07], 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 every 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, thereby expanding the tools used to study curves of arbitrary genus over function fields.

Following [GU20], we compute the L-function using two different techniques: once using the arithmetic of Gauss sums (Section 4) and a second time via a cohomological computation (Section 5). In [GU20], the authors were able to apply results of Shioda [Shi92] to compute the L-functions of their family of elliptic curves. Since Shioda's results depend upon the classification of reduction types of elliptic curves, they do not apply directly to higher genus curves, such as our family of superelliptic curves. Fortunately, we have a detailed description of the minimal proper regular SNC model (Section 2), which we use to extend Shioda's argument to compute the L-function of our family.

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. 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, as q varies, either the the rank is always 0 or the rank is unbounded, 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) $ao_p(a)$ and $bo_p(b)$ are relatively prime;

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

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

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

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, and r 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 the residue class of $q \mod ab$ such that $H(J) = r^{Dq+E}$. In particular, the order of $Ш(J)$ grows exponentially in q as q varies.

Theorem 1.5 generalizes [GdW21, Theorem C], which exhibits a sequence 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 [Fly19] 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 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.

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, and r, 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, to show 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 the Brauer–Siegel theorem.) In Section 7.3 we prove:

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

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

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

Several sequences of elliptic curves A/K are known to satisfy a similar asymptotic description of $|\text{Ш}(A)| \operatorname{Reg}(A)$ in terms of the height $H(A)$ as in Corollary 1.7. (For instance, see [HP16, Gri16, Gri18, Gri19, GU20].) However, such asymptotic results for sequences of simple abelian varieties of higher dimension are much rarer: the only previous examples we are aware of appear in [Ulm19, §10.4, §11.4]. Corollary 1.7 thus provides some more evidence towards the conjecture in [HP16] to the effect that the ratio $\log\big(|\text{Ш}(A)| \operatorname{Reg}(A)\big)/\log H(A)$ should have a limit as $H(A) \to \infty$.

1.1 Roadmap to this article.

The paper is organized as follows. In Section 2, we study the geometry of C and use [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 provide a second computation of the L-function of the Jacobian, this time using the geometry of the minimal proper regular SNC model $\mathcal{S}$ of C, confirming our computation in the previous section. In Section 6, we use p-adic valuations of Gauss sums to prove estimates on $\operatorname{rank} J(K)$ 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 $\text{Ш}(J)$ as q varies.

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 warmly for his guidance, encouragement and support throughout the realization of this project, and for his fruitful comments on a previous draft. Thanks are also due to Daniel Litt for providing help with the proof in Appendix A, to Baptiste Peaucelle and Abel Lacabanne for helpful discussions, and to Rachel Pries and Dino Lorenzini for their careful reading and helpful comments. We also thank the anonymous referee for their detailed reading of the first version of the manuscript: they made a number of constructive comments and suggested some improvements, for which we are grateful.

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 $a, b > 1$ 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 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 $\pi : \mathcal{S} \to \mathbb{P}^1_{\mathbb{F}_r}$ of $C/\mathbb{F}_r(t)$ 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.

We now recall the definition of a simple normal crossings model. We note that some authors call this a strict normal crossings model instead. First, recall (e.g. from [Sta21, Section 0CBN, Definition 41.21.1]) that a *simple normal crossings divisor* on a locally Noetherian scheme $\mathcal{W}$ is an effective Cartier divisor $D \subset \mathcal{W}$ such that for every prime $w \in D$, the local ring $\mathcal{O}_{W,w}$ is regular and there exists a regular system of parameters $x_1, \ldots, x_d$ in the maximal ideal $\mathfrak{m}_w$ and $1 \leq r \leq d$ such that D is cut out by the product $x_1 \cdots x_r$ in $\mathcal{O}_{X,p}$. When $\mathcal{W}$ is a curve over a DVR or a surface over a finite field, these conditions amount to saying that the irreducible components of D are smooth and any singular points of D 'look like' the intersection of the coordinate axes in $\mathbb{A}^2$. More generally, an effective Cartier divisor E on $\mathcal{W}$ is *supported on a simple normal crossings divisor* if there is some simple normal crossing divisor D on $\mathcal{W}$ such that $E \subset D$ set-theoretically. In this situation, if D decomposes into irreducible components as $\bigcup_{i \in I} D_i$, then $E = \sum_{i \in I} a_i D_i$ for some integers $a_i \geq 0$.

Definition 2.2. Given a smooth proper curve W over the fraction field K_v of a discrete valuation ring $\mathcal{O}_{K_v}$, a *simple normal crossings model* of W is a scheme $\mathcal{W}$ over $\mathcal{O}_{K_v}$ such that the generic fiber $\mathcal{W}_{K_v}$ is isomorphic to W and the special fiber $\mathcal{W}_{k_v}$, viewed as a Cartier divisor on $\mathcal{W}$, is supported on a simple normal crossing divisor.

More generally, given a smooth proper curve $W/\mathbb{F}_r(t)$, a *simple normal crossings model* of W is a surface $\mathcal{W}/\mathbb{F}_r$ equipped with a map $\pi : \mathcal{W} \to \mathbb{P}^1_{\mathbb{F}_r}$ such that the fiber over the generic point of $\mathbb{P}^1_{\mathbb{F}_r}$ is isomorphic to W and the fiber $\mathcal{W}_v$ over any closed point of $v \in \mathbb{P}^1_{\mathbb{F}_r}$ is supported on a simple normal crossings divisor of $\mathcal{W}$.

For $v \in \mathbb{P}^1$ a closed point, we study the fiber $\mathcal{S}_v$ of the minimal proper regular simple normal crossings model $\pi : \mathcal{S} \to \mathbb{P}^1_{\mathbb{F}_r}$ of $C/\mathbb{F}_r(t)$. Taking $K_v^{\text{unram.}}$ to be the maximal unramified extension of the completion of K at v, we will also describe the special fiber of the minimal proper regular simple normal crossings model of the base change $C \otimes_{\operatorname{Spec} K} \operatorname{Spec} K_v^{\text{unram.}}$. We call this special fiber $\mathcal{S}_{\overline{v}}$. As we shall see, $\mathcal{S}_{\overline{v}} \cong \mathcal{S}_v \otimes_{\operatorname{Spec} k_v} \operatorname{Spec} \overline{k_v}$.

We abuse notation slightly by writing $v \in \mathbb{F}_q \cup \{\infty\}$ to mean that v decomposes into degree one points over the compositum $\mathbb{F}_r\mathbb{F}_q$. Equivalently, $v \in \mathbb{F}_q \cup \{\infty\}$ if every element of $v(\overline{\mathbb{F}_q})$ is fixed by the $\operatorname{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-action on $\mathbb{P}^1(\overline{\mathbb{F}_q})$.

When $v \notin \mathbb{F}_q \cup \{\infty\} \subset \mathbb{P}^1$, the curve C has good reduction, so $\mathcal{S}_v/k_v$ and $\mathcal{S}_{\overline{v}}/\overline{k_v}$ are smooth curves 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.

Moreover, we note that the Newton polytopes associated to $C \otimes_{\operatorname{Spec} K} K_v^{\text{unram.}}$ are the same as those associated to C at v. In particular, $\mathcal{S}_{\overline{v}}$ admits the same description as a tree of $\mathbb{P}^1$s with multiplicity as does $\mathcal{S}_v$. It follows immediately that $\mathcal{S}_{\overline{v}}$ is obtained from $\mathcal{S}_v$ via base change to $\overline{k_v}$. More precisely, $\mathcal{S}_{\overline{v}} \cong \mathcal{S}_v \otimes_{\operatorname{Spec} k_v} \operatorname{Spec} \overline{k_v}$.

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. This means that $\mathcal{S}_{K_v^{\text{unram.}}}$ is a (Spec $\mathcal{O}_{K_v^{\text{unram.}}}$)-curve (or S-curve) in the notation of [Lor90].

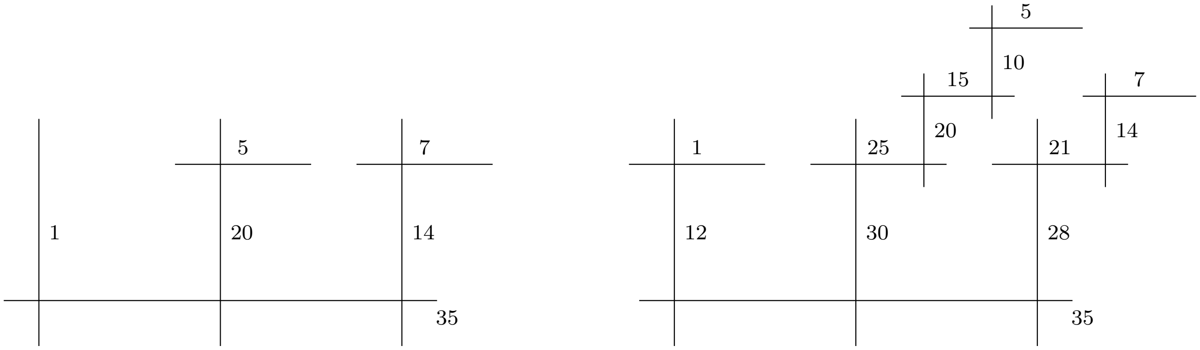

Figure 1: Fibers of the minimal proper regular SNC model of $y^5 + x^7 = t^{67} - t$ over $\mathbb{P}^1_{\mathbb{F}_{67}}$ at finite places of bad reduction (left) and at infinity (right)

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, unipotent reduction above any $v \in \mathbb{F}_q \cup \{\infty\} \subset \mathbb{P}^1$, 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.

When $v \in \mathbb{F}_q \cup \{\infty\}$, we can read off the reduction of the Jacobian from the special fiber of the simple normal crossings model $\mathcal{S}$. Write $\mathcal{J}/\mathbb{F}_r$ for the (global) Néron model of J. Given a point $v \in \mathbb{P}^1$, let k_v denote the residue field at v and let $\mathcal{J}_v^0$ denote the connected component of the identity of the fiber of $\mathcal{J}$ above v.

Similarly, let $\mathcal{J}_{\overline{v}}^0$ denote the connected component of the identity of the special fiber of the Néron model of the base change $J_{K_v^{\text{unram.}}}$. Since $\mathcal{S}_{\overline{v}} \cong \mathcal{S}_v \otimes_{\operatorname{Spec} k_v} \operatorname{Spec} \overline{k_v}$, we have $\mathcal{J}_{\overline{v}}^0 \cong (\mathcal{J}_v \otimes_{\operatorname{Spec} k_v} \operatorname{Spec} \overline{k_v})^0$. The advantage of passing to a Néron model over $K_v^{\text{unram.}}$ is that we may apply results from [Lor90], which requires an algebraically closed residue field.

We recall some facts on the structure of $\mathcal{J}_{\overline{v}}^0$ 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:

$$0 \to U \times T \to \mathcal{J}_{\overline{v}}^0 \to A \to 0\,.$$

Since the $\mathcal{S}_v$ is the special fiber of a simple normal crossings model of a curve over $K_v^{\text{unram.}}$, Corollary 1.4 of [Lor90] states that $\dim(T)$ is equal to the first Betti number of the dual graph of $\mathcal{S}_{\overline{v}}$. The dual graph of $\mathcal{S}_{\overline{v}}$ is a tree, so it has trivial homology. Hence, T is trivial.

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

In summary, for any place v of bad reduction for C, the group scheme $\mathcal{J}_{\overline{v}}^0$ is unipotent, since both the toric and abelian parts are trivial. We conclude that, up to twist, the same is true of $\mathcal{J}_v^0$. □

2.3 Tamagawa numbers of J.

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

Given an abelian variety A/K and a place v of K, let $\mathcal{A}/\mathcal{O}_v$ be the Néron model of A_{K_v}. The special fiber $\mathcal{A}_v$ (over the residue field k_v) of $\mathcal{A}$ may have multiple components. Let $\mathcal{A}_v^0$ be the component containing the identity. The quotient $\mathcal{A}_v/\mathcal{A}_v^0$ is a finite group scheme.

Definition 2.4 (Tamagawa Number)**.** For any abelian variety A/K and place v of K, the *local Tamagawa number* is defined by $c_v(A) := \#\left(\mathcal{A}_v/\mathcal{A}_v^0\right)(k_v)$. Equivalently, $c_v(A)$ is the number of irreducible components of $\mathcal{A}_v/k_v$ which remain irreducible after base change to $\overline{k_v}$. The *Tamagawa number* $\mathcal{T}(A/K)$ of A is defined as the product $\prod_v c_v(A)$ over all places of K.

If A has good reduction at v, the special fiber $\mathcal{A}_v$ is connected, so that $\mathcal{A}_v/\mathcal{A}_v^0$ is trivial. Hence, as v varies among all places of K, all but finitely many of the local Tamagawa numbers $c_v(A)$ are equal to 1. The Tamagawa number $\mathcal{T}(A/K)$ is therefore well defined.

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. As mentioned above, if v is a place of good reduction for J, then $c_v(J) = 1$.

To compute the local Tamagawa numbers from the simple normal crossings model at each place of bad reduction, we show that $\#\left(\mathcal{J}_v/\mathcal{J}_v^0\right)(\overline{k_v}) = 1$. Since $1 \leq \#\left(\mathcal{J}_v/\mathcal{J}_v^0\right)(k_v) \leq \#\left(\mathcal{J}_v/\mathcal{J}_v^0\right)(\overline{k_v})$, it will follow that $c_v(J) = 1$ as well.

Let $\mathcal{J}_{\overline{v}}$ be the special fiber of the Néron model of the base change $J \otimes_{\operatorname{Spec} K_v} \operatorname{Spec} K_v^{\text{unram.}}$. As in the proof of Proposition 2.3, since $\mathcal{S}_{\overline{v}} \cong \mathcal{S}_v \otimes_{\operatorname{Spec} k_v} \operatorname{Spec} \overline{k_v}$, we have $\mathcal{J}_{\overline{v}} \cong \mathcal{J}_v \otimes_{\operatorname{Spec} k_v} \operatorname{Spec} \overline{k_v}$. In particular, we have $\#\left(\mathcal{J}_v/\mathcal{J}_v^0\right)(\overline{k_v}) \leq \#\left(\mathcal{J}_{\overline{v}}/\mathcal{J}_{\overline{v}}^0\right)(\overline{k_v})$.

The advantage of base change to $K_v^{\text{unram.}}$ is that we may apply Corollary 1.5 of [Lor90] 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 $\mathcal{J}_v$ (and so also $\mathcal{J}_{\overline{v}}$) 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 $\#\left(\mathcal{J}_{\overline{v}}/\mathcal{J}_{\overline{v}}^0\right)(\overline{k_v}) = (ab)^1 a^{-1} b^{-1} 1^{-1} = 1$. We conclude that $c_v(J) = 1$ as well.

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 $N_J \in \operatorname{Div}(\mathbb{P}^1)$ 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 $\operatorname{Gal}(\overline{K}/K)$. 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

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

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

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

of differentials restricted to the generic fiber C of $\mathcal{S} \to \mathbb{P}^1$ 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

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

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 $\mathrm{ord}_v(\pi_*\eta)$. 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 nonvanishing on $\mathcal{S}_f$. In other words, $\mathrm{ord}_f(\pi_*\eta) = 0$. It follows that $\deg(\omega_J) = \mathrm{ord}_\infty(\eta)$.

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,

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

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 a, b and 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 Simplicity of the Jacobian

In this section, we prove Theorem 1.4 on the simplicity of J. In Section 6.5, we produce examples of abelian varieties with large rank. In Section 7.3, we show that J satisfies an analogue of the Brauer–Siegel theorem as q varies. In Section 8, we produce examples of abelian varieties whose Tate–Shafarevich groups have large order. Theorem 1.4 shows that, provided we add some mild assumptions, the abelian varieties involved in these sequences are simple (that is, do not have proper positive-dimensional abelian subvarieties defined over K).

Theorem 1.4. *The Jacobian $J = J_{a,b,q}$ is K-simple if and only if a and b are both prime.*

The proof of the "only if" direction of the statement is rather short: Suppose that at least one of a and b is composite. Assume, by symmetry, that a is composite and let d be one of its proper divisors. Let $C_{d,b,q}$ be the projective curve defined over K with affine open defined by $x^d + y^b = t^q - t$, and let $J_{d,b,q}/K$ denote its Jacobian variety. The same computation as in Proposition 2.1 shows that $C_{d,b,q}$ has genus $g' = (d-1)(b-1)/2$. Since $1 < d < a$, we have $0 < g' < g$. The map $(x, y) \mapsto (x^{a/d}, y)$ extends to a nonconstant K-morphism $C_{a,b,q} \to C_{d,b,q}$. The contravariant functoriality of the Jacobian then implies the existence of a morphism of abelian varieties $J_{d,b,q} \hookrightarrow J_{a,b,q}$, whose image is a positive-dimensional strict abelian subvariety of $J_{a,b,q}$ defined over K. Hence $J_{a,b,q}$ is not simple over K.

Our proof of the converse implication is more subtle, and requires an auxiliary discussion, which we carry out before continuing on with the proof of Theorem 1.4.

We first describe the ℓ-adic Tate module of an auxiliary curve. For any integer $n \geq 1$ we let μ_n denote the group of n^{th} roots of unity in $\overline{\mathbb{F}_r}$. Let a and b be coprime integers which are both coprime to p, let $\mathbb{F}$ be the finite extension of $\mathbb{F}_r$ generated by μ_{ab}, and write κ for $|\mathbb{F}|$. Throughout this section, we let $\mathsf{C}_{a,b}/\mathbb{F}$ be the projective curve with a dense open subset defined by the affine equation

$$\mathsf{C}_{a,b}: \qquad x^a + y^b = 1\,. \tag{2.1}$$

Given our assumptions on a and b, it is straightforward to check that $\mathsf{C}_{a,b}$ is smooth of genus $g = (a-1)(b-1)/2$. The curve $\mathsf{C}_{a,b}$ admits an action of μ_{ab} by

$$\forall \zeta \in \mu_{ab}, \qquad \zeta \cdot (x, y) = (\zeta^b x, \zeta^a y)\,. \tag{2.2}$$

By functoriality, this action induces an action of μ_{ab} on the Jacobian $\mathsf{J}_{a,b}/\mathbb{F}$ of $\mathsf{C}_{a,b}$, therefore also on its ℓ-adic Tate module $V_\ell(\mathsf{J}_{a,b})$ for any prime $\ell \neq p$. For simplicity, we pick a prime $\ell \neq p$ such that $\ell \equiv 1 \bmod ab$ (there are infinitely many such primes). This choice of ℓ ensures that $\mathbb{Q}_\ell$ contains all $(ab)^{\text{th}}$ roots of unity.

The $\mathbb{Q}_\ell$-vector space $V_\ell(\mathsf{J}_{a,b})$ is dual to the first ℓ-adic cohomology group $H^1_{\text{ét}}(\mathsf{C}_{a,b}, \mathbb{Q}_\ell)$. The latter can easily (by a direct generalization of Corollary 2.4 in [Kat81]) be decomposed as a direct sum of $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-stable lines. In terms of $V_\ell(\mathsf{J}_{a,b})$, this result reads as follows: $V_\ell(\mathsf{J}_{a,b})$ decomposes as a direct sum of lines

$$V_\ell(\mathsf{J}_{a,b}) = \bigoplus_{\substack{\chi_a:\mu_a\to\mathbb{Q}_\ell^\times \\ \chi_b:\mu_b\to\mathbb{Q}_\ell^\times \\ \text{both nontrivial}}} L_{(\chi_a,\chi_b)}, \tag{2.3}$$

where the sum is over nontrivial $\mathbb{Q}_\ell$-valued characters χ_a and χ_b of μ_a and μ_b respectively. Because of our assumption on ℓ, there are $(a-1)(b-1) = 2g$ such pairs (χ_a, χ_b).

As proven by the analysis on p. 180 in [Kat81], the Frobenius map $\mathfrak{Fr} : x \mapsto x^\kappa$, which topologically generates $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$, acts on the line indexed by (χ_a, χ_b) as multiplication by the inverse of a certain Jacobi sum $j_{\mathbb{F}}(\chi_a, \chi_b)$ associated to the pair (χ_a, χ_b). (Since the characteristic polynomial of $\mathfrak{Fr}^{-1}$ acting on $V_\ell(\mathsf{J}_{a,b})$ is the numerator $L(\mathsf{C}_{a,b}/\mathbb{F}, x) \in \mathbb{Z}[x]$ of the zeta function of $\mathsf{C}_{a,b}/\mathbb{F}$, the above decomposition implies that the inverse roots of $L(\mathsf{C}_{a,b}/\mathbb{F}, x)$ are the Jacobi sums $j_{\mathbb{F}}(\chi_a, \chi_b)$). The action of μ_{ab} on $V_\ell(\mathsf{J}_{a,b})$ induced from the action on $\mathsf{C}_{a,b}$ defined by (2.2) also preserves the direct sum decomposition in (2.3). More precisely, for a given pair (χ_a, χ_b), a short computation shows that

$$\forall z \in L_{(\chi_a,\chi_b)},\ \forall \zeta \in \mu_{ab}, \qquad \zeta \cdot z = \chi_a(\zeta^b)\chi_b(\zeta^a)\, z = (\chi_a^b \chi_b^a)(\zeta)\, z. \tag{2.4}$$

Now let $V_\ell(\mathsf{J}_{a,b})_{\text{prim}}$ denote the subspace $\bigoplus_{(\chi_a,\chi_b)} L_{(\chi_a,\chi_b)}$ of $V_\ell(\mathsf{J}_{a,b})$ where the sum is over pairs of characters $\chi_a : \mu_a \to \mathbb{Q}_\ell^\times$, $\chi_b : \mu_b \to \mathbb{Q}_\ell^\times$ where χ_a has exact order a and χ_b has exact order b. One sees that $V_\ell(\mathsf{J}_{a,b})_{\text{prim}}$ is endowed with a μ_{ab}-action, and that $\dim_{\mathbb{Q}_\ell} V_\ell(\mathsf{J}_{a,b})_{\text{prim}} = \phi(a)\phi(b)$.

As a consequence of (2.3) and its compatibility with the action of μ_{ab}, we have:

Lemma 2.10. *Let V be a nonzero subspace of $V_\ell(\mathsf{J}_{a,b})_{\text{prim}}$ which is stable under the action of μ_{ab}. Then the action of μ_{ab} on V is faithful i.e., the induced map $\mu_{ab} \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ is injective.*

Proof. Since V is μ_{ab}-stable, the action of μ_{ab} on $V_\ell(\mathsf{J}_{a,b})_{\text{prim}}$ restricts to an action on V. The subspace V decomposes as $V = \bigoplus_{(\chi_a,\chi_b)} V \cap L_{(\chi_a,\chi_b)}$ where the sum is over pairs of characters (χ_a, χ_b) where χ_a has exact order a and χ_b has exact order b. Let χ_a have exact order a and χ_b have exact order b. Since a and b are coprime and given our assumptions on χ_a, χ_b, the character $\chi_a^b\chi_b^a$ of $\mu_{ab} \cong \mu_a \times \mu_b$ has exact order ab. In other words, the map $\chi_a^b\chi_b^a : \mu_{ab} \to \mathbb{Q}_\ell^\times$ is injective.

By (2.4), any $\zeta \in \mu_{ab}$ which acts trivially on $V \cap L_{(\chi_a,\chi_b)}$ satisfies $(\chi_a^b\chi_b^a)(\zeta) = 1$, and the above shows that ζ must be 1. □

We now relate the Jacobian $\mathsf{J}_{a,b}$ to our main subject of investigation J. We fix a separable closure $\overline{K}$ of K, and we let $K' = \mathbb{F} \cdot K = \mathbb{F}(t)$. We pick an element u in $\overline{K}$ such that $u^{ab} = t^q - t$, and we set $L' = \overline{\mathbb{F}}(u)$. The extension L'/K' is Galois; further, we know from Kummer theory that

$$\mathrm{Gal}(L'/K') = \mathrm{Gal}\left(\overline{\mathbb{F}}(\sqrt[ab]{t^q - t})/\mathbb{F}(t)\right) \cong \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \times \mathrm{Gal}(\mathbb{F}(u)/\mathbb{F}(t)).$$

The first factor $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ is topologically generated by the Frobenius $\mathfrak{Fr} : x \mapsto x^\kappa$ and is isomorphic to $\widehat{\mathbb{Z}}$; while the second factor $\mathrm{Gal}(\mathbb{F}(u)/\mathbb{F}(t))$ is isomorphic to $\mu_{ab}(K') = \mu_{ab}(\mathbb{F})$ *via* the map $\sigma \mapsto \sigma(u)/u$. We thus deduce that $\mathrm{Gal}(L'/K') \cong \widehat{\mathbb{Z}} \times \mu_{ab}$.

The morphism $\phi : \mathsf{C}_{a,b} \times_{\mathbb{F}} L' \to C \times_K L'$, which extends the map on affine patches given by $(x, y) \mapsto (u^{-a}x, u^{-b}y)$, yields an isomorphism between $\mathsf{C}_{a,b} \times_{\mathbb{F}} L'$ and $C \times_K L'$. By functoriality, ϕ induces an isomorphism between $(\mathsf{J}_{a,b})_{L'} = \mathsf{J}_{a,b} \times_{\mathbb{F}} L'$ and $J_{L'} = J \times_K L'$, as well as an isomorphism of $\mathbb{Q}_\ell$-vector spaces $V_\ell((\mathsf{J}_{a,b})_{L'}) \cong V_\ell(J_{L'})$. The Jacobian $\mathsf{J}_{a,b}$ is defined over $\mathbb{F}$, hence the ℓ-power torsion points on the base change $\mathsf{J}_{a,b} \times_{\mathbb{F}} L'$ are defined over $\overline{\mathbb{F}}$; thus there is a natural isomorphism $V_\ell((\mathsf{J}_{a,b})_{L'}) \simeq V_\ell(\mathsf{J}_{a,b})$. Similarly, we have $V_\ell(J_{K'}) \simeq V_\ell(J_{L'})$. Composing these, we obtain an isomorphism of $\mathbb{Q}_\ell$-vector spaces

$$\phi_\ell : V_\ell(\mathsf{J}_{a,b}) \xrightarrow{\cong} V_\ell(J_{K'}).$$

Both of these vector spaces are equipped with a Galois action: the leftmost with a $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-action, and the rightmost with a $\mathrm{Gal}(\overline{K}/K')$-action.

Our next task is to describe the action of $\mathrm{Gal}(\overline{K}/K')$ on $V_\ell(J_{K'})$. We first note that the corresponding representation $\mathrm{Gal}(\overline{K}/K') \to \mathrm{Aut}_{\mathbb{Q}_\ell}\big(V_\ell(J_{K'})\big)$ factors through $\mathrm{Gal}(L'/K')$, as follows from the previous paragraph. Though ϕ_ℓ is not equivariant for the Galois actions, we can describe how ϕ_ℓ "transports" the Galois structure, as follows.

In the Kummer isomorphism $\mathrm{Gal}(L'/K') \cong \widehat{\mathbb{Z}} \times \mu_{ab}$, an element $\sigma \in \mathrm{Gal}(L'/K')$ corresponds to a pair $(\mathfrak{Fr}^m, \zeta)$ for an integer m and $\zeta \in \mu_{ab}$. By construction of this isomorphism, for any $z = f(u)$ with $f(X) \in \overline{\mathbb{F}}(X)$, we have $\sigma(z) = (\mathfrak{Fr}^m(f))(\zeta\, u)$. By definition of ϕ, we deduce that, for all $(x, y) \in \mathsf{C}_{a,b}(\overline{\mathbb{F}})$, we have

$$\sigma(\phi(x,y)) = \sigma(u^{-b}x, u^{-a}y) = (\zeta^{-b}u^{-b}\mathfrak{Fr}^m(x), \zeta^{-a}u^{-a}\mathfrak{Fr}^m(y)) = \zeta^{-1} \cdot \mathfrak{Fr}^m\big(\phi(x,y)\big).$$

So, the action of $\mathrm{Gal}(L'/K') \cong \widehat{\mathbb{Z}} \times \mu_{ab}$ on $C(L')$ is carried through ϕ^{-1} to the action on $\mathsf{C}_{a,b}(\overline{\mathbb{F}})$ given by the product of the usual action of $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ on $\mathsf{C}_{a,b}$ by the *inverse* of the action of μ_{ab} on $\mathsf{C}_{a,b}$ defined by (2.2). By functoriality again, a similar conclusion holds for the $\mathrm{Gal}(L'/K')$-action on $V_\ell(J_{K'})$ and $V_\ell(\mathsf{J}_{a,b})$. Explicitly, the isomorphism ϕ_ℓ^{-1} carries the action of $\mathrm{Gal}(L'/K')$ on $V_\ell(J_{K'})$ to the action on $V_\ell(\mathsf{J}_{a,b})$ given by the product of the standard $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-action on $V_\ell(\mathsf{J}_{a,b})$ by the inverse of the action of μ_{ab} on $V_\ell(\mathsf{J}_{a,b})$ induced by (2.2).

Combining the above paragraph with the properties of the decomposition (2.3) of $V_\ell(\mathsf{J}_{a,b})$ explained above proves that $V_\ell(J_{K'})$ decomposes as

$$V_\ell(J_{K'}) = \bigoplus_{\substack{\chi_a : \mu_a \to \mathbb{Q}_\ell^\times \\ \chi_b : \mu_b \to \mathbb{Q}_\ell^\times \\ \text{both nontrivial}}} L'_{(\chi_a, \chi_b)}, \tag{2.5}$$

where the sum is over pairs (χ_a, χ_b) of nontrivial $\mathbb{Q}_\ell$-valued characters of μ_a, μ_b respectively, and where each $L'_{(\chi_a,\chi_b)}$ is one-dimensional. Furthermore, the action of $\mathrm{Gal}(\overline{K}/K')$ on $V_\ell(J_{K'})$, which factors through $\mathrm{Gal}(L'/K')$, preserves this direct sum decomposition. More precisely, if $\sigma \in \mathrm{Gal}(L'/K')$ corresponds to a pair $(\mathfrak{Fr}^m, \zeta)$ for $m \in \mathbb{Z}$ and $\zeta \in \mu_{ab}$, then for any pair (χ_a, χ_b) of characters as above, we have

$$\forall z \in L'_{(\chi_a,\chi_b)}, \qquad \sigma \cdot z = (\chi_a^{-b}\chi_b^{-a})(\zeta)\, j_{\mathbb{F}}(\chi_a, \chi_b)^{-m}\, z.$$

In particular, the subgroup $\mathrm{Gal}(\mathbb{F}(u)/\mathbb{F}(t)) \simeq \mu_{ab}$ of $\mathrm{Gal}(L'/K')$ acts on $V_\ell(J_{K'})$. Note that this action of μ_{ab} is not the same as the μ_{ab}-action induced by the action on C defined in an analogous way to the one on $\mathsf{C}_{a,b}$ by (2.2). Similarly to what we did earlier, we now let $V_\ell(J_{K'})_{\mathrm{prim}}$ denote the subspace $\bigoplus_{(\chi_a,\chi_b)} L'_{(\chi_a,\chi_b)}$ of $V_\ell(J_{K'})$, in which the sum is over pairs (χ_a, χ_b) of characters of $\mu_a \times \mu_b \cong \mu_{ab}$ where χ_a (resp. χ_b) has exact order a (resp. b). This space is equipped with an action of μ_{ab} and has dimension $\phi(a)\phi(b)$.

Since $\mathrm{Gal}(\mathbb{F}(u)/\mathbb{F}(t)) \simeq \mu_{ab}$, a direct consequence of Lemma 2.10 and the above argument is:

Lemma 2.11. *Let W be a nonzero subspace of $V_\ell(J_{K'})_{\mathrm{prim}}$. If W is stable under the action of $\mathrm{Gal}(\mathbb{F}(u)/\mathbb{F}(t))$, then there is an injective map $\mu_{ab} \to \mathrm{Aut}_{\mathbb{Q}_\ell}(W)$.*

End of the proof of Theorem 1.4. We now finally prove the "if" direction of the statement. Assume, then, that a, b are distinct prime numbers both different from p, and pick a prime $\ell \neq p$ so that $\ell \equiv 1 \bmod ab$. We let $\mathbb{F}$ denote the finite extension of $\mathbb{F}_r$ containing all the ab^{th} roots of unity, and set $K' = \mathbb{F}(t)$ and $L' = \overline{\mathbb{F}}(u)$ as above. We actually prove the slightly stronger statement that the base changed Jacobian $J_{K'} = J \times_K K'$ is simple.

Let A be a positive-dimensional abelian subvariety of $J_{K'}$ defined over K'. The ℓ-adic Tate module $W_\ell := V_\ell(A)$ is then a nonzero subspace of $V_\ell(J_{K'})$, which is stable under the action of $\mathrm{Gal}(L'/K')$. *A fortiori*, W_ℓ is stable under the action of $\mathrm{Gal}(\mathbb{F}(u)/K') \simeq \mu_{ab}$. Applying Lemma 2.11 to W_ℓ (given that a and b are primes, we have $V_\ell(J_{K'})_{\mathrm{prim}} = V_\ell(J_{K'})$), there is an injective map $j : \mu_{ab} \hookrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(W_\ell)$. Faltings' isogeny theorem (proved by Zarhin in the context of function fields) shows that $\mathrm{End}_{\mathbb{Q}_\ell}(W_\ell) \simeq \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. It follows from the existence and injectivity of j that the $\mathbb{Q}$-algebra $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains a subalgebra E which is isomorphic to the ab^{th} cyclotomic field extension $\mathbb{Q}(\xi_{ab})$ of $\mathbb{Q}$. On the other hand, we know from the Corollary to Theorem 4 in §19 of [Mum08] that the dimension of a semi-simple commutative subalgebra of $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ cannot exceed $2 \dim A$. Thus the chain of inequalities:

$$2 \dim J_{K'} \geq \ 2 \dim A \geq \dim_{\mathbb{Q}} E = [\mathbb{Q}(\xi_{ab}) : \mathbb{Q}] = \phi(ab) = (a-1)(b-1) = 2g = 2 \dim J_{K'}.$$

We conclude that $\dim A = \dim J_{K'}$, so that $A = J_{K'}$. This shows that $J_{K'}$ is simple. □

Before we close off this discussion about the simplicity of J, we remark that the "primitive" part $V_\ell(J_{K'})_{\mathrm{prim}}$ of $V_\ell(J_{K'})$ "comes" from an abelian subvariety J_{prim} of $J_{K'}$. We begin by a lemma.

Lemma 2.12. *Let G be a finite group, and X be a curve over $\mathbb{F}$ equipped with a G-action. We let $Y = X/G$ and $f : X \to Y$ be the quotient map. Write J_X and J_Y for the Jacobians of X and Y, respectively. Then J_Y is isogenous to the G-invariant subabelian variety $(J_X)^G \subset J_X$. Moreover, for any prime $\ell \neq p$ there is an isomorphism $V_\ell((J_X)^G) \cong V_\ell(J_Y)$.*

Proof. By the isogeny theorem of Tate (see [Mum08, Appendix I]), the second assertion follows from the first one: if indeed J_Y and J_X^G are isogenous then, on the level of ℓ-adic Tate modules, we have an isomorphism between $V_\ell(J_Y)$ and $V_\ell((J_X)^G) \simeq V_\ell(J_X)^G$.

The quotient map $f : X \to Y$ induces, by contravariance of the Jacobian, an algebraic group morphism $f^* : J_Y \to J_X$. The image of f^* is then contained in the subabelian variety $(J_X)^G$ formed by G-invariant elements in J_X. By restriction, we thus obtain an algebraic group morphism $\phi : J_Y \to (J_X)^G$. Since J_Y and $(J_X)^G$ have the same dimension, it suffices to prove that ϕ is finite in order to conclude. Let $x \in (J_X)^G$ be a G-invariant point, and pick a divisor $D \in \mathrm{Div}(X)$ on X whose image in J_X is x. Let $\widetilde{D} := \sum_{g \in G} g \cdot D \in \mathrm{Div}(X)$. Writing n for the order of G, the image of $\widetilde{D}$ in J_X is $\sum_{g \in G} g \cdot x = [n]x$. On the other hand, it is clear that $\widetilde{D}$ is G-invariant, so that $\widetilde{D}$ is the pullback by f of some divisor D' on Y. Let $y \in J_Y$ denote the image of D' in J_Y. We thus have $[n]x = f^*(y) = \phi(y)$.

This shows that the image of $\phi : J_Y \to (J_X)^G$ has finite index, which implies that ϕ is an isogeny, thus concluding the proof. □

Let a and b be coprime integers, both coprime to p, and fix a power q of p. For any divisors $\alpha \mid a$ and $\beta \mid b$, we let $\mathsf{C}_{\alpha,\beta}$ be the smooth projective curve over $\mathbb{F}$ with open affine defined by $x^\alpha + y^\beta = 1$, and denote by $\mathsf{J}_{\alpha,\beta}/\mathbb{F}$ its Jacobian. We have mentioned above (Proposition 2.1) that $\mathsf{C}_{\alpha,\beta}$ has genus $(\alpha-1)(\beta-1)/2 = \dim \mathsf{J}_{\alpha,\beta}$. The map $(x,y) \mapsto (x^{a/\alpha}, y^{b/\beta})$ extends into a surjective morphism $\mathsf{C}_{a,b} \to \mathsf{C}_{\alpha,\beta}$. Functoriality of the Jacobian yields a surjective push-forward morphism of abelian varieties $\varpi_{\alpha,\beta} : \mathsf{J}_{a,b} \to \mathsf{J}_{\alpha,\beta}$. We then let

$$(\mathsf{J}_{a,b})_{\mathrm{prim}} := \ker\left(\mathsf{J}_{a,b} \xrightarrow{\prod \varpi_{\alpha,\beta}} \prod_{\substack{\alpha\mid a\\ 1<\alpha<a}} \prod_{\substack{\beta\mid b\\ 1<\beta<b}} \mathsf{J}_{\alpha,\beta}\right),$$

where the right-most product is over proper divisors α of a and β of b. This subabelian variety of $\mathsf{J}_{a,b}$ is defined over $\mathbb{F}$. We remark the following:

Lemma 2.13. *There is an $\mathbb{F}$-isogeny $\mathsf{J}_{a,b} \to \prod_{\alpha\mid a}\prod_{\beta\mid b}(\mathsf{J}_{\alpha,\beta})_{\mathrm{prim}}$.*

Proof. Let $\mathsf{J}'_{a,b}$ denote the product $\prod_{\alpha\mid a}\prod_{\beta\mid b}(\mathsf{J}_{\alpha,\beta})_{\mathrm{prim}}$. Both $\mathsf{J}_{a,b}$ and $\mathsf{J}'_{a,b}$ are abelian varieties over the finite field $\mathbb{F}$. We know by Tate's isogeny theorem (see [Mum08, Appendix I]) that there is an isomorphism between $\mathrm{Hom}(\mathsf{J}_{a,b}, \mathsf{J}'_{a,b}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ and the subspace of $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-invariants in $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(\mathsf{J}_{a,b}), V_\ell(\mathsf{J}'_{a,b}))$. In order to conclude, it thus suffices to prove that there is a $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-equivariant isomorphism of $\mathbb{Q}_\ell$-vectors spaces between $V_\ell(\mathsf{J}_{a,b})$ and $V_\ell(\mathsf{J}'_{a,b})$.

By definition of $\mathsf{J}'_{a,b}$, we have $V_\ell(\mathsf{J}'_{a,b}) \cong \bigoplus_{\alpha\mid a}\bigoplus_{\beta\mid b} V_\ell((\mathsf{J}_{\alpha,\beta})_{\mathrm{prim}})$. Note that the summands with $\alpha = 1$ or $\beta = 1$ are trivial (since $\mathsf{J}_{\alpha,\beta}$ then has dimension zero). Combining this with the decomposition (2.3), we have $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-equivariant isomorphisms

$$V_\ell(\mathsf{J}'_{a,b}) \cong \bigoplus_{\substack{\alpha\mid a\\ \alpha>1}}\bigoplus_{\substack{\beta\mid b\\ \beta>1}} V_\ell((\mathsf{J}_{\alpha,\beta})_{\mathrm{prim}}) \cong \bigoplus_{\substack{\alpha\mid a\\ \alpha>1}}\bigoplus_{\substack{\beta\mid b\\ \beta>1}}\left(\bigoplus_{\substack{\chi_\alpha \text{ of order } \alpha\\ \chi_\beta \text{ of order } \beta}} L_{(\chi_\alpha,\chi_\beta)}\right) \cong \bigoplus_{\substack{\chi_a \text{ of order } >1\\ \chi_b \text{ of order } >1}} L_{(\chi_a,\chi_b)}.$$

The right-most sum equals $V_\ell(\mathsf{J}_{a,b})$, by decomposition (2.3). This concludes the proof. □

We may now prove

Lemma 2.14. *$V_\ell((\mathsf{J}_{a,b})_{\mathrm{prim}})$ is isomorphic, as a $\mathbb{Q}_\ell$-vector space with μ_{ab}-action, to $V_\ell(\mathsf{J}_{a,b})_{\mathrm{prim}}$.*

Proof. Combining Lemma 2.13 to a straightforward application of the inclusion-exclusion principle (using that $\sum_{\delta\mid d}\phi(\delta) = d$ for any integer $d \geq 1$), one shows that $(\mathsf{J}_{a,b})_{\mathrm{prim}}$ has dimension $\phi(a)\phi(b)/2$ for any $a, b > 1$. Since $(\mathsf{J}_{a,b})_{\mathrm{prim}}$ is contained in $\mathsf{J}_{a,b}$, we may view $V_\ell((\mathsf{J}_{a,b})_{\mathrm{prim}})$ as a subspace of $V_\ell(\mathsf{J}_{a,b})$. By the dimension computations we did, we know that $\dim V_\ell((\mathsf{J}_{a,b})_{\mathrm{prim}}) = \dim V_\ell(\mathsf{J}_{a,b})_{\mathrm{prim}} = \phi(a)\phi(b)$. It thus suffices to show one inclusion.

To do so, we note the following. For any divisors $\alpha \mid a$ and $\beta \mid b$, there is a unique subgroup $\gamma_{\alpha,\beta}$ of μ_{ab} of order $ab/(\alpha\beta)$. This subgroup $\gamma_{\alpha,\beta}$ acts on $\mathsf{C}_{a,b}$ (and thus, on $\mathsf{J}_{a,b}$) and the quotient $\mathsf{C}_{a,b}/\gamma_{\alpha,\beta}$ is isomorphic to $\mathsf{C}_{\alpha,\beta}$, the quotient map being $\varpi_{\alpha,\beta} : \mathsf{C}_{a,b} \to \mathsf{C}_{\alpha,\beta}$. Lemma 2.12 yields an isogeny $\mathsf{J}_{\alpha,\beta} \to (\mathsf{J}_{a,b})^{\gamma_{\alpha,\beta}}$ and an isomorphism $V_\ell(\mathsf{J}_{\alpha,\beta}) \cong V_\ell(\mathsf{J}_{a,b})^{\gamma_{\alpha,\beta}}$. Since $\mu_{ab} \simeq \mu_a \times \mu_b$, we may write $\gamma_{\alpha,\beta} \simeq \gamma_\alpha \times \gamma_\beta$. With our description (2.4) of the μ_{ab}-action on the lines the decomposition (2.3), we immediately see that

$$V_\ell(\mathsf{J}_{a,b})^{\gamma_{\alpha,\beta}} = \bigoplus_{\substack{\chi_a,\ \chi_b \text{ nontrivial}\\ \chi_a|_{\gamma_\alpha} \text{ trivial}\\ \chi_b|_{\gamma_\beta} \text{ trivial}}} L_{(\chi_a,\chi_b)}.$$

The condition that a character $\chi_a : \mu_a \to \mathbb{Q}_\ell^\times$ is trivial on γ_α is equivalent to requiring that this character has order dividing $a/|\gamma_\alpha| = \alpha$. Similarly for characters χ_b.

With this at hand, let χ_a, χ_b be a pair of non trivial characters of μ_a and μ_b. By definition, the line $L_{(\chi_a,\chi_b)}$ appears in $V_\ell(\mathsf{J}_{a,b})_{\mathrm{prim}}$ if and only if χ_a has exact order a and χ_b has exact order b. Recalling how $(\mathsf{J}_{a,b})_{\mathrm{prim}}$ was constructed, the above shows that the line $L_{(\chi_a,\chi_b)}$ appears in $V_\ell((\mathsf{J}_{a,b})_{\mathrm{prim}})$ if and only if χ_a does not factor through any proper subgroup of μ_a and χ_b does not factor through any proper subgroup of μ_b. Thus, the conditions for the line $L_{(\chi_a,\chi_b)}$ to appear in one of $V_\ell(\mathsf{J}_{a,b})_{\mathrm{prim}}$ or $V_\ell((\mathsf{J}_{a,b})_{\mathrm{prim}})$ match. Hence the result. □

Recall from the preceding discussion that there is an isomorphism $\phi^* : (\mathsf{J}_{a,b})_{L'} \to J_{L'}$. We let

$$J_{\mathrm{prim}} := \phi^*((\mathsf{J}_{a,b})_{\mathrm{prim}} \times_{\mathbb{F}} L') \subset J_{L'}.$$

The subabelian variety $(\mathsf{J}_{a,b})_{\mathrm{prim}}$ is defined over $\mathbb{F}$ and is stable under the action of μ_{ab}. As was proved above, $(\phi^*)^{-1}$ carries the $\mathrm{Gal}(L'/K')$-action on $J_{L'}$ to the action on $V_\ell(\mathsf{J}_{a,b})$ given by the product of the standard $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-action on $V_\ell(\mathsf{J}_{a,b})$ by the inverse of the action of μ_{ab} on $V_\ell(\mathsf{J}_{a,b})$ induced by (2.2). Given the invariance of $(\mathsf{J}_{a,b})_{\mathrm{prim}}$ under both of these latter actions, we deduce that J_{prim} is an abelian subvariety of $J_{K'}$ which is defined over K'. Moreover, Lemma 2.14 yields a $\mathrm{Gal}(\overline{K}/K')$-equivariant isomorphism

$$V_\ell(J)_{\mathrm{prim}} \cong V_\ell(J_{\mathrm{prim}}).$$

With this notation we obtain the following strengthening of (part of) Theorem 1.4:

Theorem 2.15. *Let a, b be two coprime positive integers which are both coprime to p, and q be any power of p. Let $J = J_{a,b,q}/K$ be as before, and $J_{\mathrm{prim}} \subset J_{K'}$ be the abelian subvariety defined above. Then J_{prim} is simple over K'.*

Proof. One simply has to repeat the argument proving the 'if' part of Theorem 1.4 with $J_{K'}$ replaced by J_{prim}, and $V_\ell(J_{K'})$ replaced by $V_\ell(J_{\mathrm{prim}}) \cong V_\ell(J_{K'})_{\mathrm{prim}}$. □

Remark 2.16. Note that Theorem 1.4 cannot be refined to show that J is geometrically simple when a, b are both primes. Under certain congruence conditions on a, b, and r, the Jacobian $\mathsf{J}_{a,b}$ indeed has repeated isogeny factors over $\overline{\mathbb{F}_r}$. For instance, the Jacobian of the genus 2 curve $y^2 + x^5 = 1$ over $\mathbb{F}_{19}$ is geometrically isogenous to the square of a supersingular elliptic curve. Since J and $\mathsf{J}_{a,b}$ become isomorphic after a suitable base change, the Jacobian of the genus 2 curve $y^2 + x^5 = t^q - t$ over $\mathbb{F}_{19}(t)$ is not geometrically simple.

3 Background on Gauss sums

In this section, we gather some facts about Gauss sums which will prove 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 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 define a multiplicative character $\chi_{\mathbb{F},n}$ on $\mathbb{F}$ by

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

A straightforward computation shows that $\chi_{\mathbb{F},n}$ 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 $\mathbb{Q}(\zeta_p)$. 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 define an additive character $\psi_{\mathbb{F},\alpha}$ on $\mathbb{F}$ by

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

The character $\psi_{\mathbb{F},\alpha}$ 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 $\mathbb{F}$, the following hold:

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

(For proofs of these, see [Was97, Chapter VI, §1-2] for instance.)

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, $\langle r \rangle$ acts on $(\mathbb{Z}/a\mathbb{Z} \smallsetminus \{0\}) \times (\mathbb{Z}/b\mathbb{Z} \smallsetminus \{0\})$ 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. For any integer $n \geq 1$ coprime to p, recall that we write $o_p(n)$ (resp. $o_r(n)$) for 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 let $\kappa_{r,n}(i)$ denote 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 $(i,j,\alpha) \in S$, its length $|o|$ is the least integer $f \geq 1$ such that $\alpha \in \mathbb{F}_{r^f}$, a divides $i(r^f - 1)$, and b divides $j(r^f-1)$. This shows that

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

For any integer n coprime to p, let

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

We endow S'_n with an action of $\langle r \rangle$ *via* the rule $r \cdot (i, \alpha) = (ri, \alpha^{1/r})$. We 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 both $\alpha \in \mathbb{F}_{r^f}$ and n divides $i(r^f - 1)$. In other words,

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

Notation being as above, the natural projection maps $S_{a,b,q} \to S'_a$ and $S_{a,b,q} \to S'_b$ clearly 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

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

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 nontrivial 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, we have $\alpha^{r^{|o'|}} = \alpha$, so that $\alpha \in \mathbb{F}'$. Hence, we may consider the nontrivial 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 $i\,(r^{|o|}-1) = i\,|\mathbb{F}'^{\times}|$. We may thus introduce a nontrivial 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 allows to consider the Gauss sum $\mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(i,\alpha)}, \Psi_{(i,\alpha)}\big)$, about which we prove the following:

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,

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

The map $x \mapsto x^r$ being a bijection $(\mathbb{F}')^\times \to (\mathbb{F}')^\times$, we may reindex by setting $y = x^r$. 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 $\mathbb{F}_r \subset \mathbb{F}'$, any $z \in \mathbb{F}'$ is conjugate to z^r over $\mathbb{F}_r$, and hence $\mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_p}(z) = \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}_p}(z^r)$. We finally get

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

□

Lemma 3.4 allows us to associate a Gauss sum to each $\langle r\rangle$-orbit:

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, equation (3.1) shows that

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

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 as above, 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 the definition of $\mathbf{G}\left(o'\right)$ and equation (3.2), we have

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

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 $g_{o'} := \mathrm{G}_{\mathbb{F}}\Big(\chi_{\mathbb{F},|\mathbb{F}|}^{i|\mathbb{F}^\times|/a}, \psi_{\mathbb{F},1}\Big)$. Then, $g_{o'}$ is a Weil integer of size $p^{\kappa_{p,a}(i)/2}$ according to (3.1). Applying the Hasse–Davenport relation (3.3) for Gauss sums, we deduce that

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

A similar argument shows that, if we define $\zeta_{\pi_b(o)} := \boldsymbol{\lambda}_{(j,\alpha)}(\alpha)^{-1}$ and $g_{\pi_b(o)} := \mathrm{G}_{\mathbb{F}}\Big(\chi_{\mathbb{F},|\mathbb{F}|}^{j|\mathbb{F}^\times|/b}, \psi_{\mathbb{F},1}\Big)$, 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 and the BSD conjecture

In this section, we provide an explicit formula for the L-function of the Jacobian J of the curve C. (See Theorem 4.2.) Our first proof, given in this section, is based on a computation with character sums. In Section 4.5, we remark that J satisfies the BSD conjecture: this fact will be crucial in Section 6 for us to make further observations about the rank of J. Section 5 contains an alternate cohomological proof of our explicit formula (4.2) for $L(J,T)$.

4.1 Definition of the L-function

Fix a prime number $\ell \neq p$, and let $H^1(J) := H^1_{\text{ét}}(J, \overline{\mathbb{Q}_\ell})$ 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 I_v denote an inertia group at v (the possible choices form a conjugacy class), Fr_v denote a geometric Frobenius at v (the possible choices form a coset of I_v), and we 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 $V_\ell(J) \otimes \overline{\mathbb{Q}_\ell}$. (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 $H^1(J)$. Recall from [ST68] that 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 $2g$.

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_v 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 $L(J,T)$, defined to the degree of the numerator minus the degree of the denominator, 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 J in Theorem 4.2, we check the degree in Remark 4.9 using the formula $b(J) = \deg N_J - 4g$. This formula will also be used in the cohomological computation of $L(J,T)$ in Section 5.

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 most of the rest of Section 4. 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 unipotent reduction at all of its places of bad reduction. At a place v of unipotent reduction for J, $\dim_{\mathbb{Q}_\ell} H^1(J)^{I_v} = 0$, as shown in [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. Consequently, 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 $\dim_{\mathbb{Q}_\ell} H^1(J)^{I_v} = 2g$. 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 write $m = k \deg v$ and reindex the outer sums. By definition, we have

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

hence the reindexation 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 that $\deg(v_\beta) = [\mathbb{F}_r(\beta) : \mathbb{F}_r]$. Note that tshe 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_β.

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

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

The Grothendieck–Lefschetz trace formula then yields

$$\operatorname{Tr}(\operatorname{Fr}_{v_\beta}^{m/\deg v_\beta} | H^1(J)) = |\mathbb{F}_{r^m}| + 1 - |X_\beta(\mathbb{F}_{r^m})| = A_J(\beta, m).$$

Plugging this last identity into (4.5) concludes the proof. □

We now interpret the quantities $A_J(\beta, m)$ appearing in Lemma 4.3 in terms of character sums. For any $m \geq 1$, we write $\mathbf{1}$ for the trivial multiplicative character on $\mathbb{F}_{r^m}$.

For any $m \geq 1$ and $c \geq 2$ we set

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

We further define $M'_{a,b}(r^m) = M'_a(r^m) \times M'_b(r^m)$. We extend all nontrivial multiplicative characters λ on $\mathbb{F}_m$ by $\lambda(0) = 0$. For any pair (λ_1, 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 nontrivial 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 appears to depend on the choice of a nontrivial additive character ψ_r while 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. The curve $X_\beta/\mathbb{F}_{r^m}$ has a unique point at infinity, and this point is rational over $\mathbb{F}_{r^m}$. As a consequence, 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

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

It is classical (see [Coh07, Lemma 2.5.21]) that for any integer $N \geq 2$ and 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 $\lambda = \mathbf{1} \in M_N(r^m)$ contributes 1. Evaluating (4.7) with $N = b$ and $z = -x^a + \beta^q - \beta$ into (4.6), and swapping the sums yields

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

For all $\beta \in \mathbb{F}_{r^m}^\times$, we therefore 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 $\beta^q - \beta = 0$, including if $\beta = 0$. It follows 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 nontrivial 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 nontrivial 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 proves 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 nontrivial multiplicative characters on $\mathbb{F} = \mathbb{F}_{r^m}$, a nontrivial 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

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

Reindexing 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. *Let $c \geq 1$ be an integer coprime to p. For $i \in \mathbb{Z}/c\mathbb{Z} \smallsetminus \{0\}$, let $\kappa_i = o_r\big(c/\gcd(c,i)\big)$. Then, the map*

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

is a bijection.

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

Conversely, let λ be a nontrivial 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_i of r modulo c' divides m and so $i'(r^{\kappa_i} - 1)/c'$ is an integer. We have $\ell = i(r^m - 1)/c$. So, for all $x \in \mathbb{F}_{r^m}^\times$,

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

Hence λ has the desired form. □

We now connect our last results with the discussion in §3.3–§3.4. There we introduced the set $O = O_{a,b,q}$ of orbits of the action of $\langle r \rangle$ on $(\mathbb{Z}/a\mathbb{Z} \smallsetminus \{0\}) \times (\mathbb{Z}/b\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q^\times$, as well as the set O'_n of $\langle r \rangle$-orbits of $(\mathbb{Z}/n\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q^\times$. We also defined two natural surjective maps

$$\pi_a : O \to O'_a \quad \text{and} \quad \pi_b : O \to O'_b.$$

Fix a nontrivial additive character ψ_0 on $\mathbb{F}_p$. For any $m \geq 1$ and $\alpha \in \mathbb{F}_{r^m} \cap \mathbb{F}_q$, define an additive character $\psi_{m,\alpha} : \mathbb{F}_{r^m} \to \overline{\mathbb{Q}}$ by putting $\psi_{m,\alpha}(x) = (\psi_0 \circ \mathrm{Tr}_{\mathbb{F}_{r^m}/\mathbb{F}_p})(\alpha x)$ for all $x \in \mathbb{F}_{r^m}$.

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 $o \in O$, recall from §3.3 that $|\pi_a(o)|$ and $|\pi_b(o)|$ both divide $|o|$. If $|o|$ divides m, then $|\pi_a(o)|$ and $|\pi_b(o)|$ *a fortiori* do so. Since $\nu_a(o) = |o|/|\pi_a(o)|$, we have

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

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

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 $\kappa_{r,a}(i) = o_r(a/\gcd(a,i))$ and $\kappa_{r,b}(j) = o_r(b/\gcd(b,j))$. We have

$$\sum_{\substack{o\in O\\ |o| \text{ divides } m}} |o|\,\boldsymbol{\omega}(o)^{m/|o|} = \sum_{\substack{(i,j,\alpha)\in S\\ \alpha\in\mathbb{F}_{r^m}^\times\\ \kappa_{r,a}(i)|m\\ \kappa_{r,b}(j)|m}} \mathrm{G}_{r^m}\big(\boldsymbol{\lambda}_{(i,\alpha)} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_a}}, \psi_{m,\alpha}\big)\mathrm{G}_{r^m}\Big(\boldsymbol{\lambda}_{(j,\alpha)} \circ \mathrm{N}_{\mathbb{F}_{r^m}/\mathbb{F}_{r_b}}, \psi_{m,\alpha}\Big)\,. \tag{4.10}$$

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

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

For any $m \geq 1$, Lemma 4.7 states that, as i runs through 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 runs through all elements of $(\mathbb{Z}/b\mathbb{Z} \smallsetminus \{0\})$ such that $\kappa_{r,b}(j) \mid m$, 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, recalling that $S = (\mathbb{Z}/a\mathbb{Z} \smallsetminus \{0\}) \times (\mathbb{Z}/b\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q^\times$, we see that if $(i,j,\alpha) \in S$, then $\alpha \in \mathbb{F}_q^\times$. Altogether, we conclude by reindexing the sum on the right-hand side of (4.10) from a sum over $(i,j,\alpha) \in S$ such that $\alpha \in \mathbb{F}_{r^m}^\times$, $\kappa_{r,a}(i) \mid m$ and $\kappa_{r,b}(j) \mid m$ to a sum over $(\alpha, \lambda_1, \lambda_2) \in (\mathbb{F}_{r^m} \cap \mathbb{F}_q)^\times \times M'_{a,b}(r^m)$. □

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 $\mathrm{G}_{\mathbb{F}}(\lambda_1,\psi_{m,0})\mathrm{G}_{\mathbb{F}}(\lambda_2,\psi_{m,0})$ 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. Theorem 4.1 yields that $\deg L(J,T) = b(J) = \deg N_J - 4g$. From this formula and the computation of $\deg N_J$ in Proposition 2.6, we find

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

On the other hand, from our Theorem 4.2, we see that the degree of $L(J,T)$ equals $\sum_{o\in O}|o|$, where O is the set of $\langle r\rangle$-orbits on $S = (\mathbb{Z}/a\mathbb{Z}\smallsetminus\{0\})\times(\mathbb{Z}/b\mathbb{Z}\smallsetminus\{0\})\times\mathbb{F}_q^\times$. Since S may be written as the disjoint union of the $\langle r\rangle$-orbits $o\in O$, it is clear that $\sum_{o\in O}|o| = |S|$.

Since $|S| = (a-1)(b-1)(q-1)$, we recover the result.

4.5 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 $[3/2,\infty)$. 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 nonnegative. Since $L^*(J)$ is, by definition, a nonzero 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 $P_1,\ldots,P_r$ for $J(K)$ modulo torsion and a basis $\widehat{P_1},\ldots,\widehat{P_r}$ for $\widehat{J}(K)$ modulo torsion, the regulator of J is defined to be

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

These definitions allow us to sate our Theorem 1.1, proving the Birch and Swinnerton-Dyer conjecture for J/K :

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 $\text{Ш}(J)$ is finite.*
- *The BSD formula holds:*
$$L^*(J) = \frac{|\text{Ш}(J)|\,\operatorname{Reg}(J)\,\prod_v c_v(J)}{H(J)\,r^{-g}\,|J(K)_{\mathrm{tors}}|^2}, \tag{4.11}$$
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 background about the Birch and Swinnerton-Dyer conjecture for Jacobians over function fields.

Proof. Theorem 1.1 is but a special case of [PU16, Theorem 3.1.2]. One of the main argument in their proof can, in essence, be traced back to Shioda's work on surfaces defined by 4-nomials (see [Shi86]). □

This result will allow us to derive precise information about $\operatorname{rank} J(K)$ in Section 6.

Remark 4.10. The BSD formula is probably more typically stated as
$$L^*(J) = \frac{|\text{Ш}(J)|\,\operatorname{Reg}(J)\,\prod_v c_v(J)}{H(J)\,r^{-g}\,|J(K)_{\mathrm{tors}}|\,|J^\vee(K)_{\mathrm{tors}}|}. \tag{4.12}$$
In our case, J is principally polarized because J is a Jacobian, so that $J \cong J^\vee$. In particular, $|J(K)_{\mathrm{tors}}|\,|J^\vee(K)_{\mathrm{tors}}| = |J(K)_{\mathrm{tors}}|^2$, and our statement agrees with the typical one.

5 Cohomological computation of $L(J,T)$

Our goal in this section is to provide an alternative computation of the L-function $L(J,T)$ using the geometry of the minimal proper regular SNC model $\mathcal{S}$ of C. In particular, we compute the zeta function of $\mathcal{S}$ in two different ways – first by decomposing it via the fibers over $\mathbb{P}^1$ and a second time by understanding the cohomology of $\mathcal{S}$ in terms of a product of curves which dominates $\mathcal{S}$.

This computation generalizes the one found in [GU20, §7] for $a = 2$ and $b = 3$.

Throughout the section, we denote by $H^n(-)$ the n^{th} ℓ-adic cohomology group of a variety over $\mathbb{F}_r$. That is, $H^n(X)$ denotes $H^n_{\text{ét}}(X \times_{\mathbb{F}_r} \overline{\mathbb{F}_r}, \overline{\mathbb{Q}_\ell})$ for a prime $\ell \neq p$. This cohomology group is endowed with a natural action of the geometric r^{th} power Frobenius Fr_r.

The following linear algebra fact (also used in [Ulm07], [GU20]) will be useful for the linear algebra arguments in our cohomology computation:

Lemma 5.1. *Let V be a finite-dimensional vector space with subspaces W_i indexed by $i \in \mathbb{Z}/m\mathbb{Z}$ such that $V = \bigoplus_{i\in\mathbb{Z}/m\mathbb{Z}} W_i$, and let $\phi : V \to V$ be a linear map such that $\phi(W_i) \subset W_{i+1}$ for all $i \in \mathbb{Z}/m\mathbb{Z}$. Then*
$$\det\left(1 - \phi T\,|V\right) = \det\left(1 - \phi^m T^m |W_0\right).$$

5.1 Preliminaries about Artin–Schreier curves

For any prime-to-p integer $d \geq 1$ and any power q of p, let $X_{d,q}$ be the smooth projective curve over $\mathbb{F}_r$ defined by the affine equation

$$X_{d,q}: \qquad w^d = z^q - z\,.$$

Since d and q are relatively prime, $X_{d,q}$ admits a unique point at infinity which we denote by $P_\infty \in X_{d,q}$. We note that P_∞ is $\mathbb{F}_r$-rational. A straightforward application of the Riemann–Hurwitz formula yields that $X_{d,q}$ has genus $(q-1)(d-1)/2$. Hence, $\dim_{\mathbb{Q}_\ell} H^1(X_{d,q}) = (q-1)(d-1)$.

The curve $X_{d,q} \times_{\mathbb{F}_r} \overline{\mathbb{F}_r}$ is naturally endowed with an action of $\mu_d \times \mathbb{F}_q$, defined as follows: for any $\zeta \in \mu_d$ and any $\alpha \in \mathbb{F}_q$, set $(\zeta, \alpha) \cdot (w, z) := (\zeta w, z + \alpha)$ for any $(w, z) \in X_{d,q} \smallsetminus \{P_\infty\}$, and $(\zeta, \alpha) \cdot P_\infty = P_\infty$. By the functoriality of cohomology, this induces an action of $\mu_d \times \mathbb{F}_q$ on $H^1(X_{d,q})$. For any $(i, \alpha) \in S'_d$, we denote by $H^1(X_{d,q})^{(i,\alpha)}$ the subspace of $H^1(X_{d,q})$ on which $\mu_d \times \mathbb{F}_q$ acts as multiplication by $\lambda_{(i,\alpha)}\psi_{(i,\alpha)}$. By [Kat81], each $H^1(X_{d,q})^{(i,\alpha)}$ has dimension 1.

Recall from §3.3 that we defined $S'_d = (\mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q^\times$ and endowed it with an action by $\langle r \rangle$, and let O'_d be the set of orbits of S'_d under this action. Moreover for any $(i, \alpha) \in S'_d$, we defined (in §3.4) an additive character $\boldsymbol{\lambda}_{(i,\alpha)}$ and a multiplicative character $\Psi_{(i,\alpha)}$ on $\mathbb{F}_{r^{|o|'}}$. By construction, $\boldsymbol{\lambda}_{(i,\alpha)}$ induces a character $\lambda_{(i,\alpha)}$ of μ_d by composition with the quotient map

$$(\mathbb{F}_{r^{|o'|}})^\times \to (\mathbb{F}_{r^{|o'|}})^\times / \ker \lambda_{(i,\alpha)} \simeq \mu_{d/(d,i)} \subset \mu_d,$$

and $\Psi_{(i,\alpha)}$ induces an additive character $\psi_{(i,\alpha)}$ of $\mathbb{F}_q$ by composition with the trace map $\mathrm{Tr}_{\mathbb{F}_{r^{|o'|}}/\mathbb{F}_q}$. The map which takes (i, α) to the product character $\lambda_{(i,\alpha)}\psi_{(i,\alpha)}$ is a bijection between S'_d and the group of characters of $\mu_d \times \mathbb{F}_q$. Using this bijection, the decomposition of $H^1(X_{d,q})$ as a direct sum of lines alluded to in the previous paragraph then reads

$$H^1(X_{d,q}) = \bigoplus_{(i,\alpha) \in S'_d} H^1(X_{d,q})^{(i,\alpha)}. \tag{5.1}$$

The action of Fr_r on $H^1(X_{d,q})$ sends the line $H^1(X_{d,q})^{(i,\alpha)}$ indexed by $(i, \alpha) \in S'_d$ onto the line indexed by $(ri, \alpha^{1/r})$. We deduce from the above that, for any orbit $o' \in O'_d$, the $|o'|^{\text{th}}$ iterate of Fr_r stabilizes the line $H^1(X_{d,q})^{(i,\alpha)}$ for any representative $(i, \alpha) \in o'$. By [Kat81], the eigenvalue of $(\mathrm{Fr}_r)^{|o'|}$ acting on the line $H^1(X_{d,q})^{(i,\alpha)}$ is the Gauss sum $\mathbf{G}\,(o')$ which we defined in §3.4, Definition 3.6. In other words, we have

$$\det\left(1 - \mathrm{Fr}_r^{|o'|}\, T \,\middle|\, H^1(X_{d,q})^{(i,\alpha)}\right) = 1 - \mathbf{G}\left(o'\right) T, \tag{5.2}$$

for any $(i, \alpha) \in o'$. Furthermore, the direct sum

$$H^1(X_{d,q})_{o'} := \bigoplus_{(i,\alpha) \in o'} H^1(X_{d,q})^{(i,\alpha)}$$

is stable under the action of Fr_r, and the action of Fr_r cyclically permutes the summands thereof. By Lemma 5.1, we thus have

$$\det\left(1 - \mathrm{Fr}_r\, T \,\middle|\, H^1(X_{d,q})_{o'}\right) = 1 - \mathbf{G}\left(o'\right) T^{|o'|}\,.$$

We conclude that

$$\det\left(1 - \mathrm{Fr}_r\, T \,\middle|\, H^1(X_{d,q})\right) = \prod_{o' \in O'_d} \left(1 - \mathbf{G}\left(o'\right) T^{|o'|}\right)\,,$$

is the L-function of the curve $X_{d,q}/\mathbb{F}_r$ (*i.e.*, the numerator of its Hasse–Weil ζ-function, viewed as a rational function in T).

5.2 Domination by a product of curves

Let $a, b \geq 1$ be relatively prime integers which are both coprime to p, and let q be a power of p.

Let X_a and Y_b be smooth projective curves over $\overline{\mathbb{F}_r}$ defined by the (singular) affine equations

$$\begin{aligned} X_a : x^a &= u_1 \,, \\ Y_b : y^b &= u_2 \,. \end{aligned}$$

Let ∞_a denote the unique point at infinity on X_a and let ∞_b denote the unique point at infinity on Y_b. Let $\mathcal{P}$ be the product $X_a \times Y_b$ and let $\pi : \mathcal{S}_0 \to \mathbb{P}^1_{\overline{\mathbb{F}_r}}$ be the minimal proper regular model of the curve with affine equation $x^a + y^b = u$ over $\overline{\mathbb{F}_r}(u)$.

The surface $\mathcal{P}$ is equipped with a rational map $\pi_0 : \mathcal{P} \dashrightarrow \mathbb{P}^1$ defined on the affine patch by

$$\begin{array}{cccc} \pi_0 : & \mathcal{P} & \dashrightarrow & \mathbb{P}^1, \\ & ((x, u_1), (y, u_2)) & \mapsto & u_1 + u_2 \,. \end{array}$$

The rational map π_0 also maps $\{\infty_a\} \times (Y_b \smallsetminus \{\infty_b\})$ and $\{\infty_a\} \times (Y_b \smallsetminus \{\infty_b\})$ to $\infty \in \mathbb{P}^1$, and has a unique point of indeterminacy at (∞_a, ∞_b). As is explained in the proof of Proposition 3.1.5 of [PU16], one can resolve the indeterminacy in π_0 through a series of blow-ups at the point of indeterminacy. Moreover, as [PU16] explains in Remark 3.1.6, the exceptional fiber of the last blow-up maps isomorphically to $\mathbb{P}^1$ and all other fibers map to $\infty \in \mathbb{P}^1$. Let $\mathcal{R}$ be the result of this blow-up. Examining the construction and comparing to the recipe for constructing minimal proper regular SNC models from [Dok20], we find that in fact, $\mathcal{R}$ is the minimal proper regular model of the curve with affine equation $x^a + y^b = u$ over $\overline{\mathbb{F}_r}(u)$.

Let $\mathcal{P}_{q,q} = X_{a,q} \times Y_{b,q}$. The surface $\mathcal{P}_{q,q}$ is a Galois cover of $\mathcal{P}$ with Galois group $\mathbb{F}_q \times \mathbb{F}_q$. Let $\mathcal{R}_{q,q}$ be the fiber product $\mathcal{R} \times_{\mathcal{P}} \mathcal{P}_{q,q}$. Then, $\mathcal{R}_{q,q}$ is a Galois cover of $\mathcal{R}$ with Galois group $\mathbb{F}_q \times \mathbb{F}_q$. There is an 'antidiagonal' action of $\mathbb{F}_q$ on $\mathcal{P}_{q,q}$ and $\mathcal{R}_{q,q}$ where α acts by $(\alpha, -\alpha)$ and this action preserves fibers of the rational map $\mathcal{P}_{q,q}$ to $\mathbb{P}^1$. Let $\mathcal{P}_q := \mathcal{P}_{q,q}/\mathbb{F}_q$ and $\mathcal{R}_q := \mathcal{R}_{q,q}/\mathbb{F}_q$ be the quotients by this action. By construction, $\mathcal{P}_q$ is a $\mathbb{F}_q$-Galois cover of $\mathcal{P}$ and $\mathcal{R}_q$ is a $\mathbb{F}_q$-Galois cover of $\mathcal{R}$. We can also recognize $\mathcal{P}_q$ and $\mathcal{R}_q$ as pullbacks. We have $\mathcal{P}_q = \mathcal{P} \times_{\mathbb{P}^1_u} \mathbb{P}^1_t$ and $\mathcal{R}_q = \mathcal{R} \times_{\mathcal{P}} \mathcal{P}_q$. We summarize these maps in the following commutative diagram:

$$\begin{tikzcd}
\mathcal{R}_{q,q} \arrow[r, "/\mathbb{F}_q"] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & \mathcal{R}_q \arrow[r] \arrow[d] \arrow[dr, phantom, "\lrcorner", very near start] & \mathcal{R} \arrow[d] \\
\mathcal{P}_{q,q} = X_{a,q} \times Y_{b,q} \arrow[r, "/\mathbb{F}_q"] \arrow[d, dashed] & \mathcal{P}_q \arrow[r] \arrow[d, dashed] \arrow[dr, phantom, "\lrcorner", very near start] & \mathcal{P} = X_a \times Y_b \arrow[d, dashed, "\pi_0"] \\
\mathbb{P}^1_t \arrow[r, equal] & \mathbb{P}^1_t \arrow[r, "u=t^q-t"] & \mathbb{P}^1_u
\end{tikzcd}$$

We now relate the surfaces appearing in the commutative diagram above to the minimal proper regular SNC model $\mathcal{S}$ of $\mathcal{C}_{a,b}$, as defined in §2.

First, let $\pi : \mathcal{S}_0 \to \mathbb{P}^1_{\overline{\mathbb{F}_r}}$ be the minimal proper regular model of the curve with affine equation $x^a + y^b = u$ over $\overline{\mathbb{F}_r}(u)$. There is a rational map $\phi : \mathcal{P} \to \mathcal{S}_0$ defined on the affine patch by

$$\begin{array}{cccc} \phi : & \mathcal{P} & \dashrightarrow & \mathcal{S}_0, \\ & ((x, u_1), (y, u_2)) & \mapsto & (x, y, u_1 + u_2) \,. \end{array}$$

The rational map ϕ has a unique point of indeterminacy at (∞_a, ∞_b), and this indeterminacy can be resolved by the same series of blow-ups that resolves π_0, yielding a morphism $\phi : \mathcal{R} \to \mathcal{S}_0$. In fact, we have already remarked that $\mathcal{R}$ is the minimal proper regular model of the curve $x^a + y^b = u$, and $\phi : \mathcal{R} \to \mathcal{S}_0$ is an isomorphism.

Now, set $\mathcal{S}_q := \mathcal{S}_0 \times_{\mathbb{P}^1_u} \mathbb{P}^1_t$ where the second fiber maps $\mathbb{P}^1_t \to \mathbb{P}^1_u$ via the Artin–Schreier map $t \mapsto t^q - t$, so that $\mathcal{S}_q$ is a model of $x^a + y^b = t^q - t$. The rational map $\phi_{q,q} : \mathcal{P}_{q,q} \dashrightarrow \mathcal{S}_q, ((x, t_1), (y, t_2)) \mapsto (x, y, t_1 + t_2)$ is invariant under the antidiagonal $\mathbb{F}_q$-action. The induced rational map $\phi_q : \mathcal{P}_q \dashrightarrow \mathcal{S}_q$ from the quotient is the same as the pullback of $\phi : \mathcal{P} \dashrightarrow \mathcal{S}_0$. We now resolve the indeterminacy of these rational maps.

The isomorphism $\phi : \mathcal{R} \to \mathcal{S}_0$ pulls back to an isomorphism $\phi_q : \mathcal{R}_q \to \mathcal{S}_q$ which resolves the indeterminacy of $\phi_q : \mathcal{P}_q \dashrightarrow \mathcal{S}_q$. Moreover, the induced map $\mathcal{R}_{q,q} \to \mathcal{S}_q$ given by composing ϕ_q with the antidiagonal quotient resolves the indeterminacy of the rational map $\phi_{q,q} : \mathcal{P}_{q,q} \to \mathcal{S}_q$.

In Section 5.4, these morphisms will allow us to relate the action of Frobenius on the 'antidiagonal $\mathbb{F}_q$'-invariant subspace of $H^2(\mathcal{P}_{q,q})$ to the action of Frobenius on $H^2(\mathcal{S}_q)$ modulo its 'trivial lattice'.

We summarize in Figure 2 the maps considered here in a commutative diagram, where dashed arrows denote rational maps and solid arrows are everywhere defined. The maps from $\mathcal{R}_{q,q}, \mathcal{R}_q$, and $\mathcal{R}$ resolve the indeterminacy of the maps from $\mathcal{P}_{q,q}, \mathcal{P}_q$ and $\mathcal{P}$ with the same targets.

$$\begin{tikzcd}
 & & \mathcal{R} \arrow[dd] \arrow[ddrr] & & \\
 & \mathcal{R}_q \arrow[ur] \arrow[dd] \arrow[ddrr] & & & \\
\mathcal{R}_{q,q} \arrow[ur] \arrow[drrr] \arrow[dd] & & \mathcal{P} \arrow[rr, dashed] \arrow[dd, dashed] & & \mathcal{S}_0 \arrow[dd] \\
 & \mathcal{P}_q \arrow[ur] \arrow[rr, dashed] \arrow[dd, dashed] & & \mathcal{S}_q \arrow[ur] \arrow[dd] & \\
\mathcal{P}_{q,q} \arrow[ur] \arrow[urrr, dashed] \arrow[dd, dashed] & & \mathbb{P}^1_u \arrow[rr, equal] & & \mathbb{P}^1_u \\
 & \mathbb{P}^1_t \arrow[ur] \arrow[rr, equal] & & \mathbb{P}^1_t \arrow[ur] & \\
\mathbb{P}^1_t \arrow[ur, equal] & & & &
\end{tikzcd}$$

Figure 2: Summary of maps

Finally, we relate $\mathcal{S}_q$ to $\mathcal{S}$. In Section 5.5, this relationship will allow us to identify the action of Frobenius on $H^2(\mathcal{S})$ modulo its 'trivial lattice' to the action of Frobenius on $H^2(\mathcal{S}_q)$ modulo its 'trivial lattice'.

Upon restricting to the fibers over $\mathbb{P}^1 \setminus (\mathbb{F}_q \cup \{\infty\})$, the surfaces $\mathcal{S}$ and $\mathcal{S}_q$ become isomorphic as models of $\mathcal{C}_{a,b}$. However, since $\mathcal{S}_q$ is a ramified cover of $\mathcal{S}_0$, the surface $\mathcal{S}_q$ may not be a regular model for $\mathcal{C}_{a,b}$, and there need not be morphisms between $\mathcal{S}_q$ and $\mathcal{S}$ in either direction.

Now, $\mathcal{S}_q \to \mathcal{S}_0$ is étale away from the fiber above infinity, so the only singularities of $\mathcal{S}_q$ lie on the fiber above infinity. When blowing up these singularities to get a proper regular model, the exceptional fibers all map to $\infty \in \mathbb{P}^1_t$. After further blow-ups at the singularities on fibers, one gets a proper regular SNC model $\mathcal{S}'$ of $\mathcal{C}_{a,b}$ equipped with a blow-up map $\mathcal{C}_{a,b} \to \mathcal{S}_q$. The exceptional fibers of the blow-ups are components of the singular fibers (above $\mathbb{F}_q$ and ∞). By the minimality of $\mathcal{S}$ and since $\mathcal{S}, \mathcal{S}'$, and $\mathcal{S}_q$ are all isomorphic away from the singular fibers, the birational isomorphism $\mathcal{S}' \to \mathcal{S}$ defined away from the singular fibers extends to a morphism which is defined by iteratively contracting certain -1 curves which are contained in singular fibers of the composition $\mathcal{S}' \to \mathcal{S}_q \to \mathbb{P}^1_t$.

5.3 Cohomology of $\mathcal{S}$ in degree 1

Our next goal is to show that the H^1 of the minimal proper regular SNC model $\mathcal{S}$ of C is trivial by comparing it with the cohomology of the product of Artin–Schreier curves $\mathcal{P}_{q,q}$ constructed in Section 5.2.

First, we relate the cohomology of $\mathcal{R}_q$ to the cohomology of the curves $X_{a,q}$ and $Y_{b,q}$. Since we construct $\mathcal{R}_q$ from $\mathcal{P}_q$ by repeatedly blowing up at a point and the exceptional divisor (as a union of $\mathbb{P}^1$s) has trivial H^1, the blow-up formula (see [Mil80]) gives

$$H^1(\mathcal{R}_q) \cong H^1(\mathcal{P}_q)\,. \tag{5.3}$$

Since $\mathcal{P}_q = (X_{a,q} \times Y_{b,q})/\mathbb{F}_q$, we have

$$H^1(\mathcal{P}_q) \cong H^1(X_{a,q} \times Y_{b,q})^{\mathbb{F}_q}\,. \tag{5.4}$$

The Kunneth formula gives

$$H^1(X_{a,q} \times Y_{b,q}) \cong (H^1(X_{a,q}) \otimes H^0(Y_{b,q}) \oplus H^0(X_{a,q}) \otimes H^1(Y_{b,q}))^{\mathbb{F}_q}\,. \tag{5.5}$$

Now, $\mathbb{F}_q$ acts trivially on $H^0(X_{a,q})$ and $H^0(Y_{b,q})$, and we saw in Section 5.1 that the subspaces of $H^1(X_{a,q})$ and $H^1(Y_{b,q})$ fixed by $\mathbb{F}_q$ are both trivial. So, combining (5.3), (5.4), and (5.5), we find $H^1(\mathcal{R}_q) = \{0\}$. Since $\mathcal{R}_q \to \mathcal{S}_q$ is a dominant morphism, the induced map $H^1(\mathcal{R}_q) \to H^1(\mathcal{S}_q)$ is surjective, whence $H^1(\mathcal{S}_q)$ is trivial. Using the blow-up formula as in the justification of (5.3) gives $H^1(\mathcal{S}_q) \cong H^1(\mathcal{S})$. We conclude that $H^1(\mathcal{S}) = \{0\}$.

5.4 Cohomological interpretation of the L-function

Our goal in this subsection is to relate $L(J,T)$ to the characteristic polynomial of Frobenius acting on a certain quotient of $H^2(\mathcal{S})$.

As before, let $K = \mathbb{F}_r(t)$. We choose an algebraic closure $\overline{K}$ of K and a separable closure K^{sep} within $\overline{K}$. Denote by G the absolute Galois group of K. Fix a pair (a,b) of positive coprime integers which are both coprime to p as well as a power q of p. Write $C = C_{a,b,q}$ and $J = J_{a,b,q}$.

For any place v of K, we let Fr_v denote the *geometric* Frobenius at v. (The geometric Frobenius Fr_v is a well-defined up to conjugacy in G.) Recall from §4.1 that the L-function of J is defined by

$$L(J,T) := \prod_v \det\left(1 - \mathrm{Fr}_v\, T \,\middle|\, H^1(\mathcal{J}_v)^{I_v}\right)^{-1}. \tag{5.6}$$

If v is a place of bad reduction of J, we know from Proposition 2.3 that J has unipotent reduction at v. Hence, by [ST68, pg. 504, Remark 2], the action of inertia group at v on $H^1(\mathcal{J}_v)$ only fixes the trivial subspace, so that $H^1(\mathcal{J}_v)^{I_v} = \{0\}$. On the other hand, if v is a place of good reduction of J, we have $H^1(\mathcal{J}_v)^{I_v} = H^1(\mathcal{J}_v)$ since I_v acts trivially. Furthermore, at such a place v, the space

$H^1(\mathcal{J}_v)$ is canonically isomorphic to $H^1(\mathcal{S}_v)$ by (for instance) [Poo06, 5.3.5], compatibly with the action of Fr_v. The Euler product in (5.6) thus simplifies to

$$L(J,T) = \prod_{v \text{ good}} \det\left(1 - \mathrm{Fr}_v\, T \,\middle|\, H^1(\mathcal{S}_v)\right)^{-1}, \tag{5.7}$$

where the product is restricted to places of good reduction of J. In order to shorten notation, we set $P_v(T) := \det\left(1 - \mathrm{Fr}_v\, T \,\middle|\, H^1(\mathcal{S}_v)\right)$ for any place v of K.

For a variety X over $\mathbb{F}_r$, recall (e.g. from [Poo06, Def. 3.4.1]) that its zeta function is defined by

$$Z(X,T) = \prod_{P \in |X|} \left(1 - T^{\deg P}\right)^{-1},$$

where the product runs over the set of closed points of X. If X is smooth and projective, by Grothendieck–Lefschetz trace formula (see [Del77, Corollary 3.7]), we have

$$Z(X,T) = \prod_{i=0}^{2\dim X} (-1)^{i+1} \det\left(1 - \mathrm{Fr}_r\, T \,\middle|\, H^i(X)\right).$$

In particular, we have $Z(\mathbb{P}^1_{\mathbb{F}_r}, T) = \left((1-T)(1-rT)\right)^{-1}$.

We showed in Section 5.3 that $H^1(\mathcal{S}) = \{0\}$. It follows from Poincaré duality (see [Har77, Appendix C.3]) that $H^3(\mathcal{S}) = \{0\}$ as well. These remarks show that

$$Z(\mathcal{S},T) = \frac{1}{(1-T)\,\det\left(1 - \mathrm{Fr}_r\, T \,|\, H^2(\mathcal{S})\right)\,(1-r^2T)}. \tag{5.8}$$

Similarly, for any place v of good reduction, we have

$$Z(\mathcal{S}_v,T) = \frac{P_v(T)}{(1-T^{\deg v})(1-(rT)^{\deg v})}.$$

Since $\mathcal{S}$ is a disjoint union of the fibers of the map $\mathcal{S} \to \mathbb{P}^1$, we can also express $Z(\mathcal{S},T)$ in terms of the zeta functions of the fibers:

$$Z(\mathcal{S},T) = \prod_{v} Z(\mathcal{S}_v,T) = \prod_{v \text{ good}} Z(\mathcal{S}_v,T) \prod_{v \text{ bad}} Z(\mathcal{S}_v,T).$$

Combining the last two displayed formulas and (5.7), we find that

$$\begin{aligned}\prod_{v \text{ good}} Z(\mathcal{S}_v,T) &= \prod_{v \text{ good}} \frac{P_v(T)}{(1-T^{\deg v})(1-(rT)^{\deg v})} = \prod_{v \text{ good}} \frac{1}{P_v(T)^{-1}} \frac{1}{(1-T^{\deg v})(1-(rT)^{\deg v})} \\ &= \left(\prod_{v \text{ good}} \frac{1}{P_v(T)^{-1}}\right)\left(\prod_{v} \frac{1}{(1-T^{\deg v})(1-(rT)^{\deg v})}\right)\left(\prod_{v \text{ bad}} (1-T^{\deg v})(1-(rT)^{\deg v})\right) \\ &= \frac{Z(\mathbb{P}^1_{\mathbb{F}_r},T)Z(\mathbb{P}^1_{\mathbb{F}_r},rT)}{L(J,T)}\left(\prod_{v \text{ bad}} (1-T^{\deg v})(1-(rT)^{\deg v})\right)\end{aligned}$$

This gives us another expression for $Z(\mathcal{S},T)$:

$$Z(\mathcal{S},T) = \frac{1}{(1-T)(1-rT)^2(1-r^2T)L(J,T)} \prod_{v \text{ bad}} Z(\mathcal{S}_v,T)(1-T^{\deg v})(1-(rT)^{\deg v}). \tag{5.9}$$

In fact, we can simplify this further since we know (from Section 2.1) that the fiber $\mathcal{S}_v$ at a place v of bad reduction is a tree of $\mathbb{P}^1$s. For any such place v, let m_v be the number of irreducible components of $\mathcal{S}_v$. Then, a straightforward computation shows that

$$Z(\mathcal{S}_v, T) = \frac{Z(\mathbb{P}^1_{\mathbb{F}_v}, T)^{m_v}}{Z(\operatorname{Spec}\mathbb{F}_v, T)^{m_v - 1}} = \frac{1}{(1 - T^{\deg v})(1 - (rT)^{\deg v})^{m_v}} .$$

Plugging this into (5.9) yields that

$$Z(\mathcal{S}, T) = \frac{1}{(1-T)(1-rT)^2(1-r^2T)L(J,T)} \prod_{v \text{ bad}} (1 - (rT)^{\deg v})^{1-m_v} . \tag{5.10}$$

Comparing formulas (5.8) and (5.10) for $Z(\mathcal{S}, T)$ and rearranging terms, we find

$$\begin{aligned} L(J,T) &= \frac{P_2(T)}{(1-rT)^2} \prod_{v \text{ bad}} Z(\mathcal{S}_v, T)(1 - T^{\deg v})(1 - (rT)^{\deg v}) \\ &= \frac{P_2(T)}{(1-rT)^2} \prod_{v \text{ bad}} (1 - (rT)^{\deg v})^{1-m_v} . \end{aligned} \tag{5.11}$$

Let $s_\infty : \mathbb{P}^1 \to \mathcal{S}$ be the 'infinity section' s_∞ which maps each point $t \in \mathbb{P}^1$ to the unique 'point at infinity' on the fiber $\mathcal{S}_t$. Let $\Lambda \subset H^2(\mathcal{S})$ be the trivial lattice, that is the subspace spanned by the images under the cycle class map of (the image of) s_∞ and all components of fibers of $\mathcal{S} \to \mathbb{P}^1$.

Let D be an irreducible (over $\mathbb{F}_r$) component of a fiber of $\mathcal{S} \to \mathbb{P}^1$. After base change to $\overline{\mathbb{F}_r}$, we can decompose D as $D_{\overline{\mathbb{F}_r}} = \bigcup_{j \in \mathbb{Z}/n\mathbb{Z}} D_j$ with indices chosen so that $\operatorname{Fr}_r D_j = D_{j+1}$. Let W_j be the subspace of $H^2(\mathcal{S})$ spanned by the image of 1_{D_j} under $i_* : H^0(D_j)(-1) \to H^2(\mathcal{S})$. We have $\operatorname{Fr}_r W_j \subset W_{j+1}$, and Fr_{r^n} acts on each W_j by multiplication by r^n. Since W_j is one-dimensional, we find $\det(1 - \operatorname{Fr}_r^n T^n | W_0) = 1 - r^n T^n$. Hence, by Lemma 5.1, the characteristic polynomial of Fr_r acting on the subspace of $H^2(\mathcal{S})$ spanned by the classes of the components of $D_{\overline{\mathbb{F}_r}}$ is $(1 - (rT)^n)$.

Now, the trivial lattice Λ has a basis consisting of the image of s_∞ (which is defined over $\mathbb{F}_r$), the fiber over any $\mathbb{F}_r$-rational point of $\mathbb{P}^1$ (which is again defined over $\mathbb{F}_r$) and the components of the singular fibers which do not meet s_∞. We conclude that

$$\det(1 - \operatorname{Fr}_r T \,|\Lambda) = (1 - rT)^2 \prod_{v \text{ bad}} (1 - (rT)^{\deg v})^{m_v - 1} .$$

Combining (5.11) with the above finally yields the following:

Proposition 5.2. *We have*

$$L(J,T) = \det\left(1 - \operatorname{Fr}_r T \,\middle|H^2(\mathcal{S})/\Lambda\right) .$$

With our computation of the degree of the conductor of J/K (see Proposition 2.6), the Néron–Ogg–Shafarevich formula (see Appendix A) yields that $\deg L(J,T) = (a-1)(b-1)(q-1)$. It follows from the above that

$$\dim H^2(\mathcal{S})/\Lambda = (a-1)(b-1)(q-1). \tag{5.12}$$

5.5 Cohomology of $\mathcal{S}$ in degree 2

Our next goal is to relate the H^2 of the minimal proper regular SNC model $\mathcal{S}$ of C to the cohomology of the product of Artin–Schreier curves $\mathcal{P}_{q,q}$ constructed in Section 5.2. Our strategy will mirror that of Section 5.3. The main differences are that the blow-up divisor has nontrivial H^2, which we will need to track more carefully, and that we will need to use (5.12) to show that the surjection we construct is actually an isomorphism.

First, we relate the cohomology of $\mathcal{R}_q$ to the cohomology of the curves $X_{a,q}$ and $Y_{b,q}$. Let B be the subspace of $H^2(\mathcal{R}_q)$ spanned by the pullbacks of the blow-up divisor from $\mathcal{R} \to \mathcal{P}$ (see Section 5.2). Successively applying the blow-up formula, taking invariants, and applying the Künneth formula, we find

$$\begin{aligned}H^2(\mathcal{R}_q) &\cong H^2(\mathcal{P}_q) \oplus B \cong H^2((X_{a,q} \times Y_{b,q})/\mathbb{F}_q) \oplus B \cong H^2(X_{a,q} \times Y_{b,q})^{\mathbb{F}_q} \oplus B \\ &\cong (H^1(X_{a,q}) \otimes H^1(Y_{b,q}))^{\mathbb{F}_q} \oplus (H^0(X_{a,q}) \otimes H^2(Y_{b,q}))^{\mathbb{F}_q} \oplus (H^2(X_{a,q}) \otimes H^0(Y_{b,q}))^{\mathbb{F}_q} \oplus B.\end{aligned}$$

Now let Λ_q be the subspace of $H^2(\mathcal{S}_q)$ which is spanned by components of fibers of $\mathcal{S}_q \to \mathbb{P}^1$ together with the class of the 'infinity section' $s_{\infty,q} : \mathbb{P}^1 \to \mathcal{S}_q$ which takes $t \in \mathbb{A}^1 \subset \mathbb{P}^1$ to the unique 'point at infinity' on that fiber. Recall that $\mathcal{S}$ is the minimal proper regular SNC model of C and that we have defined $\Lambda \subset H^2(\mathcal{S})$ to be the trivial lattice. Since $\mathcal{S}$ and $\mathcal{S}_q$ are related by a series of blow-ups and blow-downs where the exceptional fibers lie in the fibers over $\mathbb{P}^1$, we automatically have $H^2(\mathcal{S}_q)/\Lambda_q \cong H^2(\mathcal{S})/\Lambda$.

The blow-up divisor in $\mathcal{R}_q$ maps to the union of (the image of) the infinity section $s_{\infty,0}$ and the fiber at infinity of $\mathcal{S}_0$. Similarly, the blow-up divisor in $\mathcal{R}_q$ maps to the union of the infinity section $s_{\infty,q}$ and the fiber at infinity of $\mathcal{S}_q$. Moreover, the classes in $H^0(X_{a,q}) \otimes H^2(Y_{b,q})$ and $H^2(X_{a,q}) \otimes H^0(Y_{b,q})$ are generated by the strict transforms of the images of $X_{a,q} \times \infty_b$ and $\infty_a \times Y_{b,q}$, which also map to the fiber above $\infty \in \mathbb{P}^1$ in $\mathcal{S}_q$.

All told, we find that the image of $(H^0(X_{a,q}) \otimes H^2(Y_{b,q})) \oplus (H^2(X_{a,q}) \otimes H^0(Y_{b,q})) \oplus B$ under the induced map $H^2(\mathcal{R}_q) \to H^2(\mathcal{S}_q)$ is contained in Λ_q. Since $\mathcal{R}_q \to \mathcal{S}_q$ is a dominant morphism, the induced map $H^2(\mathcal{R}_q) \to H^2(\mathcal{S}_q)$ is surjective and induces a Galois-equivariant canonical surjection

$$\varpi : (H^1(X_{a,q}) \otimes H^1(Y_{b,q}))^{\mathbb{F}_q} \to H^2(\mathcal{S}_q)/\Lambda_q \cong H^2(\mathcal{S})/\Lambda\,.$$

From the description of $(H^1(X_{a,q}) \otimes H^1(Y_{b,q}))^{\mathbb{F}_q}$ obtained in Section 5.6 below (see (5.14)), we see that that space has dimension $(a-1)(b-1)(q-1)$. Formula (5.12) in the previous subsection yields that $H^2(\mathcal{S})/\Lambda$ has the same dimension. We deduce that ϖ is a Galois-equivariant isomorphism. Therefore,

$$\det\left(1 - \mathrm{Fr}_r\, T \,\middle|\, H^2(\mathcal{S})/\Lambda\right) = \det\left(1 - \mathrm{Fr}_r\, T \,\middle|\, (H^1(X_{a,q}) \otimes H^1(Y_{b,q}))^{\mathbb{F}_q}\right)\,. \tag{5.13}$$

5.6 Computation of the L-function

Combining Proposition 5.2 with (5.13), we find that

$$L(J,T) = \det\left(1 - \mathrm{Fr}_r\, T \,\middle|\, (H^1(X_{a,q}) \otimes H^1(Y_{b,q}))^{\mathbb{F}_q}\right).$$

Finally, we use the facts about the cohomology of Artin–Schreier curves from Section 5.1 to give a more explicit expression for $L(J,T)$. Recall from Section 5.1 that we have

$$H^1(X_{a,q}) = \bigoplus_{(i,\alpha)\in S'_a} H^1(X_{a,q})^{(i,\alpha)} \quad \text{and} \quad H^1(Y_{b,q}) = \bigoplus_{(i,\alpha)\in S'_b} H^1(Y_{b,q})^{(i,\alpha)}\,.$$

In each of these direct sums indexed by elements of $S'_a = (\mathbb{Z}/a\mathbb{Z} \smallsetminus \{0\}) \times \mathbb{F}_q$ or S'_b respectively, each summand $H^1(X_{a,q})^{(i,\alpha)}$ and $H^1(Y_{b,q})^{(i,\alpha)}$ is one-dimensional. This means that

$$H^1(X_{a,q}) \otimes H^1(Y_{b,q}) = \bigoplus_{(i_1,\alpha_1)\in S'_a} \bigoplus_{(i_2,\alpha_2)\in S'_b} H^1(X_{a,q})^{(i_1,\alpha_1)} \otimes H^1(Y_{b,q})^{(i_2,\alpha_2)}$$

decomposes as a direct sum of lines. Tracing through the definitions, one sees that, among the lines $H^1(X_{a,q})^{(i_1,\alpha_1)} \otimes H^1(Y_{b,q})^{(i_2,\alpha_2)}$, the $\mathbb{F}_q$-invariant lines are those indexed by pairs $(i_1,\alpha_1),(i_2,\alpha_2)$ with $\alpha_1=\alpha_2$. So,

$$(H^1(X_{a,q}) \otimes H^1(Y_{b,q}))^{\mathbb{F}_q} = \bigoplus_{(i_1,i_2,\alpha)\in S} H^1(X_{a,q})^{(i_1,\alpha)} \otimes H^1(Y_{b,q})^{(i_2,\alpha)}\,. \tag{5.14}$$

We now compute the characteristic polynomial of Frobenius on this space in the same way that we computed the characteristic polynomial of Frobenius acting on $H^1(X_{d,q})$ in Section 5.1. For any orbit $o \in O = O_{r,a,b,q}$ (as defined in Section 3.3) the $|o|^{\text{th}}$ iterate of Fr_r stabilizes the line $H^1(X_{a,q})^{(i_1,\alpha)} \otimes H^1(Y_{b,q})^{(i_2,\alpha)}$ for any representative $(i_1,i_2,\alpha) \in o'$. For any $(i_1,i_2,\alpha)\in o$, we deduce from the computation following (5.1) in Section 5.1 that the eigenvalue of $(\mathrm{Fr}_r)^{|o|}$ acting on the line $H^1(X_{a,q})^{(i_1,\alpha)} \otimes H^1(Y_{b,q})^{(i_2,\alpha)}$ is $\boldsymbol{\omega}(o) = \mathbf{G}\left(\pi_a(o)\right)^{\nu_a(o)}\mathbf{G}\left(\pi_b(o)\right)^{\nu_b(o)}$. In other words, for any $(i_1,i_2,\alpha)\in o$, we have

$$\det\left(1-(\mathrm{Fr}_r)^{|o|}\,T\,\middle|\,H^1(X_{a,q})^{(i_1,\alpha)} \otimes H^1(Y_{b,q})^{(i_2,\alpha)}\right) = 1-\boldsymbol{\omega}(o)T.$$

Since Fr_r cyclically permutes the lines $H^1(X_{a,q})^{(i_1,\alpha)} \otimes H^1(Y_{b,q})^{(i_2,\alpha)}$ for $(i_1,i_2,\alpha)\in o$, Lemma 5.1 yields

$$\det\left(1-\mathrm{Fr}_r\,T\,\middle|\,\bigoplus_{(i_1,i_2,\alpha)\in o} H^1(X_{a,q})^{(i_1,\alpha)} \otimes H^1(Y_{b,q})^{(i_2,\alpha)}\right) = 1-\boldsymbol{\omega}(o)T^{|o|}\,.$$

Taking the product over all orbits $o\in O$, we finally obtain

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

This confirms our result in Theorem 4.2.

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

By the BSD conjecture (Theorem 1.1), we have

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

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. *In the previously introduced notation, 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*

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

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

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 $n \geq 2$ 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 $n \geq 1$, we denote by $o_p(n)$ the multiplicative order of p modulo n *i.e.*, $o_p(n)$ is the least integer $e \geq 1$ 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 $\nu \geq 1$ such that $p^\nu \equiv -1 \pmod{n}$.

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

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

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 $2i \neq n$, 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*

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

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

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

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

For the second claim, we note that if $[\mathbb{F}_r : \mathbb{F}_p]$ is a multiple of 4, then so is $[\mathbb{F}' : \mathbb{F}_p]$. 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

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

Then, the Hasse–Davenport relation (3.3) for Gauss sums implies that

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

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

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

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* $p^{\nu_i} \equiv -1 \bmod n/\gcd(n, i)$*. Then,*

$$\mathbf{G}\left(o'\right) = (-1)^{\left(1+\frac{i(p^{\nu_i}+1)}{n}\right)\frac{|o'|\,[\mathbb{F}_r:\mathbb{F}_p]}{2\nu_i}} \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1} r^{|o'|/2} . \tag{6.5}$$

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

$$\mathbf{G}\left(o'\right) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1} r^{|o'|/2} . \tag{6.6}$$

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

$$\mathbf{G}\left(o'\right) = r^{|o'|/2} . \tag{6.7}$$

We remark that by construction, the exponent of -1 in (6.5) is an integer.

Proof. Let $\mathbb{F}'$ denote the extension of $\mathbb{F}_r$ of degree $|o'|$. As in the previous proof, combining Definition 3.5 with equation (3.2) in §3.2 yields

$$\mathbf{G}\left(o'\right) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}\,\mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(i,\alpha)}, \psi_{\mathbb{F}',1}\big)\,. \tag{6.8}$$

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 $\mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(i,\alpha)}, \psi_{\mathbb{F}',1}\big)$.

Since n' divides n and n is supersingular for p, 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) for Gauss sums (see §3.2), we have

$$\mathrm{G}_{\mathbb{F}'}\big(\boldsymbol{\lambda}_{(i,\alpha)}, \psi_{\mathbb{F}',1}\big) = \mathrm{G}_{\mathbb{F}'}\Big(\boldsymbol{\chi}|_{\mathbb{F}}{}^{i(|\mathbb{F}|-1)/n} \circ \mathrm{N}_{\mathbb{F}'/\mathbb{F}}, \psi_{\mathbb{F},1} \circ \mathrm{Tr}_{\mathbb{F}'/\mathbb{F}}\Big) = \mathrm{G}_{\mathbb{F}}\Big(\boldsymbol{\chi}^{i(|\mathbb{F}|-1)/n}, \psi_{\mathbb{F},1}\Big)^{[\mathbb{F}':\mathbb{F}]}. \tag{6.9}$$

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

$$\mathrm{G}_{\mathbb{F}}(\chi, \psi_{\mathbb{F},1}) = (-1)^{1+i(p^{\nu_i}+1)/n}|\mathbb{F}|^{1/2}. \tag{6.10}$$

We now put (6.8), (6.9), and (6.10) 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 (6.5).

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 $\mathbf{G}\,(o') = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1}|\mathbb{F}'|^{1/2}$. Finally, 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 nonnegative rational number.

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

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

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

Our goal in this section is to control $\text{Д}(o')$ 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 $o' \in O'_n$, $\mathrm{H}(o')/\text{Д}(o') = 1/2$.*

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

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,*

$$\frac{\nu_{\mathfrak{p}}(\mathbf{G}(o'))}{|o'|} = \frac{1}{\mu} \sum_{k=0}^{\mu-1} \left\{ \frac{-ip^k}{n} \right\}, \tag{6.11}$$

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*

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

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,

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

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

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

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

□

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

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

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

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 (6.11) from Lemma 6.9. □

We now prove a more precise estimate on the denominator of $\nu_{\mathfrak{p}}(\mathbf{G}\,(o'))/|o'|$. 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,*

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

In particular, $\text{Д}(o')$ 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

$$\frac{\mathrm{H}(o')}{\text{Д}(o')} = \frac{\nu_{\mathfrak{p}}(\mathbf{G}\,(o'))}{|o'|} = \frac{1}{\mu}\sum_{k=0}^{\mu-1}\left\{\frac{-ip^k}{n}\right\}. \tag{6.12}$$

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 (6.12), 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 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 all equal as y varies. More precisely, we have

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

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

$$\frac{\mathrm{H}(o')}{\text{Д}(o')} = \frac{1}{\mu}\sum_{y=0}^{\kappa-1}\frac{\mu}{\kappa}\left\{\frac{-ip^y}{n}\right\} = \frac{1}{\kappa}\sum_{y=0}^{\kappa-1}\left\{\frac{-ip^y}{n}\right\}. \tag{6.13}$$

Each term $\{-ip^y/n\}$ in the right-most sum in (6.13) is a rational number with denominator $n/\gcd(n, ip^y) = n/\gcd(n,i)$. So, the right-most sum in (6.13) is a rational number with denominator dividing $n/\gcd(n,i)$. After division by $\kappa = o_p(n/\gcd(n,i))$, we conclude that $\text{Д}(o')$ 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 $\boldsymbol{\omega}(o)$

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 §3.3. For any orbit $o \in O$, in the notation introduced in §6.2, we thus have

$$\frac{\nu_{\mathfrak{p}}(\boldsymbol{\omega}(o))}{|o|} = \frac{\mathrm{H}(\pi_a(o))}{\text{Д}(\pi_a(o))} + \frac{\mathrm{H}(\pi_b(o))}{\text{Д}(\pi_b(o))}. \tag{6.14}$$

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; or

(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 $\gcd(\text{Д}(\pi_a(o)), \text{Д}(\pi_b(o)) = 1$ by Proposition 6.12. Hence, $\text{Д}(\pi_a(o)) \neq \text{Д}(\pi_b(o))$ unless both $\text{Д}(\pi_a(o)) = 1$ and $\text{Д}(\pi_b(o)) = 1$. This situation does not occur, by Corollary 6.11.

If a is supersingular for p, then $\text{Д}(\pi_a(o)) = 2$ by Lemma 6.8. By Proposition 6.12, $\text{Д}(\pi_b(o))$ divides $bo_r(b)$. Hence, if $bo_r(b)$ is odd, so is $\text{Д}(\pi_b(o))$. In particular, if *(3)* is satisfied, then $\text{Д}(\pi_a(o)) \neq \text{Д}(\pi_b(o))$.

The case where *(2)* holds is treated in a similar way, by switching the roles of a and b.

In all three situations, we have shown that $\text{Д}(\pi_a(o)) \neq \text{Д}(\pi_b(o))$. Since two reduced fractions with different denominators cannot sum to 1, the result now immediately follows from (6.14). □

Let us now show 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 coprime integers a and b which are both relatively prime to p.

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

Proof. We first focus on 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 set $a = (p^k - 1)/(p - 1)$. 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; or

(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.

Remark 6.16. One can provide a second proof of the BSD conjecture (Theorem 1.1) in the case that $L(J, r^{-1}) \neq 0$, as follows. By a theorem of Tate [Tat65], one has

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

(This essentially follows from injectivity of the cycle class map.) If the parameters a, b, q are such that $L(J, T)$ does not vanish at $T = r^{-1}$, we deduce from the above that $\operatorname{rank} J(K) = \operatorname{ord}_{T=r^{-1}} L(J, T) = 0$. In other words, the "weak BSD conjecture" holds for J.

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 6.17. *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

$$\boldsymbol{\omega}(o) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1} \boldsymbol{\lambda}_{(j,\alpha)}(\alpha)^{-1} r^{|o|}. \tag{6.15}$$

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 $(i, j, \alpha) \in S$. We then have $|o| = |\pi_a(o)| = |\pi_b(o)|$. In particular,

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

We may now apply Lemma 6.5 (resp. Lemma 6.7) to compute $\mathbf{G}(\pi_a(o))$ 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 $\mathbf{G}(\pi_a(o))$ are divisors of ν_a, we have $4\nu_i | [\mathbb{F}_r : \mathbb{F}_p]$. So, equations (6.3) and (6.6) hold. We find that $\mathbf{G}(\pi_a(o)) = \boldsymbol{\lambda}_{(i,\alpha)}(\alpha)^{-1} r^{|o'|/2}$. Computing $\mathbf{G}(\pi_b(o))$ in the same way yields that

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

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 $\mathbb{F}_r$ with degrees $|\pi_a(o)|$ and $|\pi_b(o)|$ coincide: they are both equal to $\mathbb{F}_r(\alpha)$. This extension $\mathbb{F}_r(\alpha)$ is the one over which both $\boldsymbol{\lambda}_{(i,\alpha)}$ and $\boldsymbol{\lambda}_{(j,\alpha)}$ are defined. To conclude, we 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 Lemmas 6.1 and 6.17 yields 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 $(ab)^{\text{th}}$ 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 $\mathbb{F}_p(\alpha)$. Each orbit of $\langle r \rangle$ on $\mathbb{F}_q^\times$ contains at most $[\mathbb{F}_q : \mathbb{F}_p] = \log_p(q)$ elements and so contains at most $\log_p(q)$ 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 6.18. *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, Lemmas 6.1 and 6.17 together imply the desired equality. □

Remark 6.19. [Hypotheses of Theorems 1.3 and 6.18] For any fixed p, there are infinitely many choices of a, b, r satisfying the hypotheses of Theorem 1.3 and Theorem 6.18, as we now explain.

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 6.18 are satisfied whenever $\mathbb{F}_r \supset \mathbb{F}'$.

In fact, if a and b are prime, a and b are supersingular for p 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 6.18.

Remark 6.20. 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

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

As discussed in Section 4.5, 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.

Throughout this section, we will use Vinogradov's asymptotic notation. Namely, for two functions f, g of a variable x on $[0, \infty)$, we use $f(x) \ll_a g(x)$ 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 $x \to \infty$.

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 $\zeta \cdot (zp^{-\theta})^L = 1$ or, in any complex embedding $|\cdot|$ of $\overline{\mathbb{Q}}$ in $\mathbb{C}$, we have*

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

where $c_0, c_1 > 0$ are effective constants depending at most on p, θ, the degree of z over $\mathbb{Q}$, and the (multipicative) 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 for 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, p and r 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 $(ab)^{\text{th}}$ root of unity, g_o is a Weil integer of size $p^{\theta_{a,b}}$, 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

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

Applying Theorem 7.1 and the definition of L_0 yields that

$$\log\left|1 - \zeta_o \cdot \left(g_o p^{-\theta_{a,b}}\right)^{L_o}\right| \geq -c_0 - c_1 \log|L_o| \geq (-c_0 - c_1 \log[\mathbb{F}_r : \mathbb{F}_p]) - c_1 \log|o|,$$

for 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 may in turn be bounded solely in terms of a, b, and p. Indeed, 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 $\theta_{a,b}$ is at most $o_p(a)o_p(b) \leq \phi(a)\phi(b) \leq ab$. □

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

$$0 \le \frac{1}{q}\sum_{o\in O_0}\log|o| \le \frac{1}{q}\sum_{o\in O_*}\log|o| \ll \frac{q}{q}\frac{\log\log q}{\log q} \ll \frac{\log\log q}{\log q}. \tag{7.3}$$

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

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

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

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

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, p, and r. 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, and r, 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 fixed a, b, and r. 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, and r 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, so that $\operatorname{Reg}(J) = 1$. 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*

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

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 ensures that the Jacobian $J_{a,b,q}$ is K-simple for any power q of p. By Theorem 1.5, the sequence $(J_{a,b,q})_q$ satisfies $|\text{Ш}(J_{a,b,q})| = H(J_{a,b,q})^{1+o(1)}$ 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.

[Del77] P. Deligne. *Cohomologie étale*, volume 569 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 1977. Séminaire de géométrie algébrique du Bois-Marie SGA $4\frac{1}{2}$.

[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.

[Fly19] E. V. Flynn. Arbitrarily large 2-torsion in Tate-Shafarevich groups of abelian varieties. *Acta Arith.*, 191(2):101–114, 2019.

[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`.

[Har77] R. Hartshorne. *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[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.

[Kat81] N. Katz. Crystalline cohomology, Dieudonné modules, and Jacobi sums. In *Automorphic forms, representation theory and arithmetic*, pages 165–246. Springer, 1981.

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

[Mil80] J.S. Milne. *Étale cohomology.* Princeton Mathematical Series, No. 33. Princeton University Press, Princeton, N.J., 1980.

[Mum08] D. Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[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.

[Shi92] T. Shioda. Some remarks on elliptic curves over function fields. *Astérisque*, 209(12):99–114, 1992.

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

[Sta21] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2021.

[Tat65] J. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. *Séminaire Bourbaki*, 9(306):415–440, 1965.

[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.

[Ulm07] D. Ulmer. L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields. *Invent. Math.*, 167:379–408, 2007.

[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*) – Laboratoire de Mathématiques B. Pascal, 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*) – Department of Mathematics, University of Georgia, Athens, GA 30602 (USA).

A Conductor Computations

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

Proposition A.1. *We prove the statement from Theorem 4.1 regarding the global 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 global 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 global 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, namely $r = \sum_{\text{bad } v} \deg v$. Therefore $\chi(U, \overline{\mathbb{Q}_\ell}) = 2 - r$.

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

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

[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

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

□