On the arithmetic of twists of superelliptic curves

Sungkon Chang

ABSTRACT

In this paper, we consider a family of twists of a superelliptic curve over a global field, and obtain results on the distribution of the Mordell-Weil rank of these twists. Our results have applications to the distribution of the number of rational points.

1. Introduction

By Faltings' theorem, a (smooth complete geometrically irreducible) curve over a number field has finitely many rational points. By [CJB97], it is widely believed that the number of rational points of a curve of genus > 1 over a number field K is bounded in terms of the genus of the curve. In [Maz86], prior to [CJB97], Mazur asked whether the number of rational points can be bounded in terms of the genus and the Mordell-Weil rank of its Jacobian variety. For the case of twists of curves, in [Sil93], Silverman proves that Mazur's question has a positive answer. However, for general cases, this question is totally open.

By Silverman's result, given a curve of genus > 1 over a number field, finding infinitely many twists with a bounded number of rational points becomes a problem of finding infinitely many twists with bounded Mordell-Weil rank. Even for special cases such as Thue equations (see [LT02]), an answer to this problem is sometimes not known. For the case of elliptic curves, by Kolyvagin's result [Kol88] and the modularity of elliptic curves proved by Wiles et al, results such as [OC98], in which quadratic twists with analytic rank 0 are computed, imply that given an elliptic curve over $\mathbb{Q}$, there are infinitely many quadratic twists with Mordell-Weil rank 0, i.e., algebraic rank 0. There are also results of this type such as Heath-Brown's [HB94], [Won99] and [Yu03] which rather directly show that there is a "positive proportion" of algebraic rank-0 quadratic twists of certain elliptic curves.

In this paper, we consider a family of twists of superelliptic curves over a global field, and prove that for these twists, the problem of finding infinitely many twists with bounded Mordell-Weil rank has a positive answer and, hence, there are infinitely many twists with bounded number of rational points if the genus > 1. Some Thue equations can be mapped down to superelliptic curves considered in this paper and, hence, for these Thue equations, this problem has a positive answer. For the case of superelliptic curves over a constant field and the case of hyperelliptic curves over $\mathbb{Q}$, finer results are obtained. Especially, using superelliptic curves over a constant field, we show that there are (infinitely many twists of) curves of arbitrarily large genus over a function field with Mordell-Weil rank 0. Over a number field, examples of such curves are not known. In this section, we also introduce the application of our result to cubic twists of some elliptic curves.

Let $n \geqslant 2$ be a positive integer, and let R be an integral domain of characteristic not dividing n, with field of fractions K. Let $f(x)$ be a monic polynomial in $R[x]$ such that n is coprime to $\deg(f)$, and $f(x)$ has distinct roots. In this paper, *a superelliptic curve* is the projective K-model of the affine plane curve $y^n = f(x)$.

1.1. Let K be a field, and let ℓ be a prime number different from $\operatorname{char} K$. Let C/K be the normalization of a superelliptic curve given by $y^\ell = f(x)$. For $D \in K^*$, we denote by C_D/K the normalization of the curve given by $y^\ell = D^d f(x/D)$ where $d := \deg(f)$, and by J_D/K, the Jacobian variety of C_D. The Jacobian variety J_D is called *an ℓ-th power twist of J*. For the case of hyperelliptic curves (where $\ell = 2$), the plane curve $Dy^2 = f(x)$

is isomorphic to $y^2 = D^d f(x/D)$. We denote by *rank* $J_D(K)$ the Mordell-Weil rank of $J_D(K)$ if $J_D(K)$ is a finitely generated (abelian) group. Let ζ_ℓ be a primitive ℓ-th root of unity, let F be $K(\zeta_\ell)$, and let $\lambda := 1 - \zeta_\ell$. Throughout the paper, we denote also by λ the endomorphism $1 - \zeta_\ell$ on J_F defined in [Sch98], Sec 3, and by $\mathsf{Sel}^{(\lambda)}(J, F)$ *the λ-Selmer group of* J_F.

In this work, we shall consider both the number field case and the function field case. We begin by introducing our results for number fields. Let $k > 1$ be a positive integer, and let us denote by $\mathscr{P}_k(X)$ the set of all positive k-th power-free integers up to X. Given a polynomial $f(x)$, let Δ_f denote the discriminant of $f(x)$. Let F be the field of fractions of a Dedekind domain $\mathscr{O}_F$, and let $\mathscr{D}$ be a set of prime ideals of $\mathscr{O}_F$. A nonzero element D of $\mathscr{O}_F$ is *supported by* $\mathscr{D}$ if $D\mathscr{O}_F$ is divisible only by prime ideals contained in $\mathscr{D}$.

THEOREM 4.10 *Let K denote the ℓ-th cyclotomic field extension $\mathbb{Q}(\zeta_\ell)$ where ℓ is a regular prime number. Let $f(x)$ be a monic polynomial of prime degree p defined over $\mathbb{Z}$ such that $f(x)$ is irreducible over K, and $\ell \neq p$. Let $C/\mathbb{Q}$ be the normalization of the superelliptic curve $y^\ell = f(x)$, and let $J/\mathbb{Q}$ be the Jacobian variety of C.*

Let D_0 be a positive integer. Let $N := \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0}, K)$, and let M be the number of prime ideals of $\mathscr{O}_K$ dividing $\ell\Delta_f D_0$. Then there is a set $\mathscr{D}$ of prime numbers with Dirichlet density at least $(p-1)/\left(\ell^{(N+M+1)p!}(\ell-1)p!\right)$ such that whenever a positive integer D is supported by $\mathscr{D}$,

$$\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0 D}, K) = N.$$

Moreover, there is a positive constant $\varepsilon < 1$ depending on C and D_0 such that

$$\#\left\{D \in \mathscr{P}_\ell(X) : \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) = N\right\} \gg_{J, D_0} \frac{X}{(\log X)^\varepsilon}.$$

This theorem is proved using Schaefer's description of the λ-Selmer group [Sch98]. The case of superelliptic curves $y^\ell = x^2 - A$ is considered by Stoll in [Sto98], which in fact inspired our work (see Corollary 4.13 on p.15). Schaefer's description is more complicated when $\ell \mid \deg(f)$; see [PE97].

Finer results on the distribution of Selmer ranks of twists of the Jacobian variety of a curve have only been obtained in very special cases. Let $T(X)$ be the set of nonzero square-free integers D such that $|D| < X$. In [HB94], Heath-Brown studies the distribution of 2-Selmer ranks of quadratic twists of the elliptic curve $E/\mathbb{Q}$ given by $y^2 = x^3 - x$. For example, given a positive integer n, he computes explicitly

$$\lim_{X \to \infty} \frac{\#\{D \in T(X) : \dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(E_D, \mathbb{Q}) = n, \ D \equiv 1 \bmod 8\}}{\#\{D \in T(X) : D \equiv 1 \bmod 8\}}.$$

In [Yu03], for infinitely many elliptic curves $E/\mathbb{Q}$ with a nontrivial rational 2-torsion point, Gang Yu computes an upper bound for a certain average of $\dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(E_D, \mathbb{Q})$. Let $K := \mathbb{Q}(\zeta_3)$, and let $E/\mathbb{Q}$ be the elliptic curve given by $y^2 = x^3 - A$ where A is an integer. Let λ be the endomorphism defined in 1.1 for $\ell = 3$. In [Cha], we computed an upper bound for a certain average of λ-Selmer rank of E_D over K where E_D is a quadratic twist of $E/\mathbb{Q}$. Given an integer n, computed also in [Cha] is a lower bound for

$$\liminf_{X \to \infty} \frac{\#\{D \in T(X) : \dim_{\mathbb{F}_3} \mathsf{Sel}^{(\lambda)}(E_D, K) \leqslant 2n, \ D \equiv 1 \bmod 12A\}}{\#\{D \in T(X) : D \equiv 1 \bmod 12A\}}.$$

The results in [HB94], [Yu03], and [Cha] have applications to the distribution of Mordell-Weil ranks of quadratic twists of elliptic curves considered in these papers. Using Theorem 4.10, we obtain the following result on the distribution of Mordell-Weil ranks of ℓ-th power twists of the Jacobian variety of C.

COROLLARY 4.11 *Assume the same hypotheses in Theorem 4.10. Then there is a positive constant $\varepsilon < 1$ such that*

$$\#\left\{D \in \mathscr{P}_\ell(X) : \operatorname{rank} J_D(\mathbb{Q}) \leqslant N\right\} \gg_{J, D_0} \frac{X}{(\log X)^\varepsilon}. \tag{1}$$

If a Jacobian variety J considered in Corollary 4.11 has an ℓ-th power twist with λ-Selmer rank 0, then the corollary implies that there are infinitely many ℓ-th power twists with Mordell-Weil rank 0.

THEOREM 5.5 *Let K denote the ℓ-th cyclotomic field extension $\mathbb{Q}(\zeta_\ell)$ where ℓ is a regular prime number. Let $f(x)$ be a monic polynomial defined over $\mathbb{Z}$ such that $f(x)$ has a root in K, and $\ell \nmid \deg(f)$. Let $C/\mathbb{Q}$ be the normalization of the superelliptic curve $y^\ell = f(x)$.*

Given a positive integer n, there is a positive constant $\varepsilon < 1$ depending on C and n such that

$$\#\{D \in \mathscr{P}_\ell(X) : \dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(J_D, K) > n\} \gg_{C,n} \frac{X}{(\log X)^\varepsilon}.$$

In particular, $\limsup_D \dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(J_D, K) = \infty$.

Recall that for $D \in \mathbb{Q}^*$, $\mathrm{Sel}^{(2)}(J_D, \mathbb{Q}) \cong J_D(\mathbb{Q})/2J_D(\mathbb{Q}) \oplus \text{Ш}(J_D, \mathbb{Q})[2]$ where $\text{Ш}(J_D, \mathbb{Q})$ is the Tate-Shafarevich group of $J_D/\mathbb{Q}$. Suppose that $\ell = 2$, and that $f(x)$ is any polynomial of odd degree with a root in $\mathbb{Q}$ such that $f(x)$ has distinct roots. Theorem 5.5 implies in particular that the 2-Selmer groups of quadratic twists of the hyperelliptic curve $y^2 = f(x)$ can be arbitrarily large, and this result seems to be new. However, for some elliptic curves, more is known. For instance, it is proved in [Ata01] as a generalization of Lemmermeyer's work [Lem] that the 2-part of the Tate-Shafarevich groups of quadratic twists of the elliptic curves considered in the paper can be arbitrarily large.

Consider a Fermat curve $x^\ell + y^\ell = 1$. It is in fact isomorphic to a superelliptic curve $y^\ell = f(x)$ (where $\ell \nmid \deg(f)$), and using Theorem 5.5, we obtain the following result on Fermat twists.

COROLLARY 5.7 *Let K denote the ℓ-th cyclotomic field extension $\mathbb{Q}(\zeta_\ell)$ where ℓ is an odd regular prime number. Let F_D/K be the Fermat curve given by $x^\ell + y^\ell = Dz^\ell$ where $D \in \mathbb{Z}$ is nonzero, and let $\mathrm{Jac}(F_D)$ be the Jacobian variety of F_D/K. Let ζ_ℓ denote the automorphism of order ℓ on F_D given by $x \mapsto x$, $y \mapsto y$, and $z \mapsto z\zeta_\ell$. Let λ be the endomorphism $1 - [\zeta_\ell]$ on $\mathrm{Jac}(F_D)$ where $[\zeta_\ell]$ denotes the automorphism on $\mathrm{Jac}(F_D)$ induced by the automorphism on F_D. Then*

$$\limsup_D \dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(\mathrm{Jac}(F_D), K) = \infty.$$

Let us further consider applications of Theorem 4.10. Let $C/\mathbb{Q}$ be the normalization of a superelliptic curve of genus > 1, and C_D, the twist of C as defined in 1.1 for some $D \in \mathbb{Q}^*$. We apply Silverman's result [Sil93], p. 234, that if K is a number field, then the number of K-rational points on a twist C_D of C/K is bounded in terms of a constant γ depending on C, and in terms of the Mordell-Weil rank of the Jacobian variety J_D, namely,

$$\#C_D(K) < \gamma \, 7^{\mathrm{rank}\, J_D(K)}. \tag{2}$$

COROLLARY 1.2. *Let C be the normalization of a superelliptic curve considered in Theorem 4.10. Let $N := \dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(J_{D_0}, K)$ for a nonzero positive integer D_0. If the genus of C is > 1, then there are positive constants $\varepsilon < 1$, and γ depending on C and D_0 such that*

$$\#\{D \in \mathscr{P}_\ell(X) : \# C_D(\mathbb{Q}) \leqslant \gamma \, 7^N\} \gg \frac{X}{(\log X)^\varepsilon}.$$

Proof. The proof is left to the reader. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

For the case of hyperelliptic curves C, using [Sto], Theorem 1, we obtain a sharper upper bound on the number of rational points on quadratic twists of C/K.

COROLLARY 4.12 *Let $C/\mathbb{Q}$ be the normalization of a hyperelliptic curve $y^2 = f(x)$ where $f(x) \in \mathbb{Z}[x]$ is monic and irreducible over $\mathbb{Q}$, and has odd prime degree $p \geqslant 5$. Suppose that there is a positive integer D_0 such that $N := \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(J_{D_0}, \mathbb{Q}) < (p-1)/2$. Then there is a positive constant $\varepsilon < 1$ depending on C and*

D_0 such that

$$\# \{D \in \mathscr{P}_2(X) : \# C_D(\mathbb{Q}) \leqslant 2N+1\} \gg \frac{X}{(\log X)^\varepsilon}. \tag{3}$$

J. Silverman asked (see [OC98], p. 653.) whether given an elliptic curve $E/\mathbb{Q}$, there are infinitely many prime numbers p for which either E_p or E_{-p} has Mordell-Weil rank zero. We can show:

COROLLARY 1.3. *Let $E/\mathbb{Q}$ be an elliptic curve without $\mathbb{Q}$-rational 2-torsion points. If $\dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(E, \mathbb{Q}) = 0$, then there is a set $\mathscr{D}$ of prime numbers with positive Dirichlet density such that $\mathrm{rank}\, E_p(\mathbb{Q}) = 0$ for all $p \in \mathscr{D}$. In particular, there are infinitely many prime numbers p such that $\mathrm{rank}\, E_p(\mathbb{Q}) = 0$.*

Proof. The proof is left to the reader. $\qquad\square$

In [OC98], Corollary 3, Ono and Skinner proved that the question of Silverman has a positive answer for all elliptic curves with conductor $\leqslant 100$. Theorem 4.10 and Corollary 1.3 in particular imply that there are infinitely many elliptic curves over $\mathbb{Q}$ for which the question of Silverman has a positive answer: Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - 2$. Then, $\dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(E, \mathbb{Q}) = 0$ and, by Theorem 4.10, there are infinitely many quadratic twists E_D with $\dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(E_D, \mathbb{Q}) = 0$. Now, Corollary 1.3 implies a positive answer to the question of Silverman for these elliptic curves E_D.

Little is known about the distribution of quadratic twists of an elliptic curve with Mordell-Weil rank 1. Vatsal's result [Vat98] is unconditional: He proved that for the elliptic curve $E = X_0(19)$,

$$\#\{|D| < X : \mathrm{rank}\, E_D(\mathbb{Q}) = 1\} \gg X.$$

Assuming the Riemann Hypothesis, Iwaniek and Sarnak proved in [IP00] that $\#\{|D| < X : \mathrm{rank}\, E_D(\mathbb{Q}) = 1\} \gg_E X$ for all elliptic curves $E/\mathbb{Q}$. We prove here:

COROLLARY 1.4. *Assume the finiteness of the Tate-Shafarevich groups of all elliptic curves over $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve without $\mathbb{Q}$-rational 2-torsion points such that $\dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(E_{D_0}, \mathbb{Q}) = 1$ for some positive integer D_0. Then there is a positive constant $\varepsilon < 1$ such that*

$$\# \{D \in \mathscr{P}_2(X) : \mathrm{rank}\, E_D(\mathbb{Q}) = 1,\ \text{Ш}(E_D, \mathbb{Q})[2] = \{0\}\} \gg_{E,D_0} \frac{X}{(\log X)^\varepsilon}. \tag{4}$$

Proof. Let E be an elliptic curve with $\dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(E, \mathbb{Q}) = 1$. The finiteness of the Tate-Shafarevich group $\text{Ш}(E, \mathbb{Q})$ of $E/\mathbb{Q}$ implies that the Cassels-Tate pairing $\text{Ш}(E, \mathbb{Q}) \times \text{Ш}(E, \mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$ is a non-degenerate alternating bilinear pairing. By this pairing, $\dim_{\mathbb{F}_2} \text{Ш}(E, \mathbb{Q})[2] \leqslant 1$ implies $\mathrm{rank}\, E(\mathbb{Q}) = 1$ and $\dim_{\mathbb{F}_2} \text{Ш}(E, \mathbb{Q})[2] = 0$. Then (4) follows immediately from Theorem 4.10. $\qquad\square$

Very little is known about the distribution of Mordell-Weil ranks of cubic twists of an elliptic curve. Let $E/\mathbb{Q}$ be the elliptic curve given by $x^3 + y^3 = 1$. In [Lie94], Lieman showed that given an integer c and a prime number p, there are infinitely many cubic twists $E_D : x^3 + y^3 = D$ such that $D \equiv c \bmod p$ and $\mathrm{rank}\, E_D(\mathbb{Q}) = 0$. We show here

COROLLARY 4.13 *Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 - A$ where A is a positive square-free integer such that $A \equiv 1$ or $25 \bmod 36$ and $\dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{-A}))[3] = 0$. For a non-zero cube-free integer D, let E_D be the cubic twist: $y^2 = x^3 - AD^2$. Then there is a positive integer $\varepsilon < 1$ such that*

$$\#\{D \in \mathscr{P}_3(X) : \mathrm{rank}\, E_D(\mathbb{Q}) = 0\} \gg \frac{X}{(\log X)^\varepsilon}. \tag{5}$$

A function field of one variable over an arbitrary field k is a field extension K of k with transcendence degree 1 such that K is finitely generated over k, and k is algebraically closed in K. *A function field of one variable with a rational divisor v_∞* is a function field K of one variable over a finite field k with a non-archimedean absolute value v_∞ on K/k of *degree* 1. Such function fields correspond to smooth complete curves $\mathscr{Z}$ over k with a k-rational point p_∞ corresponding to the absolute value v_∞. For this type of function

fields, we choose $\mathcal{O}_K := \{\alpha \in K : |\alpha|_{v_\infty} > 1\}$, as a ring of integers in K, i.e., $\mathcal{O}_K$ is the ring of regular functions on the open subset $\mathscr{Z} \setminus \{p_\infty\}$. In Corollary 4.20 and Theorem 5.6, we prove function field analogues of Theorem 4.10 and 5.5.

1.5. Let ℓ be a prime number, and let k be a finite field containing a primitive ℓ-th root of unity. Hence, $\operatorname{char} k \neq \ell$. Let K be a function field of one variable with a rational divisor v_∞, and let $\mathscr{Z}/k$ be a smooth complete curve with function field K. Let C/K, C_D/K, J/K, and J_D/K be as defined in the case of number fields.

Over a number field K, given any positive integer g_0, it does not seem to be known how to produce a (superelliptic) curve C/K of genus $g(C) > g_0$ such that there are infinitely many twists with (λ-) Selmer rank 0, or such that the Selmer rank for C/K is 0. We use Theorem 4.22 below to show that a function field analogue of this problem can be solved even for (infinitely many) function fields K with arbitrarily large genus $g(K/k)$.

THEOREM 4.22 *Assume the hypotheses in 1.5. Suppose that $f(x)$ is defined over the constant field k, irreducible over the finite field k, and has prime degree p. Let k' be the field extension of k of degree $p \neq \operatorname{char} k$. Let $L := K \otimes k'$, and let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in L.*

Let A/k be the Jacobian variety of the normalization of the superelliptic curve $y^\ell = f(x)$ defined over the constant field k, so $A_K = J$. If $\#\operatorname{Cl}(\mathcal{O}_L) \not\equiv 0 \bmod \ell$, then $\dim_{\mathbb{F}_\ell} \operatorname{Sel}^{(\lambda)}(J,K) = 0$. Moreover, there is a set $\mathscr{D}$ of prime ideals of $\mathcal{O}_K$ with Dirichlet density $(p-1)/p$ such that whenever D is a nonzero element of $\mathcal{O}_K$ supported by $\mathscr{D}$,

$$\dim_{\mathbb{F}_\ell} \operatorname{Sel}^{(\lambda)}(J_D,K) = 0, \ \text{and} \ \# C_D(K) \leqslant \# A(k).$$

The hypothesis in Theorem 4.22 is often satisfied. Let K be a function field of one variable with a rational divisor v_∞, and let $\mathscr{Z}/k$ be the smooth curve with function field K. Then, by Proposition 4.24, $\#\operatorname{Cl}(\mathcal{O}_K) = \#\operatorname{Pic}^0(\mathscr{Z})$. Let $L := K \otimes k'$ for a finite extension k' of k, and let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in L. Then $\#\operatorname{Cl}(\mathcal{O}_L) = \#\operatorname{Pic}^0(\mathscr{Z}_{k'})$. Therefore, for all but finitely many prime numbers ℓ, we have $\#\operatorname{Cl}(\mathcal{O}_L) = \#\operatorname{Pic}^0(\mathscr{Z}_{k'}) \not\equiv 0 \bmod \ell$. Thus, we find examples of superelliptic curves of arbitrarily large genus which satisfy the conditions in Theorem 4.22.

For the curves C considered in Theorem 4.22, there are infinitely many D's such that $\# C_D(K)$ is bounded. In [Sch90], Schoen considered hyperelliptic curves defined over certain geometric fields, and showed that for these curves, the number of rational points of their quadratic twists can be arbitrarily large.

We conclude this introduction by providing the reader with a road map for Schaefer's description for the λ-Selmer group, and for the proof of Theorem 4.10. Recall that in this case, $f(x)$ is irreducible over $K := \mathbb{Q}(\zeta_\ell)$. Let L be a field isomorphic to $K[x]/(f)$. Using Schaefer's method, we have the first two rows of the commutative diagram (6).

Recall from 1.1 that a twist J_D/K is the Jacobian variety of C_D/K for some $D \in \mathcal{O}_K \setminus \{0\}$, and the curve C_D is given by $y^\ell = f_D(x) := D^p f(x/D)$. Since $L \cong K[x]/(f_D)$, as in the case of J/K, we can construct a map

$$\text{(6)}$$

$\theta^D : H^1(K, J_D[\lambda]) \to L^*/(L^*)^\ell$. When we consider the λ-Selmer groups of both J and J_D, we establish that the first two rows and the last two rows of (6) are commutative. It is noteworthy that the targets of θ and θ^D are both $L^*/(L^*)^\ell$, and it can be understood as a consequence of the fact that the two group schemes $J[\lambda]$ are $J_D[\lambda]$ are isomorphic to each other.

Two key points we shall prove in Section 3 are the following: First, if D is an ℓ-th power in K_v for v, then there is a map $\mathscr{H}_v^D : J(K_v) \to J_D(K_v)$ such that the diagram (6) commutes (see Proposition 3.5). It is clear that there is an isomorphism: $J(K_v) \to J_D(K_v)$, but it is not so obvious, unless one knows the horizontal maps, that it commutes with the identiy map on $L_v^*/(L_v^*)^\ell$. Secondly, if D is divisible only by prime ideals $\mathfrak{p}$ of $\mathscr{O}_K$ such that $\mathfrak{p}\mathscr{O}_L$ is prime, then $\ker \Psi_J = \ker \Psi_D$ in the diagram (6) (see Theorem 4.3). These two results immediately imply that $\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K)) \subset \theta(\mathsf{Sel}^{(\lambda)}(J, K))$ (see the proof of Theorem 4.10). By posing more conditions on D, we can prove $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) = \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J, K)$. To exhibit the existence of (enough) such D's, we use the Cebotarev density theorem and the general reciprocity laws.

Notation

1.6. *A global field* is either a number field or a function field of one variable over a finite field k. Let K be a global field. We denote by M_K the set of all places of K. Suppose that K is a function field of one variable over a finite field k. We choose a finite set of places of K, which will be denoted by M_K^∞, and consider the Dedekind domain

$$R := \{\alpha \in K^* : |\alpha|_v \leqslant 1, \text{ for all } v \in M_K \backslash M_K^\infty\}.$$

We shall denote $M_K \backslash M_K^\infty$ by M_K^0.

In this paper, by a global field, we shall mean a number field with $\mathscr{O}_K$, the integral closure of $\mathbb{Z}$, or a function field of one variable over a finite field k with the Dedekind domain $\mathscr{O}_K$ determined by a choice of M_K^∞. For both cases, $\mathscr{O}_K$ is called the ring of integers of K. Throughout the paper, if L is a finite separable extension of K, let $\mathscr{O}_L$ denote the integral closure of $\mathscr{O}_K$ in L. When K is a function field of one variable, our choice of M_K^∞ determines $\mathscr{O}_K$ and, hence, $\mathscr{O}_L$ and M_L^∞. For a function field K of one variable with a rational divisor v_∞ we choose $M_K^\infty := \{v_\infty\}$.

1.7. Throughout the paper, given a field K, let $\overline{K}$ denote the algebraic closure of K, and K_{sep}, the (algebraic) separable closure of K. Let K be a global field. We denote by G_K the absolute Galois group $\mathrm{Gal}(K_{\mathrm{sep}}/K)$. For each $\mathfrak{q} \in M_K$, let $K_\mathfrak{q}$ denote the completion of K at $\mathfrak{q}$. We fix the algebraic closures $\overline{K}$ and $\overline{K}_\mathfrak{q}$, and fix an embedding $\kappa_\mathfrak{q} : K_{\mathrm{sep}} \hookrightarrow K_{\mathfrak{q}, \mathrm{sep}}$.

In this paper, *a variety J over an arbitrary field K* is a separated scheme of finite type over K such that $J_{\overline{K}}$ is integral (that is, reduced and irreducible). Let J/K be a variety. For a field extension F of K, *the F-points of J* is the set $J(F)$. We denote by $\overline{J}$ the variety $J_{\overline{K}}$, and by J_{sep} the variety $J_{K_{\mathrm{sep}}}$.

2. Schaefer's description of the λ-Selmer group

In this section, we introduce Schaefer's method for computing Selmer groups. This method is introduced in [Sch98] for number fields; however, his proofs carry over to the case of global fields.

2.1. Let ℓ be a prime number, and let K be a global field of characteristic $\neq \ell$ such that K contains a primitive ℓ-th root of unity ζ_ℓ. Let C/K denote the normalization of a superelliptic curve given by $y^\ell = f(x)$ with $d := \deg(f)$. Let J/K be the Jacobian variety of C. Let ζ_ℓ also denote the K-automorphism on J defined in [Sch98], Sec 3, and $\lambda := 1 - \zeta_\ell \in \mathrm{End}(J)$, which we also denote by $[\lambda]$. Recall that $f(x)$ has distinct roots, and let $\{z_i \in K_{\mathrm{sep}} : i = 1, \ldots, d\}$ be the roots of $f(x)$. Let $P_i := [(z_i, 0) - (\infty)] \in J(K_{\mathrm{sep}})$. By [Sch98], Proposition 3.2, the set $\{P_1, \ldots, P_d\}$ generates the $\mathbb{F}_\ell$-vector space $J[\lambda](K_{\mathrm{sep}})$ of dimension $d - 1$. We choose a G_K-set X as small as possible such that X spans $J[\lambda](K_{\mathrm{sep}})$: If $f(x)$ does not have a K-rational root, then we set $d' := d$, and if $f(x)$ has a K-rational root z_d, then we set $d' := d - 1$. Then we define $X := \{P_1, \ldots, P_{d'}\}$.

The K_{sep}-algebra of all functions from X to K_{sep} is denoted by $\overline{A}_X$. As described in [Sch98], Sec 2, $\overline{A}_X$ has G_K-action, and the G_K-invariants are denoted by A_X.

2.2. From the Galois cohomology for the sequence $0 \to J[\lambda](K_{\text{sep}}) \to J(K_{\text{sep}}) \xrightarrow{\lambda} J(K_{\text{sep}}) \to 0$, we have the following injective map:

$$\delta : J(K)/\lambda J(K) \longrightarrow \mathsf{H}^1(K, J[\lambda]). \tag{7}$$

For each $v \in M_K$, we denote by res_v the map: $\mathsf{H}^1(K, J[\lambda]) \to \mathsf{H}^1(K_v, J[\lambda])$, and by δ_v the coboundary map: $J(K_v) \to \mathsf{H}^1(K_v, J[\lambda])$ defined for K_v. *The λ-Selmer group of J/K is*

$$\mathsf{Sel}^{(\lambda)}(J, K) := \{\xi \in \mathsf{H}^1(K, J[\lambda]) : \text{res}_v(\xi) \in \text{Im}\,\delta_v, \text{ for all } v \in M_K\}. \tag{8}$$

By definition, *the λ-part of the Tate-Shafarevich group of J/K*, denoted by $\text{Ш}(J/K)[\lambda]$, is canonically isomorphic to $\mathsf{Sel}^{(\lambda)}(J, K)/\text{Im}\,\delta$. Let S be a subset of M_K containing all archimedean places of K. The subgroup of $\mathsf{H}^1(K, J[\lambda])$ unramified outside the set S is denoted by by $\mathsf{H}^1(K, J[\lambda])_S$. Then the following result is standard: Let S be a subset of M_K containing all archimedean places, the places above $\deg(\lambda)$, and the places of bad reduction of J/K. Then,

$$\mathsf{Sel}^{(\lambda)}(J, K) = \{\xi \in \mathsf{H}^1(K, J[\lambda])_S : \text{res}_v(\xi) \in \text{Im}\,\delta_v \text{ for all } v \in S\}. \tag{9}$$

Moreover, $\mathsf{Sel}^{(\lambda)}(J, K)$ is finite, and contains $\delta(J(K)/\lambda J(K))$.

Suppose that $f(x)$ does not have a K-rational root. Then $\dim_{\mathbb{F}_\ell} \mu_\ell(\overline{A}_X^*) = d$ since $\#X = d$, and that $\dim_{\mathbb{F}_\ell} J[\lambda](K_{\text{sep}}) = d - 1$. By [Sch98], Proposition 3.4, the following is a split short exact sequence of G_K-modules, which is due to the fact that $\ell \nmid d$:

$$0 \longrightarrow J[\lambda](K_{\text{sep}}) \xrightarrow{w} \mu_\ell(\overline{A}_X^*) \xrightarrow{\mathsf{N}_{\overline{A}_X/\overline{K}}} \mu_\ell(K_{\text{sep}}^*) \longrightarrow 0$$

where w is the map defined in [Sch98], page 452. Since this exact sequence splits, the following natural map on the cohomology groups is injective:

$$\tilde{w} : \mathsf{H}^1(K, J[\lambda]) \longrightarrow \mathsf{H}^1(K, \mu_\ell(\overline{A}_X^*)). \tag{10}$$

Suppose that $f(x)$ has a K-rational root, say z_d. We choose $X := \{P_1, \ldots, P_{d-1}\}$ as in 2.1. Then it is clear that $w : J[\lambda](K_{\text{sep}}) \to \mu_\ell(\overline{A}_X^*)$ is an isomorphism of G_K-modules since $\dim_{\mathbb{F}_\ell} J[\lambda](K_{\text{sep}}) = \dim_{\mathbb{F}_\ell} \mu_\ell(\overline{A}_X^*) = d - 1$. Therefore, the following natural map is an isomorphism:

$$\tilde{w} : \mathsf{H}^1(K, J[\lambda]) \longrightarrow \mathsf{H}^1(K, \mu_\ell(\overline{A}_X^*)). \tag{11}$$

2.3. Consider the Kummer sequence for $\overline{A}_X^*$ with respect to the homomorphism $\alpha \mapsto \alpha^\ell$. By Hilbert Theorem 90, we have a natural isomorphism: $\Phi : \mathsf{H}^1(K, \mu_\ell(\overline{A}_X^*)) \to A_X^*/(A_X^*)^\ell$ and, hence, have an injective homomorphism

$$\Phi \circ \tilde{w} : \mathsf{H}^1(K, J[\lambda]) \longrightarrow A_X^*/(A_X^*)^\ell. \tag{12}$$

Let S be a subset of M_K containing M_K^∞, places above ℓ, and places of bad reduction of J/K. If $f(x)$ has a K-rational root, then $\mathsf{H}^1(K, J[\lambda])_S \cong A_X(S, \ell)$ where $A_X(S, \ell)$ is the subgroup of $A_X^*/(A_X^*)^\ell$ defined in [Sch98], Sec 2. If $f(x)$ does not have a K-rational root, then, [Sch98], Proposition 3.4 gives us the following isomorphism:

$$\mathsf{H}^1(K, J[\lambda])_S \cong \ker\left(\mathsf{N}_{A_X/K} : A_X(S, \ell) \to K(S, \ell)\right).$$

2.4. For each $v \in M_K$, we take the image of X in $J[\lambda](K_{v,\text{sep}})$ to be a G_{K_v}-stable spanning subset, and denote it by X_v. Then we have an induced map

$$\overline{A}_X \longrightarrow \overline{A}_{X_v} \tag{13}$$

obtained by pulling back the natural map $X_v \to X$, and it is denoted by $\tilde{\kappa}_v^*$. Moreover, we have the maps δ_v, $\tilde{w}_v$, and Φ_v as in the case of K.

Let S be a set of the places containing M_K^∞, the places above ℓ, and the places of bad reduction of J/K. For each $v \in M_K$, the following diagram is commutative:

$$
\begin{array}{ccccc}
J(K)/\lambda J(K) & \xrightarrow{\ \delta\ } & \mathsf{H}^1(K,J[\lambda])_S & \xrightarrow{\ \Phi\circ\tilde{w}\ } & A_X(S,\ell) \\
{\scriptstyle \kappa_v}\downarrow & & {\scriptstyle \mathrm{res}_v}\downarrow & & \downarrow{\scriptstyle \tilde{\kappa}_v^*} \\
J(K_v)/\lambda J(K_v) & \xrightarrow{\ \delta_v\ } & \mathsf{H}^1(K_v,J[\lambda]) & \xrightarrow{\ \Phi_v\circ\tilde{w}_v\ } & A_{X_v}^*/(A_{X_v}^*)^\ell
\end{array}
\quad .
$$

Suppose that $f(x)$ does not have a K-rational root. Then

$$\mathsf{Sel}^{(\lambda)}(J,K) \cong \{\alpha \in A_X(S,\ell) : \mathrm{N}_{A_X/K}(\alpha) = 1,\ \tilde{\kappa}_v^*(\alpha) \in \mathrm{Im}\,\Phi_v \circ \tilde{w}_v \circ \delta_v \text{ for all } v \in S\}.$$

Suppose that $f(x)$ has a K-rational root. Then, we have a simpler description:

$$\mathsf{Sel}^{(\lambda)}(J,K) \cong \{\alpha \in A_X(S,\ell) : \tilde{\kappa}_v^*(\alpha) \in \mathrm{Im}\,\Phi_v \circ \tilde{w}_v \circ \delta_v \text{ for all } v \in S\}.$$

Let Φ and $\tilde{w}$ be the maps defined in (12). Let δ be the coboundary map defined in (7). Then, we have an injective homomorphism

$$\Phi \circ \tilde{w} \circ \delta : J(K)/\lambda J(K) \longrightarrow A_X^*/(A_X^*)^\ell, \tag{14}$$

and there is a useful description of this map which given below.

Write $K_{\mathrm{sep}}(C_{\mathrm{sep}})$ as the field of fractions of $K_{\mathrm{sep}}[x,y]/(y^\ell - f(x))$. Then $x - z_i$ is an element of this function field, which we will denote by $f_{P_i}(x,y)$;

$$f_{P_i}(x,y) := x - z_i. \tag{15}$$

Note that f_{P_i} can be thought as a function on divisors of C. If E is a divisor in $\mathrm{Div}(C)$ *avoiding* the set X (see [Sch98], page 450), then we denote by $f_\bullet(E)$ the function: $X \to \overline{K}^*$ given by $P \mapsto f_P(E)$ for all $P \in X$. Let $Y := \{P_1, \ldots, P_d\}$. If E is a divisor in $\mathrm{Div}(C)$ avoiding Y, then, as long as there is no confusion, we also denote by $f_\bullet(E)$ the extended function: $Y \to \overline{K}^*$ given by $P \mapsto f_P(E)$ for all $P \in Y$. If $E := \sum(R)$ is a divisor in $\mathrm{Div}(C)$ avoiding X such that $K(R)/K$ is separable, then $f_\bullet(E) \in A_X^*$, and if E is a divisor in $\mathrm{Div}(C)$ avoiding Y such that $K(R)/K$ is separable, then $f_\bullet(E) \in A_Y^*$.

2.5. Let us define a group homomorphism $\mathrm{Pic}^0(C) \to A_X^*/(A_X^*)^\ell$ as follows: It is well-known that for each $[D] \in \mathrm{Pic}^0(C)$, we can choose a divisor $E = \sum(R)$ avoiding any given finite set of C such that $K(R)/K$ is separable and $[E] = [D]$. Then we define a group homomorphism given by

$$[D] \mapsto \mathrm{class}(f_\bullet(E)) \in A_X^*/(A_X^*)^\ell, \tag{16}$$

and denote it by $\overline{\delta}$.

The following corollary follows from [Sch98], Theorem 2.3 and Proposition 3.3. The proposition essentially shows that $[(\infty)] = [D]$ for some divisor D avoiding Y such that $f_\bullet(D) \in (A_Y^*)^\ell$:

LEMMA 2.6. *Let $\overline{\delta}$ be the map defined in 2.5 for X. Then $\Phi \circ \tilde{w} \circ \delta = \overline{\delta}$.*

Suppose that $f(x)$ has a K-rational root z_d, so we choose $X := \{P_1, \ldots, P_{d-1}\} \subset J(K_{\mathrm{sep}})$. If E is a nonzero divisor in $\mathrm{Div}^0(C)$ such that $E = (Q) - (\deg_K(Q))(\infty)$ for some Q avoiding X, and such that $K(Q)/K$ is separable, then $[E]$ is mapped to $\mathrm{class}(f_\bullet(Q)) \in A_X^*/(A_X^*)^\ell$ under $\overline{\delta}$. In particular, $[(z_d,0) - (\infty)] \mapsto \mathrm{class}(f_\bullet(z_d,0)) \in A_X^*/(A_X^*)^\ell$.

Proof. The proof is left to the reader. $\qquad\square$

3. Two Key Propositions

Let us recall the diagram (6). In this section, we prove the commutativity of this diagram in a slightly more general context. Let ℓ be a prime number, and let K be a global field of characteristic $\neq \ell$, containing a

primitive ℓ-th root ζ_ℓ of unity. Let C/K be the normalization of a superelliptic curve given by $y^\ell = f(x)$, and let $d := \deg(f)$.

3.1. For each $\mathfrak{q} \in M_K$, we fix an embedding $\kappa_\mathfrak{q} : \overline{K} \to \overline{K}_\mathfrak{q}$. Let X and $X_\mathfrak{q}$ for each $\mathfrak{q} \in M_K$ be the G_K-stable spanning sets of $J[\lambda](K_{\mathrm{sep}})$ and $J[\lambda](K_{\mathfrak{q},\mathrm{sep}})$, respectively, defined in 2.1 and 2.4. For each $\mathfrak{q} \in M_K$, let $\kappa_\mathfrak{q}$ and $\tilde{\kappa}_\mathfrak{q}^*$ be the maps defined in Section 2;

$$\kappa_\mathfrak{q} : X \longrightarrow X_\mathfrak{q}, \quad \tilde{\kappa}_\mathfrak{q}^* : \overline{A}_X \longrightarrow \overline{A}_{X_\mathfrak{q}}.$$

Let P_i for $i = 1, \ldots, d'$ be the points in X. Note that $f(x) = (x - z_1) \cdots (x - z_d)$, and for $D \in K^*$, $D^d f(x/D) = (x - z_1 D) \cdots (x - z_d D)$. For $D \in K^*$ and $\mathfrak{q} \in M_K$, we define

$$X^D := \{[(z_i D, 0) - (\infty)] \in J_D(K_{\mathrm{sep}}) : i = 1, \ldots, d'\};$$
$$X_\mathfrak{q}^D := \{[(\kappa_\mathfrak{q}(z_i D), 0) - (\infty)] \in J_D(K_{\mathfrak{q},\mathrm{sep}}) : i = 1, \ldots, d'\};$$
$$P_i^D := [(z_i D, 0) - (\infty)] \in J_D(K_{\mathrm{sep}}),$$

and let Φ^D, $\Phi_\mathfrak{q}^D$, $\tilde{w}^D$, $\tilde{w}_\mathfrak{q}^D$, $\delta_\mathfrak{q}$, and $\delta_\mathfrak{q}^D$ be the maps for the twist J_D as in Section 2. Then we have the following sequences of injective maps:

$$\begin{array}{ccccccc}
J_D(K)/\lambda J_D(K) & \xrightarrow{\delta^D} & \mathsf{H}^1(K, J_D[\lambda]) & \xrightarrow{\tilde{w}^D} & \mathsf{H}^1(K, \mu_\ell(\overline{A}_{X^D}^*)) & \xrightarrow{\Phi^D} & A_{X^D}^*/(A_{X^D}^*)^\ell; \qquad (17)\\
\downarrow{\scriptstyle\kappa_\mathfrak{q}} & & \downarrow{\scriptstyle\mathrm{res}_\mathfrak{q}} & & \downarrow{\scriptstyle\mathrm{res}_\mathfrak{q}} & & \downarrow{\scriptstyle\tilde{\kappa}_\mathfrak{q}^*}\\
J_D(K_\mathfrak{q})/\lambda J_D(K_\mathfrak{q}) & \xrightarrow{\delta_\mathfrak{q}^D} & \mathsf{H}^1(K_\mathfrak{q}, J_D[\lambda]) & \xrightarrow{\tilde{w}_\mathfrak{q}^D} & \mathsf{H}^1(K_\mathfrak{q}, \mu_\ell(\overline{A}_{X_\mathfrak{q}^D}^*)) & \xrightarrow{\Phi_\mathfrak{q}^D} & A_{X_\mathfrak{q}^D}^*/(A_{X_\mathfrak{q}^D}^*)^\ell.
\end{array}$$

Let $Z(J) := \{T_i \in X : i = 1, \ldots, s\}$ be a set of representatives of G_K-orbits in X, and $Z(J_D) := \{P_j^D \in X^D : P_j \in Z(J)\}$ which is said to be *compatible with* $Z(J)$. Let L_i be the subfield of K_{sep}, generated by T_i for $i = 1, \ldots, s$. Since the action of G_K is made through the divisors representing the points in X, the subfield $K(P_j^D)$ of K_{sep} is $K(z_j)$, and $Z(J_D)$ is a set of representatives of G_K-orbits in X^D. For $\mathfrak{q} \in M_K$, let $Z(J, \mathfrak{q})$ be a set of representatives of $\mathsf{G}_{K_\mathfrak{q}}$-orbits such that $Z(J) \subset Z(J, \mathfrak{q})$. Then, we choose $Z(J_D, \mathfrak{q})$ compatible with $Z(J, \mathfrak{q})$; hence, $Z(J_D) \subset Z(J_D, \mathfrak{q})$.

3.2. Note that if $\alpha \in A_{X^D}$, then the evaluation of α at $P_j^D \in Z(J_D)$ is contained in $K(z_j) = L_i$ for some i, i.e., $\alpha(P_j^D) \in L_i$. For $D \in K^*$ and $\mathfrak{q} \in M_K$, let $\Psi_{Z(J_D)}$ and $\Psi_{Z(J_D, \mathfrak{q})}$ be the evaluation maps of $A_{X^D}^*/(A_{X^D}^*)^\ell$ and $A_{X_\mathfrak{q}^D}^*/(A_{X_\mathfrak{q}^D}^*)^\ell$ at $Z(J_D)$ and $Z(J_D, \mathfrak{q})$, respectively, and define

$$\mathscr{C} := \Psi_{Z(J_D)}\left(A_{X^D}^*/(A_{X^D}^*)^\ell\right) = \prod_{P \in Z(J_D)} K(P)^*/(K(P)^*)^\ell = \prod_{i=1}^s L_i^*/(L_i^*)^\ell;$$
$$\mathscr{C}_\mathfrak{q} := \Psi_{Z(J_D, \mathfrak{q})}\left(A_{X_\mathfrak{q}^D}^*/(A_{X_\mathfrak{q}^D}^*)^\ell\right) = \prod_{P \in Z(J, \mathfrak{q})} K_\mathfrak{q}(P)^*/(K_\mathfrak{q}(P)^*)^\ell.$$

Since we choose $Z(J_D, \mathfrak{q})$ compatible with $Z(J, \mathfrak{q})$, the group $\mathscr{C}_\mathfrak{q}$ is defined not depending on D as $\mathscr{C}$.

Recall the maps in (17). For each $D \in K^*$, we denote by θ and θ^D the injective maps $\Psi_{Z(J)} \circ \Phi \circ \tilde{w}$ and $\Psi_{Z(J_D)} \circ \Phi^D \circ \tilde{w}^D$, respectively. For each $D \in K^*$ and $\mathfrak{q} \in M_K$, we denote, respectively, by $\theta_\mathfrak{q}$ and $\theta_\mathfrak{q}^D$ the injective maps

$$\Psi_{Z(J, \mathfrak{q})} \circ \Phi_\mathfrak{q} \circ \tilde{w}_\mathfrak{q} : \mathsf{H}^1(K_\mathfrak{q}, J[\lambda]) \longrightarrow \mathscr{C}_\mathfrak{q}; \qquad (18)$$
$$\Psi_{Z(J_D, \mathfrak{q})} \circ \Phi_\mathfrak{q}^D \circ \tilde{w}_\mathfrak{q}^D : \mathsf{H}^1(K_\mathfrak{q}, J_D[\lambda]) \longrightarrow \mathscr{C}_\mathfrak{q}. \qquad (19)$$

Remark 3.3. It is noteworthy to observe that the targets of the following maps are defined depending only on C/K:

$$\theta^D : \mathsf{H}^1(K, J_D[\lambda]) \longrightarrow \mathscr{C}, \quad \theta_\mathfrak{q}^D : \mathsf{H}^1(K_\mathfrak{q}, J_D[\lambda]) \longrightarrow \mathscr{C}_\mathfrak{q}.$$

Let S be a subset of M_K containing M_K^∞, the places above ℓ, and the places of bad reduction of J/K and J_D/K. If $f(x)$ does not have a K-rational root, then

$$\theta^D(\mathrm{H}^1(K,J_D[\lambda])_S) = \ker\left(\prod_i \mathrm{N}_{L_i/K} : \prod_i L_i(S,\ell) \to K(S,\ell)\right) = \theta(\mathrm{H}^1(K,J[\lambda])_S).$$

If $f(x)$ has a K-rational root, then

$$\theta^D\left(\mathrm{H}^1(K,J_D[\lambda])_S\right) = \prod_{i=1}^s L_i(S,\ell) = \theta\left(\mathrm{H}^1(K,J[\lambda])_S\right).$$

Recall the diagram (6) from the introduction. In a slightly more general context, we constructed above all the horizontal maps in (6). Proposition 3.4 below is one of the key propositions which will establish the commutativity of the diagram formed by the restriction maps in the second and the third columns of (6). The proof is left to the reader.

PROPOSITION 3.4. *For each $\mathfrak{q} \in M_K$, there is a natural map $\mathscr{C} \to \mathscr{C}_\mathfrak{q}$ such that the following diagram commutes for all $D \in K^*$:*

$$
\begin{array}{ccccccc}
\mathrm{H}^1(K,J_D[\lambda]) & \xrightarrow{\tilde{w}^D} & \mathrm{H}^1(K,\mu_\ell(\overline{A}_{X^D}^*)) & \xrightarrow{\Phi^D} & A_{X^D}^*/(A_{X^D}^*)^\ell & \xrightarrow{\Psi_{Z(J_D)}} & \mathscr{C} \\
\downarrow{\scriptstyle\mathrm{res}_\mathfrak{q}} & & \downarrow{\scriptstyle\mathrm{res}_\mathfrak{q}} & & \downarrow{\scriptstyle\tilde{\kappa}_\mathfrak{q}^*} & & \downarrow{\scriptstyle\mathrm{res}_\mathfrak{q}} \\
\mathrm{H}^1(K_\mathfrak{q},J_D[\lambda]) & \xrightarrow{\tilde{w}_\mathfrak{q}^D} & \mathrm{H}^1(K_\mathfrak{q},\mu_\ell(\overline{A}_{X_\mathfrak{q}^D}^*)) & \xrightarrow{\Phi_\mathfrak{q}^D} & A_{X_\mathfrak{q}^D}^*/(A_{X_\mathfrak{q}^D}^*)^\ell & \xrightarrow{\Psi_{Z(J_D,\mathfrak{q})}} & \mathscr{C}_\mathfrak{q}
\end{array}
$$

Proposition 3.5 below completes the proof of the commutativity of the diagram (6).

PROPOSITION 3.5. *Let $\mathfrak{q}$ be a place in M_K. For all nonzero elements D of $\mathscr{O}_K$ such that $D \in (K_\mathfrak{q}^*)^\ell$, there is an isomorphism $\mathscr{H}_D : J(K_\mathfrak{q}) \to J_D(K_\mathfrak{q})$ such that the following is a commutative diagram:*

$$
\begin{array}{ccc}
J_D(K_\mathfrak{q})/\lambda J_D(K_\mathfrak{q}) & \xrightarrow{\theta_\mathfrak{q}^D \delta_\mathfrak{q}^D} & \mathscr{C}_\mathfrak{q} \\
\uparrow{\scriptstyle\mathscr{H}_D} & & \uparrow{\scriptstyle\mathrm{id}} \\
J(K_\mathfrak{q})/\lambda J(K_\mathfrak{q}) & \xrightarrow{\theta_\mathfrak{q} \delta_\mathfrak{q}} & \mathscr{C}_\mathfrak{q}
\end{array}
\qquad (20)
$$

In particular, $\mathrm{Im}\,\theta_\mathfrak{q}^D \delta_\mathfrak{q}^D = \mathrm{Im}\,\theta_\mathfrak{q} \delta_\mathfrak{q}$ for all nonzero $D \in \mathscr{O}_K$ and $\mathfrak{q} \in M_K$ such that $D \in (K_\mathfrak{q}^*)^\ell$.

Proof. Let D be a nonzero element of $\mathscr{O}_K$ such that $D \in (K_\mathfrak{q}^*)^\ell$. Then, we have an isomorphism $(C_D)_{K_\mathfrak{q}} \to C_{K_\mathfrak{q}}$ given by $(x,y) \mapsto (x/D, y/\sqrt[\ell]{D^d})$, and this isomorphism induces an isomorphism $\mathscr{H}_D : J(K_\mathfrak{q}) \to J_D(K_\mathfrak{q})$ by pulling back on the divisors.

Recall $Z(J_D,\mathfrak{q}) = \{P^D := [(zD,0) - (\infty)] : [(z,0) - (\infty)] \in Z(J,\mathfrak{q})\}$. Let $E := \sum n_j(R_j)$ be a divisor in $\mathrm{Div}^0(C_{K_\mathfrak{q},\mathrm{sep}})$ avoiding X such that $K(R_j)/K$ are separable, and write $R_j = (x_j,y_j)$. Then,

$$f_\bullet\left(\mathscr{H}_D(E)\right)(P^D) = \prod_j \left(f_{P^D}(x_j D, y_j \sqrt[\ell]{D^d})\right)^{n_j} = \prod_j (x_j D - zD)^{n_j}$$

$$= D^{\Sigma n_j} \prod_j (x_j - z)^{n_j} = \prod_j (x_j - z)^{n_j};$$

$$f_\bullet(E)\,(P) = \prod_j \left(f_P(x_j,y_j)\right)^{n_j} = \prod_j (x_j - z)^{n_j}.$$

This proves the commutativity of the diagram (20). $\qquad\qquad\square$

Remark 3.6. The diagram in Proposition 3.5 can be put into the following diagram:

$$
\begin{array}{ccccccc}
J_D(K_\mathfrak{q})/\lambda J_D(K_\mathfrak{q}) & \xrightarrow{\delta_\mathfrak{q}^D} & \mathrm{H}^1(K_\mathfrak{q},J_D[\lambda]) & \xrightarrow{\Phi_\mathfrak{q}^D \circ \tilde{w}_\mathfrak{q}^D} & A_{X_\mathfrak{q}^D}^*/(A_{X_\mathfrak{q}^D}^*)^\ell & \xrightarrow{\Psi_{Z(J_D,\mathfrak{q})}} & \mathscr{C}_\mathfrak{q} \\
\uparrow{\scriptstyle\mathscr{H}_D} & & \uparrow{\scriptstyle\tilde{\mathscr{H}}} & & \uparrow{\scriptstyle\mathrm{id}_D} & & \uparrow{\scriptstyle\mathrm{id}} \\
J(K_\mathfrak{q})/\lambda J(K_\mathfrak{q}) & \xrightarrow{\delta_\mathfrak{q}} & \mathrm{H}^1(K_\mathfrak{q},J[\lambda]) & \xrightarrow{\Phi_\mathfrak{q} \circ \tilde{w}_\mathfrak{q}} & A_{X_\mathfrak{q}}^*/(A_{X_\mathfrak{q}}^*)^\ell & \xrightarrow{\Psi_{Z(J_D,\mathfrak{q})}} & \mathscr{C}_\mathfrak{q}
\end{array}
$$

10

where $\tilde{\mathcal{H}}$ and id_D are isomorphisms induced from the natural isomorphism: $J[\lambda] \to J_D[\lambda]$.

All the vertical maps in the above diagram, except the first one, exist whether or not D is an ℓ-th power in $K_{\mathfrak{q}}$, and the entire diagram commutes when $D \in (K_{\mathfrak{q}}^*)^\ell$.

3.7. Recall the maps θ^D and $\theta_{\mathfrak{q}}^D$ for $\mathfrak{q} \in M_K$ and $D \in \mathcal{O}_K$ defined in 3.2. Let S be a subset of M_K containing M_K^∞, the places above ℓ, and the places of bad reduction of J_D/K. Then, $\mathsf{Sel}^{(\lambda)}(J_D, K)$ is described as a subgroup of $\mathscr{C}$ as follows:

$$\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K)) = \{\alpha \in \theta^D(\mathsf{H}^1(K, J_D[\lambda])_S) : \mathrm{res}_{\mathfrak{q}}(\alpha) \in \mathrm{Im}\,\theta_{\mathfrak{q}}^D \delta_{\mathfrak{q}}^D \text{ for all } \mathfrak{q} \in S\}.$$

4. The Jacobian Varieties Without λ-torsion Points

In this section, we prove Theorem 4.10 and its analogue for a function field. Let ℓ be a prime number, and let K be a a global field of characteristic $\neq \ell$, containing a primitive ℓ-th root of unity ζ_ℓ. Let C/K be the normalization of a superelliptic curve $y^\ell = f(x)$. Let Δ_f be the discriminant of $f(x)$ where $f(x)$ is irreducible over K with prime degree p. Let J/K be the Jacobian variety of C. We keep all the notation and definitions introduced in Section 3.

4.1. Let S_J denote the subset of M_K containing M_K^∞, the places dividing $\ell\Delta_f$. For each nonzero element D of $\mathcal{O}_K$, let S_D denote the set $S_J \cup \{\mathfrak{p} \in M_K^0 : \mathfrak{p} \mid D\mathcal{O}_K\}$. Then, the sets S_J and S_D contain the set of places of bad reduction of J/K and J_D/K, respectively.

4.2. Recall that $X := \{P_1, \dots, P_d\}$ is the subset of $J[\lambda](K_{\mathrm{sep}})$. Since X forms one orbit, $Z(J)$ contains a single point, and we choose $Z(J) := \{P_1\}$ as a representative. Let L denote the finite separable field extension $L_1 := K(P_1)$ of degree p. Then $\mathscr{C} := L^*/(L^*)^\ell$ as defined in 3.2.

THEOREM 4.3. *Let D be a nonzero element of $\mathcal{O}_K$, and suppose that $D\mathcal{O}_K$ is supported by the set of prime ideals $\mathfrak{q}$ of $\mathcal{O}_K$ such that either $\mathfrak{q}\mathcal{O}_L$ is prime in $\mathcal{O}_L$ or $\mathfrak{q}\mathcal{O}_L = \mathfrak{p}^p$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$. Then, $\ker\left(N_{L/K} : L(S_J, \ell) \to K(S_J, \ell)\right) = \ker\left(N_{L/K} : L(S_D, \ell) \to K(S_D, \ell)\right)$. Hence, $\theta\left(\mathsf{H}^1(K, J[\lambda])_{S_J}\right) = \theta^D\left(\mathsf{H}^1(K, J_D[\lambda])_{S_D}\right)$ as subgroups of L^*.*

Proof. Since $S_J \subset S_D$, it is clear that

$$\ker\left(N_{L/K} : L(S_J, \ell) \to K(S_J, \ell)\right) \subset \ker\left(N_{L/K} : L(S_D, \ell) \to K(S_D, \ell)\right).$$

Let α be a nonzero element of $\mathcal{O}_L$ such that $\alpha\mathcal{O}_L = \mathfrak{a}\mathfrak{b}^\ell$ where $\mathfrak{a}$ is an ideal *supported by* S_D and such that $N_{L/K}(\alpha) = \beta^\ell$ for some $\beta \in \mathcal{O}_K$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_K$ dividing $D\mathcal{O}_K$ such that $\mathfrak{q}\mathcal{O}_L$ is $\mathfrak{p}$ or $\mathfrak{p}^p$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$. Let $n := \mathrm{ord}_{\mathfrak{p}}(\alpha\mathcal{O}_L)$, and let m be the residue degree of $\mathfrak{p}$ with respect to $\mathfrak{q}$. Since $m \not\equiv 0 \bmod \ell$, and there is only one prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{q}$, it follows that $\mathrm{ord}_{\mathfrak{q}}(\beta^\ell \mathcal{O}_K) = \mathrm{ord}_{\mathfrak{q}}(N_{L/K}(\alpha\mathcal{O}_L)) = nm$. On the other hand, $\mathrm{ord}_{\mathfrak{q}}(\beta^\ell \mathcal{O}_K) \equiv 0 \bmod \ell$ and, hence, $n \equiv 0 \bmod \ell$. Therefore, $\mathrm{ord}_{\mathfrak{p}}(\alpha\mathcal{O}_L) \equiv 0 \bmod \ell$ for all $\mathfrak{p}$ dividing $D\mathcal{O}_L$, and $\alpha\mathcal{O}_L = \mathfrak{a}'(\mathfrak{b}')^\ell$ for some ideal $\mathfrak{a}'$ supported by S_J, i.e., $\mathrm{class}(\alpha) \in L(S_J, \ell)$. $\square$

The Legendre symbol is used throughout Sections 4 and 5. Definitions and results on Legendre symbols required for our main results are introduced and proved in Section 6. In 6.1, we extend the definition of the symbol for prime ideals dividing $\ell\mathcal{O}_K$ and archimedean places, so that given $\alpha \in \mathcal{O}_K$ and $\mathfrak{p} \in M_K$, $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell = 1$ implies $\alpha \in (K_{\mathfrak{p}}^*)^\ell$.

4.1 The case of number fields

For Lemma 4.5, Proposition 4.6, and Lemma 4.7, we assume a slightly more general context: Let $K/\mathbb{Q}$ be the ℓ-th cyclotomic field extension of $\mathbb{Q}$ where ℓ is a regular prime number. Let L be a field extension of K such that $p := [L : K]$ is a prime number not equal to ℓ.

4.4. Let W be a finite subset of $\mathscr{O}_L \backslash \{0\}$. We denote by $\mathscr{D}_W$ the set of prime numbers $q \in \mathbb{Z}$ not dividing ℓ which satisfy the following properties: for all prime ideals $\mathfrak{q}$ of $\mathscr{O}_K$ dividing q,

  i) The ideal $\mathfrak{q}\mathscr{O}_L$ is prime;

  ii) For all $\alpha \in W$, $\alpha \not\equiv 0 \bmod \mathfrak{q}\mathscr{O}_L$, and $\left(\frac{\alpha}{\mathfrak{q}\mathscr{O}_L} \right)_\ell = 1$.

LEMMA 4.5. *Let $\mathfrak{q}$ be a prime ideal of $\mathscr{O}_K$ not dividing $\ell\mathscr{O}_K$ such that $\mathfrak{q}\mathscr{O}_L$ is prime. If $\alpha \in \mathscr{O}_K$ is such that $\left(\frac{\alpha}{\mathfrak{q}\mathscr{O}_L} \right)_\ell = 1$, then $\left(\frac{\alpha}{\mathfrak{q}} \right)_\ell = 1$.*

Proof. Let k_L be the residue field $\mathscr{O}_L/\mathfrak{q}\mathscr{O}_L$, and k be the residue field $\mathscr{O}_K/\mathfrak{q}$. For $z \in \mathscr{O}_L$, let $\bar{z}$ denote the residue class in k_L. Since $\left(\frac{\alpha}{\mathfrak{q}\mathscr{O}_L} \right)_\ell = 1$, let $\beta \in \mathscr{O}_L$ such that $\beta^\ell \equiv \alpha \bmod \mathfrak{q}\mathscr{O}_L$, i.e., $\bar{\beta}^\ell = \bar{\alpha}$ in k_L. The degree of the extension $k(\bar{\beta})/k$ is either 1 or ℓ since k contains a primitive ℓ-th root of unity. Since $\ell \neq p$, $k(\bar{\beta}) = k$. Thus, $\left(\frac{\alpha}{\mathfrak{q}} \right)_\ell = 1$. $\qquad\square$

PROPOSITION 4.6. *Let W be a finite subset of $\mathscr{O}_L \backslash \{0\}$, and let $\mathscr{D}_W$ be the set of prime numbers defined in 4.4. Then $\mathscr{D}_W$ contains a set of prime numbers in $\mathbb{Z}$ with positive Dirichlet density at least $(p-1)/\left(\ell^{(\#W)p!}(\ell-1)p! \right)$.*

Proof. Let M be the Galois closure of $L(\sqrt[\ell]{\alpha} : \alpha \in W)$ over $\mathbb{Q}$. Let M' be the Galois closure of L over $\mathbb{Q}$. Then $m := [M' : L] \not\equiv 0 \bmod p$ since f is defined over $\mathbb{Z}$, and $\deg f =: p$ is a prime number. Note that $M = M'(\sqrt[\ell]{\tau\alpha} : \alpha \in W$ and $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$. Since $\zeta_\ell \in K$, and ℓ is a prime number, $[M : M']$ is a power of ℓ and, hence, $[M : M'] = \ell^n$ for some non-negative integer n.

It follows that $[M : K] = pm\ell^n$. Let G denote the group $\mathrm{Gal}(M/\mathbb{Q})$. Then $\mathrm{Gal}(M/K)$ is a subgroup of G, and the group G contains an automorphism τ of order p acting trivially on K. Moreover, the subgroup $\langle \tau \rangle$ of G is stable under conjugation since $\mathrm{Gal}(M/K)$ is normal in G. Therefore, the subset $H := \{ \tau^k : k = 1, \ldots, p-1 \}$ is stable under conjugation in G.

Let $\mathscr{D}$ be the set of all prime numbers q such that q is unramified in M and its Frobenius automorphisms are contained in H. Then, since $[M : \mathbb{Q}]$ divides $(\ell-1) \cdot p! \cdot \ell^{(\#W)p!}$, by the Cebotarev Density Theorem, $\mathscr{D}$ has positive Dirichlet density at least $(p-1)/\left(\ell^{(\#W)p!}(\ell-1)p! \right)$. Since W is a finite set, the following set of prime ideals has Dirichlet density equal to the Dirichlet density of $\mathscr{D}$:

$$\{ q \in \mathscr{D} : \alpha \not\equiv 0 \bmod \mathfrak{q} \text{ for all prime ideals } \mathfrak{q} \mid q\mathscr{O}_L \text{ and for all } \alpha \in W \}.$$

Thus, let us assume that $\mathscr{D}$ is the above set.

Let $q \in \mathscr{D}$, and let $\mathfrak{Q}$ be a prime ideal of $\mathscr{O}_M$ lying over q. Let $\mathfrak{Q}_L := \mathfrak{Q} \cap \mathscr{O}_L$, and $\mathfrak{q} := \mathfrak{Q} \cap \mathscr{O}_K$. Let us show that $\mathfrak{q}\mathscr{O}_L$ is a prime ideal. Let $f(\mathfrak{q}/q)$, $f(\mathfrak{Q}_L/\mathfrak{q})$, and $f(\mathfrak{Q}/\mathfrak{Q}_L)$ denote the residue degrees. Then

$$p = |\mathrm{Frob}(\mathfrak{Q}/q)| = f(\mathfrak{Q}/q) = f(\mathfrak{Q}/\mathfrak{Q}_L)f(\mathfrak{Q}_L/\mathfrak{q})f(\mathfrak{q}/q). \tag{21}$$

Since $\tau = \mathrm{Frob}(\mathfrak{Q}/q) \in \mathrm{Gal}(M/K)$, and $K/\mathbb{Q}$ is Galois, $\mathrm{Frob}(\mathfrak{q}/q) = \mathrm{res}_K(\tau) = 1$. Hence, $1 = |\mathrm{Frob}(\mathfrak{q}/q)| = f(\mathfrak{q}/q)$. Thus, $p = f(\mathfrak{Q}/\mathfrak{Q}_L)f(\mathfrak{Q}_L/\mathfrak{q})$. Since M/L is Galois, $f(\mathfrak{Q}/\mathfrak{Q}_L)$ divides $m\ell^n \equiv 0 \bmod p$ and, hence, $f(\mathfrak{Q}/\mathfrak{Q}_L) \not\equiv 0 \bmod p$. Therefore, $f(\mathfrak{Q}/\mathfrak{Q}_L) = 1$ and $f(\mathfrak{Q}_L/\mathfrak{q}) = p$. In other words, the prime ideal $\mathfrak{q}$ remains prime in $\mathscr{O}_L$. Moreover, $f(\mathfrak{Q}/\mathfrak{Q}_L) = 1$ implies that $\mathscr{O}_M/\mathfrak{Q} \cong \mathscr{O}_L/\mathfrak{Q}_L$ and, hence, $\sqrt[\ell]{\alpha}$ for all $\alpha \in W$ are defined in $\mathscr{O}_L/\mathfrak{Q}_L$. In other words, since $\mathfrak{Q}_L = \mathfrak{q}\mathscr{O}_L$, $1 = \left(\frac{\alpha}{\mathfrak{q}\mathscr{O}_L} \right)_\ell$ for all $\alpha \in W$. Therefore, $q \in \mathscr{D}_W$. $\qquad\square$

Recall that ℓ is a regular prime number. The following lemma is the key place in our work where the additional hypothesis of ℓ being regular is needed.

LEMMA 4.7. *Let W be a finite subset of $\mathscr{O}_L \backslash \{0\}$ containing ζ_ℓ and $\lambda := 1 - \zeta_\ell$. Let $\mathscr{D}_W$ be the set of prime numbers defined in 4.4. Let $\mathfrak{q}$ be a place of K. If $\mathfrak{q}$ is a prime ideal of $\mathscr{O}_K$, then we choose $\alpha_\mathfrak{q} \in \mathscr{O}_K$ such that $\mathfrak{q}^m = \alpha_\mathfrak{q}\mathscr{O}_K$ where m is the order of $\mathfrak{q}$ in $\mathrm{Cl}(\mathscr{O}_K)$, and if $\mathfrak{q} = \lambda\mathscr{O}_K$, then we choose $\alpha_\mathfrak{q} := \lambda$.*

If $\mathfrak{q}$ is an infinite place of K, or if $\mathfrak{q}$ is a prime ideal of $\mathscr{O}_K$ such that $\alpha_\mathfrak{q} \in W$, then $\left(\frac{D}{\mathfrak{q}}\right)_\ell = 1$ for all positive integers D supported by $\mathscr{D}_W$.

Proof. Suppose that $\mathfrak{q}$ is a prime ideal of $\mathscr{O}_K$ not dividing $\ell\mathscr{O}_K$, and $\mathfrak{q}^m = \alpha_\mathfrak{q}\mathscr{O}_K$ where $\alpha_\mathfrak{q} \in \mathscr{O}_K$ and m is the order of $\mathfrak{q}$ in $\mathrm{Cl}(\mathscr{O}_K)$. Then, since ℓ is regular, $m \not\equiv 0 \bmod \ell$. Let q be a prime number dividing D, and suppose that $\alpha_\mathfrak{q} \in W$. Let $q\mathscr{O}_K$ be decomposed into $\prod_{k=1}^t \mathfrak{p}_j^n$ where $\mathfrak{p}_j$ are prime ideals coprime to ℓ and n is an integer. Since $q \in \mathscr{D}_W$, it follows that $\left(\frac{\alpha_\mathfrak{q}}{\mathfrak{p}_j\mathscr{O}_L}\right)_\ell = 1$ and, hence, by Lemma 4.5, $\left(\frac{\alpha_\mathfrak{q}}{\mathfrak{p}_j}\right)_\ell = 1$. Then

$$\left(\frac{\alpha_\mathfrak{q}}{q}\right)_\ell = \prod_{j=1}^t \left(\frac{\alpha_\mathfrak{q}}{\mathfrak{p}_j^n}\right)_\ell = \prod_{j=1}^t \left(\frac{\alpha_\mathfrak{q}}{\mathfrak{p}_j}\right)_\ell^n = 1.$$

Since W contains ζ_ℓ and λ, it follows that $\left(\frac{\zeta_\ell}{\mathfrak{p}_1}\right)_\ell = 1$. If $\ell = 2$, then $K = \mathbb{Q}$, and it follows that $\left(\frac{-1}{\mathfrak{p}_1}\right)_2 = \left(\frac{2}{\mathfrak{p}_1}\right)_2 = 1$. By Lemma 6.3, $\left(\frac{q}{\lambda\mathscr{O}_K}\right)_\ell = 1$. Since $\mathfrak{q} \nmid \ell\mathscr{O}_K$ and $\alpha_\mathfrak{q} \not\equiv 0 \bmod \mathfrak{p}_j$ for all $j = 1,\ldots,t$, by Corollary 6.4,

$$1 = \left(\frac{\alpha_\mathfrak{q}}{q}\right)_\ell = \left(\frac{q}{\alpha_\mathfrak{q}}\right)_\ell = \left(\frac{q}{\mathfrak{q}}\right)_\ell^m.$$

Since $m \not\equiv 0 \bmod \ell$, we proved that $\left(\frac{q}{\mathfrak{q}}\right)_\ell = 1$ for all prime numbers q dividing D.

Let $\mathfrak{q} := \lambda\mathscr{O}_K$. Then $\left(\frac{q}{\lambda\mathscr{O}_K}\right)_\ell = 1$ for all $q \mid D$ was already shown above. Since $D > 0$, it is clear that $\left(\frac{D}{v}\right)_\ell = 1$ for all infinite places $v \in M_K$. $\qquad\qquad\square$

Let us return to the context of our superelliptic curves. Recall from 4.2 the point $P_1 \in X$ and the field $L := K(P_1)$. For all $D \in K^*$, we have the following injective maps:

$$\mathsf{Sel}^{(\lambda)}(J_D, K) \subset \mathsf{H}^1(K, J_D[\lambda])_{S_D} \xrightarrow{\theta^D} L^*/(L^*)^\ell.$$

THEOREM 4.8. *Let $K := \mathbb{Q}(\zeta_\ell)$ where ℓ is a regular prime number. Let $f(x)$ be a monic polynomial of prime degree p defined over $\mathbb{Z}$ such that $f(x)$ is irreducible over K, and $\ell \neq p$. Let $C/\mathbb{Q}$ be the normalization of the superelliptic curve $y^\ell = f(x)$. Let $N := \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J, K)$, and M, the number of prime ideals of $\mathscr{O}_K$ dividing $\ell\Delta_f$. Then there is a set $\mathscr{D}$ of prime numbers with Dirichlet density at least $(p-1)/\left(\ell^{(N+M+1)p!}(\ell-1)p!\right)$ such that whenever a positive integer D is supported by $\mathscr{D}$, $\theta\left(\mathsf{Sel}^{(\lambda)}(J, K)\right) = \theta^D\left(\mathsf{Sel}^{(\lambda)}(J_D, K)\right)$. In particular, $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J, K) = \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K)$.*

Proof. Recall from 3.2 the map $\theta : \mathsf{H}^1(K, J[\lambda]) \to L^*/(L^*)^\ell$. Let W_J be a subset of $\mathscr{O}_L$ generating $\theta(\mathsf{Sel}^{(\lambda)}(J, K))$. For each prime ideal $\mathfrak{q}$ of $\mathscr{O}_K$ coprime to ℓ, let us fix an element $\alpha_\mathfrak{q}$ of $\mathscr{O}_K$ such that $\alpha_\mathfrak{q}\mathscr{O}_K = \mathfrak{q}^m$ where m is the order of $\mathfrak{q}$ in $\mathrm{Cl}(\mathscr{O}_K)$. For $\mathfrak{q} := \lambda\mathscr{O}_K$, we choose $\alpha_\mathfrak{q} := \lambda$.

Recall S_J from (4.1), and let

$$Y_J := \{\zeta_\ell\} \cup W_J \cup \{\alpha_\mathfrak{q} \in \mathscr{O}_K : \mathfrak{q} \in S_J \cap M_K^0\}.$$

Let $\mathscr{D}_{Y_J}$ be the set of prime numbers defined in 4.4 for $W = Y_J$. Then, by Proposition 4.6, $\mathscr{D}_{Y_J}$ contains a set $\mathscr{D}$ of prime numbers with Dirichlet density at least $(p-1)/\left(\ell^{(N+M+1)p!}(\ell-1)p!\right)$. Since ℓ is regular, by Lemma 4.7, if D is a positive integer supported by $\mathscr{D}$ and $\mathfrak{q} \in S_J$, then

$$\left(\frac{D}{\mathfrak{q}}\right)_\ell = 1. \tag{22}$$

Let D be a positive integer supported by $\mathscr{D}$. Let us show that $\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K)) \subset \theta(\mathsf{Sel}^{(\lambda)}(J, K))$. Let α be an element of $\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K))$. By 3.7,

$$\theta(\mathsf{Sel}^{(\lambda)}(J, K)) = \{\alpha \in \theta\left(\mathsf{H}^1(K, J[\lambda])_{S_J}\right) : \mathrm{res}_\mathfrak{q}(\alpha) \in \mathrm{Im}\,\theta_\mathfrak{q}\delta_\mathfrak{q} \text{ for all } \mathfrak{q} \in S_J\};$$
$$\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K)) = \{\alpha \in \theta^D\left(\mathsf{H}^1(K, J_D[\lambda])_{S_D}\right) : \mathrm{res}_\mathfrak{q}(\alpha) \in \mathrm{Im}\,\theta_\mathfrak{q}^D\delta_\mathfrak{q}^D \text{ for all } \mathfrak{q} \in S_D\}. \tag{23}$$

By Theorem 4.3, we have

$$\theta^D\big(\mathsf{H}^1(K,J_D[\lambda])_{S_D}\big) = \theta\big(\mathsf{H}^1(K,J[\lambda])_{S_J}\big);\tag{24}$$

hence, α is contained in $\theta\big(\mathsf{H}^1(K,J[\lambda])_{S_J}\big)$. Let $\mathfrak{q}$ be a place in S_J, and recall the set S_D from (4.1). Then $\mathfrak{q}$ is contained in S_D. By Lemma 6.7, (22) implies that $D \in (K_\mathfrak{q}^*)^\ell$. By Proposition 3.5, it follows that $\mathrm{Im}\,\theta_\mathfrak{q}\delta_\mathfrak{q} = \mathrm{Im}\,\theta_\mathfrak{q}^D\delta_\mathfrak{q}^D$ and, hence, α is contained in $\mathrm{Im}\,\theta_\mathfrak{q}\delta_\mathfrak{q}$ since $\alpha \in \theta^D(\mathsf{Sel}^{(\lambda)}(J_D,K))$ and $\mathfrak{q} \in S_D$. Thus, $\alpha \in \theta(\mathsf{Sel}^{(\lambda)}(J,K))$.

Let us show that $\theta(\mathsf{Sel}^{(\lambda)}(J,K)) \subset \theta^D(\mathsf{Sel}^{(\lambda)}(J_D,K))$. Let α be an element of $\theta(\mathsf{Sel}^{(\lambda)}(J,K))$. By (24), α is contained in $\theta^D\big(\mathsf{H}^1(K,J_D[\lambda])_{S_D}\big)$. If $\mathfrak{q}$ is a place in S_J, then by (22), $D \in (K_\mathfrak{q}^*)^\ell$, and by Proposition 3.5, $\mathrm{Im}\,\theta_\mathfrak{q}\delta_\mathfrak{q} = \mathrm{Im}\,\theta_\mathfrak{q}^D\delta_\mathfrak{q}^D$. Thus, $\alpha \in \mathrm{Im}\,\theta_\mathfrak{q}^D\delta_\mathfrak{q}^D$ for all $\mathfrak{q} \in S_J$. Let $\mathfrak{q}$ be a prime ideal in $S_D \setminus S_J$. Since D is supported by $\mathscr{D}$, the prime ideal $\mathfrak{q}$ is contained in $\mathscr{D}$ and, hence, $\left(\frac{\beta}{\mathfrak{q}}\right)_\ell = 1$ for all $\beta \in W_J$. Since W_J generates $\theta(\mathsf{Sel}^{(\lambda)}(J,K))$, it follows that $\left(\frac{\alpha}{\mathfrak{q}\mathscr{O}_L}\right)_\ell = 1$, i.e., $\alpha \in (L_\mathfrak{P}^*)^\ell$ where $\mathfrak{P} := \mathfrak{q}\mathscr{O}_L$. Recall that $\mathrm{res}_\mathfrak{q}$ is a map: $L^*/(L^*)^\ell \to \mathscr{C}_\mathfrak{q} := \prod_{P \in Z(J,\mathfrak{q})} K_\mathfrak{q}(P)^*/(K_\mathfrak{q}(P)^*)^\ell$. Since $\mathfrak{q}\mathscr{O}_L$ is prime, $f(x)$ is irreducible over $K_\mathfrak{q}$ and, hence, $Z(J,\mathfrak{q})$ contains a single point P. Thus, $\mathscr{C}_\mathfrak{q} = L_\mathfrak{P}^*/(L_\mathfrak{P}^*)^\ell$. Thus, $\mathrm{res}_\mathfrak{q}(\alpha) = 1$ and, in particular, $\mathrm{res}_\mathfrak{q}(\alpha) \in \mathrm{Im}\,\theta_\mathfrak{q}^D\delta_\mathfrak{q}^D$. We established that $\mathrm{res}_\mathfrak{q}(\alpha) \in \mathrm{Im}\,\theta_\mathfrak{q}^D\delta_\mathfrak{q}^D$ for all $\mathfrak{q} \in S_D$. Therefore, α is contained in $\theta^D(\mathsf{Sel}^{(\lambda)}(J_D,K))$. Since θ and θ^D are injective maps, the dimensions of the two selmer groups are equal to each other. $\qquad\square$

Recall that $\mathscr{P}_\ell(X)$ is the set of positive ℓ-th power free integers up to X. The following lemma is easily deduced from [Ser76], Theorem 2.4, and the proof is left to the reader:

LEMMA 4.9. *Let $\mathscr{D}$ be a set of prime numbers in $\mathbb{Z}$ with positive Dirichlet density < 1. Let $\mathscr{P}_\ell(\mathscr{D},X)$ denote the set of all positive integers up to X, which are ℓ-th power-free and supported by $\mathscr{D}$. Let $\mathscr{P}_\ell(\mathscr{D}) := \cup_{X=1}^\infty \mathscr{P}_\ell(\mathscr{D},X)$. Then there are positive constants c and $\varepsilon < 1$ depending on $\mathscr{P}_\ell(\mathscr{D})$ such that $\#\mathscr{P}_\ell(\mathscr{D},X) \sim \frac{X}{(\log X)^\varepsilon}$ as $X \to \infty$.*

Let D_0 be a positive ℓ-th power free integer. Then there is a positive constant $\varepsilon < 1$ depending on $\mathscr{D}$ such that

$$\#\{D_0 D \in \mathscr{P}_\ell(X) : D \in \mathscr{P}_\ell(\mathscr{D},X)\} \gg \frac{X}{(\log X)^\varepsilon}.$$

THEOREM 4.10. *Let K, $f(x)$, and $C/\mathbb{Q}$ be as in Theorem 4.8. Let D_0 be a positive integer. Let $N := \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0},K)$, and let M be the number of prime ideals of $\mathscr{O}_K$ dividing $\ell\Delta_f D_0$. Then there is a set $\mathscr{D}$ of prime numbers with Dirichlet density at least $(p-1)/\big(\ell^{(N+M+1)p!}(\ell-1)p!\big)$ such that whenever a positive integer D is supported by $\mathscr{D}$,*

$$\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0 D},K) = N.\tag{25}$$

Moreover, there is a positive constant $\varepsilon < 1$ such that

$$\#\{D \in \mathscr{P}_\ell(X) : \mathsf{Sel}^{(\lambda)}(J_D,K) = N\} \gg_{J,D_0} \frac{X}{(\log X)^\varepsilon}.\tag{26}$$

Proof. Recall that J_{D_0} is the Jacobian variety of the normalization of $y^\ell = (D_0)^p f(x/D_0)$. Let $g := (D_0)^p f(x/D_0)$. Then $\Delta_g = \Delta_f D_0^b$ for some positive integer b and, hence, the number of prime ideals of $\mathscr{O}_K$ dividing $\ell\Delta_g$ is equal to M. Since $(J_{D_0})_D = J_{D_0 D}$, by applying Theorem 4.8 to J_{D_0}, (25) is proved. The proof of (26) follows immediately from Lemma 4.9. $\qquad\square$

COROLLARY 4.11. *Assume the same hypotheses in Theorem 4.10. Then there is a positive constant $\varepsilon < 1$ such that*

$$\#\{D \in \mathscr{P}_\ell(X) : \mathrm{rank}\,J_D(\mathbb{Q}) \leqslant N\} \gg_{J,D_0} \frac{X}{(\log X)^\varepsilon}.\tag{27}$$

Proof. Note $\mathsf{Sel}^{(\lambda)}(J_D, K) \cong J_D(K)/\lambda J_D(K) \oplus \text{Ш}(J_D, K)[\lambda]$. Then, by [Sch98], Corollary 3.7 and Proposition 3.8, $\mathsf{Sel}^{(\lambda)}(J_D, K) \geqslant \mathrm{rank}\, J_D(\mathbb{Q})$. Hence, (27) follows. □

COROLLARY 4.12. *Let $C/\mathbb{Q}$ be the normalization of a hyperelliptic curve $y^2 = f(x)$ where $f(x) \in \mathbb{Z}[x]$ is monic and irreducible over $\mathbb{Q}$ and has odd prime degree $p \geqslant 5$. Suppose that there is a positive integer D_0 such that $N := \dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(J_{D_0}, \mathbb{Q}) < (p-1)/2$. Then there is a positive constant $\varepsilon < 1$ depending on C and D_0 such that*

$$\# \{D \in \mathscr{P}_2(X) : \# C_D(\mathbb{Q}) \leqslant 2N+1\} \gg \frac{X}{(\log X)^\varepsilon}.$$

Proof. Let ι be *the hyperelliptic involution on C_D.* In [Sto], Theorem 1.1, Stoll proved that if D is coprime to a fixed finite set T of prime numbers determined by C and D_0, then any set $S \subset C_D(\mathbb{Q})$ such that $\#S \leqslant (p-1)/2$ and $S \cap \iota(S) = \emptyset$ generates a subgroup of rank $\#S$ in $J_D(\mathbb{Q})$.

By Theorem 4.10,

$$\# \{D \in \mathscr{P}_2(X) : \dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(J_D, \mathbb{Q}) = N\} \gg \frac{X}{(\log X)^\varepsilon}.$$

We count the D's supported by a set $\mathscr{D}$ of prime numbers with positive Dirichlet density in order to find such a lower bound. Since T is finite, we may assume that $\mathscr{D}$ does not intersect T. Let D be a positive integer not supported by T such that $\dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(J_D, \mathbb{Q}) = N$. Then, by Stoll's theorem, Thus, $C_D(\mathbb{Q})$ can not contain a subset S such that $\#S > N$ and $S \cap \iota(S) = \emptyset$; otherwise, $\mathrm{rank}\, J_D(\mathbb{Q}) > N$. Since $C_D(\mathbb{Q})$ does not contain a point fixed under the involution, except ∞, we conclude $\# C_D(\mathbb{Q}) \leqslant 2N+1$. □

COROLLARY 4.13. *Let $E/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 - A$ where A is a positive square-free integer such that $A \equiv 1$ or $25 \bmod 36$ and $\dim_{\mathbb{F}_3} \mathrm{Cl}(\mathbb{Q}(\sqrt{-A}))[3] = 0$. For a non-zero cube-free integer D, let E_D be the cubic twist: $y^2 = x^3 - AD^2$. Then there is a positive integer $\varepsilon < 1$ such that*

$$\# \{D \in \mathscr{P}_3(X) : \mathrm{rank}\, E_D(\mathbb{Q}) = 0\} \gg \frac{X}{(\log X)^\varepsilon}.$$

Proof. By [Sto98], Corollary 2.1, $\dim_{\mathbb{F}_3} \mathsf{Sel}^{(\lambda)}(E, K) = 0$ where $\lambda = 1 - \zeta_3$ and $K = \mathbb{Q}(\zeta_3)$. As A is square-free and coprime to 3, the polynomial $y^2 + AD^2$ is irreducible over K. The result follows immediately from Theorem 4.10 with $\ell = 3$. □

4.2 The case of function fields

In this section, we shall prove two results for function fields that are analogous to Theorem 4.10. For Lemma 4.15, Proposition 4.16, and Lemma 4.18, let us assume a slightly more general context: Let k be a finite field containing a primitive ℓ-th root of unity ζ_ℓ; hence, $\mathrm{char}\, k \neq \ell$. Let K/k be a function field of one variable with a rational divisor v_∞ such that $\mathrm{Cl}(\mathscr{O}_K)[\ell] \not\equiv 0 \bmod \ell$ defined in 1.6. Let L be a field extension of K such that $p := [L:K]$ is a prime number not equal to ℓ.

4.14. Let W be a finite subset of $\mathscr{O}_L \setminus \{0\}$. We denote by $\mathscr{D}_W$ the set of prime ideals $\mathfrak{q}$ of $\mathscr{O}_K$ which satisfy the following properties:

   i) The ideal $\mathfrak{q}\mathscr{O}_L$ is prime;

   ii) for all $\alpha \in W$, $\alpha \not\equiv 0 \bmod \mathfrak{q}\mathscr{O}_L$, and $\left(\frac{\alpha}{\mathfrak{q}\mathscr{O}_L}\right)_\ell = 1$.

LEMMA 4.15. *Let $\mathfrak{q}$ be a prime ideal of $\mathscr{O}_K$ such that $\mathfrak{q}\mathscr{O}_L$ is prime. If $\alpha \in \mathscr{O}_K$ such that $\left(\frac{\alpha}{\mathfrak{q}\mathscr{O}_L}\right)_\ell = 1$, then $\left(\frac{\alpha}{\mathfrak{q}}\right)_\ell = 1$.*

Proof. The proof is similar to that of Lemma 4.5. □

PROPOSITION 4.16. *Let W be a finite subset of $\mathscr{O}_L \backslash \{0\}$. Then $\mathscr{D}_W$ contains a set of prime ideals of $\mathscr{O}_K$ with positive Dirichlet density at least $(p-1)/\left(\ell^{(\#W)p!}p!\right)$.*

Proof. The proof is similar to that of Proposition 4.6. □

Recall that K/k is a function field of one variable with a rational divisor v_∞, and let $\mathscr{O}_\infty$, $\mathfrak{M}_\infty$, and π_∞ be the discrete valuation ring, the maximal ideal, and a uniformizer at v_∞, respectively.

4.17. Let K_{v_∞} be the completion of K at v_∞. Let us define

$$\left(\frac{g}{v_\infty}\right)_\ell := \begin{cases} 1 & \text{if } g \in (K_{v_\infty}^*)^\ell \\ -1 & \text{if } g \notin (K_{v_\infty}^*)^\ell \end{cases}.$$

Note that each non-constant element g of $\mathscr{O}_K$ is not an element of the valuation ring $\mathscr{O}_\infty$, i.e., $\mathrm{ord}_{v_\infty}(g) < 0$. *The leading coefficient of a nonzero element g of $\mathscr{O}_K$ is the constant $a \in k^*$ such that $\pi_\infty^m g \equiv a \bmod \pi_\infty$ for some $m \in \mathbb{Z}$. The element g is monic if the leading coefficient is 1. The degree of an element g of $\mathscr{O}_K$*, denoted by $\deg(g)$, is $-\mathrm{ord}_\infty(g)$. Let g be an element of $\mathscr{O}_K$ with the leading coefficient $a \in k^*$. Then $g \in \left(K_{v_\infty}^*\right)^\ell$ if and only if $a \in (k^*)^\ell$ and $\deg(g)$ is divisible by ℓ.

LEMMA 4.18. *Let W be a finite subset of $\mathscr{O}_L \backslash \{0\}$ containing $-1 \in k$, and let $\mathscr{D}_W$ be the set of prime ideals of $\mathscr{O}_K$ defined in 4.14. Let $\mathfrak{q}$ be a prime ideal of $\mathscr{O}_K$, and $\alpha_\mathfrak{q}$, an element of $\mathscr{O}_K$ such that $\alpha_\mathfrak{q} \mathscr{O}_K = \mathfrak{q}^m$ where m is the order of $\mathfrak{q}$ in $\mathrm{Cl}(\mathscr{O}_K)$. If $\alpha_\mathfrak{q} \in W$, and D is a nonzero monic element in $\mathscr{O}_K$, supported by $\mathscr{D}_W$ such that $\deg(D) \equiv 0 \bmod \ell$, then*

$$\left(\frac{D}{v_\infty}\right)_\ell = \left(\frac{D}{\mathfrak{q}}\right)_\ell = 1.$$

Proof. Suppose that $\alpha_\mathfrak{q} \in W$, and let D be a nonzero monic element in $\mathscr{O}_K$, supported by $\mathscr{D}_W$ such that $\deg(D) \equiv 0 \bmod \ell$. Then, $\left(\frac{D}{v_\infty}\right)_\ell = 1$. Following the proof of Lemma 4.7, we find $\left(\frac{\alpha_\mathfrak{q}}{D}\right)_\ell = 1$. Since $-1 \in W$, it follows that $\left(\frac{-1}{D}\right)_\ell = 1$. By Lemma 6.6, $1 = \left(\frac{\alpha_\mathfrak{q}}{D}\right)_\ell = \left(\frac{D}{\alpha_\mathfrak{q}}\right)_\ell$. It follows that $1 = \left(\frac{D}{\alpha_\mathfrak{q}}\right)_\ell = \left(\frac{D}{\mathfrak{q}}\right)_\ell^m$ where $m \not\equiv 0 \bmod \ell$. Therefore, $\left(\frac{D}{\mathfrak{q}}\right)_\ell = 1$. □

THEOREM 4.19. *Assume that $\# \mathrm{Cl}(\mathscr{O}_K) \not\equiv 0 \bmod \ell$. Let $f(x)$ be a monic polynomial of prime degree p defined over $\mathscr{O}_K$ such that $f(x)$ is irreducible over K, and $\ell \neq p$. Let C/K be the normalization of the superelliptic curve $y^\ell = f(x)$. Let $N := \dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(J,K)$, and let M be the number of prime ideals of $\mathscr{O}_K$ dividing $\ell \Delta_f$. Then there is a set $\mathscr{D}$ of prime ideals with Dirichlet density at least $(p-1)/(\ell^{(N+M+1)p!}p!)$ such that whenever D is a monic element of $\mathscr{O}_K$ supported by $\mathscr{D}$ such that $\deg(D)$ is divisible by ℓ,*

$$\theta\left(\mathrm{Sel}^{(\lambda)}(J,K)\right) = \theta^D\left(\mathrm{Sel}^{(\lambda)}(J_D,K)\right).$$

Proof. Recall S_J from 4.1. For each prime ideal $\mathfrak{q}$ of $\mathscr{O}_K$, choose a monic element $\alpha_\mathfrak{q}$ of $\mathscr{O}_K$ such that $\alpha_\mathfrak{q} \mathscr{O}_K = \mathfrak{q}^m$ where m is the order of $\mathfrak{q}$ in $\mathrm{Cl}(\mathscr{O}_K)$. Let W_J be the subset of $\mathscr{O}_L$ generating $\theta(\mathrm{Sel}^{(\lambda)}(J,K))$. Let

$$Y_J := \{-1\} \cup W_J \cup \{\alpha_\mathfrak{q} \in \mathscr{O}_K : \mathfrak{q} \in S_J \cap M_K^0\},$$

and let $\mathscr{D}_{Y_J}$ be the set of prime ideals defined in 4.14 for $W = Y_J$. Then, by Proposition 4.16, $\mathscr{D}_{Y_J}$ contains a set of prime ideals $\mathscr{D}$ with Dirichlet density at least $(p-1)/(\ell^{(N+M+1)p!}p!)$. The proof of $\theta\left(\mathrm{Sel}^{(\lambda)}(J,K)\right) = \theta^D\left(\mathrm{Sel}^{(\lambda)}(J_D,K)\right)$ is identical with that of Theorem 4.10, when Lemma 4.18 is applied to $W = Y_J$. □

COROLLARY 4.20. *Assume the same hypotheses as in Theorem 4.19. Let D_0 be a nonzero element of $\mathscr{O}_K$. Let $N := \dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(J_{D_0},K)$, and M, the number of prime ideals of $\mathscr{O}_K$ dividing $\ell \Delta_f D_0$. Then there is a set $\mathscr{D}$ of prime ideals of $\mathscr{O}_K$ with Dirichlet density at least $(p-1)/(\ell^{(N+M+1)p!}p!)$ such that whenever D is a monic element of $\mathscr{O}_K$ supported by $\mathscr{D}$ such that $\deg(D)$ is divisible by ℓ,*

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(J_{D_0 D},K) = N.$$

Proof. The proof is similar to that of Theorem 4.10. □

4.21. Given a set $\mathscr{D}$ of prime ideals of $\mathscr{O}_K$, there are indeed infinitely many classes in $K^*/(K^*)^\ell$ represented by $D \in \mathscr{O}_K$ supported by $\mathscr{D}$ and $\deg(D) \equiv 0 \bmod \ell$. Let $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$ be a finite set of prime ideals of $\mathscr{O}_K$ contained in $\mathscr{D}$ for $n \geqslant 2$. Let $\mathfrak{p}_i^{m_i} = \alpha_{\mathfrak{p}_i} \mathscr{O}_K$ for some $\alpha_{\mathfrak{p}_i} \in \mathscr{O}_K$ where m_i is the order of $\mathfrak{p}_i$ in $\mathrm{Cl}(\mathscr{O}_K)$. Then, since $\mathrm{Cl}(\mathscr{O}_L) \not\equiv 0 \bmod \ell$ and $\deg(\alpha_{\mathfrak{p}_n}) = \mathrm{ord}_{\mathfrak{p}_n}(\alpha_{\mathfrak{p}_n})$, there is a positive integer s such that $D := \alpha_{\mathfrak{p}_n}^s \prod_{i=1}^{n-1} \alpha_{\mathfrak{p}_i}$ has degree divisible by ℓ.

THEOREM 4.22. *Assume the same hypotheses as in Theorem 4.19. Suppose that $f(x)$ is defined over k. Let k' be the finite extension of k of degree $p := \deg(f)$. Let $L := K \otimes k'$, and $\mathscr{O}_L$, the integral closure of K in L. Suppose that $\dim_{\mathbb{F}_\ell} \mathrm{Cl}(\mathscr{O}_L)[\ell] = 0$. Then $\dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(J, K) = 0$.*

Let E/k be the constant Jacobian variety of the normalization of the superelliptic curve $y^\ell = f(x)$ over k. Then there is a set $\mathscr{D}$ of prime ideals of $\mathscr{O}_K$ with Dirichlet density $(p-1)/p$ such that whenever D is an element of $\mathscr{O}_K$ supported by $\mathscr{D}$,

$$\dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(J_D, K) = 0 \quad and \quad \# C_D(K) \leqslant \# E(k).$$

Proof. Note that L/K is Galois. Recall S_J from (4.1). Then $S_J = M_K^\infty$, and $\mathsf{H}^1(K, J[\lambda])_{M_K^\infty} \cong \ker\big(\mathrm{N}_{L/K} : L(M_K^\infty, \ell) \to K(M_K^\infty, \ell)\big)$. Note that $\# \mathrm{Sel}^{(\lambda)}(J, K) \leqslant \# \mathsf{H}^1(K, J[\lambda])_{M_K^\infty} = \# \ker\big(\mathrm{N}_{L/K} : L(M_K^\infty, \ell) \to K(M_K^\infty, \ell)\big)$. Since the subgroup $\mathrm{Cl}(\mathscr{O}_L)[\ell]$ is trivial, by Lemma 4.23 below, $\mathsf{H}^1(K, J[\lambda])_{M_K^\infty} = 1$ and, hence, $\mathrm{Sel}^{(\lambda)}(J, K) = 0$.

Let $\mathscr{D}$ be the set of prime ideals $\mathfrak{q}$ of $\mathscr{O}_K$ such that $\mathfrak{q}\mathscr{O}_L$ is prime. Since $\mathrm{Gal}(L/K)$ has order p, by the Cebotarev Density Theorem, $\mathscr{D}$ has Dirichlet density $(p-1)/p$. Let D be an element of $\mathscr{O}_K$ supported by $\mathscr{D}$. Then, by Theorem 4.3, $\theta^D(\mathsf{H}^1(K, J_D[\lambda])_{S_D}) = \theta(\mathsf{H}^1(K, J[\lambda])_{S_J}) = 1$ and, hence, $\dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(J_D, K) = 0$.

By [Sch98], Corollary 3.7, $\mathrm{rank}\, J_D(K) \leqslant (\ell-1)\dim_{\mathbb{F}_\ell} \mathrm{Sel}^{(\lambda)}(J_D, K) = 0$. Suppose that D is not a unit in $\mathscr{O}_K$, and let $F := K(\sqrt[\ell]{D})$. Then k is algebraically closed in F, and $F \subset K_{\mathrm{sep}}$ since $\ell \neq \mathrm{char}\, K$. Since $(C_D)_F \cong C_F$ as F-schemes, by Proposition 4.25 below, $\# J_D(K)_{\mathrm{Tor}} \leqslant \# E(k)$. Since $J_D(K) = J_D(K)_{\mathrm{Tor}}$, and $C_D(K) \hookrightarrow J_D(K)$, it follows that $\# C_D(K) \leqslant \# J_D(K)_{\mathrm{Tor}} \leqslant \# E(k)$. □

LEMMA 4.23. *(Suppose that M_K^∞ consists of a single place of degree 1.) Let $L := K \otimes k'$ where k' is a finite (separable) extension of k of degree d coprime to ℓ, and suppose that $\mathrm{Cl}(\mathscr{O}_L)[\ell]$ is trivial. Then $\ker\big(\mathrm{N}_{L/K} : L(M_K^\infty, \ell) \to K(M_K^\infty, \ell)\big) = 1$.*

Proof. Since the extension L/K is obtained from base change, M_L^∞ still consists of a single place of degree 1, and L is a function of field of one variable over k'. With $S = M_K^\infty$, $L(M_K^\infty, \ell) \cong \mathscr{O}_L^*/(\mathscr{O}_L^*)^\ell$ since $\mathrm{Cl}(\mathscr{O}_L)[\ell] = 1$. It follows from Proposition 4.24 below that $\mathscr{O}_L^* = (k')^*$. Hence,

$$\ker\big(\mathrm{N}_{L/K} : L(M_K^\infty, \ell) \longrightarrow K(M_K^\infty, \ell)\big) \cong \ker\big(\mathrm{N}_{k'/k} : k'^*/(k'^*)^\ell \longrightarrow k^*/(k^*)^\ell\big). \tag{28}$$

Let a be a positive integer such that $da \equiv 1 \bmod \ell$. Note that there is a section $u : k^*/(k^*)^\ell \to k'^*/(k'^*)^\ell$ to the norm map $\mathrm{N}_{k'/k}$ in (28), given by $\mathrm{class}(\alpha) \mapsto \mathrm{class}(\alpha^a)$. Hence, the norm map $\mathrm{N}_{k'/k}$ is surjective. Since k^* and $(k')^*$ are both cyclic groups of order divisible by ℓ, it follows that $\mathrm{N}_{k'/k}$ is an isomorphism of the $\mathbb{F}_\ell$-vector spaces. Therefore, the kernel is trivial. □

PROPOSITION 4.24. *Let k' be a finite field. Let $\mathscr{X}/k'$ be a smooth complete curve with function field F such that $\mathscr{X}$ has a rational divisor v_∞. Then there is a k'-morphism: $\mathscr{X} \to \mathbb{P}_{k'}^1$ such that v_∞ is totally ramified over a rational divisor in $\mathbb{P}_{k'}^1$.*

Let $\mathscr{O}_F$ be the ring of integers defined in 1.6 with choice of $M_F^\infty := \{v_\infty\}$. Then the group of units $\mathscr{O}_F^*$ is $(k')^*$, and $\# \mathrm{Cl}(\mathscr{O}_F) = \# \mathrm{Pic}^0(\mathscr{X})$. Hence, the class number of $\mathscr{O}_F$ does not depend on the choice of a rational divisor on F.

Proof. Using the Riemann-Roch theorem, we can find a function g in $k'(\mathscr{X})$ with poles supported only by v_∞. Then the function g induces a morphism $\mathscr{X} \to \mathbb{P}_{k'}^1$ such that v_∞ is totally ramified over a rational point $\infty \in \mathbb{P}_{k'}^1$. To finish the proof, use [Lor96], Sec VIII, p. 299-300. □

PROPOSITION 4.25. *Let k be a perfect field, and let K be a field extension of k such that k is algebraically closed in K. Let E/k be a smooth complete geometrically connected curve with a k-rational point.*

Let C'/K be a twist of E_K/K, and suppose that there is a field extension F of K such that k is algebraically closed in F and such that $C'_F \cong E_F$ (as F-schemes). Let J/k be the Jacobian variety of E/k, and let $J_{C'}/K$ be the Jacobian variety of C'/K. Then $J_{C'}(K)_{\mathrm{Tor}} \hookrightarrow J(k)$.

Proof. Note that $J(\overline{k})_{\mathrm{Tor}} = J(\overline{K})_{\mathrm{Tor}} = J(K_{\mathrm{sep}})_{\mathrm{Tor}}$. Then, $J_{C'}(K)_{\mathrm{Tor}} \subset J_{C'}(F)_{\mathrm{Tor}} \cong J_F(F)_{\mathrm{Tor}} \cong J(F)_{\mathrm{Tor}} = J(k)$. $\qquad\square$

5. The Jacobian Varieties With λ-Torsion Points

In this section we prove Theorem 5.5 and its analogue for a function field, introduced in Section 1. Let ℓ be a prime number, and let $K := \mathbb{Q}(\zeta_\ell)$ for which we assume ℓ is regular, or a function field of one variable with a rational divisor v_∞ such that $\#\mathrm{Cl}(\mathscr{O}_K) \not\equiv 0 \bmod \ell$. Let $f(x)$, C/K, C_D/K, J/K, and J_D/K be as in Section 3, and we keep the notation used in that section. Let Δ_f be the discriminant of f. Recall $z_1, \ldots, z_d \in K_{\mathrm{sep}}$, the roots of $f(x)$, and suppose that z_d is contained in K. Recall that $Z(J) := \{T_1, \ldots, T_s\}$ is a set of representatives of G_K-orbits in X, and $L_i := K(T_i)$ for $i = 1, \ldots, s$. Let L be the compositum of $L_1, \ldots, L_s$ in K_{sep}.

5.1. Let us fix a set of generators of $\theta(\mathsf{Sel}^{(\lambda)}(J, K))$, and note that each generator is an s-tuple with entries in L. Let W_J be the union of all entries of the generators. Then W_J is a subset of L^*. For each prime ideal $\mathfrak{q}$ of $\mathscr{O}_K$, choose an element $\alpha_\mathfrak{q}$ of $\mathscr{O}_K$ as in the proof of Theorem 4.8 or Theorem 4.19, depending on the cases of K. Recall $S_J := M_K^\infty \cup \{\mathfrak{q} \in M_K^0 : \mathfrak{q} \mid \ell\Delta_f\mathscr{O}_K\}$, and let

$$Y_J := \{\zeta_\ell, -1\} \cup W_J \cup \{\alpha_\mathfrak{q} \in \mathscr{O}_K : \mathfrak{q} \in S_J \cap M_K^0\}.$$

When $K = \mathbb{Q}(\zeta_\ell)$, let M be the Galois closure of $L(\sqrt[\ell]{\alpha} : \alpha \in Y_J)$ over $\mathbb{Q}$. When K is a function field, let M be the Galois closure of $L(\sqrt[\ell]{\alpha} : \alpha \in Y_J)$ over K.

If $K = \mathbb{Q}(\zeta_\ell)$, let us denote by $\mathscr{D}'_{Y_J}$ the set of prime numbers q in $\mathbb{Z}$ such that q splits completely in $\mathscr{O}_M$ and coprime to α for all $\alpha \in Y_J$. If K is a function field, let us denote by $\mathscr{D}'_{Y_J}$ the set of prime ideals $\mathfrak{q}$ of $\mathscr{O}_K$ such that $\mathfrak{q}$ splits completely in $\mathscr{O}_M$ and coprime to α for all $\alpha \in Y_J$. By the Cebotarev Density Theorem with H being the trivial subgroup of $\mathrm{Gal}(M/\mathbb{Q})$ or $\mathrm{Gal}(M/K)$, depending on both cases of K, the set of prime ideals of $\mathbb{Z}$ or $\mathscr{O}_K$ that split completely in M has positive Dirichlet density. Since there are finitely many prime ideals $\mathfrak{q}$ of $\mathbb{Z}$ or $\mathscr{O}_K$ that are not coprime to α for some $\alpha \in Y_J$, $\mathscr{D}'_{Y_J}$ has positive Dirichlet density.

Recall from 4.17 the definition of $\left(\frac{\bullet}{v_\infty}\right)_\ell$ when K is a function field, and that $\#\mathrm{Cl}(\mathscr{O}_K) \not\equiv 0 \bmod \ell$.

LEMMA 5.2. *Suppose that $K = \mathbb{Q}(\zeta_\ell)$. If D is a positive integer supported by $\mathscr{D}'_{Y_J}$, and $\mathfrak{q}$ is a place in S_J, then $\left(\frac{D}{\mathfrak{q}}\right)_\ell = 1$.*

Suppose that K is a function field. Let D be a monic element of $\mathscr{O}_K$, of degree divisible by ℓ supported by $\mathscr{D}'_{Y_J}$. If $\mathfrak{q}$ is a place in S_J, then $\left(\frac{D}{\mathfrak{q}}\right)_\ell = 1$.

Proof. The proof is identical with those of Lemma 4.7 and 4.18. $\qquad\square$

PROPOSITION 5.3. *Suppose that $K = \mathbb{Q}(\zeta_\ell)$. Let D be a positive ℓ-th power free integer in $\mathbb{Z}$ which is supported by $\mathscr{D}'_{Y_J}$. Then*

$$\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) > \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J, K). \tag{29}$$

Suppose that K is a function field. Let D be a monic element of $\mathscr{O}_K \setminus \{0\}$ of degree divisible by ℓ such that $D\mathscr{O}_K$ is not an ℓ-th power of an ideal and D is supported by $\mathscr{D}'_{Y_J}$. Then

$$\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) > \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J, K). \tag{30}$$

For both cases of K, $\limsup_D \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) = \infty$.

Proof. Let D be a positive ℓ-th power free integer in $\mathbb{Z}$ which is supported by $\mathscr{D}'_{Y_J}$ or a monic element D of $\mathscr{O}_K$ of degree divisible by ℓ supported by $\mathscr{D}'_{Y_J}$. Let $S_D := S_J \cup \{\mathfrak{q} \in M_K^0 : \mathfrak{q} \mid D\mathscr{O}_K\}$. Then,

$$\theta(\mathsf{H}^1(K, J[\lambda])_{S_J}) = \prod_{i=1}^s L_i(S_J, \ell), \quad \theta^D(\mathsf{H}^1(K, J_D[\lambda])_{S_D}) = \prod_{i=1}^s L_i(S_D, \ell).$$

By 3.7,

$$\theta(\mathsf{Sel}^{(\lambda)}(J, K)) = \{\alpha \in \theta\big(\mathsf{H}^1(K, J[\lambda])_{S_J}\big) : \mathrm{res}_{\mathfrak{q}}(\alpha) \in \mathrm{Im}\,\theta_{\mathfrak{q}}\delta_{\mathfrak{q}} \text{ for all } \mathfrak{q} \in S_J\};$$
$$\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K)) = \{\alpha \in \theta^D\big(\mathsf{H}^1(K, J_D[\lambda])_{S_D}\big) : \mathrm{res}_{\mathfrak{q}}(\alpha) \in \mathrm{Im}\,\theta_{\mathfrak{q}}^D\delta_{\mathfrak{q}}^D \text{ for all } \mathfrak{q} \in S_D\}. \tag{31}$$

Let us show that $\theta(\mathsf{Sel}^{(\lambda)}(J, K)) \subset \theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K))$. Let α be an element of $\theta(\mathsf{Sel}^{(\lambda)}(J, K))$. Then $\alpha \in \prod_{i=1}^s L_i(S_J, \ell)$. Since S_J is contained in S_D, we have $\alpha \in \theta^D\big(\mathsf{H}^1(K, J_D[\lambda])_{S_D}\big) = \prod_{i=1}^s L_i(S_D, \ell)$. If $\mathfrak{q}$ is a place in S_J, then by Lemma 5.2, D is an ℓ-th power in $K_{\mathfrak{q}}$. By Proposition 3.5, $\mathrm{Im}\,\theta_{\mathfrak{q}}^D\delta_{\mathfrak{q}}^D = \mathrm{Im}\,\theta_{\mathfrak{q}}\delta_{\mathfrak{q}}$ and, hence, $\alpha \in \mathrm{Im}\,\theta_{\mathfrak{q}}^D\delta_{\mathfrak{q}}^D$. Let $\mathfrak{q}$ be a prime ideal in $S_D \setminus S_J$. Then $\mathfrak{q} \mid D$ and, hence, $\mathfrak{q} \in \mathscr{D}'_{Y_J}$. Suppose that α is represented by $(\beta_1, \ldots, \beta_s)$ for some $\beta_i \in \mathscr{O}_L$. Then, since Y_J contains W_J defined in 5.1, and all $\sqrt[\ell]{\beta_i}$ are defined over $K_{\mathfrak{q}}$, it follows $\mathrm{res}_{\mathfrak{q}}(\alpha) = 1 \in \mathscr{C}_{\mathfrak{q}}$ and, in particular, $\mathrm{res}_{\mathfrak{q}}(\alpha) \in \mathrm{Im}\,\theta_{\mathfrak{q}}^D\delta_{\mathfrak{q}}^D$. Therefore, by (31), α is contained in $\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K))$.

Note that $\theta(\mathsf{Sel}^{(\lambda)}(J, K)) \subset \prod_{i=1}^s L_i(S_J, \ell)$. Lemma 5.4 below shows that there is an element α of $\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K))$ which is contained in $\prod_{i=1}^s L_i(S_D, \ell) \setminus \prod_{i=1}^s L_i(S_J, \ell)$. Therefore, $\alpha \notin \theta(\mathsf{Sel}^{(\lambda)}(J, K))$, and we proved that $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) > \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J, K)$.

If K is a function field, then as illustrated in 4.21, there is a monic element D of $\mathscr{O}_K$ of degree divisible by ℓ such that $D\mathscr{O}_K$ is not an ℓ-th power of an ideal and D is supported by $\mathscr{D}'_{Y_J}$. Using induction, one can easily show that $\limsup_D \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) = \infty$. $\qquad\square$

Recall that $P_d^D := [(z_d D, 0) - (\infty)]$ is a point in $J_D[\lambda](K_{\mathrm{sep}})$ but $P_d^D \notin X^D$.

LEMMA 5.4. *Let D be an ℓ-th power free positive integer supported by $\mathscr{D}'_{Y_J}$, or a monic element of $\mathscr{O}_K$ supported by $\mathscr{D}'_{Y_J}$ such that $D\mathscr{O}_K$ is not an ℓ-th power of an ideal. Consider the map*

$$\theta^D\delta^D : J_D(K)/\lambda J_D(K) \longrightarrow \mathscr{C} := \prod_{i=1}^s L_i^*/(L_i^*)^\ell.$$

Then the K-rational point $P_d^D \in J_D[\lambda](K)$ is mapped to $\prod L_i(S_D, \ell) \setminus \prod L_i(S_J, \ell)$ under $\theta^D\delta^D$.

Proof. Since D is supported by $\mathscr{D}'_{Y_J}$, D is coprime to Δ_f and to all prime ideals $\mathfrak{q} \in S_J$. Recall that $P_i^D := [(z_i D, 0) - (\infty)]$ for $i = 1, \ldots, d$. Since $P_d^D := [(z_d D, 0) - (\infty)]$ is a point in $J_D(K)$, by Lemma 2.6,

$$\theta^D(\delta^D(P_d^D)) = (f_{P^D}(z_d D, 0) : P \in Z(J)) = (z_d D - D\,x(P) : P \in Z(J))$$
$$= (D(x(P_d) - x(P)) : P \in Z(J)). \tag{32}$$

Note that for all $P \in Z(J)$, the difference $x(P_d) - x(P)$ divides Δ_f and hence, it is coprime to D. Since $D\mathscr{O}_K$ is not an ℓ-th power of an ideal, it follows that $D\big(x(P_d) - x(T_i)\big) \in L_i(S_D, \ell) \setminus L_i(S_J, \ell)$ for all $i = 1, \ldots, s$. $\qquad\square$

THEOREM 5.5. *Suppose that $K = \mathbb{Q}(\zeta_\ell)$. Given a positive integer n, there is a positive constant $\varepsilon < 1$ depending on C and n such that*

$$\#\{D \in \mathscr{P}_\ell(X) : \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) > n\} \gg \frac{X}{(\log X)^\varepsilon}. \tag{33}$$

Proof. By Proposition 5.3, there is a positive ℓ-th power-free rational integer D_0 such that $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0}, K) > n$. Proposition 5.3 applied to $J = J_{D_0}$ and Lemma 4.9 together imply (33). $\qquad\square$

THEOREM 5.6. *Suppose that K is a function field. Given a positive integer n, there are $D_0 \in \mathscr{O}_K$ and a set of prime ideals $\mathscr{D}$ of $\mathscr{O}_K$ with positive Dirichlet density such that whenever D is a monic element of $\mathscr{O}_K$ of degree divisible by ℓ such that $D\mathscr{O}_K$ is not an ℓ-th power of an ideal and D is supported by $\mathscr{D}$,*

$$\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0 D}, K) > n. \tag{34}$$

Proof. By 4.21 and Proposition 5.3, there is D_0 such that $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0}, K) > n$. Then, by Proposition 5.3 applied to J_{D_0}, we prove the result. $\square$

COROLLARY 5.7. *Let $K = \mathbb{Q}(\zeta_\ell)$ where ℓ is an odd regular prime number. Let F_D/K be the Fermat curve given by $x^\ell + y^\ell = Dz^\ell$ where $D \in \mathbb{Z}$ is nonzero, and let $\mathrm{Jac}(F_D)/K$ be the Jacobian variety of F_D/K. Let ζ_ℓ denote the automorphism of order ℓ on F_D given by $x \mapsto x$, $y \mapsto y$, and $z \mapsto z\zeta_\ell$. Let λ be the endomorphism $1 - [\zeta_\ell]$ on $\mathrm{Jac}(F_D)$ where $[\zeta_\ell]$ denotes the automorphism on $\mathrm{Jac}(F_D)$ induced by the automorphism on F_D. Then $\limsup_D \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(\mathrm{Jac}(F_D), K) = \infty$.*

Proof. Let C_D be the curve given by the homogeneous equation

$$D z^\ell = \sum_{k=0}^{(\ell-1)/2} x^{\ell-2k} y^{2k} \binom{\ell}{2k} (2\ell)^{(\ell-1-2k)a} \ell^{-1} \tag{35}$$

where a and b are integers such that $a > 0$ and $(\ell - 1)a + \ell b = 1$. Then we have the isomorphism $F_D \to C_D$ given by

$$(x : y : z) \mapsto (x + y : (2\ell)^a (x - y) : 2^{1-b} \ell^{-b} z).$$

Dehomogenized with respect to x, the equation (35) is written $Dz^\ell = f(y)$ for some monic polynomial $f(y)$ of degree $\ell - 1$, defined over $\mathbb{Z}$. Note that the K-rational points $(\zeta_\ell^s : -\zeta_\ell : 0)$ in F_D for $1 < s \leqslant \ell$ are mapped to the K-rational points

$$\left(1 : (2\ell)^a \cdot \frac{\zeta_\ell^s + \zeta_\ell}{\zeta_\ell^s - \zeta_\ell} : 0 \right) \in C_D \text{ for } 1 < s \leqslant \ell.$$

Thus, $f(y)$ has $(\ell - 1)$ K-rational roots, and Corollary 5.7 follows from Theorem 5.5. $\square$

6. The General Reciprocity Laws

The general reciprocity law is used in this paper to show the existence of infinitely many prime numbers or ideals satisfying a set of conditions under which we are able to control the size of the Selmer groups. We recall it below.

Let K be a number field or a function field of one variable with a rational divisor v_∞ such that K contains a primitive n-th root of unity. Let $\mathfrak{p}$ be a place in M_K^0. For a non-archimedean place $\mathfrak{p}$, we have the Hilbert norm residue symbol which is nondegenerate, and bilinear:

$$\left(\frac{\bullet, \bullet}{\mathfrak{p}} \right)_n : K_{\mathfrak{p}}^* / (K_{\mathfrak{p}}^*)^n \times K_{\mathfrak{p}}^* / (K_{\mathfrak{p}}^*)^n \longrightarrow \mu_n.$$

The norm residue symbol extends for an archimedean place v of K in an obvious way.

Let F be a global field. Let $\mathfrak{p}$ be a prime ideal of $\mathscr{O}_F$, and $\alpha \in \mathscr{O}_F$ such that $\mathfrak{p}$, $\alpha\mathscr{O}_F$, and $n\mathscr{O}_F$ are pairwise coprime. We define

$$\left(\frac{\alpha}{\mathfrak{p}} \right)_n := \zeta_n^j \text{ for some } j \text{ such that } \zeta_n^j \equiv \alpha^{((\#\mathscr{O}_F/\mathfrak{p})-1)/n} \bmod \mathfrak{p}.$$

Note that $\left(\frac{\alpha}{\mathfrak{p}} \right)_n = 1$ if and only if $x^n - \alpha$ has a root mod $\mathfrak{p}$, (provided that $\alpha \not\equiv 0 \bmod \mathfrak{p}$).

If $\beta \in \mathscr{O}_F$ is coprime to n and α, we extend the power residue symbol as follows: let $\beta \mathscr{O}_F = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}$ be the prime ideal decomposition.

$$\left(\frac{\alpha}{\beta}\right)_n := \prod_{i=1}^{t} \left(\frac{\alpha}{\mathfrak{p}_i}\right)_n^{a_i}.$$

6.1. Let ℓ be a prime number. Let K be a number field containing ζ_ℓ. For an archimedean place $v \in M_K^\infty$, and for a prime ideal $\mathfrak{p}$ of $\mathscr{O}_K$ which divides $\ell \mathscr{O}_K$, we extend the symbol as follows only for convenience: Let $e := \mathrm{ord}_\mathfrak{p}(\ell \mathscr{O}_K)$, and let m be the smallest integer which is (strictly) greater than $e\ell/(\ell-1)$.

$$\left(\frac{\alpha}{v}\right)_\ell := \begin{cases} 1 & \text{if } x^\ell - \alpha = 0 \text{ is solvable over } K_v \text{ ,} \\ -1 & \text{if } x^\ell - \alpha = 0 \text{ is not solvable over } K_v \text{ ,} \\ 0 & \text{if } \alpha = 0 \end{cases}$$

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell := \begin{cases} 1 & \text{if } \alpha \equiv a^\ell \bmod \mathfrak{p}^m \text{ for some } a \not\equiv 0 \bmod \mathfrak{p}, \\ -1 & \text{if } \alpha \not\equiv a^\ell \bmod \mathfrak{p}^m \text{ for all } a \not\equiv 0 \bmod \mathfrak{p} \\ 0 & \text{if } \alpha \equiv 0 \bmod \mathfrak{p} \end{cases} .$$

THEOREM 6.2. (THE GENERAL RECIPROCITY LAW) *Let K be a number field or a function field of one variable with a rational divisor v_∞. Suppose that K contains a primitive n-th root of unity where $n \geqslant 2$ is a positive integer coprime to $\mathrm{char}\,K$.*

Let α and β be non-zero elements of $\mathscr{O}_K$ coprime to each other and to n. Then

$$\left(\frac{\alpha}{\beta}\right)_n \cdot \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p} \in S_\infty} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n$$

where $S_\infty := \{v \in M_K : v \mid n \text{ or } v \in M_K^\infty\}$.

Proof. See [Neu99], Theorem 8.3, p.415, or [Tat], p. 352 $\qquad \square$

LEMMA 6.3. *Let ℓ be a prime number. Let q be a rational prime coprime to ℓ, and let K be the ℓ-th cyclotomic extension of $\mathbb{Q}$. Let $\lambda := 1 - \zeta_\ell$. Let $\mathfrak{p}$ be a prime ideal of $\mathscr{O}_K$ lying over q. Suppose that ℓ is odd. If $\left(\frac{\zeta_\ell}{\mathfrak{p}}\right)_\ell = 1$, then $q \equiv a^\ell \bmod \ell^2$ for some $a \in \mathbb{Z}$, and $\left(\frac{q}{\lambda \mathscr{O}_K}\right)_\ell = 1$.*

Suppose that $\ell = 2$, i.e., $K = \mathbb{Q}$. If q is an odd prime such that $\left(\frac{-1}{q}\right)_\ell = \left(\frac{2}{q}\right)_\ell = 1$, then $\left(\frac{q}{2\mathbb{Z}}\right)_\ell = 1$.

Proof. Suppose that ℓ is odd, and $\left(\frac{\zeta_\ell}{\mathfrak{p}}\right)_\ell = 1$. By definition,

$$1 = \left(\frac{\zeta_\ell}{\mathfrak{p}}\right)_\ell = \zeta_\ell^{(q^m-1)/\ell} \text{ where } m \text{ is the residue degree of } \mathfrak{p} \text{ over } q.$$

Hence, $(q^m - 1)/\ell \equiv 0 \bmod \ell$, i.e., $q^m \equiv 1 \bmod \ell^2$. Note that $K/\mathbb{Q}$ being Galois implies that $m \mid (\ell - 1)$ and, hence, $(m, \ell) = 1$. Then there are integers a and b such that $am + b\ell = 1$. It follows that $q = q^{am+b\ell} \equiv (q^b)^\ell \bmod \ell^2$. By definition,

$$\left(\frac{q}{\lambda \mathscr{O}_K}\right)_\ell = 1 \text{ if and only if } q \equiv \gamma^\ell \bmod \lambda^{\ell+1} \text{ for some } \gamma \in \mathscr{O}_K.$$

Since $\ell \mathscr{O}_K = \lambda^{\ell-1} \mathscr{O}_K$, we have $q \equiv (q^b)^\ell \bmod \lambda^{2(\ell-1)} \mathscr{O}_K$. Hence, if $\ell \geqslant 3$, then $2(\ell - 1) \geqslant \ell + 1$ and, hence, $\left(\frac{q}{\lambda \mathscr{O}_K}\right)_\ell = 1$.

Suppose that $\ell = 2$. Then $\zeta_\ell = -1$. By the supplementary quadratic reciprocity laws, $1 = \left(\frac{-1}{q}\right)_\ell = (-1)^{(q-1)/2}$ and $1 = \left(\frac{2}{q}\right)_\ell = (-1)^{(q^2-1)/8}$ and, hence, $q \equiv 1 \bmod 4$, and $q^2 \equiv 1 \bmod 16$. It follows that $q \equiv 1 \bmod 8$. If $q \equiv 1 \bmod 8$, then $\left(\frac{q}{2\mathbb{Z}}\right)_\ell = 1$. $\qquad \square$

COROLLARY 6.4. *If a is a positive rational integer coprime to ℓ such that $\left(\frac{a}{\lambda \mathscr{O}_K}\right)_\ell = 1$, then*

$$\left(\frac{a}{\alpha}\right)_\ell = \left(\frac{\alpha}{a}\right)_\ell$$

for all $\alpha \in \mathscr{O}_K$ coprime to $a\ell$.

Proof. Since $\left(\frac{a}{\lambda \mathscr{O}_K}\right)_\ell = 1$, by definition, it implies that $a \in (K_\lambda^*)^\ell$ and, hence, the Hilbert residue symbol $\left(\frac{\alpha,a}{\lambda}\right)_\ell = 1$. If $\ell = 2$, then there is an infinite place v for which $K_v \cong \mathbb{R}$. Since $a \in (\mathbb{R}^*)^2$, $\left(\frac{\alpha,a}{v}\right)_\ell = 1$. If $\ell \geqslant 3$, then the Hilbert residue symbol is trivial at all infinite places. Therefore, $\prod_{\mathfrak{q}|\ell\infty} \left(\frac{\alpha,a}{\mathfrak{q}}\right)_\ell = 1$ and, hence, the assertion follows from Theorem 6.2. $\qquad\square$

Let k be a finite field of characteristic q, and let K/k be a function field of one variable with a rational divisor v_∞ (with $M_K^\infty = \{v_\infty\}$). Let π_∞ be a uniformizer of the discrete valuation ring $\mathscr{O}_\infty$ of K at v_∞, and let $\mathrm{ord}_\infty := \mathrm{ord}_{v_\infty}$. Recall that a nonzero element $\alpha \in \mathscr{O}_K$ is *monic* (with respect to π_∞) if $\pi_\infty^m \alpha \equiv 1 \bmod \pi_\infty$ for some integer $m \in \mathbb{Z}$.

THEOREM 6.5. (THE GENERAL RECIPROCITY LAW FOR FUNCTION FIELDS) *Let q be a prime number, and let n be a positive integer not divisible by q. Let k be a finite field with q^r elements such that k contains a primitive n-th root of unity. Let K/k be a function field of one variable with a rational divisor v_∞.*

If g and h are monic distinct elements of $\mathscr{O}_K$ such that g is coprime to h, then

$$\left(\frac{-1}{g}\right)_n = (-1)^{\left((q^r-1)/n\right)\cdot\,\mathrm{ord}_\infty(g)};$$

$$\left(\frac{g}{h}\right)_n \left(\frac{h}{g}\right)_n^{-1} = (-1)^{\left((q^r-1)/n\right)\cdot\,\mathrm{ord}_\infty(g)\,\mathrm{ord}_\infty(h)}.$$

Proof. Let K_{v_∞} be the completion of K at v_∞. Let $\widehat{\mathscr{O}}_\infty := \{\alpha \in K_{v_\infty} : |\alpha|_{v_\infty} \leqslant 1\}$, and $\widehat{\mathfrak{M}}_\infty := \{\alpha \in \widehat{\mathscr{O}}_\infty : |\alpha|_{v_\infty} < 1\}$. Since $\deg(v_\infty) = 1$, let us define $\omega : \widehat{\mathscr{O}}_\infty^* \to k^*$ by $\alpha \mapsto a$ such that $\alpha \equiv a \bmod \widehat{\mathfrak{M}}_\infty$. By [Neu99], Chapter V, Sec 3, Proposition 3.4, for nonzero elements α and β in $\mathscr{O}_K$,

$$\left(\frac{\alpha,\beta}{v_\infty}\right)_n = \omega\left((-1)^{\mathrm{ord}_\infty(\alpha)\,\mathrm{ord}_\infty(\beta)}\frac{\beta^{\mathrm{ord}_\infty(\alpha)}}{\alpha^{\mathrm{ord}_\infty(\beta)}}\right)^{(q^r-1)/n}. \tag{36}$$

Let $\pi_\infty \in K^*$ be a uniformizer of K_{v_∞}. Let g and h be monic distinct elements of $\mathscr{O}_K$ coprime to each other. Then, by Theorem 6.2,

$$\left(\frac{-1}{g}\right)_n = \left(\frac{-1,g}{v_\infty}\right)_n = \omega\left((-1)^{\mathrm{ord}_\infty(g)}\right)^{(q^r-1)/n} = (-1)^{\mathrm{ord}_\infty(g)\,(q^r-1)/n}.$$

Since g and h are monic, there are a and b in $\widehat{\mathscr{O}}_\infty^*$ such that $a \equiv b \equiv 1 \bmod \widehat{\mathfrak{M}}_\infty$, $g = a\pi_\infty^{\mathrm{ord}_\infty(g)}$, and $h = b\pi_\infty^{\mathrm{ord}_\infty(h)}$. It follows from Hensel's lemma that a and b are contained in $(K_{v_\infty}^*)^n$. Then, by Theorem 6.2,

$$\left(\frac{g}{h}\right)_n \left(\frac{h}{g}\right)_n^{-1} = \left(\frac{\pi_\infty,\pi_\infty}{v_\infty}\right)_n^{\mathrm{ord}_\infty(g)\,\mathrm{ord}_\infty(h)}.$$

By (36),

$$\left(\frac{\pi_\infty,\pi_\infty}{v_\infty}\right)_n = (-1)^{(q^r-1)/n}.$$

$\qquad\square$

LEMMA 6.6. *If g is a monic element of $\mathscr{O}_K$ such that $\left(\frac{-1}{g}\right)_n = 1$, then for all monic elements h of $\mathscr{O}_K$ coprime to g,*

$$\left(\frac{h}{g}\right)_n = \left(\frac{g}{h}\right)_n.$$

Proof. The condition: $\left(\frac{-1}{g}\right)_n = 1$ implies that $\mathrm{ord}_\infty(g) \cdot (q^r - 1)/n \equiv 0 \bmod 2$ and, hence, $\mathrm{ord}_\infty(h)\,\mathrm{ord}_\infty(g) \cdot (q^r - 1)/n \equiv 0 \bmod 2$. By Theorem 6.5, we proved the lemma. $\qquad\square$

LEMMA 6.7. *Let α be an element of $\mathscr{O}_K$, and let $\mathfrak{p} \in M_K$. Then $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell = 1$ implies that $\alpha \in (K_\mathfrak{p}^*)^\ell$.*

Proof. The only non-trivial case is that $\mathfrak{p} \mid \ell$. Suppose that $\mathfrak{p}$ is a prime ideal of $\mathscr{O}_K$ such that $\mathfrak{p} \mid \ell$ and $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell = 1$. Let m be an integer $> e\ell/(\ell - 1)$ where $e := \mathrm{ord}_\mathfrak{p}(\ell\mathscr{O}_K)$. Then $\alpha \equiv a^\ell \bmod \mathfrak{p}^m$ for some $a \in \mathscr{O}_K$ implies that $\alpha \in (K_\mathfrak{p}^*)^\ell$. $\qquad\square$

ACKNOWLEDGEMENTS

REFERENCES

Ata01   D. Atake, *On elliptic curves with large Tate-Shafarevich Groups*, J. Number Theory **87** (2001), 282–300.

Cha   S. Chang, *Note on the rank of quadratic twists of Mordell equations,* to appear in J. Number Theory.

CJB97   L. Caporaso, J. Harris, and B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), 1–35.

HB94   D.R. Heath-Brown, *The size of Selmer groups for the congruent number problem II*, Invent. Math. **118** (1994), 331–370.

IP00   H. Iwaniec and P. Sarnak, *The non-vanishing of central values of automorphic L-functions and Landau-Siegel zeros*, Israel J. Math **120** (2000), 155–177.

Kol88   V.A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $\mathrm{III}(E, \mathbb{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Serl. Mat. **52** (1988), 1154–1180.

Lem   F. Lemmermeyer, *On Tate-Shafarevich groups of some elliptic curves*, in "Proc. Conf., Graz", 1998.

Lie94   D. Lieman, *Non-vanishing of L-series associated to cubic twists of elliptic curves*, Ann. of Math. **140** (1994), 181–108.

Lor96   D. Lorenzini, *Invitation to Arithmetic Geometry*, AMS, 1996.

LT02   D. Lorenzini and T. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), 47–77.

Maz86   B. Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. **14** (1986), 207–260.

Neu99   J. Neukirch, *Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg, 1999.

OC98   K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), 651–660.

PE97   B. Poonen and E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. reine angew. Math. **488** (1997), 141–188.

Sch90   C. Schoen, *Bounds for rational points on twists of constant hyperelliptic curves*, J. reine angew. Math. **411** (1990), 196–204.

Sch98   E Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), 447–471.

Ser76   J.P. Serre, *Divisibilité de certaines fonctions arithmétiques,* Enseign. Math. **22** (1976), 227–260, Enseign. Math. **22** (1976), 227–260.

Sil93   J. Silverman, *A uniform bound for rational points on twists of a given curve*, J. London Math. Soc (2) **47** (1993), 385–394.

Sto   M. Stoll, *Independence of rational points on twists of a given curve,* submitted.

Sto98 _____, *On the arithmetic of the curves $y^2 = x^\ell + A$ and their Jacobians*, J. reine angew. Math. **501** (1998), 171–189.

Tat   J. Tate, *Fourier analysis in number fields and Hecke's Zeta-functions,* In: J.W.S. Cassels and A. Fröhlich (eds): Algebraic Number Theory, Academic Press 1967 .

Vat98 V. Vatsal, *Rank-one twists of a certain elliptic curve*, Math. Ann. **311** (1998), 791–794.

Won99 S. Wong, *Elliptic curves and class number divisibility*, Internat. Math. Res. Notices **12** (1999), 661–672.

Yu03   G. Yu, *Rank* 0 *quadratic twists of a family of elliptic curves*, Compositio Math. **135** (2003), 331–356.

Sungkon Chang   changsun@mail.armstrong.edu
Department of Mathematics, Armstrong Atlantic State University , 11935 Abercorn St , Savannah, GA 31419