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 \( n \geq 2 \) 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 \( \ell \) be a prime number different from \( \text{char} \ K \). 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 \( \ell \)-th power twist of \( J \). For the case of hyperelliptic curves (where \( \ell = 2 \), the plane curve \( Dy^2 = f(x) \)

2000 Mathematics Subject Classification

14H45

Keywords: Twists, Superelliptic curves, Mordell-Weil rank
In [Cha], we computed an upper bound for a certain average of \( \text{dim } \lambda \). Let \( f \) 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 \( N := \dim \mathcal{F}_r \text{Sel}^{(\lambda)}(J_{D_0}, K) \), and let \( M \) be the number of prime ideals of \( \mathcal{O}_K \) dividing \( \Delta_f D_0 \). Then there is a set \( \mathcal{D} \) of prime numbers with Dirichlet density at least \( (p - 1)/(\ell^{(N+M+1)} p^\ell (\ell - 1) p!) \) such that whenever a positive integer \( D \) is supported by \( \mathcal{D} \),

\[
\dim \mathcal{F}_r \text{Sel}^{(\lambda)}(J_{D_0 D}, K) = N.
\]

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

\[
\# \{ D \in \mathcal{D}_r(X) : \dim \mathcal{F}_r \text{Sel}^{(\lambda)}(J_D, K) = N \} \gg_{D_0} X / (\log X)^\varepsilon.
\]

This theorem is proved using Schaefer’s description of the \( \lambda \)-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 \( E/Q \) given by \( y^2 = x^3 - x \). For example, given a positive integer \( n \), he computes explicitly

\[
\lim_{X \to \infty} \frac{\# \{ D \in T(X) : \dim \mathcal{F}_r \text{Sel}^{(2)}(E_D, Q) = n, D \equiv 1 \bmod 8 \}}{\# \{ D \in T(X) : D \equiv 1 \bmod 8 \}}.
\]

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

\[
\liminf_{X \to \infty} \frac{\# \{ D \in T(X) : \dim \mathcal{F}_r \text{Sel}^{(\lambda)}(E_D, K) \leq 2n, D \equiv 1 \bmod 12A \}}{\# \{ D \in T(X) : D \equiv 1 \bmod 12A \}}.
\]

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 \( \ell \)-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

\[
\# \{ D \in \mathcal{D}_r(X) : \text{rank} J_D(Q) \leq N \} \gg_{D_0} X / (\log X)^\varepsilon.
\]
ON THE ARITHMETIC OF TWISTS OF SUPERELLIPTIC CURVES

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

**Theorem 5.5** Let \( K \) denote the \( \ell \)-th cyclotomic field extension \( \mathbb{Q}(\zeta_\ell) \) where \( \ell \) 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
\[
\# \{ D \in \mathcal{P}_\ell(X) : \dim \mathbb{F}_\varepsilon \text{Sel}^{(\lambda)}(J_{D,K}) > n \} \gg_{C,n} X^{\frac{1}{\log X^\varepsilon}}.
\]

In particular, \( \limsup_{D} \dim \mathbb{F}_\varepsilon \text{Sel}^{(\lambda)}(J_{D,K}) = \infty \).

Recall that for \( D \in \mathbb{Q}^* \), \( \text{Sel}^{(2)}(J_D, \mathbb{Q}) \cong J_D(\mathbb{Q})/2J_D(\mathbb{Q}) \oplus \text{III}(J_D, \mathbb{Q})[2] \) where \( \text{III}(J_D, \mathbb{Q}) \) is the Tate-Shafarevich group of quadratic twists of the elliptic curves considered in Corollary 4.11 has an \( \ell \)-Selmer rank 0, then the \( \ell \)-th power twists with Mordell-Weil rank 0. 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 \( \gamma \) depending on \( C \), and in terms of the Mordell-Weil rank of the Jacobian variety \( J_D \), namely,
\[
\#C_D(K) < \gamma^{7\text{rank}_{J_D}(K)}.
\]

**Corollary 5.7** Let \( K \) denote the \( \ell \)-th cyclotomic field extension \( \mathbb{Q}(\zeta_\ell) \) where \( \ell \) 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 \( \text{Jac}(F_D) \) be the Jacobian variety of \( F_D/K \). Let \( \zeta_\ell \) denote the automorphism of order \( \ell \) on \( F_D \) given by \( x \mapsto x \), \( y \mapsto y \), and \( z \mapsto z \zeta_\ell \). Let \( \lambda \) be the endomorphism \( 1 - [\zeta_\ell] \) on \( \text{Jac}(F_D) \) where \( [\zeta_\ell] \) denotes the automorphism on \( \text{Jac}(F_D) \) induced by the automorphism on \( F_D \). Then
\[
\limsup_{D} \dim \mathbb{F}_\varepsilon \text{Sel}^{(\lambda)}(\text{Jac}(F_D), K) = \infty.
\]

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 \( \gamma \) depending on \( C \), and in terms of the Mordell-Weil rank of the Jacobian variety \( J_D \), namely,
\[
\#C_D(K) < \gamma^{7\text{rank}_{J_D}(K)}.
\]

**Corollary 1.2.** Let \( C \) be the normalization of a superelliptic curve considered in Theorem 4.10. Let \( N := \dim \mathbb{F}_\varepsilon \text{Sel}^{(\lambda)}(J_{D_0}, K) \) for a nonzero positive integer \( D_0 \). If the genus of \( C \) is \( > 1 \), then there are positive constants \( \varepsilon < 1 \), and \( \gamma \) depending on \( C \) and \( D_0 \) such that
\[
\# \{ D \in \mathcal{P}_\ell(X) : \# C_{D}(\mathbb{Q}) \leq \gamma^N \} \gg X^{\frac{1}{\log X^\varepsilon}}.
\]

**Proof.** The proof is left to the reader. \( \square \)

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 \( p \geq 5 \). Suppose that there is a positive integer \( D_0 \) such that \( N := \dim \mathbb{F}_\varepsilon \text{Sel}^{(2)}(J_{D_0}, \mathbb{Q}) < (p - 1)/2 \). Then there is a positive constant \( \varepsilon < 1 \) depending on \( C \) and
Assuming the Riemann Hypothesis, Iwaniek and Sarnak proved in [IP00] that the question of Silverman for these elliptic curves be the elliptic curve many quadratic twists infinitely many elliptic curves over integer such that let positive integer /E. In particular, there are infinitely many prime numbers p such that rankE_p(Q) = 0.

Proof. The proof is left to the reader.

In [OC98], Corollary 3, Ono and Skinner proved that the question of Silverman has a positive answer for all elliptic curves with conductor \( \leq 100 \). 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 given by \( y^2 = x^3 - 2 \). Then, \( \dim \mathbb{F}_2 \text{Sel}^2(E, \mathbb{Q}) = 0 \) and, by Theorem 4.10, there are infinitely many quadratic twists \( E_D \) with \( \dim \mathbb{F}_2 \text{Sel}^2(E_D, \mathbb{Q}) = 0 \). 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 \( E = X_0(19) \),
\[
\# \{ |D| < X : \text{rank} E_D(Q) = 1 \} \gg X.
\]
Assuming the Riemann Hypothesis, Iwaniek and Sarnak proved in [IP00] that \( \# \{ |D| < X : \text{rank} E_D(Q) = 1 \} \gg E \) 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 \( E/Q \) be an elliptic curve without \( \mathbb{Q} \)-rational 2-torsion points such that \( \dim \mathbb{F}_2 \text{Sel}^2(E_{D_0}, \mathbb{Q}) = 1 \) for some positive integer \( D_0 \). Then there is a positive constant \( \varepsilon < 1 \) such that
\[
\# \{ D \in \mathcal{P}_2(X) : \text{rank} E_D(Q) = 1, \text{III}(E_D, \mathbb{Q})[2] = \{0\} \} \gg_{E, D_0} \frac{X}{(\log X)^{\varepsilon}}.
\]

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

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 [Lye94], 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 \( D \equiv c \mod p \) and \( \text{rank} E_D(Q) = 0 \).

**Corollary 4.13.** Let \( E/Q \) 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 mod 36 and \( \dim \mathbb{F}_3 \text{Cl}(\mathbb{Q}(\sqrt{-A}))[3] = 0 \). For a non-zero cube-free integer \( D \), let \( E_D \) be the cubic twist: \( y^2 = x^3 - AD^3 \). Then there is a positive integer \( \varepsilon < 1 \) such that
\[
\# \{ D \in \mathcal{P}_3(X) : \text{rank} E_D(Q) = 0 \} \gg \frac{X}{(\log X)^{\varepsilon}}.
\]

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 \( v_{\infty} \) is a function field \( K \) of one variable over a finite field \( k \) with a non-archimedean absolute value \( v_{\infty} \) on \( K/k \) of degree 1. Such function fields correspond to smooth complete curves \( \mathcal{Z} \) over \( k \) with a \( k \)-rational point \( p_{\infty} \) corresponding to the absolute value \( v_{\infty} \). For this type of function
For these curves, the number of rational points of their quadratic twists can be arbitrarily large.

Let \( \ell \) be a prime number, and let \( k \) be a finite field containing a primitive \( \ell \)-th root of unity. Hence, \( \text{char } k \neq \ell \). Let \( K \) be a function field of one variable with a rational divisor \( v_0 \), and let \( \mathcal{Z}/k \) 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 \((\lambda-)\) 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 \( p \neq \text{char } k \). Let \( L := K \otimes k' \), and let \( \bar{\mathcal{O}}_L \) be the integral closure of \( \mathcal{O}_K \) in \( L \).

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

\[
\dim \overline{\mathcal{O}} \text{Sel}(\lambda)(J_D,K) = 0, \quad \text{and} \quad \# C_D(K) \leq \# A(k).
\]

The hypothesis in Theorem 4.22 is often satisfied. Let \( K \) be a function field of one variable with a rational divisor \( v_0 \), and let \( \mathcal{Z}/k \) be the smooth curve with function field \( K \). Then, by Proposition 4.24

\[
\# \text{Cl}(\bar{\mathcal{O}}_L) = \# \text{Pic}^0(\mathcal{Z}/k).
\]

Let \( L := K \otimes k' \) for a finite extension \( k' \) of \( k \), and let \( \bar{\mathcal{O}}_L \) be the integral closure of \( \mathcal{O}_K \) in \( L \). Then \( \# \text{Cl}(\bar{\mathcal{O}}_L) = \# \text{Pic}^0(\mathcal{Z}/k') \). Therefore, for all but finitely many prime numbers \( \ell \), we have \( \# \text{Cl}(\bar{\mathcal{O}}_L) = \# \text{Pic}^0(\mathcal{Z}/k) \not\equiv 0 \) mod \( \ell \). 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 \( \lambda \)-Selmer group, and for the proof of Theorem 4.10. Recall that in this case, \( f(x) \) is irreducible over \( K := \mathbb{Q}(\sqrt{c}) \). 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 [11] 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 \( y^d = f_D(x) := D^p f(x/D) \). Since \( L \cong K[x]/(f_D) \), as in the case of \( J/K \), we can construct a map

\[
\begin{array}{c}
\begin{array}{c}
J(K)/\lambda J(K) \\
| \varepsilon_i \\
| \delta_i \\
| \theta_i \\
\end{array}
\xrightarrow{\delta} \begin{array}{c}
\begin{array}{c}
\text{H}^1(K,J[\lambda])_{S_J} \\
\text{res}_y \\
\theta_y \\
\end{array}
\xrightarrow{\text{res}} \begin{array}{c}
\begin{array}{c}
L(S_J,\ell) \\
\text{res}_y \\
L^*/(L^*)^\ell \\
\end{array}
\xrightarrow{\psi_D} \overline{\psi}_D \\
\Psi_D \\
\overline{\psi}_{D,K} \\
\end{array}
\end{array}
\end{array}
\end{array}
\]
Throughout the paper, given a field divisor choice of then there is a map of For each \( M \), immediately imply that it is clear that there is an isomorphism:

Two key points we shall prove in Section 3 are the following: First, if then \( \ker \Phi_\ell = \ker \Phi_p \) in the diagram (see Theorem 4.3). These two results immediately imply that \( \theta^D(\text{Sel}^\lambda(J_D, K)) \subset \theta(\text{Sel}^\lambda(J, K)) \) (see the proof of Theorem 4.10). By posing more conditions on \( D \), we can prove \( \dim_{\mathbb{F}_p} \text{Sel}^\lambda(J_D, K) = \dim_{\mathbb{F}_p} \text{Sel}^\lambda(J, K) \). 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 \( M_K^\infty \), and consider the Dedekind domain

We shall denote \( M_K \setminus M_K^\infty \) by \( M_K^0 \).

In this paper, by a global field, we shall mean a number field with \( \mathcal{O}_K \), the integral closure of \( \mathbb{Z} \), or a function field of one variable over a finite field \( k \) with the Dedekind domain \( \mathcal{O}_K \) determined by a choice of \( M_K^\infty \). For both cases, \( \mathcal{O}_K \) is called the ring of integers of \( K \). Throughout the paper, if \( L \) is a finite separable extension of \( K \), let \( \mathcal{O}_L \) denote the integral closure of \( \mathcal{O}_K \) in \( L \). When \( K \) is a function field of one variable, our choice of \( M_K^\infty \) determines \( \mathcal{O}_K \) and, hence, \( \mathcal{O}_L \) and \( M_L^\infty \). For a function field \( K \) of one variable with a rational divisor \( v_\infty \), 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 \( K_{\text{sep}} \), the (algebraic) separable closure of \( K \). Let \( K \) be a global field. We denote by \( G_K \) the absolute Galois group \( \text{Gal}(K_{\text{sep}}/K) \). For each \( q \in M_K \), let \( K_q \) denote the completion of \( K \) at \( q \). We fix the algebraic closures \( \overline{K} \) and \( K_q \), and fix an embedding \( \kappa_q : K_{\text{sep}} \hookrightarrow K_q \).

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 \( J_{\text{sep}} \) the variety \( J_{K_{\text{sep}}} \).

### 2. Schaefer’s description of the \( \lambda \)-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 \( \ell \) be a prime number, and let \( K \) be a global field of characteristic \( \neq \ell \) such that \( K \) contains a primitive \( \ell \)-th root of unity \( \zeta_\ell \). 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 \( \zeta_\ell \) also denote the \( K \)-automorphism on \( J \) defined in [Sch98], Sec 3, and \( \lambda := 1 - \zeta_\ell \in \text{End}(J) \), which we also denote by \( [\lambda] \). Recall that \( f(x) \) has distinct roots, and let \( \{ z_i \in K_{\text{sep}} : i = 1, \ldots, d \} \) be the roots of \( f(x) \). Let \( P_i := ([z_i, 0] - (\infty)) \in J(K_{\text{sep}}) \). By [Sch98], Proposition 3.2, the set \( \{ P_1, \ldots, P_d \} \) generates the \( \mathbb{F}_p \)-vector space \( J[\lambda](K_{\text{sep}}) \) of dimension \( d - 1 \). We choose a \( G_K \)-set \( X \) as small as possible such that \( X \) spans \( J[\lambda](K_{\text{sep}}) \): If \( f(x) \) does not have a \( K \)-rational root, then we set \( d' := d \), and if \( f(x) \) has a \( K \)-rational root \( z_0 \), then we set \( d' := d - 1 \). Then we define \( X := \{ P_1, \ldots, P_{d'} \} \).
The $K_{\text{sep}}$-algebra of all functions from $X$ to $K_{\text{sep}}$ 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:

$$\delta : J(K) / \lambda J(K) \to H^1(K, J[\lambda]). \quad (7)$$

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

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

By definition, the $\lambda$-part of the Tate-Shafarevich group of $J/K$, denoted by $\text{III}(J/K)[\lambda]$, is canonically isomorphic to $\text{Sel}^{(\lambda)}(J, K) / \text{Im} \delta$. Let $S$ be a subset of $M_K$ containing all archimedean places of $K$. The subgroup of $H^1(K, J[\lambda])$ unramified outside the set $S$ is denoted by $H^1(K, J[\lambda])_S$. 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,

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

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

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

$$0 \to J[\lambda](K_{\text{sep}}) \xrightarrow{w} \mu_\ell(\overline{A}_X^\ast) \xrightarrow{N_{\text{Gal}}(\overline{A}_X^\ast \to \mu_\ell(\overline{A}_X^\ast) \to 0}$$

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:

$$\tilde{w} : H^1(K, J[\lambda]) \to H^1(K, \mu_\ell(\overline{A}_X^\ast)). \quad (10)$$

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

$$\tilde{w} : H^1(K, J[\lambda]) \to H^1(K, \mu_\ell(\overline{A}_X^\ast)). \quad (11)$$

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

$$\Phi \circ \tilde{w} : H^1(K, J[\lambda]) \to A_X^\ast / (A_X^\ast)^\ell. \quad (12)$$

Let $S$ be a subset of $M_K$ containing $M_K^\sigma$, places above $\ell$, and places of bad reduction of $J/K$. If $f(x)$ has a $K$-rational root, then $H^1(K, J[\lambda]_S) \cong A_X(S, \ell)$ where $A_X(S, \ell)$ is the subgroup of $A_X^\ast / (A_X^\ast)^\ell$ 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:

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

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

$$\overline{A}_X \to \overline{A}_{X_v} \quad (13)$$

obtained by pulling back the natural map $X_v \to X$, and it is denoted by $\overline{A}_{X_v}$. Moreover, we have the maps $\delta_v$, $\tilde{w}_v$, and $\Phi_v$ as in the case of $K$. 

7
Let $S$ be a set of the places containing $M_K^*$, the places above $\ell$, and the places of bad reduction of $J/K$. For each $v \in M_K$, the following diagram is commutative:

$$
\begin{array}{c}
J(K) / \lambda J(K) \\
\alpha \downarrow \\
H^1(K, J[\lambda])_S \\
\phi_{\alpha} \\
A_X(S, \ell) \\
\end{array}
\begin{array}{c}
\delta \\
\kappa_v \downarrow \\
\text{res} \\
\delta_v \\
\Phi_{\alpha} \circ \delta_v \\
A_X^*/(A_X^{\ell})^\ell \\
\end{array}
$$

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

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

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

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

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

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

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

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

$$
f_P(x,y) := x - z_i.
$$

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

2.5. Let us define a group homomorphism $\text{Pic}^0(C) \rightarrow A_X^*/(A_X^{\ell})^\ell$ as follows: It is well-known that for each $[D] \in \text{Pic}^0(C)$, 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

$$
[D] \mapsto \text{class}(f_\alpha(E)) \in A_X^*/(A_X^{\ell})^\ell,
$$

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 $f_\alpha(D) \in (A_X^{\ell})^\ell$.

**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 $X := \{P_1, \ldots, P_{d-1}\} \subset J(K_{\text{sep}})$. If $E$ is a nonzero divisor in $\text{Div}^0(C)$ 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 class$(f_\alpha(Q)) \in A_X^*/(A_X^{\ell})^\ell$ under $\overline{\delta}$. In particular, $[(z_d, 0) - (\infty)] \mapsto \text{class}(f_\alpha(z_d, 0)) \in A_X^*/(A_X^{\ell})^\ell$.

**Proof:** The proof is left to the reader.

### 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 $\ell$ be a prime number, and let $K$ be a global field of characteristic $\neq \ell$, containing a
primitive $\ell$-th root $\zeta_\ell$ 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 $q \in M_K$, we fix an embedding $\kappa_q : \overline{K} \to \overline{K}_q$. Let $X$ and $X_q$ for each $q \in M_K$ be the $G_K$-stable spanning sets of $J[\lambda](K_{\text{sep}})$ and $J[\lambda](K_q, K_{\text{sep}})$, respectively, defined in 2.1 and 2.4. For each $q \in M_K$, let $\kappa_q$ and $\kappa_q^*$ be the maps defined in Section 2.

$$\kappa_q : X \to X_q, \quad \kappa_q^* : \overline{A}_X \to \overline{A}_{X_q}.$$ 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 $q \in M_K$, we define

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

$$X^D_q := \{([\kappa_q(z_i D), 0] - (\infty)) \in J_D(K_q, K_{\text{sep}}) : i = 1, \ldots, d'\};$$

$$P_i^D := ([z_i D, 0] - (\infty)) \in J_D(K_{\text{sep}}).$$

and let $\Phi^D, \Phi^D_q, \tilde{w}^D, \tilde{w}_q^D, \delta_q$, and $\delta_q^D$ be the maps for the twist $J_D$ as in Section 2. Then we have the following sequences of injective maps:

$$\begin{array}{ccc}
J_D(K)/\lambda_JD(K) & \xrightarrow{\delta^D} & H^1(K, J_D[\lambda]) \xrightarrow{\tilde{w}^D} H^1(K, \mu_\ell(\overline{A}_X^*)^\ell) \xrightarrow{\Phi^D} A_{X_D}^*/(A_{X_D}^*)^\ell; \\
J_D(K_q)/\lambda_JD(K_q) & \xrightarrow{\delta_q^D} & H^1(K_q, J_D[\lambda]) \xrightarrow{\tilde{w}_q^D} H^1(K_q, \mu_\ell(\overline{A}_{X_q}^*)^\ell) \xrightarrow{\Phi_q^D} A_{X_D}^*/(A_{X_D}^*)^\ell.
\end{array}$$

(17)

Let $Z(J) := \{T_i \in X : i = 1, \ldots, s\}$ be a set of representatives of $G_K$-orbits in $X$, and $Z(J_D) := \{P_i^D \in X^D : P_i \in Z(J)\}$ which is said to be compatible with $Z(J)$. Let $L_i$ be the subfield of $K_{\text{sep}}$, 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 $K(P_i^D)$ of $K_{\text{sep}}$ is $K(z_j)$, and $Z(J_D)$ is a set of representatives of $G_K$-orbits in $X^D$. For $q \in M_K$, let $Z(J, q)$ be a set of representatives of $G_{K_q}$-orbits such that $Z(J) \subset Z(J, q)$. Then, we choose $Z(J_D, q)$ compatible with $Z(J, q)$; hence, $Z(J_D) \subset Z(J_D, q)$.

3.2. Note that if $\alpha \in A_{X_D}^*$, then the evaluation of $\alpha$ at $P_i^D \in Z(J_D)$ is contained in $K(z_{i'}) = L_{i'}$ for some $i'$, i.e., $\alpha(P_i^D) \in L_{i'}$. For $D \in K^*$ and $q \in M_K$, let $\Psi_{Z(J_D)}$ and $\Psi_{Z(J_D, q)}$ be the evaluation maps of $A_{X_D}^*/(A_{X_D}^*)^\ell$ and $A_{X_q}^*/(A_{X_q}^*)^\ell$ at $Z(J_D)$ and $Z(J_D, q)$, respectively, and define

$$\mathcal{C} := \Psi_{Z(J_D)}\left(A_{X_D}^*/(A_{X_D}^*)^\ell\right) = \prod_{P \in Z(J_D)} K(P)^*/(K(P)^*)^\ell = \prod_{i=1}^s L_{i'}^*/(L_{i'}^*)^\ell;$$

$$\mathcal{C}_q := \Psi_{Z(J_D, q)}\left(A_{X_q}^*/(A_{X_q}^*)^\ell\right) = \prod_{P \in Z(J_D, q)} K_q(P)^*/(K_q(P)^*)^\ell.$$

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

Recall the maps in (17). For each $D \in K^*$, we denote by $\theta$ and $\theta^D$ 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 $q \in M_K$, we denote, respectively, by $\theta_q$ and $\theta_q^D$ the injective maps

$$\begin{array}{ccc}
Psi_{Z(J_D)} \circ \Phi_q \circ \tilde{w}_q : H^1(K_q, J[\lambda]) & \longrightarrow & \mathcal{C}_q; \\
Psi_{Z(J_D, q)} \circ \Phi^D_q \circ \tilde{w}^D_q : H^1(K_q, J_D[\lambda]) & \longrightarrow & \mathcal{C}_q.
\end{array}$$

(18) (19)

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

$$\theta^D : H^1(K, J_D[\lambda]) \longrightarrow \mathcal{C}, \quad \theta_q^D : H^1(K_q, J_D[\lambda]) \longrightarrow \mathcal{C}_q.$$
Let $S$ be a subset of $M_K$ containing $M_K^r$, the places above $\ell$, and the places of bad reduction of $J/K$ and $J_D/K$. If $f(x)$ does not have a $K$-rational root, then

$$\theta^D(H^1(K, J_D|\lambda])) = \ker \left( \prod_i N_{L_i/K} : \prod_i L_i(S, \ell) \to K(S, \ell) \right) = \theta(H^1(K, J|\lambda]))s.$$ 

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

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

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 $q \in M_K$, there is a natural map $C \to C_q$ such that the following diagram commutes for all $D \in K^r$:

\[
\begin{array}{ccc}
H^1(K, J_D|\lambda]) & \xrightarrow{\delta^D} & H^1(K, \mu_\ell(\overline{A^{\varphi}})) \\
\downarrow{\text{res}_q} & & \downarrow{\text{res}_q} \\
H^1(K_q, J_D|\lambda]) & \xrightarrow{\delta^D_q} & H^1(K_q, \mu_\ell(\overline{A^{\varphi_q}})) \\
\end{array}
\]

\[
\begin{array}{ccc}
A^\varphi / (A^\varphi) & \xrightarrow{\psi_{Z(J_D)}} & C \\
\downarrow{\text{id}} & & \downarrow{\text{id}} \\
A^\varphi / (A^\varphi) & \xrightarrow{\psi_{Z(J_D,q)}} & C_q
\end{array}
\]

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

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

\[
\begin{array}{ccc}
J_D(K_q)/\lambda J_D(K_q) & \xrightarrow{\theta^D_q \delta^D_q} & C_q \\
\downarrow{\mathcal{H}_D} & & \downarrow{\mathcal{H}_q} \\
J(K_q)/\lambda J(K_q) & \xrightarrow{\theta_q \delta_q} & C_q
\end{array}
\]

In particular, $\text{Im} \theta^D_q \delta^D_q = \text{Im} \theta_q \delta_q$ for all nonzero $D \in \mathcal{O}_K$ and $q \in M_K$ such that $D \in (K^r_q)^\ell$.

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

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

\[
f_\ast(\mathcal{H}_D(E))(P_D) = \prod_j \left( f_{P_D}(x_jD, y_j\sqrt{D}) \right)^{n_j} = \prod_j \left( x_jD - zD \right)^{n_j} = D^\Sigma n_j \prod_j \left( x_j - z \right)^{n_j} = \prod_j \left( x_j - z \right)^{n_j};
\]

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

This proves the commutativity of the diagram (20). \qed

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

\[
\begin{array}{ccc}
J_D(K_q)/\lambda J_D(K_q) & \xrightarrow{\delta^D_q} & H^1(K_q, J_D|\lambda]) \\
\downarrow{\mathcal{H}_D} & & \downarrow{\mathcal{H}_q} \\
J(K_q)/\lambda J(K_q) & \xrightarrow{\delta_q} & H^1(K, J|\lambda])
\end{array}
\]

\[
\begin{array}{ccc}
A^\varphi / (A^\varphi) & \xrightarrow{\psi_{Z(J_D)}} & C_q \\
\downarrow{\text{id}} & & \downarrow{\text{id}} \\
A^\varphi / (A^\varphi) & \xrightarrow{\psi_{Z(J_D,q)}} & C_q
\end{array}
\]
where \( \mathcal{H} \) 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 \( \ell \)-th power in \( K_\ell \), and the entire diagram commutes when \( D \in (K_\ell^*)^\ell \).

3.7. Recall the maps \( \theta^D \) and \( \theta^D_q \) for \( q \in M_K \) and \( D \in \mathcal{O}_K \) defined in \textsection 3.2. Let \( S \) be a subset of \( M_K \) containing \( M_K^\infty \), the places above \( \ell \), and the places of bad reduction of \( J_D/K \). Then, \( \text{Sel}^\lambda(J_D,K) \) is described as a subgroup of \( \mathcal{C} \) as follows:

\[
\theta^D(Sel^\lambda(J_D,K)) = \{ \alpha \in \theta^D(H^1(K,J_D[\lambda])) : \text{res}_q(\alpha) \in \text{Im} \theta^D_q \delta^D_q \text{ for all } q \in S \}.
\]

4. The Jacobian Varieties Without \( \lambda \)-torsion Points

In this section, we prove Theorem 4.10 and its analogue for a function field. Let \( \ell \) be a prime number, and let \( K \) be a global field of characteristic \( \neq \ell \), containing a primitive \( \ell \)-th root of unity \( \zeta_\ell \). Let \( C/K \) be the normalization of a superelliptic curve \( y^\ell = f(x) \). Let \( \Delta_f \) 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 \( S_f \) denote the subset of \( M_K \) containing \( M_K^\infty \), the places dividing \( \ell \Delta_f \). For each nonzero element \( D \) of \( \mathcal{O}_K \), let \( S_D \) denote the set \( S_f \cup \{ p \in M_K^\infty : p \mid D \mathcal{O}_K \} \). Then, the sets \( S_f \) and \( S_D \) contain the set of places of bad reduction of \( J/K \) and \( J_D/K \), respectively.

4.2. Recall that \( X := \{ P_1, \ldots, P_j \} \) is the subset of \( J[\lambda](K_{sep}) \). 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 \( \mathcal{C} := L^1/(L^1)^\ell \) as defined in \textsection 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 \( q \) of \( \mathcal{O}_K \) such that either \( q \mathcal{O}_L \) is prime in \( \mathcal{O}_L \) or \( q \mathcal{O}_L = p^\ell q' \mathcal{O}_L \) for some prime ideal \( p \) of \( \mathcal{O}_L \). Then, \( \ker(N_{L/K} : L(S_f,\ell) \to K(S_f,\ell)) = \ker(N_{L/K} : L(S_D,\ell) \to K(S_D,\ell)) \). Hence, \( \theta(H^1(K,J[\lambda]))_{S_f}) = \theta^D(H^1(K,J_{D[\lambda]})) \) as subgroups of \( L^1 \).

**Proof.** Since \( S_f \subset S_D \), it is clear that

\[
\ker(N_{L/K} : L(S_f,\ell) \to K(S_f,\ell)) \subset \ker(N_{L/K} : L(S_D,\ell) \to K(S_D,\ell)).
\]

Let \( \alpha \) be a nonzero element of \( \mathcal{O}_L \) such that \( \alpha \mathcal{O}_L = a \mathcal{O}_L \) where \( a \) is an ideal supported by \( S_D \) and such that \( N_{L/K}(\alpha) = B^\ell \) for some \( B \in \mathcal{O}_K \). Let \( q \) be a prime ideal of \( \mathcal{O}_K \) dividing \( D \mathcal{O}_K \) such that \( q \mathcal{O}_L = p^\ell q' \mathcal{O}_L \) for some prime ideal \( p \) of \( \mathcal{O}_L \). Let \( n := \text{ord}_p(\alpha \mathcal{O}_L) \), and let \( m \) be the residue degree of \( p \) with respect to \( q \). Since \( m \equiv 0 \mod \ell \), and there is only one prime ideal of \( \mathcal{O}_L \) lying over \( q \), it follows that \( \text{ord}_q(\beta^\ell \mathcal{O}_L) = \text{ord}_q(N_{L/K}(\alpha \mathcal{O}_L)) = mn \). On the other hand, \( \text{ord}_p(\beta^\ell \mathcal{O}_K) \equiv 0 \mod \ell \) and, hence, \( n \equiv 0 \mod \ell \). Therefore, \( \text{ord}_p(\alpha \mathcal{O}_L) \equiv 0 \mod \ell \) for all \( p \) dividing \( D \mathcal{O}_L \), and \( \alpha \mathcal{O}_L = \alpha'(\mathcal{O}_L^\ell) \) for some ideal \( \alpha' \) supported by \( S_f \), i.e., class(\( \alpha \)) \( \in \mathcal{L}(S_f,\ell) \).

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 \( p \in M_K \), \( \left( \frac{\alpha}{p} \right)_{\ell} = 1 \) implies \( \alpha \in (K_\ell^*)^\ell \).

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 \( K/Q \) be the \( \ell \)-th cyclotomic field extension of \( Q \) where \( \ell \) 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 \( \ell \).
Thus, let us assume that $\alpha \in \mathcal{O}_K$ dividing $q$.

(i) The ideal $q\mathcal{O}_L$ is prime;

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

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

**Proof.** Let $k_L$ be the residue field $\mathcal{O}_L/q\mathcal{O}_L$, and $k$ be the residue field $\mathcal{O}_K/q$. For $\zeta \in \mathcal{O}_L$, let $\mathcal{O}$ denote the residue class in $k_L$. Since $\left(\frac{\alpha}{q\mathcal{O}_L}\right)_\ell = 1$, let $\beta \in \mathcal{O}_L$ such that $\beta^\ell \equiv \alpha \mod q\mathcal{O}_L$, i.e., $\beta^\ell = \alpha$ in $k_L$. The degree of the extension $k(\beta)/k$ is either 1 or $\ell$ since $k$ contains a primitive $\ell$-th root of unity. Since $\ell \not\equiv p$, $k(\beta)/k$ has degree 1.

Thus, $\left(\frac{\alpha}{q}\right)_\ell = 1$. □

**Proposition 4.6.** Let $W$ be a finite subset of $\mathcal{O}_L\setminus\{0\}$, and let $\mathcal{D}_W$ be the set of prime numbers defined in 4.4.

Then $\mathcal{D}_W$ contains a set of prime numbers in $\mathbb{Z}$ with positive Dirichlet density at least $(p-1)/(\ell^p(\ell - 1)p!)$.

**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 $m := [M' : L] \neq 0 \mod p$ since $f$ is defined over $\mathbb{Z}$, and $\deg f = p$ is a prime number. Note that $M = M'(\sqrt[\ell]{\alpha} : \alpha \in W$ and $\tau \in \text{Gal}(\mathbb{Q}/\mathbb{Q}))$. Since $\zeta^\ell \in K$, and $\ell$ is a prime number, $|M : M'| = \ell^m$ is a power of $\ell$ and, hence, $|M : M'| = \ell^m$ for some non-negative integer $n$.

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

Let $\mathcal{D}$ 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 $(\ell - 1) \cdot p! \cdot (\ell^p)^p$, by the Cebotarev Density Theorem, $\mathcal{D}$ has positive Dirichlet density at least $(p-1)/(\ell^p(\ell - 1)p!)$. Since $W$ is a finite set, the following set of prime ideals has Dirichlet density equal to the Dirichlet density of $\mathcal{D}$:

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

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

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

$$p = |\text{Frob}(\Omega/\|q\})| = f(\Omega/\|q\}) = f(\Omega/\Omega_L)f(\Omega_L/\|q\})f(q/\Omega).$$  

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

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

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

12
If \( q \) is an infinite place of \( K \), or if \( q \) is a prime ideal of \( \mathcal{O}_K \) such that \( \alpha_q \in W \), then \( \left( \frac{D}{q} \right)_\ell = 1 \) for all positive integers \( D \) supported by \( \mathcal{D}_W \).

**Proof.** Suppose that \( q \) is a prime ideal of \( \mathcal{O}_K \) not dividing \( \ell \mathcal{O}_K \), and \( q^m = \alpha_q \mathcal{O}_K \) where \( \alpha_q \in \mathcal{O}_K \) and \( m \) is the order of \( q \) in \( \text{Cl}(\mathcal{O}_K) \). Then, since \( \ell \) is regular, \( m \not\equiv 0 \mod \ell \). Let \( q \) be a prime number dividing \( D \), and suppose that \( \alpha_q \in W \). Let \( q \mathcal{O}_K \) be decomposed into \( \prod_{j=1}^t p_j^{n_j} \) where \( p_j \) are prime ideals coprime to \( \ell \) and \( n \) is an integer. Since \( q \in \mathcal{D}_W \), it follows that \( \left( \frac{\alpha_q p_j}{p_j} \right)_\ell = 1 \) and, hence, by Lemma 4.5 \( \left( \frac{\alpha_q}{p_j} \right)_\ell = 1 \). Then

\[
\left( \frac{\alpha_q}{q} \right)_\ell = \prod_{j=1}^t \left( \frac{\alpha_q}{p_j} \right)_\ell = \prod_{j=1}^t \left( \frac{\alpha_q}{p_j} \right)_\ell = 1.
\]

Since \( W \) contains \( \zeta_\ell \) and \( \lambda \), it follows that \( \left( \frac{\alpha_q}{q} \right)_\ell = 1 \). If \( \ell = 2 \), then \( K = \mathbb{Q} \), and it follows that \( \left( \frac{-1}{p_j} \right)_2 = 1 \). By Lemma 6.4 \( \left( \frac{\alpha_q}{x_\ell} \right)_\ell = 1 \). Since \( \alpha_q \not\equiv 0 \mod p_j \) for all \( j = 1, \ldots, t \), by Corollary 6.3

\[
1 = \left( \frac{\alpha_q}{q} \right)_\ell = \left( \frac{q}{\alpha_q} \right)_\ell = \left( \frac{q}{\alpha_q} \right)_\ell.
\]

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

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

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:

\[
\text{Sel}^\ell(J_D, K) \subset H^1(K, J_D[\lambda])_{S_D} \stackrel{\theta_D}{\longrightarrow} L^*/(L^*)^\ell.
\]

**Theorem 4.8.** Let \( K := \mathbb{Q}(\zeta_\ell) \) where \( \ell \) 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 \( N := \dim_{\mathbb{F}_\ell} \text{Sel}^\ell(J, K) \), and \( M \), the number of prime ideals of \( \mathcal{O}_K \) dividing \( \ell \Delta_f \). Then there is a set \( \mathcal{D} \) of prime numbers with Dirichlet density at least \( (p-1)/(\ell(N+M+1)p^2) \) such that whenever a positive integer \( D \) is supported by \( \mathcal{D} \), \( \theta(\text{Sel}^\ell(J, K)) = \theta_D(\text{Sel}^\ell(J, K)) \). In particular, \( \dim_{\mathbb{F}_\ell} \text{Sel}^\ell(J, K) = \dim_{\mathbb{F}_\ell} \text{Sel}^\ell(J, K) \).

**Proof.** Recall from 4.12 the map \( \theta: H^1(K, J[\lambda]) \rightarrow L^*/(L^*)^\ell \). Let \( W \) be a subset of \( \mathcal{O}_K \) generating \( \theta(\text{Sel}^\ell(J, K)) \). For each prime ideal \( q \) of \( \mathcal{O}_K \) coprime to \( \ell \), let us fix an element \( \alpha_q \) of \( \mathcal{O}_K \) such that \( \alpha_q \mathcal{O}_K = q^m \) where \( m \) is the order of \( q \) in \( \text{Cl}(\mathcal{O}_K) \). For \( q := \lambda \mathcal{O}_K \), we choose \( \alpha_q := \lambda \).

Recall \( S_J \) from 4.4, and let

\[
Y_J := \{ \zeta_\ell \} \cup W \cup \{ \alpha_q \in \mathcal{O}_K : q \in S_J \cap M_K^D \}.
\]

Let \( \mathcal{D}_W \) be the set of prime numbers defined in 4.4. For \( W = Y_J \). Then, by Proposition 4.6, \( \mathcal{D}_J \) contains a set \( \mathcal{D} \) of prime numbers with Dirichlet density at least \( (p-1)/(\ell(N+M+1)p^2) \). Since \( \ell \) is regular, by Lemma 4.7 if \( D \) is a positive integer supported by \( \mathcal{D} \) and \( q \in S_J \), then

\[
\left( \frac{D}{q} \right)_\ell = 1.
\]

Let \( D \) be a positive integer supported by \( \mathcal{D} \). Let us show that \( \theta_D(\text{Sel}^\ell(J, K)) \subset \theta(\text{Sel}^\ell(J, K)) \). Let \( \alpha \) be an element of \( \theta_D(\text{Sel}^\ell(J, K)) \). By 4.7

\[
\theta(\text{Sel}^\ell(J, K)) = \{ \alpha \in \theta(H^1(K, J[\lambda])_{S_J}) : \text{res}_q(\alpha) \in \text{Im} \theta_q \delta_q \text{ for all } q \in S_J \}.
\]

\[
\theta_D(\text{Sel}^\ell(J, K)) = \{ \alpha \in \theta^D(H^1(K, J_D[\lambda])_{S_D}) : \text{res}_q(\alpha) \in \text{Im} \theta_q^D \delta_q^D \text{ for all } q \in S_D \}.
\]
By Theorem 3.3 we have

\[ \theta^D(H^1(K, J_{D[\lambda]})) = \theta(H^1(K, J[\lambda])) \]  \hspace{1cm} (24)

hence, \( \alpha \) is contained in \( \theta(H^1(K, J[\lambda])) \). Let \( q \) be a place in \( S_f \), and recall the set \( S_D \) from (4.1). Then \( q \) is contained in \( S_D \). By Lemma 6.7 (22) implies that \( D \in (K_q^*)^\ell \). By Proposition 3.5, it follows that \( \text{Im} \theta_q \delta_q = \text{Im} \theta^D \delta_q^D \) and, hence, \( \alpha \) is contained in \( \text{Im} \theta_q \delta_q \) since \( \alpha \in \theta^D(\text{Sel}^{(\lambda)}(J_D, K)) \) and \( q \in S_D \). Thus, \( \alpha \in \theta(\text{Sel}^{(\lambda)}(J, K)) \).

Let us show that \( \theta(\text{Sel}^{(\lambda)}(J, K)) \subset \theta^D(\text{Sel}^{(\lambda)}(J_D, K)) \). Let \( \alpha \) be an element of \( \theta(\text{Sel}^{(\lambda)}(J, K)) \). By (24), \( \alpha \) is contained in \( \theta^D(H^1(K, J[\lambda])) \). If \( q \) is a place in \( S_f \), then by (22), \( D \in (K_q^*)^\ell \), and by Proposition 3.5 \( \text{Im} \theta_q \delta_q = \text{Im} \theta^D \delta_q^D \). Thus, \( \alpha \in \text{Im} \theta^D \delta_q^D \) for all \( q \in S_f \). Let \( q \) be a prime ideal in \( S_D \). Since \( D \) is supported by \( S_f \), the prime ideal \( q \) is contained in \( S_f \) and, hence, \( (\frac{\beta}{\lambda_q})_\ell = 1 \) for all \( \beta \in W_f \). Since \( W_f \) generates \( \theta(\text{Sel}^{(\lambda)}(J, K)) \), it follows that \( (\frac{\alpha}{\lambda_q})_\ell = 1 \), i.e., \( \alpha \in (L_q^*)^\ell \) where \( \mathcal{P} := q\mathcal{O}_L \). Recall that \( \text{res}_q \) is a map: \( L^*/(L^*)^\ell \rightarrow \mathcal{P}_q := \prod_{P \in \mathcal{P}(J, q)} K_q(P)^*/(K_q(P)^*)^\ell \). Since \( \mathcal{P}_q \) is prime, \( f(x) \) is irreducible over \( K_q \) and, hence, \( Z(J, q) \) contains a single point \( P \). Thus, \( \mathcal{P}_q = L_q^\mathcal{P}/(L_q^*)^\ell \). Thus, \( \text{res}_q(\alpha) = 1 \) and, in particular, \( \text{res}_q(\alpha) \in \text{Im} \theta_q \delta_q^D \). We established that \( \text{res}_q(\alpha) \in \text{Im} \theta^D \delta_q^D \) for all \( q \in S_D \). Therefore, \( \alpha \) is contained in \( \theta^D(\text{Sel}^{(\lambda)}(J_D, K)) \). Since \( \theta \) and \( \theta^D \) are injective maps, the dimensions of the two selmer groups are equal to each other.

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

Let \( D_0 \) be a positive \( \ell \)-th power free integer. Then there is a positive constant \( \varepsilon < 1 \) depending on \( \mathcal{D} \) such that

\[ \# \{ D_0 D \in \mathcal{P}_f(X) : D \in \mathcal{P}_f(\mathcal{D}, X) \} \gg \frac{X}{(\log X)^c}. \]

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

\[ \dim \mathcal{F}_f \text{Sel}^{(\lambda)}(J_{D_0D}, K) = N. \]  \hspace{1cm} (25)

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

\[ \# \{ D \in \mathcal{P}_f(X) : \text{Sel}^{(\lambda)}(J_D, K) = N \} \gg \frac{X}{(\log X)^c}. \]  \hspace{1cm} (26)

**Proof.** Recall that \( J_{D_0} \) is the Jacobian variety of the normalization of \( y^f = (D_0)^p f(x/D_0) \). Let \( g := (D_0)^p f(x/D_0) \). Then \( \Delta_g = \ell \Delta_f D_0^b \) for some positive integer \( b \) and, hence, the number of prime ideals of \( \mathcal{O}_K \) dividing \( \ell \Delta_g \) is equal to \( M \). Since \( (J_{D_0})_D = J_{D_0D} \), by applying Theorem 4.8 to \( J_{D_0} \), (25) is proved. The proof of (26) follows immediately from Lemma 4.9.

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

\[ \# \{ D \in \mathcal{P}_f(X) : \text{rank} J_D(\mathbb{Q}) \leq N \} \gg \frac{X}{(\log X)^c}. \]  \hspace{1cm} (27)
ON THE ARITHMETIC OF TWISTS OF SUPERELLIPTIC CURVES

Proof. Note Sel\(^{(2)}\)(\(J_D, K\)) \(\cong J_D(K) / \lambda J_D(K) + \mathbb{H}(J_D, K)[\lambda]\). Then, by [Sch98], Corollary 3.7 and Proposition 3.8, Sel\(^{(2)}\)(\(J_D, K\)) \(\geq\) \(\text{rank} J_D(\mathbb{Q})\). 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 \(p \geq 5\). Suppose that there is a positive integer \(D_0\) such that \(N := \dim_{\mathbb{F}_2} \text{Sel}^{(2)}(J_{D_0}, \mathbb{Q}) < (p - 1)/2\). Then there is a positive constant \(\varepsilon < 1\) depending on \(C\) and \(D_0\) such that

\[
\# \{D \in \mathcal{D}_2(X) : \# C_D(\mathbb{Q}) \leq 2N + 1\} \gg \frac{X}{(\log X)^\varepsilon}.
\]

**Proof.** Let \(t\) 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 \(\# S \leq (p - 1)/2\) and \(S \cap t(S) = \emptyset\) generates a subgroup of rank \#\(S\) in \(J_D(\mathbb{Q})\).

By Theorem 4.10,

\[
\# \{D \in \mathcal{D}_2(X) : \dim_{\mathbb{F}_2} \text{Sel}^{(2)}(J_D, \mathbb{Q}) = N\} \gg \frac{X}{(\log X)^\varepsilon}.
\]

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

**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 \(25 \mod 36\) and \(\dim_{\mathbb{F}_3} \text{Cl}(\mathbb{Q}(\sqrt{-A}))[3] = 0\). 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

\[
\# \{D \in \mathcal{D}_3(X) : \text{rank} E_D(\mathbb{Q}) = 0\} \gg \frac{X}{(\log X)^\varepsilon}.
\]

**Proof.** By [Sto], Corollary 2.1, \(\dim_{\mathbb{F}_3} \text{Sel}^{(3)}(E, K) = 0\) 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 \(\ell\)-th root of unity \(\zeta_\ell\); hence, \(\text{char} k \neq \ell\). Let \(K/k\) be a function field of one variable with a rational divisor \(v_\infty\) such that \(\text{Cl}(\mathcal{O}_K)[\ell] \neq 0\) mod \(\ell\) defined in 1.6. Let \(L\) be a field extension of \(K\) such that \(p := [L : K]\) is a prime number not equal to \(\ell\).

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

i) The ideal \(q \mathcal{O}_L\) is prime;

ii) for all \(\alpha \in W, \alpha \neq 0\) mod \(q \mathcal{O}_L\), and \(\left(\frac{\alpha}{q \mathcal{O}_L}\right)_\ell = 1\).

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

**Proof.** The proof is similar to that of Lemma 4.5.
PROPOSITION 4.16. Let $\mathcal{W}$ be a finite subset of $\mathcal{O}_L\setminus\{0\}$. Then $\mathcal{D}_W$ contains a set of prime ideals of $\mathcal{O}_K$ with positive Dirichlet density at least $(p-1)/\left(\ell^{|W|}p^p\ell!\right)$.

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 $v_m$, and let $G_\infty$, $M_\infty$, and $\pi_m$ be the discrete valuation ring, the maximal ideal, and a uniformizer at $v_m$, respectively.

4.17. Let $K_m$ be the completion of $K$ at $v_m$. Let us define

$$
\left(\frac{g}{v_m}\right)_\ell := \begin{cases} 
1 & \text{if } g \in (K_m)^\ell \\
-1 & \text{if } g \not\in (K_m)^\ell 
\end{cases}.
$$

Note that each non-constant element $g$ of $\mathcal{O}_K$ is not an element of the valuation ring $G_\infty$, i.e., $\text{ord}_{v_m}(g) < 0$. The leading coefficient of a nonzero element $g$ of $\mathcal{O}_K$ is the constant $a \in k^*$ such that $\pi_m^m g \equiv a \mod \pi_m$ for some $m \in \mathbb{Z}$. The element $g$ is monic if the leading coefficient is 1. The degree of an element $g$ of $\mathcal{O}_K$, denoted by $\text{deg}(g)$, is $-\text{ord}_{v_m}(g)$. Let $g$ be an element of $\mathcal{O}_K$ with the leading coefficient $a \in k^*$. Then $g \in (K_m)^\ell$ if and only if $a \in (k^*)^\ell$ and $\text{deg}(g)$ is divisible by $\ell$.

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

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

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

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

Proof. Recall $S_f$ from 4.4. For each prime ideal $q$ of $\mathcal{O}_K$, choose a monic element $\alpha_q$ of $\mathcal{O}_K$ such that $\alpha_q \mathcal{O}_K = q^m$ where $m$ is the order of $q$ in $\text{Cl}(\mathcal{O}_K)$. Let $W_f$ be the subset of $\mathcal{O}_L$ generating $\theta(\text{Sel}(\ell)(J, K))$. Let $Y_f := \{-1\} \cup W_f \cup \{\alpha_q \in \mathcal{O}_K : q \in S_f \cap \mathbb{M}_f\}$, and let $\mathcal{D}_Y$ be the set of prime ideals defined in 4.14 for $W = Y_f$. Then, by Proposition 4.16, $\mathcal{D}_Y$ contains a set of prime ideals $\mathcal{D}$ with Dirichlet density at least $(p-1)/((p(N+M+1)p^p)!$). The proof of $\theta(\text{Sel}(\ell)(J, K)) = \theta^D(\text{Sel}(\ell)(J_D, K))$ is identical with that of Theorem 4.10 when Lemma 4.18 is applied to $W = Y_f$.

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

16
ON THE ARITHMETIC OF TWISTS OF SUPERELLIPTIC CURVES

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

4.21. Given a set \( \mathcal{D} \) of prime ideals of \( \mathcal{O}_K \), there are indeed infinitely many classes in \( K^*/(K^*)^\ell \) represented by \( D \in \mathcal{O}_K \) supported by \( \mathcal{D} \) and \( \deg(D) \equiv 0 \mod \ell \). Let \( \{p_1, \ldots, p_n\} \) be a finite set of prime ideals of \( \mathcal{O}_K \) contained in \( \mathcal{D} \) for \( n \geq 2 \). Let \( m_i = p_i \mathcal{O}_K \) for some \( p_i \in \mathcal{O}_K \) where \( m_i \) is the order of \( p_i \) in \( \text{Cl}(\mathcal{O}_K) \). Then, since \( \text{Cl}(\mathcal{O}_L) \not\equiv 0 \mod \ell \) and \( \deg(\alpha_{p_i}) = \text{ord}_{p_i}(\alpha_{p_i}) \), there is a positive integer \( s \) such that \( D := \alpha_{p_i}^{s} \prod_{i=1}^{n} \alpha_{p_i} \) has degree divisible by \( \ell \).

**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 \( \mathcal{L} := K \otimes k' \), and \( \mathcal{O}_L \), the integral closure of \( K \) in \( L \). Suppose that \( \dim_{\mathbb{F}_\ell} \text{Cl}(\mathcal{O}_L)[\ell] = 0 \). Then \( \dim_{\mathbb{F}_\ell} \text{Sel}(\lambda)(J, K) = 0 \).

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 \( \mathcal{D} \) of prime ideals of \( \mathcal{O}_K \) with Dirichlet density \( (p-1)/p \) such that whenever \( D \) is an element of \( \mathcal{O}_K \) supported by \( \mathcal{D} \),

\[
\dim_{\mathbb{F}_\ell} \text{Sel}(\lambda)(J, K) = 0 \quad \text{and} \quad \# C_D(K) \leq \# E(k).
\]

**Proof.** Note that \( L/K \) is Galois. Recall \( S_J \) from (4.1). Then \( S_J = M^\alpha_K \), and \( H^1(K, J[\lambda])_{M^\alpha_K} \cong \ker(N_L/K : L(M^\alpha_K, \ell) \to K(M^\alpha_K, \ell)) \). Note that \( \# \text{Sel}(\lambda)(J/K) \cong \# H^1(K, J[\lambda])_{M^\alpha_K} = \# \ker(N_L/K : L(M^\alpha_K, \ell) \to K(M^\alpha_K, \ell)) \).

Since the subgroup \( \text{Cl}(\mathcal{O}_L)[\ell] \) is trivial, by Lemma 4.23 below, \( H^1(K, J[\lambda])_{M^\alpha_K} = 1 \) and, hence, \( \text{Sel}(\lambda)(J, K) = 0 \).

Let \( \mathcal{D} \) be the set of prime ideals \( q \) of \( \mathcal{O}_K \) such that \( q \mathcal{O}_L \) is prime. Since \( \text{Gal}(L/K) \) has order \( p \), by the Cebotarev Density Theorem, \( \mathcal{D} \) has Dirichlet density \( (p-1)/p \). Let \( D \) be an element of \( \mathcal{O}_K \) supported by \( \mathcal{D} \). Then, by Theorem 4.3, \( \theta^\alpha_0(H^1(K, J[\lambda])_{S_D}) = \theta(H^1(K, J[\lambda])_{S_D}) = 1 \) and, hence, \( \dim_{\mathbb{F}_\ell} \text{Sel}(\lambda)(J, K) = 0 \).

By [Sch98, Corollary 3.7, rank \( J_D(K) \leq (\ell-1) \dim_{\mathbb{F}_\ell} \text{Sel}(\lambda)(J, K) = 0 \). Suppose that \( D \) is not a unit in \( \mathcal{O}_L \), and let \( F := K(\sqrt{D}) \). Then \( k \) is algebraically closed in \( F \), and \( F \subset K_{\text{sep}} \) since \( \ell \neq \text{char} K \). Since \( (C_D)_F \cong C_F \) as \( F \)-schemes, by Proposition 4.25 below, \( \# J_D(K)_{\text{tor}} \leq \# E(k) \). Since \( J_D(K) = J_D(K)_{\text{tor}} \), \( C_D(K) \rightarrow J_D(K) \), it follows that \( \# C_D(K) \leq \# J_D(K)_{\text{tor}} \leq \# E(k) \).

**Lemma 4.23.** (Suppose that \( M^\alpha_K \) 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 \( \ell \), and suppose that \( \text{Cl}(\mathcal{O}_L)[\ell] \) is trivial. Then \( \ker(N_L/K : L(M^\alpha_K, \ell) \to K(M^\alpha_K, \ell)) = 1 \).

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

\[
\ker(N_L/K : L(M^\alpha_K, \ell) \to K(M^\alpha_K, \ell)) \cong \ker(N_{k'/k} : k^\ast/(k^\ast)^\ell \to k^\ast/(k^\ast)^\ell).
\]

Let \( a \) be a positive integer such that \( da \equiv 1 \mod \ell \). Note that there is a section \( u : k^\ast/(k^\ast)^\ell \to k^\ast/(k^\ast)^\ell \) to the norm map \( N_{k'/k} \) in (28), given by \( \text{class}(\alpha) \mapsto \text{class}(\alpha^a) \). Hence, the norm map \( N_{k'/k} \) is surjective. Since \( k^\ast \) and \( (k^\ast)^a \) are both cyclic groups of order divisible by \( \ell \), it follows that \( N_{k'/k} \) 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 \( \mathcal{O} / k' \) be a smooth complete curve with function field \( F \) such that \( \mathcal{O} \) has a rational divisor \( v_m \). Then there is a \( k' \)-morphism: \( \mathcal{O} \to \mathbb{P}_{k'}^1 \) such that \( v_m \) is totally ramified over a rational divisor in \( \mathbb{P}_{k'}^1 \).

Let \( \mathcal{O}_F \) be the ring of integers defined in (16) with choice of \( M_{\mathcal{O}_F}^\alpha := \{ v_m \} \). Then the group of units \( \mathcal{O}_F^\ast \) is \( (k')^\ast \), and \( \# \text{Cl}(\mathcal{O}_F) = \# \text{Pic}^0(\mathcal{O}) \). Hence, the class number of \( \mathcal{O}_F \) does not depend on the choice of a rational divisor on \( F \).

**Proof.** Using the Riemann-Roch theorem, we can find a function \( g \in k'((\mathcal{O})) \) with poles supported only by \( v_m \). Then the function \( g \) induces a morphism \( \mathcal{O} \to \mathbb{P}_{k'}^1 \) such that \( v_m \) is totally ramified over a rational point \( \infty \in \mathbb{P}_{k'}^1 \). To finish the proof, use [Lor90, Sec VIII, p. 299-300.]

\( \square \)
In this section we prove Theorem 5.5 and its analogue for a function field, introduced in Section 1. Let $C$ be the Jacobian variety of $E/k$, and let $J$ be the Jacobian variety of $C'$. Then $J_{C'(K)} \to J(k)$.

**Proof.** Note that $J(\overline{k})_{\text{Tor}} = J(\overline{K})_{\text{Tor}} = J(K_{\text{sep}})_{\text{Tor}}$. Then, $J_{C'(K)}_{\text{Tor}} \subset J_{C'(F)}_{\text{Tor}} \cong J(F)_{\text{Tor}} \cong J(F)_{\text{Tor}} = J(k)$. □

5. The Jacobian Varieties With $\lambda$-Torsion Points

In this section we prove Theorem 5.5 and its analogue for a function field, introduced in Section 1. Let $\ell$ be a prime number, and let $K := \mathbb{Q}(\zeta_{\ell})$ for which we assume $\ell$ is regular, or a function field of one variable with a rational divisor $v_{\infty}$ such that $\#\text{Cl}(\mathcal{O}_K) \neq 0 \mod \ell$. 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 $\Delta_f$ be the discriminant of $f$. Recall $z_1, \ldots, z_d \in K_{\text{sep}}$, 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 composum of $L_1, \ldots, L_s$ in $K_{\text{sep}}$.

5.1. Let us fix a set of generators of $\theta(\text{Sel}^{(\lambda)}(J, K))$, and note that each generator is an $s$-tuple with entries in $L$. Let $W_s$ be the union of all entries of the generators. Then $W_s$ is a subset of $L^s$. For each prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$, choose an element $\alpha_\mathfrak{q}$ of $\mathcal{O}_K$ as in the proof of Theorem 4.8 or Theorem 4.19 depending on the cases of $K$. Recall $S_J := M^K_K \cup \{q \in M^K_0 : q \mid \Delta_f \mathcal{O}_K\}$, and let

$$Y_j := \{\zeta_\mathfrak{q}, -1\} \cup W_s \cup \{\alpha_\mathfrak{q} \in \mathcal{O}_K : q \in S_j \cap M^K_0\}.$$

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

Recall from 4.14 the definition of $\left(\frac{D}{q}\right)_\ell$ when $K$ is a function field, and that $\#\text{Cl}(\mathcal{O}_K) \neq 0 \mod \ell$.

**Lemma 5.2.** Suppose that $K = \mathbb{Q}(\zeta_{\ell})$. If $D$ is a positive integer supported by $\mathcal{D}^\prime_{Y_j}$, and $q$ is a place in $S_j$, then $\left(\frac{D}{q}\right)_\ell = 1$.

Suppose that $K$ is a function field. Let $D$ be a monic element of $\mathcal{O}_K$, of degree divisible by $\ell$ supported by $\mathcal{D}^\prime_{Y_j}$. If $q$ is a place in $S_j$, then $\left(\frac{D}{q}\right)_\ell = 1$.

**Proof.** The proof is identical with those of Lemma 4.7 and 4.18. □

**Proposition 5.3.** Suppose that $K = \mathbb{Q}(\zeta_{\ell})$. Let $D$ be a positive $\ell$-th power free integer in $\mathbb{Z}$ which is supported by $\mathcal{D}^\prime_{Y_j}$. Then

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

Suppose that $K$ is a function field. Let $D$ be a monic element of $\mathcal{O}_K \setminus \{0\}$ of degree divisible by $\ell$ such that $D\mathcal{O}_K$ is not an $\ell$-th power of an ideal and $D$ is supported by $\mathcal{D}^\prime_{Y_j}$. Then

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

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

18
ON THE ARITHMETIC OF TWISTS OF SUPERELLIPTIC CURVES

Proof. Let $D$ be a positive $\ell$-th power free integer in $\mathbb{Z}$ which is supported by $\mathcal{D}_y$ or a monic element $D$ of $\mathcal{O}_K$ of degree divisible by $\ell$ supported by $\mathcal{D}_y$. Let $S_D := S_f \cup \{q \mid D \mathcal{O}_K\}$. Then,

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

By 3.7,

$$
\theta(\text{Sel}^{(\lambda)}(J, K)) = \{\alpha \in \theta(H^1(K, J[\lambda]))_{S_f} : \text{res}_q(\alpha) \in \Im \theta_q \delta_q \text{ for all } q \in S_f\};$$

$$
\theta^D(\text{Sel}^{(\lambda)}(J, D, K)) = \{\alpha \in \theta^D(H^1(K, JD[\lambda]))_{S_D} : \text{res}_q(\alpha) \in \Im \theta^D_q \delta^D_q \text{ for all } q \in S_D\}. \tag{31}
$$

Let us show that $\theta(\text{Sel}^{(\lambda)}(J, K)) \subset \theta^D(\text{Sel}^{(\lambda)}(J, D, K))$. Let $\alpha$ be an element of $\theta(\text{Sel}^{(\lambda)}(J, K))$. Then $\alpha \in \prod_{i=1}^{s} L_i(S_f, \ell)$. By Lemma 5.2, $D$ is an $\ell$-th power in $K_q$. By Proposition 5.3, $\Im \theta^D_q \delta^D_q = \Im \theta_q \delta_q$ and, hence, $\alpha \in \Im \theta^D_q \delta^D_q$. Let $q$ be a prime ideal in $S_f \setminus S_f$. Then $q \mid D$ and, hence, $q \in \mathcal{D}_f$. Suppose that $\alpha$ is represented by $(\beta_1, \ldots, \beta_s)$ for some $\beta_i \in \mathcal{O}_L$. Then, since $Y_f$ contains $W_f$ defined in 5.1 and all $\sqrt{\beta_i}$ are defined over $K_q$, it follows $\text{res}_q(\alpha) = 1 \in \mathcal{C}_q$ and, in particular, $\text{res}_q(\alpha) \in \Im \theta^D_q \delta^D_q$. Therefore, by (31), $\alpha$ is contained in $\theta^D(\text{Sel}^{(\lambda)}(J, D, K))$.

Note that $\theta(\text{Sel}^{(\lambda)}(J, K)) \subset \theta^D(\text{Sel}^{(\lambda)}(J, D, K))$ which is contained in $\prod_{i=1}^{s} L_i(S_f, \ell) \setminus \prod_{i=1}^{s} L_i(S_f, \ell)$. Therefore, $\alpha \notin \theta(\text{Sel}^{(\lambda)}(J, K))$, and we proved that $\dim_{\mathbb{F}} \text{Sel}^{(\lambda)}(J, D, K) > \dim_{\mathbb{F}} \text{Sel}^{(\lambda)}(J, K)$.

If $K$ is a function field, then as illustrated in 4.2.1 there is a monic element $D$ of $\mathcal{O}_K$ of degree divisible by $\ell$ such that $D \mathcal{O}_K$ is not an $\ell$-th power of an ideal and $D$ is supported by $\mathcal{D}_f$. Using induction, one can easily show that $\limsup_D \dim_{\mathbb{F}} \text{Sel}^{(\lambda)}(J, D, K) = \infty$. \hfill \Box

Recall that $P_d^D := [(z_d D, 0) - (\infty)]$ is a point in $JD[\lambda](\mathbb{K}_{\text{sep}})$ but $P_d^D \notin X_D$.

Lemma 5.4. Let $D$ be an $\ell$-th power free positive integer supported by $\mathcal{D}_y$, or a monic element of $\mathcal{O}_K$ supported by $\mathcal{D}_y$ such that $D \mathcal{O}_K$ is not an $\ell$-th power of an ideal. Consider the map

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

Then the $K$-rational point $P_d^D \in JD[\lambda](K)$ is mapped to $\prod_{i=1}^{s} L_i^*(S_d, \ell) \setminus \prod_{i=1}^{s} L_i(S_d, \ell)$ under $\theta^D \delta^D$.

Proof. Since $D$ is supported by $\mathcal{D}_y$, $D$ is coprime to $\Delta_f$ and to all prime ideals $q \in S_f$. 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 $JD(K)$, by Lemma 5.6

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

Note that for all $P \in Z(J)$, the difference $x(P_d) - x(P)$ divides $\Delta_f$ and hence, it is coprime to $D$. Since $D \mathcal{O}_K$ is not an $\ell$-th power of an ideal, it follows that $D(x(P_d) - x(T_i)) \in L_i(S_d, \ell) \setminus L_i(S_d, \ell)$ for all $i = 1, \ldots, s$. \hfill \Box

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

$$
\# \{D \in \mathcal{D}(X) : \dim_{\mathbb{F}} \text{Sel}^{(\lambda)}(J, D, K) > n\} \gg \frac{X}{(\log X)^\varepsilon}. \tag{33}
$$

Proof. By Proposition 5.3, there is a positive $\ell$-th power-free rational integer $D_0$ such that $\dim_{\mathbb{F}} \text{Sel}^{(\lambda)}(J, D_0, K) > n$. Proposition 5.3 applied to $J = J_{D_0}$ and Lemma 4.9 together imply (33). \hfill \Box
THEOREM 5.6. Suppose that $K$ is a function field. Given a positive integer $n$, there are $D_0 \in \mathcal{O}_K$ and a set of prime ideals $\mathfrak{P}$ of $\mathcal{O}_K$ with positive Dirichlet density such that whenever $D$ is a monic element of $\mathcal{O}_K$ of degree divisible by $\ell$ such that $D\mathcal{O}_K$ is not an $\ell$-th power of an ideal and $D$ is supported by $\mathfrak{P}$,

$$ \dim_{\mathbb{F}} \operatorname{Sel}^{(\lambda)}(J_{D_0}, K) > n. $$

(34)

Proof. By 4.2.1 and Proposition 5.3, there is $D_0$ such that $\dim_{\mathbb{F}} \operatorname{Sel}^{(\lambda)}(J_{D_0}, K) > n$. Then, by Proposition 5.3 applied to $J_{D_0}$, we prove the result.

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

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

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

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 $D z^\ell = f(y)$ for some monic polynomial $f(y)$ of degree $\ell - 1$, defined over $\mathbb{Z}$. Note that the $K$-rational points $(\zeta_\ell^s : -\zeta_\ell^r : 0)$ in $F_D$ for $1 < s \leq \ell$ are mapped to the $K$-rational points

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

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

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 $v_\infty$ such that $K$ contains a primitive $n$-th root of unity. Let $p$ be a place in $M_K$. For a non-archimedean place $p$, we have the Hilbert norm residue symbol which is nondegenerate, and bilinear:

$$ \left( \frac{\alpha}{p} \right)_n : K_p^*/(K_p^*)^n \times K_p^*/(K_p^*)^n \to \mu_n. $$

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

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

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

Note that $\left( \frac{\alpha}{p} \right)_n = 1$ if and only if $x^n - \alpha$ has a root mod $p$, (provided that $\alpha \neq 0 \mod p$).
ON THE ARITHMETIC OF TWISTS OF SUPERELLIPTIC CURVES

If $\beta \in \mathcal{O}_F$ is coprime to $n$ and $\alpha$, we extend the power residue symbol as follows: let $\beta \mathcal{O}_F = p_1^{a_1} \cdots p_t^{a_t}$ be the prime ideal decomposition.

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

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

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

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

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 $n \geq 2$ is a positive integer coprime to $\text{char } K$.

Let $\alpha$ and $\beta$ be non-zero elements of $\mathcal{O}_K$ coprime to each other and to $n$. Then

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

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.

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

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

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

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

Hence, $(q^m - 1)/\ell \equiv 0 \mod \ell$, i.e., $q^m \equiv 1 \mod \ell^2$. 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 $q = q^{am + b\ell} \equiv (q^b)^\ell \mod \ell^2$. By definition,

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

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

Suppose that $\ell = 2$. Then $\xi_\ell = -1$. By the supplementary quadratic reciprocity laws, $1 = \left( \frac{\lambda}{q} \right)_\ell = (-1)^{(q - 1)/2}$ and $1 = \left( \frac{\xi_\ell}{q} \right)_\ell = (-1)(q^2 - 1)/8$ and, hence, $q \equiv 1 \mod 4$, and $q^2 \equiv 1 \mod 16$. It follows that $q \equiv 1 \mod 8$. If $q \equiv 1 \mod 8$, then $\left( \frac{q}{\mathcal{O}_K} \right)_\ell = 1$. □
COROLLARY 6.4. If $a$ is a positive rational integer coprime to $\ell$ such that $\left(\frac{a}{\pi v}\right)_\ell = 1$, then

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

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

Proof. Since $\left(\frac{a}{\pi v}\right)_\ell = 1$, by definition, it implies that $a \in (K^*\mathcal{O}_K)_\ell$ and, hence, the Hilbert residue symbol $\left(\frac{a}{\pi v}\right)_\ell = 1$. If $\ell = 2$, then there is an infinite place $v$ for which $K_v \cong \mathbb{R}$. Since $a \in (\mathbb{R}^*)_2$, $\left(\frac{a}{v}\right)_\ell = 1$. If $\ell \geq 3$, then the Hilbert residue symbol is trivial at all infinite places. Therefore, $\prod_{v|\ell} \left(\frac{\alpha a}{v}\right)_\ell = 1$ and, hence, the assertion follows from Theorem 6.2. $\square$

Let $k$ be a finite field of characteristic $q$, and let $K/k$ be a function field of one variable with a rational divisor $v_\infty$ (with $M_k^n = \{v_\infty\}$). Let $\pi_\infty$ be a uniformizer of the discrete valuation ring $\mathcal{O}_\infty$ of $K$ at $v_\infty$, and let $\text{ord}_\infty := \text{ord}_{v_\infty}$. Recall that a nonzero element $\alpha \in \mathcal{O}_K$ is monic (with respect to $\pi_\infty$) if $\pi_\infty^m \alpha \equiv 1 \mod \pi_\infty$ 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 $v_\infty$.

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

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

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

Proof. Let $K_{v_\infty}$ be the completion of $K$ at $v_\infty$. Let $\hat{\mathcal{O}}_{v_\infty} := \{\alpha \in K_{v_\infty} : |\alpha|_{v_\infty} \leq 1\}$, and $\hat{\mathbb{M}}_{v_\infty} := \{\alpha \in \hat{\mathcal{O}}_{v_\infty} : \alpha \equiv 1 \mod \hat{\mathbb{M}}_{v_\infty}\}$. By [Neu92], Chapter V, Sec 3, Proposition 3.4, for nonzero elements $\alpha$ and $\beta$ in $\mathcal{O}_K$,

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

(36)

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

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

Since $g$ and $h$ are monic, there are $a$ and $b$ in $\hat{\mathcal{O}}_{v_\infty}$ such that $a \equiv b \equiv 1 \mod \hat{\mathbb{M}}_{v_\infty}$, $g = a^{\text{ord}_\infty(g)}$, and $h = b^{\text{ord}_\infty(h)}$. It follows from Hensel’s lemma that $a$ and $b$ are contained in $(K^n_{v_\infty})^n$. Then, by Theorem 6.2,

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

By (36),

$\left(\frac{\pi_\infty, \pi_\infty}{v_\infty}\right)_n = (-1)^{(q^r-1)/n}$. $\square$
ON THE ARITHMETIC OF TWISTS OF SUPERELLIPTIC CURVES

Lemma 6.6. If $g$ is a monic element of $\mathcal{O}_K$ such that $\left(\frac{-1}{g}\right)_n = 1$, then for all monic elements $h$ of $\mathcal{O}_K$ 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 $\text{ord}_\infty(g) \cdot (q' - 1)/n \equiv 0 \mod 2$ and, hence, $\text{ord}_\infty(h) \cdot \text{ord}_\infty(g) \cdot (q' - 1)/n \equiv 0 \mod 2$. By Theorem 6.5, we proved the lemma.

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

Proof. The only non-trivial case is that $p | \ell$. Suppose that $p$ is a prime ideal of $\mathcal{O}_K$ such that $p | \ell$ and $\left(\frac{\alpha}{p}\right)_\ell = 1$. Let $m$ be an integer $> e\ell/(\ell - 1)$ where $e := \text{ord}_p(\ell \mathcal{O}_K)$. Then $\alpha \equiv a^e \mod p^m$ for some $a \in \mathcal{O}_K$ implies that $\alpha \in (K_p^*)^\ell$.

Acknowledgements

I wish to thank Professor Dino Lorenzini for many useful suggestions on this work as well as much of his help on the exposition of this paper.

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 $\text{II}(E, \mathbb{Q})$ 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.

Lieu94 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.

Sch99 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.
ON THE ARITHMETIC OF TWISTS OF SUPERELLIPTIC CURVES

Sto98 ______, On the arithmetic of the curves $y^2 = x^3 + A$ 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