ACTA ARITHMETICA
124.4 (2006)

On the arithmetic of twists of superelliptic curves

by

Sungkon Chang (Savannah, GA)

1. Introduction. By Faltings' theorem, a (smooth complete geometrically irreducible) curve of genus > 1 over a number field has finitely many rational points. By [2], it is widely believed that the number of these rational points is bounded in terms of the genus. In [12], prior to [2], 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 [19], 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 [11]), an answer to this problem is sometimes not known. For the case of elliptic curves, by Kolyvagin's result [7] and the modularity of elliptic curves proved by Wiles *et al.*, results such as [14], 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 [4], [24], [25], and [3] 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 obtain results about the distribution of a certain Selmer rank in this family of twists. These results imply 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 is > 1. Our result can be applied to Thue equations which can be mapped down to superelliptic curves considered in this paper. For the case of superelliptic curves over a constant

2000 *Mathematics Subject Classification*: Primary 11G99.

Key words and phrases: twists, superelliptic curves, Mordell–Weil rank, Selmer rank.

field and the case of hyperelliptic curves over $\mathbb{Q}$, finer results are obtained. In particular, using superelliptic curves over a constant field, we show in Theorem 3.12 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.

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 ℓ be a prime number different from $\operatorname{char} K$. Let C/K be the normalization of a superelliptic curve given by $y^\ell = f(x)$. For $D \in K^*$, we denote by C_D/K the normalization of the curve given by $y^\ell = D^d f(x/D)$ where $d := \deg(f)$, and by J_D/K the Jacobian variety of C_D. The Jacobian variety J_D is called an *ℓth power twist* of J. For the case of hyperelliptic curves (where $\ell = 2$), the plane curve $Dy^2 = f(x)$ is isomorphic to $y^2 = D^d f(x/D)$. We denote by $\operatorname{rank} J_D(K)$ the Mordell–Weil rank of $J_D(K)$ if $J_D(K)$ is a finitely generated (abelian) group. Let ζ_ℓ be a primitive ℓth root of unity, let F be $K(\zeta_\ell)$, and let $\lambda := 1 - \zeta_\ell$. Throughout the paper, we also denote by λ the endomorphism $1 - \zeta_\ell$ on J_F defined in [16, Sec. 3], and by $\mathsf{Sel}^{(\lambda)}(J, F)$ the *λ-Selmer group* of J_F.

In our work, we shall consider both the number field case and the function field case, but in this section we state results for number fields. The function fields considered in this paper are defined in 1.5, and the function field analogues of our results are stated in Theorems 3.10 and 4.5.

Let $k > 1$ be a positive integer, and denote by $\mathscr{P}_k(X)$ the set of all positive kth power-free integers up to X. Given a polynomial $f(x)$, let Δ_f denote the discriminant of $f(x)$. Let F be the field of fractions of a Dedekind domain $\mathscr{O}_F$, and let $\mathscr{D}$ be a set of prime ideals of $\mathscr{O}_F$. A nonzero element D of $\mathscr{O}_F$ is *supported by $\mathscr{D}$* if $D\mathscr{O}_F$ is divisible only by prime ideals contained in $\mathscr{D}$.

1.2. Theorem. *Let $K := \mathbb{Q}(\zeta_\ell)$ where ℓ is a regular prime number. Let $f(x)$ be a monic polynomial of prime degree p defined over $\mathbb{Z}$ such that $f(x)$ is irreducible over K, and $\ell \neq p$. Let $C/\mathbb{Q}$ be the normalization of the superelliptic curve $y^\ell = f(x)$, and let $J/\mathbb{Q}$ be the Jacobian variety of C. Let D_0 be a positive integer. Let $N := \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0}, K)$, and let M be the number of prime ideals of $\mathscr{O}_K$ dividing $\ell \Delta_f D_0$. Then there is a set $\mathscr{D}$ of prime numbers with Dirichlet density at least $(p-1)/(\ell^{(N+M+1)p!}(\ell-1)p!)$ such that whenever a positive integer D is supported by $\mathscr{D}$,*

$$\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0 D}, K) = N. \tag{1}$$

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

$$(2) \qquad \#\{D \in \mathscr{P}_\ell(X) : \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) = N\} \gg_{J,D_0} \frac{X}{(\log X)^{\varepsilon}}.$$

This theorem is proved using Schaefer's description of the λ-Selmer group [16]. The case of superelliptic curves $y^\ell = x^2 - A$ is considered by Stoll in [21], which in fact inspired our work (see Corollary 3.9). Schaefer's description is more complicated when $\ell \mid \deg(f)$; see [15].

Finer results on the distribution of Selmer ranks of twists of the Jacobian variety of a curve have only been obtained in special cases of elliptic curves; see [4], [6], [25], and [3]. As mentioned earlier, these results have application to the distribution of Mordell–Weil ranks of quadratic twists of elliptic curves considered in these papers. For our case, Corollary 3.7 shows the application to the distribution of Mordell–Weil rank in the ℓth power twists and, hence, by Silverman's result [19, p. 234], it has application to the number of rational points on these twists. Moreover, using Stoll's result [20, Theorem 1.1] yields a sharper result (see Corollary 3.8) about the distribution of the number of rational points for hyperelliptic curves.

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

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

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

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

Suppose that $\ell = 2$, and that $f(x)$ is any polynomial of odd degree with a root in $\mathbb{Q}$ such that $f(x)$ has distinct roots. Theorem 1.3 implies in particular that the 2-Selmer groups of quadratic twists of the hyperelliptic curve $y^2 = f(x)$ can be arbitrarily large, and this result seems new. However, for some elliptic curves, more is known. For instance, it is proved in [1] as a generalization of Lemmermeyer's work [8] that the 2-part of the Tate–Shafarevich groups of quadratic twists of the elliptic curves considered in this paper can be arbitrarily large.

It was asked by J. Silverman (see [14, p. 653]) whether given an elliptic curve $E/\mathbb{Q}$, there are infinitely many prime numbers p for which either E_p or E_{-p} has Mordell–Weil rank zero. The following corollary immediately follows from Theorem 1.2:

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

In [14, Corollary 3], Ono and Skinner proved that the question of Silverman has a positive answer for all elliptic curves with conductor ≤ 100. Using a specific example such as $E : y^2 = x^3 - 2$, we can show that Theorem 1.2 and Corollary 1.4 imply that there are infinitely many elliptic curves over $\mathbb{Q}$ for which the question of Silverman has a positive answer.

Little is known about the distribution of quadratic twists of an elliptic curve with Mordell–Weil rank 1, and the distribution of cubic twists of an elliptic curve with Mordell–Weil rank 0. Vatsal's result [23] for the case of quadratic twists, which is unconditional, proves the existence of a positive density of D's with $\operatorname{rank} E_D(\mathbb{Q}) = 1$. If we assume the finiteness of the Tate–Shafarevich groups of all elliptic curves over $\mathbb{Q}$, Theorem 1.2 and properties of the Cassels–Tate pairing yield a result about the distribution of quadratic twists with Mordell–Weil rank 1 as $\dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(E_D, \mathbb{Q}) = 1$ implies that $\operatorname{rank} E_D(\mathbb{Q}) = 1$; see also [5]. While there are several on-going investigations on the cubic twists, it seems that Lieman's result [9] is the only unconditional result at the moment. In Corollary 3.9, we obtain an unconditional result for the cubic twists. This corollary might be merely an observation following from Stoll's formula [21, Corollary 2.1], but it seems worth noting it.

We conclude this introduction by providing the reader with a road map for the proof of Theorem 1.2. Let L be a field isomorphic to $K[x]/(f)$. Using Schaefer's method, we have the first two rows of the commutative diagram

$$\begin{tikzcd}
J(K)/\lambda J(K) \arrow[r, "\delta"] \arrow[d, "\kappa_v"] & \mathsf{H}^1(K, J[\lambda])_{S_J} \arrow[r, "\theta"] \arrow[d, "\mathrm{res}_v"] & L(S_J, \ell) \arrow[r, "\mathrm{incl}"] \arrow[d, "\mathrm{res}_v"] \arrow[rd, "\Psi_J"] & L^*/(L^*)^\ell \arrow[d, "\mathrm{N}_{L/K}"] \\
J(K_v)/\lambda J(K_v) \arrow[r, "\delta_v"] \arrow[d, dotted, "\mathscr{H}_v^D"] & \mathsf{H}^1(K_v, J[\lambda]) \arrow[r, "\theta_v"] \arrow[d, "\mathrm{id}^D"] & L_v^*/(L_v^*)^\ell \arrow[d, equal] & K^*/(K^*)^\ell \arrow[d, equal] \\
J_D(K_v)/\lambda J_D(K_v) \arrow[r, "\delta_v^D"] & \mathsf{H}^1(K_v, J_D[\lambda]) \arrow[r, "\theta_v^D"] & L_v^*/(L_v^*)^\ell & K^*/(K^*)^\ell \\
J_D(K)/\lambda J_D(K) \arrow[r, "\delta^D"] \arrow[u, "\kappa_v"] & \mathsf{H}^1(K, J_D[\lambda])_{S_D} \arrow[r, "\theta^D"] \arrow[u, "\mathrm{res}_v"] & L(S_D, \ell) \arrow[r, "\mathrm{incl}"] \arrow[u, "\mathrm{res}_v"] \arrow[ru, "\Psi_D"] & L^*/(L^*)^\ell \arrow[u, "\mathrm{N}_{L/K}"]
\end{tikzcd} \tag{3}$$

Recall from 1.1 that the curve C_D is given by $y^\ell = f_D(x) := D^p f(x/D)$. Since $L \cong K[x]/(f_D)$, as in the case of J/K, we can construct a map $\theta^D : \mathsf{H}^1(K, J_D[\lambda]) \to L^*/(L^*)^\ell$. It is well known that the first two rows and the last two rows of (3) are commutative. It is noteworthy, though, that the targets of θ and θ^D are both $L^*/(L^*)^\ell$, and it can be understood as a consequence of the fact that the two group schemes $J[\lambda]$ and $J_D[\lambda]$ are isomorphic to each other.

Two key points we shall prove in Section 2 are the following: First, if D is an ℓth power in K_v for some v, then there is a map $\mathscr{H}_v^D : J(K_v) \to J_D(K_v)$ such that the diagram (3) commutes (see Proposition 2.5). It is clear that there is an isomorphism $J(K_v) \to J_D(K_v)$, but it is not so obvious, unless one knows the horizontal maps, that it commutes with the identity map on $L_v^*/(L_v^*)^\ell$. Secondly, if D is divisible only by prime ideals $\mathfrak{p}$ of $\mathscr{O}_K$ such that $\mathfrak{p}\mathscr{O}_L$ is prime, then $\ker \Psi_J = \ker \Psi_D$ in the diagram (3) (see Proposition 3.1). These two results imply that $\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K))$ is contained in $\theta(\mathsf{Sel}^{(\lambda)}(J, K))$ (see the proof of Theorem 3.6). By imposing more conditions on D (see 3.II), we can prove $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) = \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J, K)$. To exhibit the existence of (enough) such D's, we use the Chebotarev density theorem and the general reciprocity laws.

Notation

1.5. A *function field* of one variable over an arbitrary field k is a field extension K of k with transcendence degree 1 such that K is finitely generated over k, and k is algebraically closed in K. A function field of one variable with a *rational divisor* v_∞ is a function field K of one variable over a finite field k with a non-archimedean absolute value v_∞ on K/k of degree 1. Such function fields correspond to smooth complete curves $\mathscr{X}$ over k with a k-rational point p_∞ corresponding to the absolute value v_∞. For this type of function fields, we choose $\mathscr{O}_K := \{\alpha \in K : |\alpha|_v \le 1 \text{ for all } v \ne v_\infty\}$ to be a ring of integers in K, i.e., $\mathscr{O}_K$ is the ring of regular functions on the open subset $\mathscr{X} \setminus \{p_\infty\}$.

1.6. In this paper, a *global field* K is either a number field or a function field of one variable with a rational divisor v_∞. We denote by M_K the set of all places of K, by M_K^∞ the set of archimedean places or $\{v_\infty\}$ if K is a function field, and by M_K^0 the set $M_K \setminus M_K^\infty$. Throughout the paper, if L is a finite separable extension of K, let $\mathscr{O}_L$ denote the integral closure of $\mathscr{O}_K$ in L. We denote by $\overline{K}$ the algebraic closure of K, and by K_{sep} the (algebraic) separable closure of K. We denote by G_K the absolute Galois group $\mathrm{Gal}(K_{\mathrm{sep}}/K)$. For each $\mathfrak{q} \in M_K$, let $K_\mathfrak{q}$ denote the completion of K at $\mathfrak{q}$. We fix the algebraic closures $\overline{K}$ and $\overline{K}_\mathfrak{q}$, and fix an embedding $\kappa_\mathfrak{q} : K_{\mathrm{sep}} \hookrightarrow K_{\mathfrak{q},\mathrm{sep}}$. A *variety* J over an arbitrary field K is a separated scheme of finite type over K such that $J_{\overline{K}}$ is integral (i.e., reduced and irreducible).

2. The λ-Selmer group of twists. In this section, we introduce Schaefer's method for computing Selmer groups, and two key propositions which will prove the commutativity of the diagram (3). This method is introduced in [16] for number fields, and Schaefer's proofs generalize to the case of global fields.

2.1. Let ℓ be a prime number, and let K be a global field of characteristic $\neq \ell$ such that K contains a primitive ℓth root of unity ζ_ℓ. Let C/K be the curve in 1.1. Recall that $f(x)$ has distinct roots, and let $\{z_i \in K_{\mathrm{sep}} : i = 1, \dots, d\}$ be the roots of $f(x)$. If $f(x)$ does not have a K-rational root, then we set $d' := d$, and if $f(x)$ has a K-rational root z_d, then we set $d' := d - 1$. Then we define $X := \{z_1, \dots, z_{d'}\}$.

Let $Z(C)$ be a set of representatives of the G_K-orbits in X. For each $v \in M_K$, we denote by X_v the image of X under κ_v defined in 1.6. We choose the set $Z(C, \mathfrak{q})$ of representatives of the G_{K_v}-orbits in X_v such that $Z(C) \hookrightarrow Z(C, \mathfrak{q})$ under $\kappa_{\mathfrak{q}}$. Write $Z(C) = \{y_1, \dots, y_s\}$, and let $L_i := K(y_i)$ for $i = 1, \dots, s$. Given a set of places S containing M_K^∞ and places over ℓ, we define

$$\mathscr{C}(S, \ell) := \prod_{z \in Z(C)} K(z)(S, \ell) = \prod_{i=1}^{s} L_i(S, \ell),$$

$$\mathscr{C}_{\mathfrak{q}} := \prod_{z \in Z(C, \mathfrak{q})} K_{\mathfrak{q}}(z)^*/(K_{\mathfrak{q}}(z)^*)^\ell;$$

see [16, Sec. 2.3] for the definition of $L_i(S, \ell)$. We denote the product $\prod_{z \in Z(C)} K(z)^*/(K(z)^*)^\ell$ by $\mathscr{C}$. Then, by the method introduced in [16], if S is a subset of M_K containing M_K^∞, the places above ℓ, and the places of bad reduction of J/K, then the subgroup $\mathsf{H}^1(K, J[\lambda])_S$ unramified outside S is isomorphic to the kernel of the norm map, $\ker(\mathrm{N} : \mathscr{C}(S, \ell) \to K(S, \ell))$ when $\# X = d$, and isomorphic to $\mathscr{C}(S, \ell)$ when $\# X = d - 1$. In fact, we have an injective map $\mathsf{H}^1(K, J[\lambda]) \to \mathscr{C}$ extending $\mathsf{H}^1(K, J[\lambda])_S \to \mathscr{C}(S, \ell)$, and we denote the extension by θ. This map is also defined for $K_{\mathfrak{q}}$, and we denote it by $\theta_{\mathfrak{q}} : \mathsf{H}^1(K_{\mathfrak{q}}, J[\lambda]) \to \mathscr{C}_{\mathfrak{q}}$. For each $\mathfrak{q} \in M_K$, we have a natural map $\mathscr{C} \to \mathscr{C}_{\mathfrak{q}}$ denoted also by $\mathrm{res}_{\mathfrak{q}}$, and $\mathsf{Sel}^{(\lambda)}(J, K)$ can be described as a subgroup of $\mathscr{C}$ as follows: If $f(x)$ does not have a K-rational root, then $\mathsf{Sel}^{(\lambda)}(J, K)$ is isomorphic to

$$\{\alpha \in \mathscr{C}(S, \ell) : \mathrm{N}(\alpha) = 1,\ \mathrm{res}_v(\alpha) \in \mathrm{Im}\, \theta_v \circ \delta_v \text{ for all } v \in S\}.$$

If $f(x)$ has a K-rational root, then we have a simpler description:

$$\mathsf{Sel}^{(\lambda)}(J, K) \cong \{\alpha \in \mathscr{C}(S, \ell) : \mathrm{res}_v(\alpha) \in \mathrm{Im}\, \theta_v \circ \delta_v \text{ for all } v \in S\}.$$

Note that we have an injective homomorphism $\theta \circ \delta : J(K)/\lambda J(K) \to \mathscr{C}$, and, in [16], a useful description of this map is provided. Write $K_{\mathrm{sep}}(C_{K_{\mathrm{sep}}})$ as the field of fractions of $K_{\mathrm{sep}}[x, y]/(y^\ell - f(x))$. Then we denote by $f_{z_i}(x, y)$ the function $x - z_i$. The function f_{z_i} can be considered as a function on divisors of C. Then, by [16, Sec. 2], we have a well defined homomorphism $\mathrm{Pic}^0(C) \to \mathscr{C}$ given by $[D] \mapsto (f_z(E) : z \in Z(C))$ where $E = \sum n_R(R)$ is a divisor in $\mathrm{Div}(C)$ such that the support of E *avoids* X (see [16, p. 450]),

$K(R)/K$ are separable for all R with $n_R \neq 0$, and $[E] = [D]$. We denote this map by $\overline{\delta}$.

The lemma below is [16, Theorem 2.3 and Proposition 3.3] if $\# X = d$. The proposition in [16] essentially shows that $[(\infty)] = [D]$ for some divisor D avoiding Y such that $(f_z(D) : z \in Z(C))$ is trivial in $\mathscr{C}$ where $Y = \{z_1, \ldots, z_d\}$. Using this, we can prove

2.2. Lemma. *The map* $\overline{\delta} : \mathrm{Pic}^0(C) \to \mathscr{C}$ *is equal to* $\theta \circ \delta$. *Suppose that* $f(x)$ *has a* K*-rational root* z_d. *If* E *is a nonzero divisor in* $\mathrm{Div}^0(C)$ *such that* $E = (Q) - (\deg_K(Q))(\infty)$ *for some* Q *avoiding* X, *and* $K(Q)/K$ *is separable*, *then* $[E]$ *is mapped to* $(f_z(Q) : z \in Z(C))$ *under* $\overline{\delta}$. *In particular*, $[(z_d, 0) - (\infty)] \mapsto (f_z(z_d, 0) : z \in Z(C))$.

Proof. The proof is left to the reader. ∎

Let us prove the commutativity of the diagram (3) in a slightly more general context. Recall that $f(x) = (x - z_1) \cdots (x - z_d)$. Then $D^d f(x/D) = (x - z_1 D) \cdots (x - z_d D)$ for $D \in K^*$. For $D \in K^*$ and $\mathfrak{q} \in M_K$, we define

$$X^D := \{z_i D : i = 1, \ldots, d'\}, \quad X_{\mathfrak{q}}^D := \{\kappa_{\mathfrak{q}}(z_i D) : i = 1, \ldots, d'\}.$$

Let $Z(C_D) := \{zD : z \in Z(C)\}$. It is a set of representatives of G_K-orbits in X^D, and this choice is said to be *compatible with* $Z(C)$. We choose $Z(C_D, \mathfrak{q})$ to be compatible with $Z(C, \mathfrak{q})$; hence, $Z(C_D) \subset Z(C_D, \mathfrak{q})$. As in the case of C/K, with respect to $Z(C_D)$ and $Z(C_D, \mathfrak{q})$, we have $\mathscr{C}_D$ and $(\mathscr{C}_{\mathfrak{q}})_D$, and the maps θ^D and $\theta_{\mathfrak{q}}^D$. Then it follows from the choice of $Z(C_D)$ and $Z(C_D, \mathfrak{q})$ that $\mathscr{C}_D = \mathscr{C}$ and $(\mathscr{C}_{\mathfrak{q}})_D = \mathscr{C}_{\mathfrak{q}}$ for all $\mathfrak{q} \in M_K$.

2.3. Let S be a subset of M_K containing M_K^∞, the places above ℓ, and the places of bad reduction of J_D/K. Then $\mathsf{Sel}^{(\lambda)}(J_D, K)$ is described as a subgroup of the fixed space $\mathscr{C}$ as follows:

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

In a slightly more general context, we introduced above all the horizontal maps in (3). Proposition 2.4 below is one of the key propositions which establishes the commutativity of the diagram formed by the restriction maps in the second and third columns of (3). The proof of this proposition is left to the reader.

2.4. Proposition. *For each* $\mathfrak{q} \in M_K$, *the following diagram commutes for all* $D \in K^*$:

$$\begin{tikzcd}
\mathsf{H}^1(K, J_D[\lambda]) \arrow[r, "\theta^D"] \arrow[d, "\mathrm{res}_{\mathfrak{q}}"] & \mathscr{C} \arrow[d, "\mathrm{res}_{\mathfrak{q}}"'] \\
\mathsf{H}^1(K_{\mathfrak{q}}, J_D[\lambda]) \arrow[r, "\theta_{\mathfrak{q}}^D"] & \mathscr{C}_{\mathfrak{q}}
\end{tikzcd}$$

Proposition 2.5 below completes the proof of the commutativity of the diagram (3).

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

$$\begin{tikzcd} J_D(K_{\mathfrak{q}})/\lambda J_D(K_{\mathfrak{q}}) \arrow[r, "\theta_{\mathfrak{q}}^D\delta_{\mathfrak{q}}^D"] & \mathscr{C}_{\mathfrak{q}} \\ J(K_{\mathfrak{q}})/\lambda J(K_{\mathfrak{q}}) \arrow[u, "\mathscr{H}_D"] \arrow[r, "\theta_{\mathfrak{q}}\delta_{\mathfrak{q}}"] & \mathscr{C}_{\mathfrak{q}} \arrow[u, "\mathrm{id}"'] \end{tikzcd} \tag{4}$$

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

Proof. Let D be a nonzero element of $\mathscr{O}_K$ such that $D \in (K_{\mathfrak{q}}^*)^\ell$. Then we have an isomorphism $(C_D)_{K_{\mathfrak{q}}} \to C_{K_{\mathfrak{q}}}$ given by $(x,y) \mapsto (x/D, y/\sqrt[\ell]{D^d})$, and this isomorphism induces an isomorphism $\mathscr{H}_D : J(K_{\mathfrak{q}}) \to J_D(K_{\mathfrak{q}})$ by pulling back on the divisors. Recall $Z(C_D,\mathfrak{q}) = \{zD : z \in Z(C,\mathfrak{q})\}$. Let $E := \sum n_j(R_j)$ be a divisor in $\mathrm{Div}^0(C_{K_{\mathfrak{q}},\mathrm{sep}})$ avoiding $X_{\mathfrak{q}}$ such that $K_{\mathfrak{q}}(R_j)/K_{\mathfrak{q}}$ are separable, and write $R_j = (x_j, y_j)$. Then, for any $z \in Z(C,\mathfrak{q})$,

$$\begin{aligned} f_{zD}(\mathscr{H}_D(E)) &= \prod_j (f_{zD}(x_jD, y_j\sqrt[\ell]{D^d}))^{n_j} = \prod_j (x_jD - zD)^{n_j} \\ &= D^{\sum n_j}\prod_j (x_j - z)^{n_j} = \prod_j (x_j - z)^{n_j}, \\ f_z(E) &= \prod_j (f_z(x_j,y_j))^{n_j} = \prod_j (x_j - z)^{n_j}. \end{aligned}$$

This proves the commutativity of the diagram (4). ∎

3. The Jacobian varieties without λ-torsion points. In this section, we prove Theorem 1.2, and state its analogue for the function field case. Let ℓ be a prime number, and let K be a global field of characteristic $\neq \ell$, containing a primitive ℓth root of unity ζ_ℓ. Let C/K be the curve in 1.1, and suppose that $f(x)$ is a monic polynomial of prime degree p defined over K such that $f(x)$ is irreducible over K, and $\ell \neq p$. For the number field case, suppose that $f(x)$ is defined over $\mathbb{Z}$. Let Δ_f be the discriminant of $f(x)$. We keep all the notation and definitions introduced in Section 2. Let S_J denote the subset of M_K containing M_K^∞, the places dividing $\ell\Delta_f$. For each nonzero element D of $\mathscr{O}_K$, let S_D denote the set $S_J \cup \{\mathfrak{p} \in M_K^0 : \mathfrak{p} \mid D\mathscr{O}_K\}$. Then the sets S_J and S_D contain the set of places of bad reduction of J/K and J_D/K, respectively. Recall that $X := \{z_1, \ldots, z_d\}$. Since X forms one orbit, $Z(C)$

contains a single point, and we choose $Z(C) := \{z_1\}$ as a representative. Let L denote the finite separable field extension $L_1 := K(z_1)$ of degree p. Then $\mathscr{C} := L^*/(L^*)^\ell$ as defined in Section 2.

3.1. Proposition. *Let D be a nonzero element of $\mathscr{O}_K$, and suppose that $D\mathscr{O}_K$ is supported by the set of prime ideals $\mathfrak{q}$ of $\mathscr{O}_K$ such that either $\mathfrak{q}\mathscr{O}_L$ is prime in $\mathscr{O}_L$ or $\mathfrak{q}\mathscr{O}_L = \mathfrak{p}^p$ for some prime ideal $\mathfrak{p}$ of $\mathscr{O}_L$. Then*

$$\ker(\mathrm{N}_{L/K} : L(S_J,\ell) \to K(S_J,\ell)) = \ker(\mathrm{N}_{L/K} : L(S_D,\ell) \to K(S_D,\ell)).$$

Hence,

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

as subgroups of $L^*/(L^*)^\ell$.

Proof. The proof is left to the reader. ∎

The Legendre symbol is used throughout Sections 3 and 4. Some results on Legendre symbols required to prove our main results are introduced in Appendix A. In A.1, we extend the definition of the symbol to prime ideals dividing $\ell\mathscr{O}_K$ and archimedean places, so that given $\alpha \in \mathscr{O}_K$ and $\mathfrak{p} \in M_K$, $\left(\frac{\alpha}{\mathfrak{p}}\right)_\ell = 1$ implies $\alpha \in (K_\mathfrak{p}^*)^\ell$.

3.I. *The case of number fields*

Suppose that $K = \mathbb{Q}(\zeta_\ell)$, and that ℓ is a regular prime number.

3.2. Let W be a finite subset of $\mathscr{O}_L\backslash\{0\}$. We denote by $\mathscr{D}_W$ the set of prime numbers $q \in \mathbb{Z}$ not dividing ℓ which have the following properties: for all prime ideals $\mathfrak{q}$ of $\mathscr{O}_K$ dividing q, (1) the ideal $\mathfrak{q}\mathscr{O}_L$ is prime; (2) $\alpha \not\equiv 0 \bmod \mathfrak{q}\mathscr{O}_L$, and $\left(\frac{\alpha}{\mathfrak{q}\mathscr{O}_L}\right)_\ell = 1$ for all $\alpha \in W$.

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

Proof. The proof is left to the reader. ∎

3.4. Proposition. *Let W be a finite subset of $\mathscr{O}_L\backslash\{0\}$, and let $\mathscr{D}_W$ be the set of prime numbers defined in* 3.2. *Then $\mathscr{D}_W$ contains a set of prime numbers in $\mathbb{Z}$ with Dirichlet density at least $(p-1)/(\ell^{(\# W)p!}(\ell-1)p!)$.*

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 $m := [M' : L] \not\equiv 0 \bmod p$, and $[M : M'] = \ell^n$ for some nonnegative integer n. Hence, $[M : K] = pm\ell^n$. Let G denote the group $\mathrm{Gal}(M/\mathbb{Q})$. Then $\mathrm{Gal}(M/K)$ is a subgroup of G, and the group G contains an automorphism τ of order p acting trivially on K. Moreover, the subgroup $\langle\tau\rangle$ of G is stable under conjugation. Therefore, the subset $H := \{\tau^k : k = 1, \ldots, p-1\}$ is stable under conjugation in G.

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

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

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

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

$$p=|\mathrm{Frob}(\mathfrak{Q}/q)|=f(\mathfrak{Q}/q)=f(\mathfrak{Q}/\mathfrak{Q}_L)f(\mathfrak{Q}_L/\mathfrak{q})f(\mathfrak{q}/q). \tag{5}$$

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

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

3.5. LEMMA. *Let W be a finite subset of $\mathscr{O}_L\backslash\{0\}$ containing ζ_ℓ. Let $\mathscr{D}_W$ be the set of prime numbers defined in* 3.2. *Let $\mathfrak{q}$ be a place of K. If $\mathfrak{q}$ is a prime ideal of $\mathscr{O}_K$, then we choose $\alpha_\mathfrak{q}\in\mathscr{O}_K$ such that $\mathfrak{q}^m=\alpha_\mathfrak{q}\mathscr{O}_K$ where m is the order of $\mathfrak{q}$ in* $\mathrm{Cl}(\mathscr{O}_K)$, *and if $\mathfrak{q}=\lambda\mathscr{O}_K$, then we choose $\alpha_\mathfrak{q}:=\lambda$. If $\mathfrak{q}$ is an infinite place of K, or if $\mathfrak{q}$ is a prime ideal of $\mathscr{O}_K$ such that $\alpha_\mathfrak{q}\in W$, then $\left(\frac{D}{\mathfrak{q}}\right)_\ell=1$ for all positive integers D supported by $\mathscr{D}_W$.*

Proof. Suppose that $\mathfrak{q}$ is a prime ideal of $\mathscr{O}_K$ not dividing $\ell\mathscr{O}_K$, and $\mathfrak{q}^m=\alpha_\mathfrak{q}\mathscr{O}_K$ where m is the order of $\mathfrak{q}$ in $\mathrm{Cl}(\mathscr{O}_K)$. Let q be a prime number dividing D, and suppose that $\alpha_\mathfrak{q}\in W$. Let $q\mathscr{O}_K=\prod_{j=1}^t\mathfrak{p}_j^n$ be a prime ideal decomposition. Since $q\in\mathscr{D}_W$, it follows that $\left(\frac{\alpha_\mathfrak{q}}{\mathfrak{p}_j\mathscr{O}_L}\right)_\ell=1$ and, hence, by Lemma 3.3, $\left(\frac{\alpha_\mathfrak{q}}{\mathfrak{p}_j}\right)_\ell=1$. Then

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

Since W contains ζ_ℓ and λ, it follows that $\left(\frac{\zeta_\ell}{\mathfrak{p}_1}\right)_\ell = 1$. If $\ell = 2$, then $K = \mathbb{Q}$, and it follows that $\left(\frac{-1}{\mathfrak{p}_1}\right)_2 = \left(\frac{2}{\mathfrak{p}_1}\right)_2 = 1$. By Lemma A.2, $\left(\frac{q}{\lambda\mathscr{O}_K}\right)_\ell = 1$. By Corollary A.3,

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

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

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

Let us return to the context of our superelliptic curves. Recall that $L := K(z_1)$. For all $D \in K^*$, we have $\mathsf{Sel}^{(\lambda)}(J_D, K) \subset \mathsf{H}^1(K, J_D[\lambda])_{S_D} \hookrightarrow L^*/(L^*)^\ell$ under θ^D.

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

Proof. Let W_J be a subset of $\mathscr{O}_L$ generating $\theta(\mathsf{Sel}^{(\lambda)}(J, K))$. For each prime ideal $\mathfrak{q}$ of $\mathscr{O}_K$, let us fix an element $\alpha_\mathfrak{q}$ of $\mathscr{O}_K$ as in Lemma 3.5. Recall the set S_J, and let $Y_J := \{\zeta_\ell\} \cup W_J \cup \{\alpha_\mathfrak{q} \in \mathscr{O}_K : \mathfrak{q} \in S_J \cap M_K^0\}$. Let $\mathscr{D}_{Y_J}$ be the set of prime numbers defined in 3.2 for $W = Y_J$. Then, by Proposition 3.4, $\mathscr{D}_{Y_J}$ contains a set $\mathscr{D}$ of prime numbers with Dirichlet density at least $(p-1)/(\ell^{(N+M+1)p!}(\ell-1)p!)$.

Let D be a positive integer supported by $\mathscr{D}$. Let us show that

$$\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K)) \subset \theta(\mathsf{Sel}^{(\lambda)}(J, K)).$$

Let $\alpha \in \theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K))$. By 2.3, $\theta(\mathsf{Sel}^{(\lambda)}(J, K))$ and $\theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K))$ are subgroups of $\theta(\mathsf{H}^1(K, J[\lambda])_{S_J})$ and $\theta^D(\mathsf{H}^1(K, J_D[\lambda])_{S_D})$, respectively. By Proposition 3.1, we have $\theta^D(\mathsf{H}^1(K, J_D[\lambda])_{S_D}) = \theta(\mathsf{H}^1(K, J[\lambda])_{S_J})$; hence, α is contained in $\theta(\mathsf{H}^1(K, J[\lambda])_{S_J})$. Let $\mathfrak{q}$ be a place in S_J. Then $\mathfrak{q}$ is contained in S_D. By Lemma 3.5, $\left(\frac{D}{\mathfrak{q}}\right)_\ell = 1$, and by Hensel's lemma, this implies that $D \in (K_\mathfrak{q}^*)^\ell$. By Proposition 2.5, it follows that $\operatorname{Im}\theta_\mathfrak{q}\delta_\mathfrak{q} = \operatorname{Im}\theta_\mathfrak{q}^D\delta_\mathfrak{q}^D$ and, hence, α is contained in $\operatorname{Im}\theta_\mathfrak{q}\delta_\mathfrak{q}$ since $\alpha \in \theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K))$. Thus, $\alpha \in \theta(\mathsf{Sel}^{(\lambda)}(J, K))$.

Let us show that

$$\theta(\mathsf{Sel}^{(\lambda)}(J, K)) \subset \theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K)).$$

Let $\alpha \in \theta(\mathsf{Sel}^{(\lambda)}(J, K))$. By Proposition 3.1, $\alpha \in \theta^D(\mathsf{H}^1(K, J_D[\lambda])_{S_D})$. If $\mathfrak{q}$ is a place in S_J, then we showed above $D \in (K_\mathfrak{q}^*)^\ell$, and by Proposition 2.5,

$\operatorname{Im}\theta_{\mathfrak{q}}\delta_{\mathfrak{q}} = \operatorname{Im}\theta_{\mathfrak{q}}^D\delta_{\mathfrak{q}}^D$. Thus, $\alpha \in \operatorname{Im}\theta_{\mathfrak{q}}^D\delta_{\mathfrak{q}}^D$ for all $\mathfrak{q} \in S_J$. Let $\mathfrak{q}$ be a prime ideal in $S_D \setminus S_J$. Since D is supported by $\mathscr{D}$, we have $\left(\frac{\beta}{\mathfrak{q}}\right)_\ell = 1$ for all $\beta \in W_J$. Since W_J generates $\theta(\mathsf{Sel}^{(\lambda)}(J,K))$, it follows that $\left(\frac{\alpha}{\mathfrak{q}\mathscr{O}_L}\right)_\ell = 1$, i.e., $\alpha \in (L_{\mathfrak{P}}^*)^\ell$ where $\mathfrak{P} := \mathfrak{q}\mathscr{O}_L$. Recall the natural map $\operatorname{res}_{\mathfrak{q}} : L^*/(L^*)^\ell \to \mathscr{C}_{\mathfrak{q}}$. Since $\mathfrak{q}\mathscr{O}_L$ is prime, $\mathscr{C}_{\mathfrak{q}} = L_{\mathfrak{P}}^*/(L_{\mathfrak{P}}^*)^\ell$. Thus, $\left(\frac{\alpha}{\mathfrak{q}\mathscr{O}_L}\right)_\ell = 1$ implies $\operatorname{res}_{\mathfrak{q}}(\alpha) = 1$ and, in particular, $\operatorname{res}_{\mathfrak{q}}(\alpha) \in \operatorname{Im}\theta_{\mathfrak{q}}^D\delta_{\mathfrak{q}}^D$. We established that $\operatorname{res}_{\mathfrak{q}}(\alpha) \in \operatorname{Im}\theta_{\mathfrak{q}}^D\delta_{\mathfrak{q}}^D$ for all $\mathfrak{q} \in S_D$. Therefore, α is contained in $\theta^D(\mathsf{Sel}^{(\lambda)}(J_D,K))$. Since θ and θ^D are injective maps, the dimensions of the two Selmer groups are equal to each other. ∎

The proof of Theorem 1.2 follows from Theorem 3.6 and [18, Theorem 2.4].

3.7. Corollary. *Assume the same hypotheses as in Theorem* 1.2. *Then there is a positive constant* $\varepsilon < 1$ *such that*

$$\#\{D \in \mathscr{P}_\ell(X) : \operatorname{rank} J_D(\mathbb{Q}) \le N\} \gg_{J,D_0} X/(\log X)^\varepsilon.$$

Proof. The result follows from [16, Corollary 3.7 and Proposition 3.8]. ∎

3.8. Corollary. *Suppose that* $\ell = 2$ *and* $\deg(f) \ge 5$, *and that there is a positive integer* D_0 *such that* $N := \dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(J_{D_0},\mathbb{Q}) < (p-1)/2$. *Then there is a positive constant* $\varepsilon < 1$ *depending on* C *and* D_0 *such that*

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

Proof. Let ι be the hyperelliptic involution on C_D. In [20, Theorem 1.1], Stoll proves 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 $\# S \le (p-1)/2$ and $S \cap \iota(S) = \emptyset$ generates a subgroup of rank $\# S$ in $J_D(\mathbb{Q})$. By Theorem 1.2, $\#\{D \in \mathscr{P}_2(X) : \dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(J_D,\mathbb{Q}) = N\} \gg X/(\log X)^\varepsilon$. Let D be a positive integer not supported by T such that $\dim_{\mathbb{F}_2} \mathsf{Sel}^{(2)}(J_D,\mathbb{Q}) = N$. Then, by Stoll's theorem and Corollary 3.7, $C_D(\mathbb{Q})$ cannot contain a subset S such that $\# S > N$ and $S \cap \iota(S) = \emptyset$. Since $C_D(\mathbb{Q})$ does not contain a point fixed under the involution, except ∞, we conclude $\# C_D(\mathbb{Q}) \le 2N+1$. ∎

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

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

Proof. By [21, Corollary 2.1], $\dim_{\mathbb{F}_3} \mathsf{Sel}^{(\lambda)}(E,K) = 0$ where $\lambda = 1 - \zeta_3$ and $K = \mathbb{Q}(\zeta_3)$. As A is square-free and coprime to 3, the polynomial $y^2 + AD^2$ is irreducible over K, and the result follows immediately from Corollary 3.7 with $\ell = 3$. ∎

3.II. *The case of function fields*

The proof of the function field analogue of Theorem 1.2 is treated differently. However, it is essentially the same, and we shall just state the result without proof. Let k be a finite field containing a primitive ℓth root of unity ζ_ℓ; hence, $\operatorname{char} k \neq \ell$. Let K/k be a function field of one variable with a rational divisor v_∞ such that $\mathrm{Cl}(\mathscr{O}_K)[\ell] \not\equiv 0 \bmod \ell$. Let π_∞ be a uniformizer of the discrete valuation ring $\mathscr{O}_\infty$ of K at v_∞, and let $\mathrm{ord}_\infty := \mathrm{ord}_{v_\infty}$. Note that each nonconstant element g of $\mathscr{O}_K$ is not an element of the valuation ring $\mathscr{O}_\infty$, i.e., $\mathrm{ord}_{v_\infty}(g) < 0$. The *leading coefficient* of a nonzero element g of $\mathscr{O}_K$ (with respect to π_∞) is the constant $a \in k^*$ such that $\pi_\infty^m g \equiv a \bmod \pi_\infty$ for some $m \in \mathbb{Z}$. The element g is *monic* if the leading coefficient is 1. The *degree* of an element g of $\mathscr{O}_K$, denoted by $\deg(g)$, is $-\mathrm{ord}_\infty(g)$.

3.10. THEOREM. *Let D_0 be a nonzero element of $\mathscr{O}_K$, define $N := \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0}, K)$, and let M the number of prime ideals of $\mathscr{O}_K$ dividing $\ell\Delta_f D_0$. Then there is a set $\mathscr{D}$ of prime ideals of $\mathscr{O}_K$ with Dirichlet density at least $(p-1)/(\ell^{(N+M+1)p!}p!)$ such that whenever D is a monic element of $\mathscr{O}_K$ supported by $\mathscr{D}$ such that* $\deg(D)$ *is divisible by ℓ, we have* $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_{D_0 D}, K) = N$.

3.11. Given an infinite set $\mathscr{D}$ of prime ideals of $\mathscr{O}_K$, there are indeed infinitely many classes in $K^*/(K^*)^\ell$ represented by $D \in \mathscr{O}_K$ which is supported by $\mathscr{D}$ and $\deg(D) \equiv 0 \bmod \ell$. Thus, Theorem 3.10 implies that there are infinitely many twists with Selmer rank N. The ℓ-divisibility condition on $\deg(D)$ is due to the local condition at $v_\infty \in M_K^\infty$—the Legendre symbol over v_∞ is introduced in Appendix A.

3.12. THEOREM. *Suppose that $f(x)$ is defined over k. Let k' be the finite extension of k of degree $p :=$* $\deg(f)$. *Let $L := K \otimes k'$. Suppose that* $\dim_{\mathbb{F}_\ell} \mathrm{Cl}(\mathscr{O}_L)[\ell] = 0$. *Then* $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J, K) = 0$.

Let E/k be the constant Jacobian variety of the normalization of the superelliptic curve $y^\ell = f(x)$ over k. Then there is a set $\mathscr{D}$ of prime ideals of $\mathscr{O}_K$ with Dirichlet density $(p-1)/p$ such that whenever D is an element of $\mathscr{O}_K$ supported by $\mathscr{D}$, $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) = 0$ *and* $\# C_D(K) \leq \# E(k)$; *moreover*, $\operatorname{rank} J_D(K) = 0$.

Proof. Note that L/K is Galois. Then $S_J = M_K^\infty$, and $\mathsf{H}^1(K, J[\lambda])_{M_K^\infty}$ is isomorphic to $\ker(\mathrm{N}_{L/K} : L(M_K^\infty, \ell) \to K(M_K^\infty, \ell))$. Since the subgroup $\mathrm{Cl}(\mathscr{O}_L)[\ell]$ is trivial, by Lemma 3.13 below, $\mathsf{H}^1(K, J[\lambda])_{M_K^\infty} = 1$ and, hence, $\mathsf{Sel}^{(\lambda)}(J, K) = 0$.

Let $\mathscr{D}$ be the set of prime ideals $\mathfrak{q}$ of $\mathscr{O}_K$ such that $\mathfrak{q}\mathscr{O}_L$ is prime. Then $\mathscr{D}$ has Dirichlet density $(p-1)/p$. If D is an element of $\mathscr{O}_K$ supported by $\mathscr{D}$, then, by Proposition 3.1, $\theta^D(\mathsf{H}^1(K, J_D[\lambda])_{S_D}) = \theta(\mathsf{H}^1(K, J[\lambda])_{S_J}) = 1$ and, hence, $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) = 0$. By [16, Corollary 3.7],

$$\operatorname{rank} J_D(K) \le (\ell - 1) \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) = 0.$$

Suppose that D is not a unit in $\mathscr{O}_K$, and let $F := K(\sqrt[\ell]{D})$. Then k is algebraically closed in F, and $F \subset K_{\mathrm{sep}}$ since $\ell \neq \operatorname{char} K$. Since $(C_D)_F \cong C_F$ as F-schemes, by Proposition 3.15 below, $\# J_D(K)_{\mathrm{Tor}} \le \# E(k)$. Since $J_D(K) = J_D(K)_{\mathrm{Tor}}$, the result follows. ∎

The hypothesis in Theorem 3.12 is often satisfied. Let K be a function field of one variable with a rational divisor v_∞, and let $\mathscr{X}/k$ be the smooth curve with function field K. Then, by Proposition 3.14, $\# \mathrm{Cl}(\mathscr{O}_K) = \# \mathrm{Pic}^0(\mathscr{X})$. Let $L := K \otimes k'$ for a finite extension k' of k. Then $\# \mathrm{Cl}(\mathscr{O}_L) = \# \mathrm{Pic}^0(\mathscr{X}_{k'})$. Therefore, for all but finitely many prime numbers ℓ, we have $\# \mathrm{Cl}(\mathscr{O}_L) = \# \mathrm{Pic}^0(\mathscr{X}_{k'}) \not\equiv 0 \bmod \ell$. Thus, we find examples of superelliptic curves of arbitrarily large genus which satisfy the conditions in Theorem 3.12. For the curves C considered in Theorem 3.12, there are infinitely many D's such that $\# C_D(K)$ is bounded. In [17], 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.

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

Proof. Since $\mathrm{Cl}(\mathscr{O}_L)[\ell] = 1$, the subgroup $L(M_K^\infty, \ell)$ is isomorphic to $\mathscr{O}_L^*/(\mathscr{O}_L^*)^\ell$. It follows from Proposition 3.14 below that $\mathscr{O}_L^* = (k')^*$. Hence, $\ker(\mathrm{N}_{L/K} : L(M_K^\infty, \ell) \to K(M_K^\infty, \ell))$ is isomorphic to $\ker(\mathrm{N}_{k'/k} : k'^*/(k'^*)^\ell \to k^*/(k^*)^\ell)$. The result follows from this description. ∎

3.14. Proposition. *Let k' be a finite field. Let $\mathscr{X}/k'$ be a smooth complete curve with function field F such that $\mathscr{X}$ has a rational divisor v_∞. Then there is a k'-morphism $\mathscr{X} \to \mathbb{P}^1_{k'}$ such that v_∞ is totally ramified over a rational divisor in $\mathbb{P}^1_{k'}$. Let $\mathscr{O}_F$ be the ring of integers defined in* 1.6 *with $M_F^\infty := \{v_\infty\}$. Then the group of units $\mathscr{O}_F^*$ is $(k')^*$, and $\# \mathrm{Cl}(\mathscr{O}_F) = \# \mathrm{Pic}^0(\mathscr{X})$. Hence, the class number of $\mathscr{O}_F$ does not depend on the choice of a rational divisor on F.*

Proof. Using the Riemann–Roch theorem, we can find a function g in $k'(\mathscr{X})$ with poles supported only by v_∞. Then the function g induces a morphism $\mathscr{X} \to \mathbb{P}^1_{k'}$ such that v_∞ is totally ramified over a rational point $\infty \in \mathbb{P}^1_{k'}$. To finish the proof, we use [10, Sec. VIII, p. 299]. ∎

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

Proof. Note that $J(\overline{k})_{\mathrm{Tor}} = J(\overline{K})_{\mathrm{Tor}} = J(K_{\mathrm{sep}})_{\mathrm{Tor}}$. Then

$$J_{C'}(K)_{\mathrm{Tor}} \subset J_{C'}(F)_{\mathrm{Tor}} \cong J_F(F)_{\mathrm{Tor}} \cong J(F)_{\mathrm{Tor}} = J(k). \ \blacksquare$$

4. The Jacobian varieties with λ-torsion points. In this section, we prove Theorem 1.3, and state its function field analogue Theorem 4.5 without proof as the proof is similar to the number field case. Let ℓ be a prime number, and let $K := \mathbb{Q}(\zeta_\ell)$ for which we assume ℓ is regular. Let C/K be the curve in 1.1, and we keep the notation used in Section 2. Let Δ_f be the discriminant of f. Recall $z_1, \ldots, z_d \in K_{\mathrm{sep}}$, the roots of $f(x)$, and suppose that z_d is contained in K. Recall the set $Z(C) := \{y_1, \ldots, y_s\}$ and the fields $L_i := K(y_i)$ for $i = 1, \ldots, s$. Let L be the compositum of $L_1, \ldots, L_s$ in K_{sep}.

4.1. Let us fix a set of generators of $\theta(\mathsf{Sel}^{(\lambda)}(J, K))$, and note that each generator is an s-tuple with entries in L. Let W_J be the union of all entries of the generators. Then W_J is a subset of L^*. For each prime ideal $\mathfrak{q}$ of $\mathscr{O}_K$, choose an element $\alpha_{\mathfrak{q}}$ of $\mathscr{O}_K$ as in the proof of Theorem 3.6. Let $S_J := M_K^\infty \cup \{\mathfrak{q} \in M_K^0 : \mathfrak{q} \mid \ell\Delta_f\mathscr{O}_K\}$, and let $Y_J := \{\zeta_\ell, -1\} \cup W_J \cup \{\alpha_{\mathfrak{q}} \in \mathscr{O}_K : \mathfrak{q} \in S_J \cap M_K^0\}$. Let M be the Galois closure of $L(\sqrt[\ell]{\alpha} : \alpha \in Y_J)$ over $\mathbb{Q}$.

Let us denote by $\mathscr{D}'_{Y_J}$ the set of prime numbers q in $\mathbb{Z}$ such that q splits completely in $\mathscr{O}_M$ and coprime to α for all $\alpha \in Y_J$. By the Chebotarev density theorem with H being the trivial subgroup of $\mathrm{Gal}(M/\mathbb{Q})$, the set of prime ideals of $\mathbb{Z}$ that split completely in M has a positive Dirichlet density. Then it is clear that $\mathscr{D}'_{Y_J}$ has a positive Dirichlet density. The proof of the following lemma is similar to that of Lemma 3.5, and we leave it to the reader.

4.2. Lemma. *Let D be a positive integer supported by $\mathscr{D}'_{Y_J}$. If $\mathfrak{q}$ is a place in S_J, then $\left(\frac{D}{\mathfrak{q}}\right)_\ell = 1$.*

4.3. Proposition. *Let D be a positive ℓth power free integer in $\mathbb{Z}$ which is supported by $\mathscr{D}'_{Y_J}$. Then $\dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) > \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J, K)$. In particular, $\limsup_D \dim_{\mathbb{F}_\ell} \mathsf{Sel}^{(\lambda)}(J_D, K) = \infty$.*

Proof. Let D be a positive ℓth power-free integer in $\mathbb{Z}$ which is supported by $\mathscr{D}'_{Y_J}$. The proof of $\theta(\mathsf{Sel}^{(\lambda)}(J, K)) \subset \theta^D(\mathsf{Sel}^{(\lambda)}(J_D, K))$ is similar to the proof in Theorem 3.6. To prove the inequality, note that $\theta(\mathsf{Sel}^{(\lambda)}(J, K)) \subset \prod_{i=1}^s L_i(S_J, \ell)$. Let $S_D := S_J \cup \{\mathfrak{q} \in M_K^0 : \mathfrak{q} \mid D\mathscr{O}_K\}$. Lemma 4.4

below shows that there is an element of $\theta^D(\mathsf{Sel}^{(\lambda)}(J_D,K))$ which is contained in $\prod_{i=1}^s L_i(S_D,\ell)$ but not in $\prod_{i=1}^s L_i(S_J,\ell)$. This proves that $\dim_{\mathbb{F}_\ell}\mathsf{Sel}^{(\lambda)}(J_D,K) > \dim_{\mathbb{F}_\ell}\mathsf{Sel}^{(\lambda)}(J,K)$. By induction, it is clear that $\limsup_D \dim_{\mathbb{F}_\ell}\mathsf{Sel}^{(\lambda)}(J_D,K)=\infty$. ∎

4.4. LEMMA. *Let D be an ℓth power-free positive integer supported by $\mathscr{D}'_{Y_J}$. Then the K-rational point $[(z_dD,0)-(\infty)]\in J_D[\lambda](K)$ is mapped to $\prod L_i(S_D,\ell)\setminus\prod L_i(S_J,\ell)$ under $\theta^D\delta^D : J_D(K)/\lambda J_D(K)\to\mathscr{C}$.*

Proof. Since D is supported by $\mathscr{D}'_{Y_J}$, D is coprime to Δ_f and to all prime ideals $\mathfrak{q}\in S_J$. Since $P:=[(z_dD,0)-(\infty)]$ is a point in $J_D(K)$, by Lemma 2.2,

$$\begin{aligned}(6)\qquad \theta^D(\delta^D(P)) &= (f_{zD}(z_dD,0): z\in Z(C)) = (z_dD-zD : z\in Z(C))\\ &= (D(z_d-z) : z\in Z(C)).\end{aligned}$$

Note that for all $z\in Z(C)$, the difference z_d-z divides Δ_f and, hence, it is coprime to D. Since $D\mathscr{O}_K$ can be assumed to be supported by prime ideals unramified in the compositum L, and is not an ℓth power of an ideal, it follows that $D(z_d-y_i)\in L_i(S_D,\ell)\setminus L_i(S_J,\ell)$ for all $i=1,\dots,s$. ∎

Proof of Theorem 1.3. By Proposition 4.3, there is a positive ℓth power-free rational integer D_0 such that $\dim_{\mathbb{F}_\ell}\mathsf{Sel}^{(\lambda)}(J_{D_0},K)>n$. Proposition 4.3 applied to $J=J_{D_0}$ and [18, Theorem 2.4] together imply the result. ∎

The theorem below is a function field analogue of Theorem 1.3.

4.5. THEOREM. *Suppose that K is a function field defined in* 1.5. *Given a positive integer n, there are $D_0\in\mathscr{O}_K$ and a set of prime ideals $\mathscr{D}$ of $\mathscr{O}_K$ with a positive Dirichlet density such that whenever D is a monic element of $\mathscr{O}_K$ of degree divisible by ℓ such that $D\mathscr{O}_K$ is not an ℓth power of an ideal and D is supported by $\mathscr{D}$, we have* $\dim_{\mathbb{F}_\ell}\mathsf{Sel}^{(\lambda)}(J_{D_0D},K)>n$.

Acknowledgements. I wish to thank Robert Rumely, Dino Lorenzini, and Michael Stoll for helpful comments.

A. 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. Results introduced in this section can be proved using the reciprocity law in [13, Theorem 8.3, p. 415], or [22, p. 352]. Except Theorem A.4, we leave to the reader the proofs of results in this section. We also refer to [13] for the definitions of symbols used here. As we omitted many proofs of the function field case, in fact, Theorem A.4 and Corollary A.4 are not used in the proofs presented in this paper. However, since a convenient form of the global reciprocity law for a general function field of one variable does not seem to be available, we include the statement and proof.

A.1. Let ℓ be a prime number. Let K be a number field containing ζ_ℓ. Given a place v dividing $\ell\infty$ and $\alpha \in K^*$ coprime to v, we define, for convenience, $\left(\frac{\alpha}{v}\right)_\ell$ to be 1 if $\alpha \in (K_v^*)^\ell$, and -1 if not.

A.2. Lemma. *Let q be a rational prime coprime to ℓ. Let $\mathfrak{p}$ be a prime ideal of $\mathscr{O}_K$ lying over q. Suppose that ℓ is odd. If $\left(\frac{\zeta_\ell}{\mathfrak{p}}\right)_\ell = 1$, then $q \equiv a^\ell \bmod \ell^2$ for some $a \in \mathbb{Z}$, and $\left(\frac{q}{\lambda\mathscr{O}_K}\right)_\ell = 1$. Suppose that $\ell = 2$, i.e., $K = \mathbb{Q}$. If q is an odd prime such that $\left(\frac{-1}{q}\right)_\ell = \left(\frac{2}{q}\right)_\ell = 1$, then $\left(\frac{q}{2\mathbb{Z}}\right)_\ell = 1$.*

A.3. Corollary. *If a is a positive rational integer coprime to ℓ such that $\left(\frac{a}{\lambda\mathscr{O}_K}\right)_\ell = 1$, then $\left(\frac{a}{\alpha}\right)_\ell = \left(\frac{\alpha}{a}\right)_\ell$ for all $\alpha \in \mathscr{O}_K$ coprime to $a\ell$.*

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_∞. Let us define $\left(\frac{g}{v_\infty}\right)_\ell$ to be 1 if $g \in (K_{v_\infty}^*)^\ell$, and -1 if $g \notin (K_{v_\infty}^*)^\ell$. Let g be an element of $\mathscr{O}_K$ with the leading coefficient $a \in k^*$ (with respect to π_∞). Then $g \in (K_{v_\infty}^*)^\ell$ if and only if $a \in (k^*)^\ell$ and $\deg(g)$ is divisible by ℓ.

A.4. Theorem (The general reciprocity law for function fields). *Let q be a prime number, and let n be a positive integer not divisible by q. Suppose that k has q^r elements, and k contains a primitive nth root of unity. If g and h are monic distinct elements of $\mathscr{O}_K$ such that g is coprime to h, then*

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

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

Proof. Let K_{v_∞} be the completion of K at v_∞. Let $\widehat{\mathscr{O}}_\infty := \{\alpha \in K_{v_\infty} : |\alpha|_{v_\infty} \le 1\}$, and $\widehat{\mathfrak{M}}_\infty := \{\alpha \in \widehat{\mathscr{O}}_\infty : |\alpha|_{v_\infty} < 1\}$. Since $\deg(v_\infty) = 1$, let us define $\omega : \widehat{\mathscr{O}}_\infty^* \to k^*$ by $\alpha \mapsto a$ such that $\alpha \equiv a \bmod \widehat{\mathfrak{M}}_\infty$. By [13, Chapter V, Sec. 3, Proposition 3.4] for nonzero elements α and β in $\mathscr{O}_K$,

$$\left(\frac{\alpha,\beta}{v_\infty}\right)_n = \omega\left((-1)^{\operatorname{ord}_\infty(\alpha)\operatorname{ord}_\infty(\beta)}\,\frac{\beta^{\operatorname{ord}_\infty(\alpha)}}{\alpha^{\operatorname{ord}_\infty(\beta)}}\right)^{(q^r-1)/n}. \tag{7}$$

Let $\pi_\infty \in K^*$ be a uniformizer of K_{v_∞}. Let g and h be monic distinct elements of $\mathscr{O}_K$ coprime to each other. Then, by [13, Theorem 8.3, p. 415],

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

Since g and h are monic, there are a and b in $\widehat{\mathscr{O}}_\infty^*$ such that $a \equiv b \equiv 1 \bmod \widehat{\mathfrak{M}}_\infty$, $g = a\pi_\infty^{\operatorname{ord}_\infty(g)}$, and $h = b\pi_\infty^{\operatorname{ord}_\infty(h)}$. It follows from Hensel's lemma that a and b are contained in $(K^*_{v_\infty})^n$. Then, by [13, Theorem 8.3, p. 415],

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

By (7), $\left(\frac{\pi_\infty,\pi_\infty}{v_\infty}\right)_n=(-1)^{(q^r-1)/n}$. ■

The following corollary easily follows from this theorem:

A.5. Corollary. *If g is a monic element of $\mathscr{O}_K$ such that $\left(\frac{-1}{g}\right)_n=1$, then $\left(\frac{h}{g}\right)_n=\left(\frac{g}{h}\right)_n$ for all monic elements h of $\mathscr{O}_K$ coprime to g.*

References

[1] D. Atake, *On elliptic curves with large Tate–Shafarevich groups*, J. Number Theory 87 (2001), 282–300.

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

[3] S. Chang, *Note on the rank of quadratic twists of Mordell equations*, J. Number Theory 118 (2006), 53–61.

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

[5] 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.

[6] K. James and K. Ono, *Selmer groups of quadratic twists of elliptic curves*, Math. Ann. 314 (1999), 1–17.

[7] V. A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 1154–1180.

[8] F. Lemmermeyer, *On Tate–Shafarevich groups of some elliptic curves*, in: Algebraic Number Theory and Diophantine Analysis (Graz, 1998), de Gruyter, 2000, 277–291.

[9] D. Lieman, *Nonvanishing of L-series associated to cubic twists of elliptic curves*, Ann. of Math. 140 (1994), 81–108.

[10] D. Lorenzini, *Invitation to Arithmetic Geometry*, Amer. Math. Soc., 1996.

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

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

[13] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, 1999.

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

[15] B. Poonen and E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. 488 (1997), 141–188.

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

[17] C. Schoen, *Bounds for rational points on twists of constant hyperelliptic curves*, J. Reine Angew. Math. 411 (1990), 196–204.

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

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

[20] M. Stoll, *Independence of rational points on twists of a given curve*, Compos. Math., to appear.

[21] —, *On the arithmetic of the curves $y^2 = x^\ell + A$ and their Jacobians*, J. Reine Angew. Math. 501 (1998), 171–189.

[22] 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, 305–347.

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

[24] S. Wong, *Elliptic curves and class number divisibility*, Int. Math. Res. Not. 1999, no. 12, 661–672.

[25] G. Yu, *Rank 0 quadratic twists of a family of elliptic curves*, Compos. Math. 135 (2003), 331–356.

Department of Mathematics
Armstrong Atlantic State University
11935 Abercorn St.
Savannah, GA 31419, U.S.A.
E-mail: changsun@mail.armstrong.edu

Received on 10.3.2006
and in revised form on 11.5.2006 (5158)