Ideal Class Groups and Torsion in Picard Groups of Varieties

Aaron Levin
Centro di Ricerca Matematica Ennio De Giorgi
Collegio Puteano
Scuola Normale Superiore
Piazza dei Cavalieri, 3
I-56100 Pisa, Italy
E-mail: aaron.levin@sns.it

Abstract

We give a new general technique for constructing and counting number fields with an ideal class group of nontrivial \( m \)-rank. Our results can be viewed as providing a way of specializing the Picard group of a variety \( V \) over \( \mathbb{Q} \) to obtain class groups for number fields \( \mathbb{Q}(P) \), \( P \in V(\overline{\mathbb{Q}}) \), for certain families of points \( P \). In particular, we show how the problem of constructing quadratic number fields with a large-rank ideal class group can be reduced to the problem of finding a hyperelliptic curve with a rational Weierstrass point and a large rational torsion subgroup in its Jacobian. Furthermore, we show how many previous results on constructing large-rank ideal class groups can be fit into our framework and rederived.

As an application of our technique, we derive a quantitative version of a theorem of Nakano. This gives the best known general quantitative result on number fields with a large-rank ideal class group.

1 Introduction

The primary purpose of this paper is to give a new general technique for constructing and counting number fields with an ideal class group of nontrivial \( m \)-rank. In spirit, our results can be viewed as providing a way of specializing the class group (Picard group) of a variety \( V \) over \( \mathbb{Q} \) to obtain class groups for number fields \( \mathbb{Q}(P) \), \( P \in V(\overline{\mathbb{Q}}) \). For instance, as an example of our results, we show how the problem of constructing quadratic number fields \( k \) with a large-rank ideal class group \( \text{Cl}(k) \) can be reduced to the problem of finding a hyperelliptic curve \( C \) with a rational Weierstrass point and a large rational torsion subgroup \( \text{Jac}(C)(\mathbb{Q})_{\text{tors}} \) in its Jacobian. More precisely, we prove:

\footnote{For a finite abelian group \( A \) and an integer \( m > 1 \), we let \( \text{rk}_m A \), the \( m \)-rank of \( A \), be the largest integer \( r \) such that \((\mathbb{Z}/m\mathbb{Z})^r \) is a subgroup of \( A \).}
Theorem 1. Let $C$ be a nonsingular hyperelliptic curve over $\mathbb{Q}$ with a rational Weierstrass point. Let $g$ denote the genus of $C$. Let $m > 1$ be an integer. Then there exist $\gg \exp \left( \frac{1}{m} \right)$ imaginary quadratic number fields $k$ with discriminant $d_k$ and
\[ \text{rk}_m \text{Cl}(k) \geq \text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}}, \quad |d_k| < X, \]
and $\gg \exp \left( \frac{1}{m} \right)$ real quadratic number fields $k$ with
\[ \text{rk}_m \text{Cl}(k) \geq \text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}} - 1, \quad d_k < X. \]

More generally, we show that if $C$ is a nonsingular projective curve with $C(\mathbb{Q}) \neq \emptyset$, then for most points $P$ in certain families of points on $C$, $\text{rk}_m \text{Cl}(\mathbb{Q}(P))$ can be bounded from below by a function of $\text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}}$, the unit group $\mathcal{O}_{\mathbb{Q}(P)}^*$, and the set of places of bad reduction of the Jacobian of $C$.

In Section 5 we show how many of the previous results on constructing large-rank ideal class groups can be explained and rederived in the arithmetic-geometric context of this paper. Thus, in the next section we give an overview and brief summary of the history of results on the problem of finding infinite families of number fields of degree $n$ over $\mathbb{Q}$ with ideal class groups of large $m$-rank. We also obtain some new quantitative results on counting number fields with a large-rank ideal class group. Of particular note is a quantitative version of a theorem of Nakano (Theorem 31).

In [40], by taking advantage of certain superelliptic curves, we obtained new results (see Theorems 30 and 35) on class groups of large $m$-rank. The proofs in [40] were given in a very explicit, concrete manner, avoiding any mention of the Jacobian or Picard group of a curve, but implicitly using the rational torsion in these objects. The present paper is an abstraction and generalization of the technique used in [40].

Fundamentally, in the simplest case, the basic idea is the following: find polynomials $p, q \in k[x,y]$, for some number field $k$, such that if $i \in \mathbb{Z}$, $p(\alpha_i, i) = 0$, and $\text{rk}_m \text{Cl}(\mathbb{Q}(\alpha_i))$ is small, then $q(x, i)$ is reducible over $k$. By Hilbert’s Irreducibility Theorem, we know that $q(x, i)$ is irreducible over $k$ for most values of $i \in \mathbb{Z}$, and therefore $\text{rk}_m \text{Cl}(\mathbb{Q}(\alpha_i))$ cannot be small for most values of $i$. In a more geometric language, this construction can be accomplished by using torsion in the Picard group of a curve. Let $C$ be a nonsingular projective curve over $\mathbb{Q}$ and let $\phi : C \to \mathbb{P}^1$ be a morphism. Using $m$-torsion in $\text{Pic}(C)$, the Picard group of $C$, we construct a certain curve $X$ and an unramified abelian cover $\pi : X \to C$. This map has the property that if $\pi(Q) = P \in C(\mathbb{Q})$, then the degree $[\mathbb{Q}(Q) : \mathbb{Q}]$ is bounded by a function of the $m$-rank of $\text{Cl}(\mathbb{Q}(P))$. Consider points $Q_i \in X(\mathbb{Q}), P_i \in C(\mathbb{Q})$, with $\pi(Q_i) = P_i$ and $\phi(P_i) = i \in \mathbb{A}^1(\mathbb{Z}) \subset \mathbb{P}^1(\mathbb{Q})$. By Hilbert’s Irreducibility Theorem, the degree $[\mathbb{Q}(Q_i) : \mathbb{Q}]$ will usually be equal to $\deg \phi \circ \pi = (\deg \phi)(\deg \pi)$. On the other hand, $[\mathbb{Q}(Q_i) : \mathbb{Q}]$ is bounded by a function of $\text{rk}_m \text{Cl}(\mathbb{Q}(P_i))$. Thus, by comparing these two statements we obtain number fields $\mathbb{Q}(P_i)$ with $[\mathbb{Q}(P_i) : \mathbb{Q}] = \deg \phi$ and $\text{rk}_m \text{Cl}(\mathbb{Q}(P_i))$ bounded from below. An alternative approach, replacing the use of Hilbert’s Irreducibility Theorem by finiteness results on integral points of bounded degree on curves, was given in [40].
Using this method, to obtain number fields of degree $n$ with ideal class groups of large $m$-rank, one needs to find $n$-gonal curves $C$ over $\mathbb{Q}$ with $\text{rk}_m \text{Pic}(C)_{\text{tors}}$ large. This leads to the following natural question, which we state in terms of Jacobians.

**Question 2.** Let $n > 1$ be a positive integer. Let $p$ be a prime not dividing $n$. Do there exist $n$-gonal curves $C$ over $\mathbb{Q}$ with $\text{rk}_p \text{Jac}(C)(\mathbb{Q})_{\text{tors}}$ arbitrarily large?

In particular, we ask the following question of hyperelliptic curves:

**Question 3.** Let $p$ be an odd prime. Do there exist hyperelliptic curves $C$ over $\mathbb{Q}$ with $\text{rk}_p \text{Jac}(C)(\mathbb{Q})_{\text{tors}}$ arbitrarily large?

We have excluded the case when $p$ divides $n$ since in this case it is easy to construct $n$-gonal curves $C$ over $\mathbb{Q}$ with $\text{rk}_p \text{Jac}(C)(\mathbb{Q})_{\text{tors}}$ arbitrarily large (analogously, when $p$ divides $n$ it is possible to construct number fields $k$ of degree $n$ with $\text{rk}_p \text{Cl}(k)$ arbitrarily large).

Previous papers studying the problem of constructing Jacobians of curves with large rational torsion subgroups have primarily focused on either curves of low genus [27, 32, 33, 36, 37, 52], or on producing a rational torsion point of large order in the Jacobian of a curve of genus $g$, for every genus $g$ [22, 23, 34, 35, 38, 39]. The main motivation in these papers seems to be to determine how Mazur’s theorem classifying rational torsion in elliptic curves might generalize to curves of higher genus. We hope to further motivate research into large rational torsion subgroups of Jacobians, though from the slightly different perspective of Questions 2 and 3.

## 2 Overview of Previous Results

In this section we give a brief summary of the history of results on the problem of finding infinite families of number fields of degree $n$ over $\mathbb{Q}$ with ideal class groups of large $m$-rank (see Tables 1 and 2 for a more comprehensive list of results). The earliest such result could be considered to be Gauss’ result determining, in modern terms, the 2-rank of the class group of a quadratic number field in terms of the primes dividing the discriminant of the quadratic field (see, e.g., [23]). In particular, it follows from Gauss’ result that the 2-rank of the ideal class group of a quadratic number field can be made arbitrarily large. In contrast to Gauss’ result, there is not a single quadratic number field $k$ and prime $p \neq 2$ for which it is known that $\text{rk}_p \text{Cl}(k) > 6$, although the Cohen-Lenstra heuristics [13, 14] predict that for any given positive integer $r$, a positive proportion of quadratic fields $k$ should have $\text{rk}_p \text{Cl}(k) = r$.

The first constructive result on $m$-ranks of class groups for arbitrary $m$ was given in 1922 by Nagell [17, 43], who proved that for any positive integer $m$, there exist infinitely many imaginary quadratic number fields whose class group

---

2 Recall that a curve $C$ is called $n$-gonal if there exists a degree $n$ map from $C$ to $\mathbb{P}^1$.

3 If $C(\mathbb{Q}) \neq \emptyset$, then $\text{Pic}(C)_{\text{tors}} \cong \text{Jac}(C)(\mathbb{Q})_{\text{tors}}$; in general, since a rational divisor class may not be represented by a rational divisor, there is only an inclusion $\text{Pic}(C)_{\text{tors}} \hookrightarrow \text{Jac}(C)(\mathbb{Q})_{\text{tors}}$. 

---
Table 1: Table of values $m$, $n$, and $r$ for which it is known that there exist infinitely many number fields $k$ of degree $n$ with $rk_m Cl(k) \geq r$ (with $r = \infty$ if $rk_m Cl(k)$ can be made arbitrarily large).

### Quadratic fields ($n = 2$)

| Author(s)                  | Year     | Type                  | $m$ | $r$ |
|----------------------------|----------|-----------------------|-----|-----|
| Gauss                      | 19th c.  | imaginary, real       | 2   | $\infty$ |
| Nagell [47, 48]            | 1922     | imaginary             | $>1$ | 1   |
| Yamamoto [60]              | 1970     | imaginary             | $>1$ | 2   |
| Yamamoto [60], Weinberger  | 1970, 1973| real                 | $>1$ | 1   |
| Craig [17]                 | 1973     | imaginary             | 3   | 3   |
|                            |          | real                  | 3   | 2   |
| Craig [18]                 | 1977     | imaginary             | 3   | 4   |
|                            |          | real                  | 3   | 3   |
| Diaz [19]                  | 1978     | real                  | 3   | 4   |
| Mestre [44, 42, 43]        | 1980     | imaginary, real       | 5, 7| 2   |
| Mestre [45]                | 1992     | imaginary, real       | 5   | 3   |

### Higher Degree Fields

| Author(s)                  | Year     | $m$ | $n$ | $r$ |
|----------------------------|----------|-----|-----|-----|
| Brumer, Rosen [6, 7]       | 1965     | $>1$| $n = m$ | \(\infty\) |
| Uchida [58]                | 1974     | $>1$| 3   | 1   |
| Ishida [29]                | 1975     | 2   | prime | \(n - 1\) |
| Azuhata, Ichimura [2]      | 1984     | $>1$| $>1$| \(\left\lfloor \frac{n}{2} \right\rfloor\) |
| Nakano [49, 50]            | 1985     | $>1$| $>1$| \(\left\lceil \frac{n}{2} \right\rceil + 1\) |
|                            |          | 2   | $>1$| \(n\) |
| Nakano [51]                | 1988     | 2   | 3   | 6   |
| Levin [40]                 | 2006     | $>1$| $>1$| \(\left\lceil \frac{n}{2} \right\rceil + \frac{n}{m-1} - m\) |
has an element of order $m$ (in particular, there are infinitely many imaginary quadratic fields with class number divisible by $m$). Nagell’s result has since been reproved by a number of different authors (e.g., [1], [28], [31]). Nearly fifty years later, working independently, Yamamoto [60] and Weinberger [59] extended Nagell’s result to real quadratic fields. Soon after, Uchida [58] proved the analogous result for cubic cyclic fields. In 1984, Azuhata and Ichimura [2] succeeded in extending Nagell’s result to number fields of arbitrary degree. In fact, they proved that for any integers $m, n > 1$ and any nonnegative integers $r_1, r_2$, with $r_1 + 2r_2 = n$, there exist infinitely many number fields $k$ of degree $n = [k : \mathbb{Q}]$ with $r_1$ real places and $r_2$ complex places such that

$$\text{rk}_m \text{Cl}(k) \geq r_2.$$  

(1)

The right-hand side of (1) was subsequently improved to $r_2 + 1$ by Nakano [49, 50]. Choosing $r_2$ as large as possible, we thus obtain, for any $m$, infinitely many number fields $k$ of degree $n > 1$ with

$$\text{rk}_m \text{Cl}(k) \geq \left\lfloor \frac{n}{2} \right\rfloor + 1,$$  

(2)

where $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$ denote the greatest and least integer functions, respectively. For general $m$ and $n$, (2) is the best result that is known on producing number fields of degree $n$ with a class group of large $m$-rank. In [10] it was shown that there exist infinitely many number fields $k$ of degree $n$ satisfying $\text{rk}_m \text{Cl}(k) \geq \left\lfloor \frac{n}{2} \right\rfloor + \frac{n}{m-1} - m$, improving (2) when $n \geq m^2$.

For certain special values of $m$ and $n$, slightly more is known. Of particular note to us are Mestre’s papers [42, 43, 44] giving the best known results for $m = 5, 7$ and $n = 2$. Although he uses a somewhat different approach, Mestre’s method also crucially relies on rational torsion in Jacobians of curves. Thus, his method lies in the same general vein as the present paper.

Recently, progress has been made on obtaining quantitative results on counting the number fields in the above results. Murty [46] gave the first results in this direction, obtaining quantitative versions of the theorems of Nagell and Yamamoto-Weinberger. His results have since been improved by, among others, Soundararajan [57] in the imaginary quadratic case and Yu [61] in the real quadratic case. In higher degrees, Hernández and Luca [24] gave the first such result for cubic number fields, while Bilu and Luca [3] succeeded in proving a quantitative theorem for number fields of arbitrary degree. Bilu and Luca’s result was improved in [40], where a quantitative version of Azuhata and Ichimura’s result was given. We give a summary of these and other quantitative results in Table 2.

3 Hilbert’s Irreducibility Theorem

The main tool in our proofs is Hilbert’s Irreducibility Theorem, which we now recall in a suitably general, quantitative form due to Cohen [15] (see also [50, Ch. 9]). Throughout, $k$ will denote a number field.
Table 2: Table of $m$, $n$, $r$, and $f(X)$, for which it is known that $N_{m,n,r}(X) \gg f(X)$, where we let $d_k$ be the discriminant of $k$ over $\mathbb{Q}$ and

$$N_{m,n,r}(X) = \#\{k \subset \overline{\mathbb{Q}} \mid [k : \mathbb{Q}] = n, \text{rk}_m \text{Cl}(k) \geq r, |d_k| < X\}.$$

### Quadratic fields ($n = 2$)

| Author(s)       | Year | Type      | $m$  | $r$      | $f(X)$                  |
|-----------------|------|-----------|------|----------|-------------------------|
| Murty           | 1999 | imaginary | $> 1$| odd      | $X^{\frac{1}{2} + \frac{1}{m}}$ |
|                 |      | real      |      |          | $X^{\frac{1}{2m}}$      |
| Soundararajan   | 2000 | imaginary |      | $m \equiv 0 \pmod{4}$ | $X^{\frac{1}{2} + \frac{1}{m} - \epsilon}$ |
|                 |      |           |      | $m \equiv 2 \pmod{4}, m \neq 2$ | $X^{\frac{1}{2} + \frac{1}{m} - \epsilon}$ |
| Yu              | 2002 | real      |      | odd      | $X^{\frac{1}{m}}$       |
| Luca            | 2003 | real      |      | even     | $X^{\frac{1}{m}}$ / log $X$ |
| Chakraborty, Murty | 2003 | real      | 3    |          | $X^{\frac{1}{m} - \epsilon}$ |
| Byeon           | 2003 | real      | 3    |          | $X^{\frac{1}{m} - \epsilon}$ |
| Byeon           | 2006 | real      | 5,7  |          | $X^{\frac{1}{m}}$       |
| Byeon           | 2006 | imaginary |      | odd      | $X^{\frac{1}{m}}$       |

### Higher Degree Fields

| Author(s)       | Year | $m$ | $n$ | $r$      | $f(X)$                  |
|-----------------|------|-----|-----|----------|-------------------------|
| Hernández, Luca | 2004 | $> 1$| 3   |          | $X^{\frac{1}{m}}$       |
| Bilu, Luca      | 2005 | $> 1$| $> 1$|          | $X^{\frac{1}{m}}$       |
| Levin           | 2006 | $> 1$| $> 1$| $> (m - 1)^2$ | $X^{\frac{m(n-1)}{m+1}} / \log X$ |
|                 |      |      |      |          | $X^{\frac{m(n-1)}{m+1} / \log X}$ |
Theorem 4 (Hilbert Irreducibility Theorem). Let \( f \in k[x, t_1, \ldots, t_n] \) be a polynomial irreducible in \( k[x, t_1, \ldots, t_n] \). Let \( g \in k[t_1, \ldots, t_n] \) be nonzero. Then for all but \( O(\sqrt{X} \log X) \) points \( (i_1, \ldots, i_n) \in [-X, X]^n \cap \mathbb{Z}^n \), the polynomial \( f(x, i_1, \ldots, i_n) \) is irreducible over \( k \) and \( g(i_1, \ldots, i_n) \neq 0 \). If \( n = 1 \), \( O(\sqrt{X} \log X) \) can be replaced by \( O(\sqrt{X}) \).

We will also find it convenient to use an equivalent geometric formulation of Hilbert’s theorem. Before stating this, we give some definitions and notation. By a variety over a field \( k \), we mean a geometrically integral, separated scheme of finite type over \( k \). A curve is a one-dimensional variety. We define a dominant rational map \( \phi : V \to W \) of varieties over \( k \) to be generically finite if the extension of function fields \( k(V)/k(W) \), induced by \( \phi \), is a finite extension. For a point \( i = (i_1, \ldots, i_n) \in \mathbb{A}^n(\mathbb{Z}) \), we define \( H(i) = \max_j |i_j| \).

Theorem 5 (Geometric Hilbert Irreducibility Theorem). Let \( V \) be a variety over \( k \) of dimension \( n \). Let \( \phi : V \to \mathbb{A}^n \) be a generically finite rational map. Let \( Z \) be a proper closed subset of \( \mathbb{A}^n \). If \( \phi \) is defined, \( i \in \phi(V) \), let \( P_i \in \phi^{-1}(i) \). Then for all but \( O(\sqrt{X} \log X) \) points \( i \in \mathbb{A}^n(\mathbb{Z}) \) with \( H(i) \leq X \), \( P_i \) is defined, \( \phi^{-1}(i) \cap Z \neq \emptyset \), and \( [k(P_i) : k] = \deg \phi \). If \( n = 1 \), \( O(\sqrt{X} \log X) \) can be replaced by \( O(\sqrt{X}) \).

For more general and precise statements of Hilbert’s Irreducibility Theorem, see [56, Ch. 9] and [15].

Remark 6. Schinzel [54] has shown that there exist arithmetic progressions \( I_1, \ldots, I_n \) such that the conclusions of Theorems 4 and 5 hold, without exception, for arbitrarily chosen elements \( i_j \in I_j, j = 1, \ldots, n \), where \( i = (i_1, \ldots, i_n) \).

Remark 7. Cohen [15] has shown, furthermore, that the implied constants in Theorems 4 and 5 can be effectively determined, as well as the arithmetic progressions in Remark 6.

A very natural problem that arises in connection with Hilbert’s Irreducibility Theorem is to determine the number of distinct number fields \( \mathbb{Q}(P_i) \) with \( H(i) \leq X \). For \( n = 1 \) this has been studied by Dvornicich and Zannier. Let \( C \) be a curve and let \( \phi : C \to \mathbb{P}^1 \) be a morphism. For each integer \( i \in \mathbb{A}^1(\mathbb{Z}) \subset \mathbb{P}^1(\mathbb{Q}) \), let \( P_i \in \phi^{-1}(i) \). Dvornicich and Zannier [20, 21] studied the degree of the field extension \( \mathbb{Q}(P_1, \ldots, P_N) \). Their results imply in particular a useful result on the number of isomorphism classes of number fields in the set \( \{\mathbb{Q}(P_1), \ldots, \mathbb{Q}(P_N)\} \).

Theorem 8 (Dvornicich, Zannier). Let \( C \) be a curve over a number field \( k \). Let \( \phi : C \to \mathbb{P}^1 \) be a morphism with \( \deg \phi > 1 \). For each integer \( i \), let \( P_i \in \phi^{-1}(i) \). Let \( g(N) \) denote the number of isomorphism classes of number fields in the set \( \{\mathbb{Q}(P_1), \ldots, \mathbb{Q}(P_N)\} \). Then \( g(N) \gg \frac{N}{\log N} \).

An analysis of the proof in [20] shows that furthermore the implied constant in Theorem 8 is effective (for this one makes use of effective versions of Hilbert’s Irreducibility Theorem (Remark 7 and the prime number theorem).
4 Theorems and Proofs

Before stating our main theorem, we introduce a little more notation. If $S$ is a set of places of a number field $k$, we let $S_{fin}$ denote the set of finite places in $S$. If $L$ is a finite extension of $k$ and $S_L$ is the set of places of $L$ lying above places of $S$, we will use $O_{L,S}$ to mean $O_{L,S_L}$, the ring of $S_L$-integers of $L$. If $G$ is an abelian group, we let $rk G$ denote the free rank of $G$ as a $\mathbb{Z}$-module.

**Theorem 9.** Let $V$ be a variety over $\mathbb{Q}$ of dimension $l$. Let $\phi: V \to k^l$ be a generically finite rational map with $\deg \phi = n > 1$. Let $I \subset \phi(V)$ be a subset of $k^l(\mathbb{Z})$ and let $I(N) = \{ i \in I \mid H(i) < N \}$. For $i \in I$, let $P_i \in \phi^{-1}(i)$. Let $m > 1$ be a positive integer. Let $f_1, \ldots, f_r \in \mathbb{Q}(V)$ be rational functions on $V$ such that

$$\left[ \mathbb{Q}(V) \left( \sqrt[1]{f_1}, \ldots, \sqrt[1]{f_r} \right) : \mathbb{Q}(V) \right] = m^r. \tag{3}$$

Let $S$ be a finite set of places of $\mathbb{Q}$ such that for all $i \in I$ and all $j$,

$$f_j(P_i)^{O_{\mathbb{Q}(P_i),S}} = a_{i,j}^m \tag{4}$$

for some fractional $O_{\mathbb{Q}(P_i),S}$-ideal $a_{i,j}$. Then for all but $O(N^{l-\frac{1}{2}} \log N)$ (or $O(\sqrt{N})$ if $l = 1$) points $i \in I(N)$, we have $|\mathbb{Q}(P_i):\mathbb{Q}| = n$ and

$$rk_m Cl(\mathbb{Q}(P_i)) \geq r + \#S_{fin} - rk O_{\mathbb{Q}(P_i),S}^*. \tag{5}$$

**Proof.** Associated to the field extension $\mathbb{Q}(V) \left( \sqrt[1]{f_1}, \ldots, \sqrt[1]{f_r} \right)$ of $\mathbb{Q}(V)$, we have a projective variety $X$ over $\mathbb{Q}$ (unique up to birational equivalence) and a morphism $\pi: X \to V$ with $\deg \pi = m^r$.

**Lemma 10.** Let $Z \subset V$ be the set of poles of the functions $f_1, \ldots, f_r$. Let $P_i \in V(\mathbb{Q}) \setminus Z$, for some $i \in I$. Let $\zeta$ be a generator for the group of roots of unity in $k = \mathbb{Q}(P_i)$. Let $L = \mathbb{Q}(\sqrt[1]{\zeta} \mid q \in S_{fin})$. Let $Q_i \in \pi^{-1}(P_i)$. Then for some prime $p$ dividing $m$,

$$[L(Q_i) : L] \leq \left[ L \left( \sqrt[1]{\zeta} \right) : L \right] [k : \mathbb{Q}]^{r \cdot rk_m Cl(k)+rk O_{L,S}^* - r \cdot \#S_{fin}}. \tag{6}$$

**Proof.** We actually prove a stronger inequality, with $rk_m Cl(k)$ replaced by $rk_m Cl(O_{k,S})$ (the class group of $O_{k,S}$) in a. We will work throughout with (fractional) $O_{k,S}$-ideals. Let $ord_p m$ denote the largest power of $p$ dividing $m$. Let $p$ be a prime dividing $m$ such that $rk_{p,ord_p} = Cl(O_{k,S}) = rk_m Cl(O_{k,S}) = t$. Let $G = \left\{ [a]^p \mid [a] \in Cl(O_{k,S}), [a]^m = 1 \right\}$, a subgroup of $Cl(O_{k,S})$. Clearly, $G \cong (\mathbb{Z}/p\mathbb{Z})^t$. Let $b_j, \ j = 1, \ldots, t$, be $(O_{k,S})$-ideals whose ideal classes generate $G$. Then for each $j$, $b_j^p = (\beta_j)$ for some $\beta_j \in k$. Let $t' = rk O_{k,S}^*$. Let $u_1, \ldots, u_{t'}, \zeta$ be generators for $O_{k,S}^*$. Let $M = k(\sqrt[1]{\beta_1}, \ldots, \sqrt[1]{\beta_t}, \sqrt[1]{u_1}, \ldots, \sqrt[1]{u_{t'}}, \sqrt[1]{\zeta})$. Let $L' = \mathbb{Q}(\sqrt[1]{\zeta} \mid q \in S_{fin})$. Note that $L' \subset L \cap M$, $[L' : \mathbb{Q}] = p^{|S_{fin}|}$, and

$$[LM : L] \leq [L(\sqrt[1]{\zeta}) : L][k : \mathbb{Q}]^{t' \cdot t' \cdot \#S_{fin}}.$$
From the definitions of \( \pi \) and \( X \), \( k(Q_i) = k(x_1, \ldots, x_r) \) for some choice of \( x_j \) satisfying \( x_j^m = f_j(P_i) \), \( j = 1, \ldots, r \). It suffices to show that \( x_j^p \in M \) for all \( j \). Indeed, this gives immediately that

\[
[L(Q_i) : L] \leq \left( \frac{m}{p} \right)^r [LM : L] \leq \left[ L \left( \sqrt[d]{\zeta} \right) : L \right] [k : \mathbb{Q}] m^i p^{l+i-t-\#S_{\text{fin}}}.
\]

By assumption, \( (x_j^m) = (f_j(P_i)) = a_j^m \) for some \( \mathcal{O}_{\kappa,S} \)-ideal \( a_j \). Since \( [a_j]^p \in G \),

\[
a_j^p = (\alpha) \prod_{s=1}^t b_{s}^{c_s}
\]

for some integers \( c_s \) and some element \( \alpha \in k \). Therefore,

\[
(x_j^m) = (a_j^p)^p = (\alpha^p) \prod_{s=1}^t (\beta_{s}^{c_s}).
\]

So \( x_j^m = u^{\alpha^p} \prod_{s=1}^t \sqrt[d]{\beta_{s}^{c_s}} \) for some unit \( u \in \mathcal{O}_{\kappa,S}^* \). Therefore, \( x_j^p = u \sqrt[d]{\alpha} \prod_{s=1}^t \sqrt[d]{\beta_{s}^{c_s}} \)

for some choice of the \( p \)-th roots. So \( x_j^p \in M \) for all \( j \) as desired. \( \Box \)

For \( i \in I \), let \( Q_i \in \pi^{-1}(P_i) \). So \( \phi(\pi(Q_i)) = i \in \mathbb{A}^I(\mathbb{Z}) \). Let \( L \) be the number field from Lemma \( \text{(10)} \). Let \( M \) be the number field generated over \( L \) by elements \( \sqrt[d]{\zeta} \), where \( \zeta \) is any root of unity appearing in a number field \( k \) with \( [k : \mathbb{Q}] \leq n \). Let \( W \) be a proper closed subset of \( \mathbb{A}^I \) containing \( \phi(\mathbb{Z}) \). By \( \text{(6)} \), for all \( i \in I \setminus W \),

\[
[M(Q_i) : M] \leq nm^r p^{\text{rk}_m \text{Cl}(Q(P_i))} + \text{rk} \mathcal{O}_{Q(i),S}^* - r - \#S_{\text{fin}}.
\]

On the other hand, \( \deg \phi \circ \pi = nm^r \). Therefore, by Hilbert’s Irreducibility Theorem over \( M \), we obtain that for all but \( O \left( N^{l-\frac{1}{2}} \log N \right) \) (or \( O(\sqrt{N}) \) if \( l = 1 \)) points \( i \in I(N) \), we have \( [Q(P_i) : \mathbb{Q}] = n \) and \( \text{rk}_m \text{Cl}(Q(P_i)) \geq r + \#S_{\text{fin}} - \text{rk} \mathcal{O}_{Q(i),S}^* \). \( \Box \)

We will frequently apply Theorem \( \text{(9)} \) to sets \( I \) and \( S \) such that for every \( i \in I \), there exists exactly one place of \( \mathbb{Q}(P_i) \) above each finite place of \( S \) (in particular, this holds if \( S = \{ \infty \} \), the archimedean place of \( \mathbb{Q} \)). Note that in this case, \( \text{(3)} \) simplifies to

\[
\text{rk}_m \text{Cl}(Q(P_i)) \geq r - \text{rk} \mathcal{O}_{Q(i),S}^*.
\]

The most natural examples of functions \( f_1, \ldots, f_r \) satisfying \( \text{(3)} \) and \( \text{(4)} \) arise from torsion in the Picard group (group of isomorphism classes of invertible sheaves) of a variety. If \( V \) is a nonsingular variety over \( \mathbb{Q} \), we can identify \( \text{Pic}(V) \) with the group of \( (\mathbb{Q}\text{-rational}) \) divisors on \( V \) modulo linear equivalence. We denote the linear equivalence class of a divisor \( D \) by \( [D] \). If \( f \) is a rational function on \( V \), we let \( (f) \) be the principal divisor associated to \( f \). 9
Corollary 11. Let $V$ be a nonsingular projective variety over $\mathbb{Q}$ of dimension $l$. Let $\phi : V \to \mathbb{A}^1$ be a generically finite rational map with $\deg \phi = n > 1$. Let $I = \{ P \in \mathbb{A}^1(\mathbb{Z}) \mid P \in \phi(V) \}$ and let $I(N) = \{ i \in I \mid H(i) < N \}$. For $i \in I$, let $P_i \in \phi^{-1}(i)$. Let $m > 1$ be a positive integer. Then there exists a finite set of places $S$ of $Q$, depending only on $V$ and $m$ and not $\phi$, such that for all but $O(N^{l-\frac{2}{3}} \log N)$ (or $O(\sqrt{N})$ if $l = 1$) points $i \in I(N)$, we have $|Q(P_i) : Q| = n$ and
\[
\text{rk}_m \ Cl(Q(P_i)) \geq \text{rk}_m \ Pic(V)_{\text{tors}} + \# S_{\text{fin}} - \text{rk} \ O_{Q(P_i),S}^*.
\] (7)

Proof. Let $r = \text{rk}_m \ Pic(V)_{\text{tors}}$. We first show that (3) holds for certain functions $f_1, \ldots, f_r$.

Lemma 12. Let $D_1, \ldots, D_r$ be divisors whose divisor classes generate a subgroup $(\mathbb{Z}/m\mathbb{Z})^r \subset \text{Pic}(V)$. Let $f_1, \ldots, f_r \in \mathbb{Q}(V)$ be rational functions such that $(f_j) = mD_j$ for all $j$. Then
\[
\left[ \mathbb{Q}(V) \left( \sqrt[m]{f_1}, \ldots, \sqrt[m]{f_r} \right) : \mathbb{Q}(V) \right] = m^r.
\]

Proof. By Kummer theory, this is equivalent to showing that $f_1, \ldots, f_r$ generate a subgroup of cardinality $m^r$ in $\mathbb{Q}(V)^*/\mathbb{Q}(V)^{m^*}$. Suppose that
\[
f_1^{i_1}f_2^{i_2} \cdots f_r^{i_r} = g^m
\] (8)
for some $g \in \mathbb{Q}(V)^*$ and integers $0 \leq i_1, \ldots, i_r < m$. Let $(g) = E$, the principal divisor associated to $g$. Then by (3), $mE = \sum_{j=1}^r mi_jD_j$. So $E = \sum_{j=1}^r i_jD_j$ is a principal divisor. Since $[D_1], \ldots, [D_r]$ are independent in $\text{Pic}(V)[m]$ (over $\mathbb{Z}/m\mathbb{Z}$), it follows that $i_j = 0$ for all $j$. \qed

Let $f_1, \ldots, f_r$ be as in Lemma 12. Since $(f_j) = mD_j$ is an “$m$-th power” in the divisor group of $V$, the values of $f_j$ must be an $m$-th power outside of some finite set of places $S$ depending only on $f_j$.

Lemma 13. There exists a finite set of places $S$ of $\mathbb{Q}$ such that for all $P \in C(\mathbb{Q})$ and all $j$,
\[
f_j(P)O_{\mathbb{Q}(P),S} = a_{P,j}^m
\]
for some fractional $O_{\mathbb{Q}(P),S}$-ideal $a_{P,j}$.

Proof. This is an immediate consequence of Weil’s Decomposition Theorem \cite[2.7.15]{1}.

Thus, (4) holds for a finite set of places $S$ of $\mathbb{Q}$ independent of $\phi$. We are now done by Theorem 9. \qed

The main content of Corollary 11 is that the set of places $S$ can be chosen independent of $\phi$. This fact is sufficient to prove the following result for superelliptic curves.
Corollary 14. Let $C$ be the normalization of a plane curve defined by

$$y^n = f(x), \quad f(x) \in \mathbb{Q}[x], \quad n > 1,$$

with $(\deg f, n) = 1$. Let $m > 1$ be an integer. Then there exist $X \gg n \log X$ number fields $k$ of degree $[k : \mathbb{Q}] = n$ with discriminant $d_k$, $|d_k| < X$, and

$$\text{rk}_m \text{Cl}(k) \geq \text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}} - \left\lceil \frac{n-1}{2} \right\rceil.$$ 

Proof. Let $t = \deg f$ and let $f = \sum_{i=0}^{t} a_i x^i$. By rescaling $x$ and $y$ we can assume that $a_i \in \mathbb{Z}$ for all $i$ and, using $(t, n) = 1$, that $a_t = -1$. Let $S$ be as in Corollary 11 for $V = C$ and $m$. Let $M = \prod_{p \in S_{\text{fin}}} p$. Let $\psi$ be the rational function on $y^n = f(x)$ defined by $\psi = x - \frac{1}{M}$. For $i \in \mathbb{Z}$, let $p_i = \psi^{-1}(i)$.

Then $\mathbb{Q}(p_i) \cong \mathbb{Q}\left(\sqrt[t]{f\left(\frac{iM+1}{n}\right)}\right)$. Let $p \in S_{\text{fin}}$. Since $a_t = -1$, we have that $\text{ord}_p f\left(\frac{iM+1}{n}\right) = -t$. This implies that $p$ totally ramifies in $\mathbb{Q}(p_i)$. Explicitly, if $i, j \in \mathbb{N}$ is such that $ni - tj = 1$, then $\left(M^i \sqrt[t]{f\left(\frac{iM+1}{n}\right)}\right)^n = (p)$ in $\mathcal{O}_{\mathbb{Q}(p_i)}$.

Note also that $[\mathbb{Q}(p_i) : \mathbb{Q}] = n$. So every prime of $S_{\text{fin}}$ is totally ramified in $\mathbb{Q}(p_i)$. Let $\phi : C \to \mathbb{P}^1$ be the morphism induced by $\psi$. The condition $(t, n) = 1$ implies that $y^n = f(x)$ has a rational point at infinity. Since $C$ has a rational point, $\text{Pic}(C)_{\text{tors}} \cong \text{Jac}(C)(\mathbb{Q})_{\text{tors}}$ (this follows, for instance, from Lemma 17). Corollary 14 applied to $\phi$ and $C$ then implies that for all but $O(\sqrt{N})$ values $i = 1, \ldots, N$, we have $[\mathbb{Q}(p_i) : \mathbb{Q}] = n$ and

$$\text{rk}_m \text{Cl}(\mathbb{Q}(p_i)) \geq \text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}} - \text{rk} \mathcal{O}_{\mathbb{Q}(p_i)}^\times.$$ 

Since $a_t = -1$, for $i > 0$, $f\left(\frac{iM+1}{n}\right)$ is negative. It follows that for $i > 0$, $\mathbb{Q}(p_i)$ has exactly one real place if $n$ is odd and no real places if $n$ is even. So by Dirichlet’s theorem, $\text{rk} \mathcal{O}_{\mathbb{Q}(p_i)}^\times = \left\lceil \frac{n-1}{2} \right\rceil$ for $i > 0$. It follows from Theorem 8 that there are $\gg N/\log N$ distinct number fields in the set $\{\mathbb{Q}(p_1), \ldots, \mathbb{Q}(p_N)\}$. An easy calculation shows that $|d_{\mathbb{Q}(p_i)}| = O(i^{(n-1)t})$. Combining the above statements then gives the corollary. \hfill $\square$

Of particular interest is the case where $C$ is a hyperelliptic curve.

Corollary 15. Let $C$ be a nonsingular hyperelliptic curve over $\mathbb{Q}$ with a rational Weierstrass point. Let $g$ denote the genus of $C$. Let $m > 1$ be an integer. Then there exist $X \gg n \log X$ imaginary quadratic number fields $k$ with

$$\text{rk}_m \text{Cl}(k) \geq \text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}}, \quad |d_k| < X,$$

and $\gg X^{\frac{1}{g+1}}/\log X$ real quadratic number fields $k$ with

$$\text{rk}_m \text{Cl}(k) \geq \text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}} - 1, \quad d_k < X.$$
Proof. Since $C$ has a rational Weierstrass point, $C$ is birational to a plane curve defined by $y^2 = f(x)$, for some $f(x) \in \mathbb{Q}[x]$ with $\deg f = 2q + 1$. The statement on imaginary quadratic fields now follows from Corollary 14. The statement for real quadratic fields follows similarly from the proof of Corollary 14 using points $P_i$, $i < 0$, with the extra $-1$ term coming from the rank-one unit group of a real quadratic field. 

As another variation on Corollary 11, we prove a theorem for curves $C$ using $\text{Jac}(C)(\mathbb{Q})_{\text{tors}}$ rather than $\text{Pic}(C)_{\text{tors}}$, and we give a simple explicit description of a viable set of places $S$ in (7). We let $\overline{C}$ be the curve $C$ base extended over $\overline{\mathbb{Q}}$, and we naturally identify objects on $C$ (rational functions, divisors, etc.) with the corresponding objects on $\overline{C}$.

**Corollary 16.** Let $C$ be a nonsingular projective curve over $\mathbb{Q}$. Let $\phi : C \to \mathbb{P}^1$ be a morphism with $\deg \phi = n > 1$. Let $m > 1$ be a positive integer. Let

$$d = \gcd\{[k : \mathbb{Q}] \mid \overline{C} \text{ has a } k\text{-rational degree one divisor}\}.$$ 

Let $m' = \frac{m}{(m,d)}$ with $m' > 1$. Let $T$ be the union of the set of primes dividing $m$, the set of primes of bad reduction of $\text{Jac}(C)$, and the archimedean prime of $\mathbb{Q}$. For $i \in \mathbb{Z}$, let $P_i \in \phi^{-1}(i)$. Then for all but $O(\sqrt{N})$ values $i = 1, \ldots, N$, we have $[\mathbb{Q}(P_i) : \mathbb{Q}] = n$ and

$$\text{rk}_{m'}(\text{Cl}(\mathbb{Q}(P_i))) \geq \text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}} + \#T_{\text{fin}} - \text{rk} \mathcal{O}_{\mathbb{Q}(P_i),T}^*.$$ 

For simplicity, we prove Corollary 16 in the case $m = m'$, or equivalently, $(d,m) = 1$. The proof of the general case of the corollary requires only minor modifications. Let $r = \text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}}$. Corollary 16 follows from Theorem 8 Lemma 12 and the following lemma.

**Lemma 17.** There exist $\mathbb{Q}$-rational divisors $D_1, \ldots, D_r$ whose divisor classes generate a subgroup $(\mathbb{Z}/m\mathbb{Z})^r \subset \text{Jac}(C)(\mathbb{Q})$ and rational functions $f_j \in \mathbb{Q}(C)$, $j = 1, \ldots, r$, such that $(f_j) = mD_j$ and for all but $O(\sqrt{N})$ values $i = 1, \ldots, N,

$$f_j(P_i)\mathcal{O}_{\mathbb{Q}(P_i),T} = a_{i,j}^m$$

for some fractional $\mathcal{O}_{\mathbb{Q}(P_i),T}$-ideal $a_{i,j}$.

Proof. Let $c_1, \ldots, c_r$ be generators for a subgroup $(\mathbb{Z}/m\mathbb{Z})^r \subset \text{Jac}(C)(\mathbb{Q})$. We first claim that it suffices to show that if $\overline{C}$ has a degree one $k$-rational divisor $D$ and $[k : \mathbb{Q}] = c$, then there exist $\mathbb{Q}$-rational divisors $D_1, \ldots, D_r$ and rational functions $f_j \in \mathbb{Q}(C)$, $j = 1, \ldots, r$, such that $[D_j] = ec_j$, $(f_j) = mD_j$, and (7) holds. This can be proven as follows. Since $(m,d) = 1$, there exist number fields $k_l$, $[k_l : \mathbb{Q}] = \epsilon_l$, $l = 1, \ldots, L$, such that $\sum_{l=1}^{L} \epsilon_l = 1 \mod m$ and for each $l$ there exists a degree one $k_l$-rational divisor on $\overline{C}$. Let $D_{j,l}$ and $f_{j,l}$ be divisors and rational functions, as in our claim above, for $k_l$. Let $D_j = \sum_{l=1}^{L} D_{j,l}$ and $f_j = \prod_{l=1}^{L} f_{j,l}$. Then using that $\sum_{l=1}^{L} \epsilon_l = 1 \mod m$, we get that $[D_j] = c_j$ and it is easily seen that $f_j$ and $D_j$ satisfy the conditions of the theorem.
Let $D$ be a degree one $k$-rational divisor on $\bar{C}$. Let $[k : \mathbb{Q}] = c$. Let $\psi : \bar{C} \to J = \text{Jac}(\bar{C})$ be the $k$-rational embedding given by $P \mapsto [P - D]$. Let $\Theta = \psi(\bar{C}) + \ldots + \psi(\bar{C})$ be the theta divisor on $J$. Let $E_j = \Theta - t_{c_j}^* \Theta$, where $t_{c_j}$ denotes the translation-by-$c_j$ map on $J$. By the theorem of the square, $mE_j$ is a principal divisor. Let $g_j \in k(J)$ be such that $(g_j) = mE_j$. Since $[m]^*E_j \sim mE_j$ is principal, where $[m]$ is multiplication by $m$ on $J$, let $h_j \in k(J)$ be such that $(h_j) = [m]^*E_j$. It follows immediately that $g_j(mx) = \alpha_j h_j(x)^m$ for some constant $\alpha_j \in k^*$. Replacing $g_j$ by $g_j/\alpha_j$, we can assume that $g_j(mx) = h_j(x)^m$.

Let $x, y \in J(\mathbb{Q})$ with $my = x$. It is a standard fact that the extension $k(y)/k(x)$ is unramified outside of (places lying above) $k$. Since $g_j(x) = g_j(my) = h_j(y)^m$ and $k(y)/k(x)$ is unramified outside of $T$, it follows that $g_j(x)O_{k(x)}T = a_j^m$ for some fractional $O_{k(x)}T$-ideal $a_j$. Let $N_q^k$ denote any map naturally induced by the norm map from $k$ to $\mathbb{Q}$. Let $f_j = N_q^k g_j|_{\bar{C}}$, via the embedding $\psi : \bar{C} \to J$. Let $D_j = N_q^k \psi^* (\Theta - t_{c_j}^* \Theta)$. Then $f_j$ and $D_j$ are both defined over $\mathbb{Q}$. Furthermore, $(f_j) = N_q^k \psi^* (mE_j) = m N_q^k \psi^*(\Theta - t_{c_j}^* \Theta) = m D_j$. Since $[\psi^*(\Theta - t_{c_j}^* \Theta)] = c_j$ [26] Th. A.8.2.1, $[D_j] = N_q^k c_j = ec_j$. By Hilbert’s Irreducibility Theorem, for all but $O(\sqrt{N})$ values $i = 1, \ldots, N$, $[k(P_i) : k] = \deg \phi = n$. For such values of $i$, $f_j(P_i) = (N_q^k g_j|_{\bar{C}})(P_i) = N_q^k(b_j)(g_j|_{\bar{C}}(P_i))$. Thus, from the corresponding property for $g_j$, we obtain that [30] holds for $f_j$ and all but $O(\sqrt{N})$ values $i = 1, \ldots, N$. \hfill $\square$

5 Applications and Examples

Using the theorems of the last section, we can rederive, in a simple manner, many of the results in Table 1. Additionally, in some cases we are able to obtain new quantitative results.

5.1 Number fields $k$ of degree $n$ with $\text{rk}_n \text{Cl}(k)$ arbitrarily large

We give a simple proof of the fact that there exist number fields $k$ of degree $n$ with $\text{rk}_n \text{Cl}(k)$ arbitrarily large. For $n = 2$, this follows, as mentioned earlier, from a much more precise result of Gauss. For arbitrary $n$, this is implicit in [6] (or possibly [7]). The following theorem and proof are essentially taken from [40].

Theorem 18. Let $n > 1$ be a positive integer. Let $f(x) = \prod_{i=1}^{r} (a_i x - b_i)$, $a_i, b_i \in \mathbb{Z}$ for all $i$, be a polynomial with $r$ distinct roots. Let

$$T = \{ x \in \mathbb{Z} \mid (a_i x - b_i, a_j x - b_j) = 1, \forall i, j, i \neq j \}. $$

Then for all but $O(\sqrt{N})$ values $x \in T \cap [-N, \ldots, N]$, \n
$$\text{rk}_n \text{Cl} \left( \mathbb{Q} \left( \sqrt[n]{f(x)} \right) \right) \geq r - \text{rk} O^* \left( \sqrt[n]{f(x)} \right) - 1. $$

13
Proof. Let $C$ be the curve defined by $y^n = f(x)$. Let $\phi : C \to \mathbb{A}^1$ be given by $(x,y) \mapsto x$. Let $x_0 \in T$ and let $y_0 = \sqrt[n]{f(x_0)}$. Let $k = \mathbb{Q}(y_0)$. From the definition of $T$ and the fact that $y_0^n = f(x_0)$, it follows that for every $j$, $(a_jx_0 - b_j) = a_j^n$ for some ideal $a_j$ of $\mathcal{O}_k$. Furthermore,

$$\left(\mathbb{Q}(C)\left(\sqrt[n]{a_1x-b_1}, \ldots, \sqrt[n]{a_{r-1}x-b_{r-1}}\right) : \mathbb{Q}(C)\right) = n^{r-1}$$

is equivalent to the assertion that

$$(a_1x-b_1)^{i_1} \cdots (a_{r-1}x-b_{r-1})^{i_{r-1}} = f(x)^{i_r}g(x)^n, \quad g \in \mathbb{Q}(x), 0 \leq i_1, \ldots, i_r < n$$

has only the trivial solution with $i_1 = \cdots = i_r = 0$. This is obviously true under our assumptions. We now apply Theorem 9 (with $V = C$, $\phi$, $I = T$, $S = \{\infty\}$, and $f_j = a_jx - b_j$, $j = 1, \ldots, r - 1$). When $(n,r) = 1$, we note that if $C$ is a nonsingular projective model of $C$, then the divisors $D_1, \ldots, D_r$ on $\tilde{C}$ with $(f_j) = nD_j$ give rise to a subgroup $(\mathbb{Z}/n\mathbb{Z})^{r-1}$ in $\text{Jac}(\tilde{C})(\mathbb{Q})$ (see Corollary 14). \hfill $\square$

The set $T$ in Theorem 18 may be infinite or empty depending upon $f$. Since $r$ can be made arbitrary large with respect to $n$, by choosing appropriate polynomials $f$ we obtain the following corollary.

Corollary 19 (Bruner, Rosen [6, 7]). Let $n > 1$ be a positive integer. Then for any integer $r_0$ there exist infinitely many number fields $k$ of degree $n$ with $\text{rk}_n \text{Cl}(k) > r_0$.

Theorem 18 fits into a series of general results [6, 7, 14, 53, 55] giving information on $\text{Cl}(k)$ in terms of the ramification behavior of rational primes in $\mathcal{O}_k$. Indeed, Theorem 18 is easily derived, at least when $n$ is prime, from the following general result of Roquette and Zassenhaus (see [16] and [55] for generalizations).

Theorem 20 (Roquette, Zassenhaus [53]). Let $k$ be a number field of degree $n$. Let $p$ be a prime dividing $n$. Let $L = \mathbb{Q}(\{a \in k \mid a^p \in \mathbb{Q}\})$. Let $r$ be the number of prime ideals of $\mathbb{Q}$ that are $p$-th powers of ideals of $k$. Then

$$\text{rk}_p \text{Cl}(k) \geq r - \text{rk} \mathcal{O}_k^* - \text{ord}_p[L : \mathbb{Q}],$$

where $\text{ord}_p m$ denotes the largest power of $p$ dividing $m$.

### 5.2 Imaginary quadratic fields with an element of order $m$ in the class group

Let $k$ be an imaginary quadratic field with an integral ideal $a$ of order $m$ in $\text{Cl}(k)$. Then $a^m = (\alpha)$ for some $\alpha \in \mathcal{O}_k$. Taking norms, we obtain an equation

$$4x^m = y^2 + t^2d$$

in integers $x$, $y$, $t$, and $d$, where $d$ is squarefree, $k = \mathbb{Q}(\sqrt{-d})$, $\alpha = \frac{a + \sqrt{-d}}{2}$, and $N(a) = x$. The next theorem gives a sort of converse to this fact.
Theorem 21. Let \( T(N) = \{(x, y) \in \mathbb{Z}^2 \mid |x|, |y| < N, y^2 - 4x^m < 0, (x, y) = 1\} \). For all but \( O(N^{2 \log N}) \) elements \( (x, y) \in T(N) \), the field \( \mathbb{Q}\left(\sqrt{y^2 - 4x^m}\right) \) has an element of order \( m \) in its class group.

Proof. Consider the surface \( V \) defined by \( z^2 = y^2 - 4x^m \). Let \( x_0, y_0 \in \mathbb{Z} \) be such that \( z_0^2 = y_0^2 - 4x_0^m < 0 \) and \( (x_0, y_0) = 1 \). Let \( k = \mathbb{Q}(z_0) \). Then \( \frac{y_0 + z_0}{2}, \frac{y_0 - z_0}{2} \in \mathcal{O}_k \) and \( \left(\frac{y_0 + z_0}{2}, \frac{y_0 - z_0}{2}\right) = (x_0, y_0) = \mathcal{O}_k \). Thus, from the factorization \( \left(\frac{y_0 + z_0}{2}\right)\left(\frac{y_0 - z_0}{2}\right) = x_0^m \), we have that \( \left(\frac{y_0 + z_0}{2}\right) = a^m \) for some ideal \( a \) of \( \mathcal{O}_k \). Furthermore, it is easy to see that

\[
\left[\mathbb{Q}(V) \left(\sqrt{\frac{y + z}{2}}\right) : \mathbb{Q}(V)\right] = m.
\]

Let \( \phi : V \to \mathbb{A}^2 \) be the projection \( (x, y, z) \mapsto (x, y) \). Then we apply Theorem 9 to \( V, \phi, I = T(\infty), S = \{\infty\} \), and \( f_1 = \frac{y + z}{2} \).

By Remark 6 there exist integers \( x_0, y_0, N \in \mathbb{Z} \) (which, from the proof in [15], can also be chosen with \( (x_0, y_0, N) = 1 \)) such that if \( (x, y) \in T, x \equiv x_0 \pmod{N}, y \equiv y_0 \pmod{N} \), then \( \mathbb{Q}\left(\sqrt{y^2 - 4x^m}\right) \) has an element of order \( m \) in its class group. Indeed, Yamamoto explicitly showed this in [60].

Theorem 22 (Yamamoto). Let \( m > 1 \) be a positive integer with prime divisors \( p_1, \ldots, p_s \). Let \( q_1, \ldots, q_s \) be primes such that

\[
q_i \equiv \begin{cases} 
1 \pmod{p_i}, & \text{if } p_i \neq 2, \\
1 \pmod{4}, & \text{if } p_i = 2.
\end{cases}
\]

Let \( x \) and \( y \) be integers such that \( (x, y) = 1, y^2 - 4x^m < 0, q_i \) divides \( x \) for all \( i \), and \( y \) is a \( p_i \)-th power nonresidue \( \pmod{q_i} \) for all \( i \). Assume also that \( \mathbb{Q}\left(\sqrt{y^2 - 4x^m}\right) \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}) \). Then \( \text{Cl}\left(\mathbb{Q}\left(\sqrt{y^2 - 4x^m}\right)\right) \) contains an element of order \( m \).

5.3 Real quadratic fields with an element of order \( m \) in the class group

It is fairly easy to construct, for any integer \( m > 1 \), hyperelliptic curves \( C \) with a rational Weierstrass point and \( \text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}} \geq 2 \). Thus, using Corollary 15 we obtain quantitative versions of results of Yamamoto and Yamamoto-Weinberger.

Theorem 23. Let \( m > 1 \) be an integer. There exist \( \gg X^\frac{1}{m^2} / \log X \) imaginary quadratic number fields \( k \) with \( |d_k| < X \) and \( \text{rk}_m \text{Cl}(k) \geq 2 \) and \( \gg X^\frac{1}{m^2} / \log X \) real quadratic number fields \( k \) with \( d_k < X \) and \( \text{rk}_m \text{Cl}(k) \geq 1 \).
Proof. We construct hyperelliptic curves $C$ of genus $m - 1$ with a rational Weierstrass point and $\text{rk}_m \text{Jac}(C)(\mathbb{Q})_{\text{tors}} \geq 2$. Let $C$ be a projective curve in $\mathbb{P}^2$ defined by $(y - az)(y - bz)z^{m-1} = x^m(y - cz)$ with $a, b, c \in \mathbb{Q}$ all distinct. This curve has a singularity only at $(0, 1, 0)$. Let $\pi : \tilde{C} \to C$ be a normalization. It is easy to see that $\pi$ is bijective on points. Let $P_0 = \pi^{-1}((0, 1, 0))$, $P_1 = \pi^{-1}((0, a, 1))$, and $P_2 = \pi^{-1}((1, 0, 0))$. Let $D_1 = P_1 - P_0$ and $D_2 = P_2 - P_0$. Then it is easily checked that $(y - az \circ \pi) = mD_1$ and $(y - bz \circ \pi) = mD_2$. Suppose that $iD_1 + jD_2$ is principal for some $0 \leq i, j < m$. This implies that $(Y - a)^i(Y - c)^j = f^m$ for some $f$ in the function field $\mathbb{Q}(X, Y)$, where $X = \frac{x}{z} \circ \pi$ and $Y = \frac{y}{z} \circ \pi$. This is clearly impossible unless $i = j = 0$. Thus $\text{rk}_m \text{Jac}(\tilde{C})(\mathbb{Q})_{\text{tors}} \geq 2$. Completing the square in $y$, we see that the set of curves $C$ for distinct $a, b, c \in \mathbb{Q}$ is the same as the set of hyperelliptic curves given by $y^2 = x^{2m} + dx^m + c^2$, $d, e \in \mathbb{Q}$, $e \neq 0, d^2 \neq 4e^2$. Such curves may have rational Weierstrass points (e.g., curves with $d = -1 - e^2$), and so the result follows from Corollary 15.

The exponent $\frac{1}{2m-1}$ in Theorem 23 is not as good as the exponent $\frac{1}{m}$ (or $\frac{1}{m} - \epsilon$) achieved in the papers of Byeon [8], Luca [31], and Yu [61]. However, the case of Theorem 23 where $k$ is imaginary quadratic and $n$ is even does not appear to have been previously covered, and so here Theorem 23 does give a new result.

To obtain their results, Byeon and Yu looked at the binary form $\frac{3}{4}(3x^m + y^m)(x^m + 3y^m)$. In the hope of improving their results (possibly to an exponent of $\frac{1}{2m-\epsilon}$), we prove a theorem involving a ternary form.

**Theorem 24.** Let $m > 1$ be a positive integer. Let

$$f(x, y, z) = x^{2m} + y^{2m} + z^{2m} - 2x^my^m - 2x^mz^m - 2y^mz^m.$$  

For all but $O(N^{2m-1} \log N)$ elements $(x, y, z) \in \mathbb{Z}^3$ with $|x|, |y|, |z| < N$ and $(x^m - y^m, z) = (x^m - z^m, y) = (y^m - z^m, x) = 1$,

$$\text{rk}_m \text{Cl}(\mathbb{Q}(\sqrt{f(x, y, z)})) \geq \begin{cases} 2 & \text{if } f(x, y, z) < 0, \\ 1 & \text{if } f(x, y, z) > 0. \end{cases}$$

**Proof.** Consider the threefold $V$ defined by $v^2 = f(x, y, z)$ and the two factorizations

$$\frac{v + (x^m + y^m - z^m)}{2} = -x^my^m, \quad \frac{v + (x^m - y^m + z^m)}{2} = -x^mz^m. \quad (10)$$

Let $x_0, y_0, z_0 \in \mathbb{Z}$ with $(x^m_0 - y_0^m, z_0) = (x^m_0 - z_0^m, y_0) = (y^m_0 - z_0^m, x_0) = 1$. Let $v_0 = \sqrt{f(x_0, y_0, z_0)}$ and $k = \mathbb{Q}(v_0)$. The coprimality conditions immediately
then we get the third factorization two factorizations (10) and (11). As noticed by Craig, if \( k \) quadratic fields \( \sqrt{f} \) hyperelliptic curves quantitative versions of Craig’s theorems and show how his constructions yield an appropriate application of Theorem 9 gives the desired result.

It follows that \( \left( \frac{v_0 + (x_0^m + y_0^m - z_0^m)}{2}, \frac{v_0 - (x_0^m + y_0^m - z_0^m)}{2} \right) = \mathcal{O}_k \) and \( \mathcal{O}_k \). Moreover, by looking at the threefold \( (v' + y^m)(v' + z^m) = v'x^m \) birational to \( V \), the proof of Theorem 23 easily translates to a proof that

\[
[\mathcal{O}(V) \left( \sqrt{\frac{v + x^m + y^m - z^m}{2}}, \sqrt{\frac{v + x^m - y^m + z^m}{2}} \right) : \mathcal{O}(V)] = m^2.
\]

So an appropriate application of Theorem 9 gives the desired result.

5.4 3-ranks of quadratic fields and constructions of Craig

In [17] and [18], Craig constructed infinitely many imaginary quadratic fields \( k \) with \( \text{rk}_3 \text{Cl}(k) \geq 3 \) and \( \text{rk}_3 \text{Cl}(k) \geq 4 \), respectively, and infinitely many real quadratic fields \( k \) with \( \text{rk}_3 \text{Cl}(k) \geq 2 \) and \( \text{rk}_3 \text{Cl}(k) \geq 3 \), respectively. We prove quantitative versions of Craig’s theorems and show how his constructions yield hyperelliptic curves \( C \) with Jacobians having large rational 3-torsion subgroups.

We begin with the constructions in [17]. Let

\[
f(x, y, z) = x^6 + y^6 + z^6 - 2x^3y^3 - 2x^3z^3 - 2y^3z^3,
\]

the function of the last section for \( m = 3 \). Then if \( v^2 = f(x, y, z) \), we have the two factorizations (10) and (11). As noticed by Craig, if

\[
2(x^3 + y^3) = z^3 + w^3,
\]

then we get the third factorization

\[
\left( \frac{v + (x^3 - y^3 + w^3)}{2} \right) \left( \frac{v - (x^3 - y^3 + w^3)}{2} \right) = -x^3w^3.
\]

There are two more such factorizations, but they will not lead to any new ideal classes. A parametric solution to (12) is given by

\[
x = 18s^4, \quad y = 3s(t^3 - 6s^3), \quad z = t^4, \quad w = t(18s^3 - t^3).
\]

Let \( F(s, t) = f(x(s, t), y(s, t), z(s, t)) \). Explicitly,

\[
F(s, t) = t^{24} - 54s^3t^{21} + 1701s^6t^{18} - 32076s^9t^{15} + 393660s^{12}t^{12} - 3464208s^{15}t^9 + 19840464s^{18}t^6 - 68024448s^{21}t^3 + 136048896s^{24}.
\]

For many values of \( s \) and \( t \), \( \text{rk}_3 \text{Cl} \left( \mathcal{O} \left( \sqrt{F(s, t)} \right) \right) \geq 3 - \text{rk} \mathcal{O}_\mathbb{Q}^* (\sqrt{F(s, t)}) \).

17
Theorem 25. Let

\[ T = \{(s, t) \in \mathbb{Z}^2 \mid (3s, t) = 1, (s, 2) = 2, (s + 2^i t, 7) = 1, i = 0, 1, 2\} \]

and let \( T(N) = \{(s, t) \in T \mid |s|, |t| < N\} \). Then for all but \( O\left(N^{\frac{2}{3}} \log N\right) \) pairs \((s, t) \in T(N),\)

\[ \text{rk}_3 \Cl\left(\mathbb{Q}\left(\sqrt{F(s, t)}\right)\right) \geq \begin{cases} 3 & \text{if } F(s, t) < 0, \\ 2 & \text{if } F(s, t) > 0. \end{cases} \]

Furthermore, there are \( \gg X^{\frac{1}{24}} / \log X \) imaginary quadratic fields \( k \) with \( |d_k| < X \)
and \( \text{rk}_3 \Cl(k) \geq 3 \) and \( \gg X^{\frac{1}{24}} / \log X \) real quadratic fields \( k \) with \( d_k < X \) and \( \text{rk}_3 \Cl(k) \geq 2 \).

Proof. Let \( x = x(s, t), y = y(s, t), z = z(s, t), \) and \( w = w(s, t) \) as in \([13]\) and \([15]\). Let \( V \) be the variety defined by \( v^2 = F(s, t) \). Then we have the three identities \([10], [11],\) and \([13]\). Furthermore, the condition that each pair on the left-hand sides of \([10], [11],\) and \([13]\) be coprime is easily seen to be equivalent to the conditions \((3s, t) = 1, (s, 2) = 2, \) and \((s + 2^i t, 7) = 1, i = 0, 1, 2\) (see \([17]\) Lemma 0). Let \( g_1 = \frac{v+x^3+y^3-z^3}{2}, \) \( g_2 = \frac{v+x^3-y^3+z^3}{2}, \) and \( g_3 = \frac{v+x^3-y^3+z^3}{2} \). Thus, if \((s, t) \in T\) and \( v^2 = F(s, t)\), then each of the ideals \((g_1(s, t, v)), (g_2(s, t, v)), \) and \((g_3(s, t, v))\) is the cube of an ideal in \( \mathcal{O}_{\mathbb{Q}(v)} \). To show the first part of the theorem, it remains to show that

\[ [\bar{\mathbb{Q}}(V)(\sqrt[3]{g_1}, \sqrt[3]{g_2}, \sqrt[3]{g_3}) : \bar{\mathbb{Q}}(V)] = 27. \] (16)

Actually, something stronger is true. Let \( C \) be the (nonsingular projective model of the) hyperelliptic curve defined by \( v^2 = F(1, t) \). Letting \( s = 1, \) we have the three rational functions \( g_1, g_2, g_3 \in \mathbb{Q}(C) \). It follows easily from \([10], [11],\) and \([13]\) that \((g_1) = 3D_1, (g_2) = 3D_2, \) and \((g_3) = 3D_3 \) for some degree zero divisors \( D_1, D_2, \) and \( D_3 \) on \( C \). Moreover, we claim that \( D_1, D_2, \) and \( D_3 \) generate a subgroup \((\mathbb{Z}/3\mathbb{Z})^3 \subset \text{Jac}(C)(\bar{\mathbb{Q}}) \). For hyperelliptic curves, there is an efficient algorithm (due to Cantor \([11]\)) for adding points in \( \text{Jac}(C) \). This has been implemented, for instance, in the computer algebra system Magma \([5]\). Using Cantor’s algorithm, it is easily verified in Magma (taking a few seconds) that \( D_1, D_2, \) and \( D_3 \) generate a 3-torsion subgroup of rank three in \( \text{Jac}(C)(\bar{\mathbb{Q}}) \), as claimed. It follows from Lemma \([12]\) that \([16]\) holds. So appropriately applying Theorem \([9]\) gives the first part of the theorem.

For the last statement of the theorem, we begin by noting that \( F(1, 2) = -1228544 < 0 \). It follows that for all sufficiently large \( u, F(84u-18, 168u-35) < 0 \) (note that \( F \) is homogeneous in \( s \) and \( t \)). Furthermore, if \( s = 84u - 18, t = 168u - 35, \) and \( u \in \mathbb{Z}, \) then \((3s, t) = 1, (s, 2) = 2, \) and \((s + 2^i t, 7) = 1, i = 0, 1, 2, \) Consider the rational function \( \phi(t, v) = \frac{16u-35}{84u-18} \) on \( C. \) Solving \( \phi(t, v) = u \) gives \( t = \frac{168u-35}{84u-18}. \) Then it follows from all of the above that by applying Theorem \([9]\) to the curve \( C \) and the rational functions \( \phi, g_1(1, t, v), g_2(1, t, v), \) and \( g_3(1, t, v), \) we obtain infinitely many imaginary quadratic fields \( k \) with \( \text{rk}_3 \Cl(k) \geq 3 \). More
precisely, using Theorem 8 since $\deg F(1, t) = 24$, we obtain $X \gg X^{1/2}$. imaginary quadratic fields $k$ with $|d_k| < X$ and $\text{rk}_3 \text{Cl}(k) \geq 3$. The proof of the statement for real quadratic fields is even easier.

We now examine the constructions of Craig from [18]. The idea in [18] is to find a nontrivial parametric family of solutions to the equations

$$f(x_0, y_0, z_0) = f(x_1, y_1, z_1) = f(x_2, y_2, z_2).$$

Since

$$f(x, y, z) = (x^3 + y^3 - z^3)^2 - 4x^3y^3 = (x^3 - y^3 + z^3)^2 - 4x^3y^3z^3 = (-x^3 + y^3 + z^3)^2 - 4y^3z^3,$$

it suffices to find solutions to

$$x_1z_1 = x_0z_0, \quad x_2y_2 = x_0y_0,$$

$$x_1^3 - y_1^3 + z_1^3 = -(x_0^3 - y_0^3 + z_0^3),$$

$$x_2^3 + y_2^3 - z_2^3 = -(x_0^3 + y_0^3 - z_0^3).$$

Craig gives a two-parameter family of solutions to (17), (18), and (19) in terms of $\alpha$, $\beta$, and $\gamma$ satisfying $\alpha + \beta + \gamma = 0$. We refer the reader to [18] for the rather involved formulas. We specialize Craig’s solution by setting $\alpha = 0$, $\beta = t$, and $\gamma = -t$. This gives a polynomial $h(t) = f(x_0(t), y_0(t), z_0(t))$ of degree 141. Let $C$ be the (nonsingular projective model of the) hyperelliptic curve defined by $Y^2 = h(t)$. We have the four identities (where $x_0 = x_0(t)$, $y_0 = y_0(t)$, etc.),

$$Y + (x_0^3 + y_0^3 - z_0^3)) (Y - (x_0^3 + y_0^3 - z_0^3)) = -4x_0^3y_0,$$

$$Y + (x_0^3 - y_0^3 + z_0^3) (Y - (x_0^3 - y_0^3 + z_0^3)) = -4x_0^3z_0^3,$$

$$Y + (x_0^3 + y_0^3 - z_0^3)) (Y - (x_0^3 + y_0^3 - z_0^3)) = -4x_0^3y_0,$$

$$Y + (-x_0^3 + y_0^3 + z_0^3)) (Y - (-x_0^3 + y_0^3 + z_0^3)) = -4y_0z_0.$$

It follows that there are divisors $D_1$, $D_2$, $D_3$, and $D_4$ on $C$ such that

$$Y + x_0^3 + y_0^3 - z_0^3) = 3D_1,$$

$$Y + x_0^3 - y_0^3 + z_0^3) = 3D_2,$$

$$Y + x_0^3 + y_0^3 - z_0^3) = 3D_3,$$

$$Y + x_0^3 + y_0^3 - z_0^3) = 3D_4.$$

Using Magma, it is easy to verify that $D_1$, $D_2$, $D_3$, and $D_4$ give independent 3-torsion elements of $\text{Jac}(C)(\mathbb{Q})$ (to simplify calculations, this can be done modulo $p = 7$, a prime of good reduction of $C$). Thus, we arrive at the following result.

**Theorem 26.** Let $C$ be the hyperelliptic curve defined by $Y^2 = h(t)$. Then $\text{rk}_3 \text{Jac}(C)(\mathbb{Q})_{\text{tors}} \geq 4$.

Since $h$ has odd degree, $C$ has a rational Weierstrass point, and so Corollary 21 applies.

**Corollary 27.** There are $\gg X^{1/2}/\log X$ imaginary quadratic fields $k$ with $|d_k| < X$ and $\text{rk}_3 \text{Cl}(k) \geq 3$ and $\gg X^{1/2}/\log X$ real quadratic fields $k$ with $d_k < X$ and $\text{rk}_3 \text{Cl}(k) \geq 3$. 

19
5.5 5-ranks of quadratic fields and a construction of Mestre

In [45], Mestre showed that there exist infinitely many imaginary and real quadratic fields \( k \) with \( \text{rk}_5 \text{Cl}(k) \geq 3 \). Fitting Mestre’s work into our framework, we show that a slight variation of Mestre’s constructions yields a one-parameter family of hyperelliptic curves \( C \) which have a rational Weierstrass point and \( \text{rk}_5 \text{Jac}(C)(\mathbb{Q})_{\text{tors}} \geq 3 \). Thus, by Corollary [15] we obtain infinitely many imaginary quadratic fields \( k \) with \( \text{rk}_5 \text{Cl}(k) \geq 3 \) and infinitely many real quadratic fields \( k \) with \( \text{rk}_5 \text{Cl}(k) \geq 2 \). Unfortunately, we are not able to fully recover Mestre’s result in the real quadratic case.

Elliptic curves with a rational point of order 10 form a one-parameter family, given explicitly by Kubert (after the change of variable \( f = \frac{u + 1}{2} \) in [30]) as

\[
y^2 = g_u(x),
\]

where

\[
g_u(x) = (x^2 - u(u^2 + u - 1))h_u(x),
\]

\[
h_u(x) = 8xu^2 + (u^2 + 1)(u^4 - 2u^3 - 6u^2 + 2u + 1).
\]

Alternatively, we can consider this as an elliptic curve over \( \mathbb{Q}(u) \) defined by

\[
y^2 = g_u(x),
\]

This has a point \( P \) over \( \mathbb{Q}(u) \) of order 10, given by

\[
P = \left( \frac{1 + 3u - u^2 - u^3}{2u}, \frac{(1 - u)(1 + u)^3(1 + 4u - u^2)}{2u} \right).
\]

Let

\[
u_1 = \frac{(t^2 + t - 1)/(t^2 + t + 1)},
\]

\[
u_2 = \frac{-(t^2 + 3t + 1)/(t^2 + t + 1)},
\]

\[
u_3 = \frac{-(t^2 - t - 1)/(t^2 + t + 1)}.
\]

Then

\[
u_1(u_1^2 + u_1 - 1) = u_2(u_2^2 + u_2 - 1) = u_3(u_3^2 + u_3 - 1).
\]

Let \( C \) be the nonsingular projective model of the curve (over \( \mathbb{Q}(t) \)) defined by

\[
y_1^2 = g_{u_1}(x), \quad \quad n_2^2 = g_{u_2}(x), \quad \quad n_3^2 = g_{u_3}(x).
\]

**Theorem 28.** The curve \( C \) is hyperelliptic of genus 5 with a \( \mathbb{Q}(t) \)-rational Weierstrass point and \( \text{rk}_{10} \text{Jac}(C)(\mathbb{Q}(t))_{\text{tors}} \geq 3 \).

**Proof.** Consider the three elliptic curves over \( \mathbb{Q}(t) \) given (in affine equations) by

\[
E_1 : y^2 = g_{u_1}(x),
\]

\[
E_2 : y^2 = g_{u_2}(x),
\]

\[
E_3 : y^2 = g_{u_3}(x).
\]

20
Let \( \phi_i, i = 1, 2, 3, \) be the natural projection map from \( C \) onto \( E_i \) induced by the map \((x, y_1, y_2, y_3) \mapsto (x, y_i)\). Let \( D_1, D_2, \) and \( D_3 \) be divisors generating the \( \mathbb{Q}(t) \)-rational 5-torsion on \( E_1, E_2, \) and \( E_3, \) respectively. Let \( D_i = \phi_i^* D_i, \) \( i = 1, 2, 3. \) Then \( \phi_i^*(a_1 D_1 + a_2 D_2 + a_3 D_3) \sim (\deg \phi_i) a_i D_i = 4 a_i D_i \) on \( E_i, \) \( i = 1, 2, 3, \) where \( \sim \) denotes linear equivalence. Since \( (4, 5) = 1, \) it follows immediately that \( D_1, D_2, \) and \( D_3 \) generate a 5-torsion subgroup of rank 3 in \( \text{Jac}(C)(\mathbb{Q}(t)). \)

Consider the curve \( C' \) over \( \mathbb{Q}(t) \) that is the nonsingular projective model of the curve defined by \( h_{u_1}(x) = v^2 h_{u_2}(x) = w^2 h_{u_3}(x). \) Then we have a degree two map \( \psi : C \rightarrow C' \) induced by the map

\[
(x, y_1, y_2, y_3) \mapsto \left( x, v = \frac{y_1}{y_2}, w = \frac{y_1}{y_3} \right)
\]

We claim that \( C' \cong \mathbb{P}^1_{\mathbb{Q}(t)}. \) In fact, an explicit parametrization (in \( z \)) of the curve \( h_{u_1}(x) = v^2 h_{u_2}(x) = w^2 h_{u_3}(x) \) is given by

\[
x = \frac{(1 + u_1^2)(1 + 2 u_1 - 6 u_1^3 - 2 u_1^3 + u_1^4) - (1 + u_2^2)(1 + 2 u_2 - 6 u_2^3 - 2 u_2^3 + u_2^4)v^2}{8(u_2^2 v^2 - u_1^4)}
\]

\[\tag{23}\]

\[
v = \frac{-1 - t + 3 t^2 + 2 t^3 - 2 z - 4 t z + 4 t^2 z + 2 t^3 z + z^2 - 2 t z^2 + t^3 z^2}{1 + 3 t^2 + 2 t^3 - 2 z - 2 t z + 6 t^2 z + 4 t^3 z - z^2 - 2 t z^2 + 2 t^2 z^2 + t^3 z^2},
\]

\[\tag{24}\]

\[
w = -\frac{-1 - t + 3 t^2 + 2 t^3 - 2 z - 4 t z + 4 t^2 z + 2 t^3 z + z^2 - 2 t z^2 + t^3 z^2}{(-1 - t + t^2)(-1 + 2 t - z^2 + t z^2)}
\]

\[\tag{25}\]

An explicit hyperelliptic equation for \( C \) can be obtained by substituting \( x = x(z) \) from (23) into any one of (20), (21), or (22). Note that the map \( \psi \) is ramified above the four \( \mathbb{Q}(t) \)-rational points on \( C' \) given by \((x, v, w) = (\infty, \pm \frac{u_1}{u_2}, \pm \frac{u_1}{u_3}). \) It follows that \( C \) has at least four rational Weierstrass points. Their pairwise differences generate a 2-torsion subgroup of rank 3 in \( \text{Jac}(C)(\mathbb{Q}(t)). \) Finally, a calculation of the explicit hyperelliptic equation for \( C \) (or a careful Riemann-Hurwitz calculation) shows that \( C \) has genus 5.

For infinitely many specializations \( t \in \mathbb{Z}, \) we obtain a hyperelliptic curve over \( \mathbb{Q} \) with the same properties as in Theorem 28. So by Corollary 15 we obtain the following.

**Corollary 29.** There are \( \gg X^{19}/\log X \) imaginary quadratic fields \( k \) with \( |d_k| < X \) and \( \text{rk}_{10}\text{Cl}(k) \geq 3 \) and \( \gg X^{19}/\log X \) real quadratic fields \( k \) with \( d_k < X \) and \( \text{rk}_{10}\text{Cl}(k) \geq 2. \)
5.6 Higher degree fields

A natural family of curves which, relatively speaking, have a lot of $m$-torsion in their Picard group are superelliptic curves $C$ of the form $y^m = a_0 \prod_{i=1}^{r} (x - a_i)$, $a_0, \ldots, a_r \in \mathbb{Z}$. We already took advantage of such curves in Section 5.1, using the projection map $\phi : C \to \mathbb{A}^1$, $(x, y) \mapsto x$, in our proof of Theorem 18. These curves, implicitly, also form the basis for the work of Azuhata, Ichimura, and Nakano on ideal class groups in higher degree number fields. In their work they use, essentially, the other simple projection map of these curves, $(x, y) \mapsto y$.

Applying a version of the technique of the present paper in this context, in [40] a quantitative version of a case of Azuhata and Ichimura’s theorem was derived.

**Theorem 30.** Let $m, n > 1$ be positive integers. There are $\gg X^{\frac{1}{m(n - 1)}} / \log X$ number fields $k$ of degree $n$ with $|d_k| < X$ and

$$\text{rk}_m \text{Cl}(k) \geq \left\lfloor \frac{n}{2} \right\rfloor.$$  

Improving on this result, we derive a quantitative version of Nakano’s theorem.

**Theorem 31.** Let $m, n > 1$ be positive integers. Let $r_1$ and $r_2$ be nonnegative integers such that $r_1 + 2r_2 = n$. Let

$$f(m, n, r_1, X) = \begin{cases} 
X^{\frac{1}{m(n - 1)}} / \log X & \text{if } n \text{ is odd and } 3 < r_1 < n, \\
X^{\frac{1}{m(n - 3)(2n - r_1 + 2)}} / \log X & \text{if } n \text{ is even and } 2 < r_1 < n, \\
X^{\frac{1}{m(n - 1)}} / \log X & \text{if } r_1 = n, \\
X^{\frac{1}{m(n - 1)}} / \log X & \text{if } m \text{ and } n \text{ are both even and } r_1 = 0, \\
X^{\frac{1}{m(n - 1)}} / \log X & \text{if } m \text{ is odd and } r_1 = 1, 3 \text{ or } 7, \\
X^{\frac{1}{m(n - 1)}} / \log X & \text{if } n \text{ is even and } r_1 = 2 \text{ or } 4, \\
X^{\frac{1}{m(n - 1)}} / \log X & \text{if } m \text{ is odd, } n \text{ is even, and } r_1 = 0.
\end{cases}$$

Then there are $\gg f(m, n, r_1, X)$ number fields $k$ of degree $n$ with $r_1$ real places and $r_2$ complex places, $|d_k| < X$, and

$$\text{rk}_m \text{Cl}(k) \geq r_2 + 1.$$  

**Proof.** Let $V \subset \mathbb{A}^{n+2}$ be the variety defined by $xt_0^m = -\prod_{j=1}^{n} (x - t_j^m)$. Let $P = (x, t_0, \ldots, t_n) \in V(\overline{\mathbb{Q}})$, with $t_0, \ldots, t_n \in \mathbb{Z}$. Let $k = \mathbb{Q}(P)$.

**Lemma 32.** Suppose that

$$\left( t_0, \prod_{1 \leq i < j \leq n} t_i^m - t_j^m \right) = 1, \quad (27)$$

$$\left( t_i, t_0^m + (-1)^{n-1} \prod_{j=1 \atop j \neq i}^{n} t_j^m \right) = 1, \quad i = 1, \ldots, n. \quad (28)$$

22
Then for \( j = 1, \ldots, n \), \( (x - t_j^m) = a_j^m \) for some ideal \( a_j \) of \( \mathcal{O}_k \).

**Proof.** Let \( \alpha_j = x - t_j^m, j = 1, \ldots, n \). Let \( i \in \{1, \ldots, n\} \). Then from the definitions, \( \alpha_i \) satisfies the equation

\[
\alpha_i \left( t_i^m + \prod_{j=1, j \neq i}^n (a_i + t_i^m - t_j^m) \right) = -(t_0 t_i)^m. \tag{29}
\]

Note that by (27) and (28),

\[
\left( (t_0 t_i)^m \right)^{m} + \prod_{j=1, j \neq i}^n (t_i^m - t_j^m) = 1.
\]

Since \( \alpha_i \) divides \( (t_0 t_i)^m \),

\[
\left( \alpha_i t_0^m + \prod_{j=1, j \neq i}^n (a_i + t_i^m - t_j^m) \right) = \left( \alpha_i t_0^m + \prod_{j=1, j \neq i}^n (t_i^m - t_j^m) \right) = \mathcal{O}_k.
\]

Using (29), we then obtain the lemma. \( \square \)

We prove the theorem by looking at certain curves on \( V \). For instance, suppose that \( n \) is odd and \( 3 < r_1 < n \) (for \( r_1 = 3 \), the proof also works, but in this case there is a better construction). We consider an affine plane curve \( C \) defined by \( (x, y) = x t_0^m = \prod_{j=1}^n (x - t_j^m) \), where

\[
t_0 = (BM y + 1)^{r_1 - 2}, \tag{30}
\]
\[
t_i = i B q y + a_i, \quad i = 1, \ldots, r_1 - 2, \tag{31}
\]
\[
t_i = p^{i-r_1+2}, \quad i = r_1 - 1, \ldots, n, \tag{32}
\]
and \( B, M, p, q, a_1, \ldots, a_{r_1-2} \in \mathbb{Z} \).

**Lemma 33.** There exist choices of primes \( p, q \), and integers \( B, M, a_1, \ldots, a_{r_1-2} \in \mathbb{Z} \) such that for all \( y \in \mathbb{Z} \), (27) and (28) hold for \( t_i \) as in (30), (31), (32),

\[
p^m, p^2m, \ldots, p^{m(n-r_1+2)}, a_1^m, \ldots, a_{r_1-2}^m
\]

are distinct and nonzero modulo \( q \), \( M \) is arbitrarily large compared to \( p, q, a_1, \ldots, a_{r_1-2} \), and \( BM \neq 0 \) (mod \( q \)).

**Proof.** Let \( b_i = a_i M - i q, i = 1, \ldots, r_1 - 2, \) and \( b_i = M p^{i-r_1+2}, i = r_1 - 1, \ldots, n \).

Let \( B_0 = \prod_{1 \leq i, j \leq n} b_i^m - b_j^m \). For \( i = 1, \ldots, r_1 - 2 \), let

\[
B_i = (i q - a_i M)^{m(r_1-2)} + (i q)^{m(r_1-2)} p^{r_1-2} \prod_{j=1, j \neq i}^n (i a_j - j a_i)^m.
\]

23
We choose $B$ such that $B = \prod_{i=0}^{r_1-2} B_i$. We claim that for this choice of $B$, Eqs. (27) and (28) can be reduced to the equations
\[
\left( a_i, (iq) \left( 1 + p^c \prod_{j \neq i}^{r_1-2} (ia_j)^m \right) \right) = 1, \quad i = 1, \ldots, r_1 - 2, \tag{33}
\]
where $c = \left( \frac{n-r_1+3}{2} \right)$. We now show this.

Suppose that (33) holds. The constant $B_0$ was chosen such that $B_0$ is in the ideal \( (BM + 1, \prod_{1 \leq j \leq n} t_j^m - t_j^m) \). Since $t_0 = (BM + 1)^{r_1-2} \equiv 1 \pmod{B_0}$, (27) holds. Similarly, for $i = 1, \ldots, r_1 - 2$, $B_i$ is in the ideal \( (t_i, t_i^m + \prod_{j \neq i} t_j^m) \) (note that since $n$ is odd, $(-1)^{n-1} = 1$). By (33), \((a_i, B_i) = 1 \) for $i = 1, \ldots, r_1 - 2$. Since $t_i \equiv a_i \pmod{B_i}$, $i = 1, \ldots, r_1 - 2$, we have that (28) holds for $i = 1, \ldots, r_1 - 2$. Since $r_1 < n$, $B \equiv 0 \pmod{p}$ and for any $i$, $t_i^m + \prod_{j \neq i} t_j^m \equiv 1 \pmod{p}$. Thus (28) holds for $i = r_1 - 1, \ldots, n$ also.

It is then fairly easy to see that there exists a choice of $B, M, p, q, a_1, \ldots, a_{r_1-2} \in \mathbb{Z}$ satisfying (33) as well as the other conditions in the statement of the lemma.

Choose $B, M, p, q, a_1, \ldots, a_{r_1-2} \in \mathbb{Z}$ as in Lemma 33 with $M$ sufficiently large compared to $p, q, a_1, \ldots, a_{r_1-2}$ (this will be quantified later). Let $f_j$ be the rational function on $C$ given by $f_j = x - t_j$, $j = 1, \ldots, n$. Let $P = (x_0, y_0) \in C(\mathbb{Q})$, with $y_0 \in \mathbb{Z}$ and $k = \mathbb{Q}(P)$. Then by Lemmas 32 and 33 for $j = 1, \ldots, n$, $f_j(P) \mathcal{O}_k = a_j^m$ for some ideal $a_j$ of $\mathcal{O}_k$. Modulo the prime $q$, the equation defining $C$ becomes
\[
x(BMy + 1)^m(r_1-2) = - \prod_{j=1}^{r_1-2} (x - a_j^m) \prod_{j=r_1-1}^{n} (x - p^m(j-r_1+2)),
\]
with $p^m, p^{2m}, \ldots, p^{m(n-r_1+2)}, a_1^m, \ldots, a_{r_1-2}^m$ distinct and nonzero modulo $q$ and $BM \not\equiv 0 \pmod{q}$. Thus, by looking modulo $q$, it follows easily that $C$ is in fact irreducible and
\[
\left[ \mathbb{Q}(C) \left( \sqrt{f_1}, \ldots, \sqrt{f_n} \right) : \mathbb{Q}(C) \right] = m^n.
\]
Let $\phi : C \to \mathbb{A}^1$ be the projection map $(x, y) \mapsto y$. Note that $\deg \phi = n$. For $i \in \mathbb{Z}$, let $P_i \in \phi^{-1}(i)$. Then by Theorem 9 for all but $O(\sqrt{N})$ values $i = 1, \ldots, N$, $[\mathbb{Q}(P_i) : \mathbb{Q}] = n$ and
\[
\text{rk}_n \text{Cl}(\mathbb{Q}(P_i)) \geq n - \text{rk} \mathcal{O}_{\mathbb{Q}(P_i)}^*.
\]
Using Theorem 8 to finish the proof of Theorem 31 when $n$ is odd and $1 < r_1 < n$, it suffices to prove:

**Lemma 34.** For $i \gg 0$, if $[\mathbb{Q}(P_i) : \mathbb{Q}] = n$ then $\mathbb{Q}(P_i)$ has exactly $r_1$ real places and
\[
d_{\mathbb{Q}(P_i)} = O(i^{(r_1-2)m(2n-r_1+1)}).
\]
Proof. We need to analyze the roots (in \(x\)) of the polynomial
\[
g_y(x) = x(BM + 1)^{m(r_1 - 2)} + \prod_{i=1}^{n-r_1+2} (x - p_i^\epsilon) \prod_{j=1}^{r_1-2} (x - (jBqy + a_j)^m)
\]
for \(y \gg 0\). We claim that for \(y \gg 0\), \(g_y(x)\) has \(r_1 - 2\) real roots with absolute value \(O(y^m)\), two real roots with absolute value \(O(1)\), and \(n-r_1\) nonreal complex roots with absolute value \(O(1)\). For \(y \gg 0\), the polynomial \(g_y(x)\) changes signs once on the interval \([y, (Bqy + a_1)^m]\) and twice on the intervals \([(2jBqy + a_{2j})^m, (2j + 1)Bqy + a_{2j+1})^m]\), \(j = 1, \ldots, (n-r_1)/2\). Thus, we obtain \(r_1 - 2\) real roots of size \(O(y^m)\). More precisely, since
\[
\lim_{y \to \infty} \frac{g_y(y^mx)}{y^{mn}} = x^{n-r_1+2} \prod_{j=1}^{r_1-2} (x - (jBq)^m)
\]
for these \(r_1 - 2\) real roots \(\alpha_1 < \alpha_2 < \cdots < \alpha_{r_1-2}\), \(\alpha_j \sim (jBqy)^m\) as \(y \to \infty\). Let \(D = ((r_1 - 2)q^{r_1-2})^m\). Then
\[
\lim_{y \to \infty} \frac{x^n g_y(\frac{x}{y})}{(By)^{m(r_1-2)}} = x^{r_1-2} \left(-D \prod_{i=1}^{n-r_1+2} (1 - p_i^\epsilon x) + M^{m(r_1-2)}x^{n-r_1+1}\right).
\]
It follows that the remaining \(n-r_1 + 2\) roots of \(g_y(x)\) converge to the reciprocals of the roots of \(h(x) = \left(-D \prod_{i=1}^{n-r_1+2} (1 - p_i^\epsilon x) + M^{m(r_1-2)}x^{n-r_1+1}\right)\) as \(y \to \infty\). In particular, all of these roots are bounded in absolute value as \(y \to \infty\). A simple computation then shows that the discriminant of \(g_y\) is \(O(y(r_1-2)m(2n-r_1+1))\), as desired. We now determine the number of real roots of \(h(x)\). Looking at sign changes of \(h(x)\), it is easily seen that \(h(x)\) has at least two real roots. Furthermore, note that
\[
\lim_{M \to \infty} \frac{h(M^{m(r_1-2)}x)}{M^{(r_1-2)m(n-r_1+2)}} = x^{n-r_1+1}(-Dp_\epsilon x + 1)
\]
and
\[
\lim_{M \to \infty} x^{n-r_1+2} h\left(\frac{1}{xM^{m(r_1-2)/(n-r_1+1)}}\right) = x(-Dx^{n-r_1+1} + 1).
\]
It follows from this that for \(M \gg 0\), \(h(x)\) has exactly two real roots. More precisely, let \(\epsilon > 0\). Then for all \(M\) sufficiently large (not depending on \(y\)), as \(y \to \infty\), among the remaining \(n-r_1 + 2\) roots of \(g_y(x)\), \(\beta_1, \ldots, \beta_{n-r_1+2}\), exactly two of them are real and the roots satisfy (after reindexing)
\[
\left|\frac{\zeta^j}{\beta_j} \left(\frac{M^{m(r_1-2)}}{D}\right)^{\frac{1}{n-r_1+1}} - 1\right| < \epsilon, \quad j = 1, \ldots, n-r_1 + 1,
\]
where \(\zeta = e^{\frac{-2\pi i}{r_1+1}}\), and \(\left|\frac{Dp_\epsilon}{\beta_{n-r_1+2}} - 1\right| < \epsilon\). Therefore, having fixed a sufficiently large integer \(M\), we see that \(g_y(x)\) has exactly \(r_1\) real roots for \(y \gg 0\). \(\square\)
The proofs of the other cases in the theorem are similar (or even easier), so we give only a few details. When $n$ is even and $2 < r_1 < n$, similar to the above, we let $t_0 = (BM + 1)^{r_1 - 3}$, \( t_i = iBqy + a_i \), \( i = 1, \ldots, r_1 - 3 \), and \( t_i = p^{i-r_1+3}, \)
\( i = r_1 - 2, \ldots, n \). The proof is then essentially identical to the proof above for $n$ odd and $3 < r_1 < n$.

To prove the cases $n$ odd, $r_1 = 1$, and $n$ even, $r_1 = 2$, we consider curves $C$ of the form $x(y + b)^m = -\prod_{i=1}^n (x - c_i^m)$. We choose $a, b, c_1, \ldots, c_n$ to be positive integers such that, for any $y \in \mathbb{Z}$, (27) and (28) hold with $t_0 = ay + b$ and $t_i = c_i$, $i = 1, \ldots, n$. For $y \gg 0$, the polynomial $x(y + b)^m + \prod_{i=1}^n (x - c_i^m)$ has exactly one real root if $n$ is odd, exactly two real roots if $n$ is even, and discriminant that is $O(y^{2m})$. So the desired result follows from Lemma 32, Theorem 8, and Theorem 3 with $V = C$, $I = \mathbb{Z}$, $\phi = y$, and $f_i = x - c_i$, $i = 1, \ldots, n$. The case $n$ odd, $r_1 = 3$, is similar, except that we consider curves of the form $x(y + b)^m = \prod_{i=1}^n (x - c_i^m)$. The case $m$ odd, $n$ even, and $r_1 = 0$, is similar except that we consider curves of the form $x^2(y + b)^m = -\prod_{i=1}^n (x - c_i^m)$ (in the case that $m$ and $n$ are both even, the proof breaks down because $-\prod_{i=1}^n (x - c_i^m) = (x(y + b)^m)^2$ and so the needed version of (3) does not hold).

In the case $r_1 = n$, we consider curves $C$ of the form
\[
g_y(x) = x(a_0 y + b_0)^m + (x - (M y + b_1))^m \prod_{i=2}^n (x - b_i^m) = 0,
\]
with $M$ sufficiently large compared to $a_0, b_0, \ldots, b_n$. With an appropriate choice of integers $a_0, b_0, \ldots, b_n, M$, we can apply Theorem 9 to $C$ with $f_1 = x - (M y + b_1)^m$, $f_i = (x - b_i^m)$, $i = 2, \ldots, n$, and $\phi : C \to \mathbb{A}^1$, $(x, y) \mapsto y$. For $M$ sufficiently large, $g_y(x)$ has $n$ real roots for $y$ sufficiently large and discriminant (in $x$) that is $O(y^{2m(n-1)})$.

Finally, when $m$ and $n$ are both even and $r_1 = 0$, we consider curves $C$ of the form
\[
g_y(x) = x(a_0 y + b_0)^{m(n-1)} + \prod_{i=1}^n (x - (M y + b_i)^m),
\]
with $M$ sufficiently large compared to $a_0, b_0, \ldots, b_n$. Again, with an appropriate choice of integers $a_0, b_0, \ldots, b_n, M$, we can apply Theorem 9 to $C$ with $f_i = (x - (M y + b_i)^m)$, $i = 1, \ldots, n$, and $\phi : C \to \mathbb{A}^1$, $(x, y) \mapsto y$. For $M$ sufficiently large, $g_y(x)$ has no real roots for $y$ sufficiently large and discriminant (in $x$) that is $O(y^{m(n-1)n})$.

For superelliptic curves $C$ of the form $y^m = a_0 \prod_{i=1}^r (x - a_i)$, $a_0, \ldots, a_r \in \mathbb{Z}$, we have discussed applying Theorem 9 to $C$ using the maps $\phi_1, \phi_2 : C \to \mathbb{A}^1$ given by $\phi_1 = x$ and $\phi_2 = y$. Using other maps, it was shown in [40] that in some situations it is possible to improve on Nakano's inequality (2).

**Theorem 35.** Let $m, n > 1$ be positive integers with $n > (m - 1)^2$. There are \( \gg X^{(m+1)n-1} / \log X \) number fields $k$ of degree $n$ with $|dk| < X$ and
\[
\operatorname{rk}_m \operatorname{Cl}(k) \geq \left\lfloor \frac{n + 1}{2} \right\rfloor + \frac{n}{m-1} - m.
\]
Since a complete proof of this theorem is given in [40], we only give a sketch of the proof.

**Proof.** Let $m, n > 1$ be integers with $n > (m - 1)^2$. Let $r$ be the largest integer such that $r - \left[ \frac{r}{m} \right] \leq n$ and $(r, m) = 1$. It is easily checked that $r \geq n + \frac{n-1}{m} - 1 + 1$. Let $C$ be the curve defined by $y^m = g(x) = -(x-a)^m \prod_{j=1}^{r-1} (x+a_j^m)$, where $a_1, \ldots, a_r$ are certain carefully chosen integers. Let $f_j = x + a_j^m$, $j = 1, \ldots, r - 1$.

Then (3) holds (with $V = C$ and $r \mapsto r - 1$). Let $h(x)$ be the Taylor series for $\sqrt[n]{g(x)}$ at $x = 0$ truncated to degree $\left[ \frac{r}{m} \right] - 1$ with $h(0) = \prod_{j=1}^r a_j$. Let $b$ be the lowest common denominator of the coefficients of $h$. Let $\phi$ be the rational function $\phi = b(y - h)$ on $C$. For $i \in \mathbb{Z}$, let $P_i \in \phi^{-1}(i)$. Having chosen $a_1, \ldots, a_r$ properly, it can be shown that there exist integers $i_0$ and $N$ such that if $i \equiv i_0 \pmod{N}$, then for all $j$, $f_j(P_i) = a_{i,j}$ for some fractional ideal $a_{i,j}$ of $\mathcal{O}_{\mathbb{Q}(P_i)}$. So (4) holds with $I = \{ i \in \mathbb{Z} \mid i \equiv i_0 \pmod{N} \}$. Furthermore, it can be computed that the map induced by $\phi$ has degree $n$, $d_{\mathbb{Q}(P_i)} = O(i^{(m+1)n-1})$, and $\mathbb{Q}(P_i)$ has at most two real places for $i \gg 0$. An appropriate application of Theorems [8] and [9] finishes the proof. 

**References**

[1] N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math. 5 (1955), no. 3, 321–324.

[2] T. Azuhata and H. Ichimura, *On the divisibility problem of the class numbers of algebraic number fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 30 (1984), no. 3, 579–585.

[3] Y. F. Bilu and F. Luca, *Divisibility of class numbers: enumerative approach*, J. Reine Angew. Math. 578 (2005), 79–91.

[4] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[6] A. Brumer, *Ramification and class towers of number fields*, Michigan Math. J. 12 (1965), no. 2, 129–131.

[7] A. Brumer and M. Rosen, *Class number and ramification in number fields*, Nagoya Math. J. 23 (1963), 97–101.

[8] D. Byeon, *Imaginary quadratic fields with noncyclic ideal class groups*, Ramanujan J. 11 (2006), no. 2, 159–163.

[9] , *Real quadratic fields with class number divisible by 5 or 7*, Manuscripta Math. 120 (2006), no. 2, 211–215.
[10] D. Byeon and E. Koh, *Real quadratic fields with class number divisible by 3*, Manuscripta Math. **111** (2003), no. 2, 261–263.

[11] D. G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), no. 177, 95–101.

[12] K. Chakraborty and R. Murty, *On the number of real quadratic fields with class number divisible by 3*, Proc. Amer. Math. Soc. **131** (2003), no. 1, 41–44 (electronic).

[13] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups*, Number theory, Lecture Notes in Math., vol. 1052, Springer, Berlin, 1984, pp. 26–36.

[14] ———, *Heuristics on class groups of number fields*, Number theory, Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.

[15] S. D. Cohen, *The distribution of Galois groups and Hilbert’s irreducibility theorem*, Proc. London Math. Soc. (3) **43** (1981), no. 2, 227–250.

[16] I. Connell and D. Sussman, *The $p$-dimension of class groups of number fields*, J. London Math. Soc. (2) **2** (1970), 525–529.

[17] M. Craig, *A type of class group for imaginary quadratic fields*, Acta Arith. **22** (1973), 449–459.

[18] ———, *A construction for irregular discriminants*, Osaka J. Math. **14** (1977), no. 2, 365–402.

[19] F. Diaz y Diaz, *Sur le 3-rang des corps quadratiques*, Publications Mathématiques d’Orsay 78, vol. 11, Université de Paris-Sud Département de Mathématique, Orsay, 1978.

[20] R. Dvornicich and U. Zannier, *Fields containing values of algebraic functions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **21** (1994), no. 3, 421–443.

[21] ———, *Fields containing values of algebraic functions. II. (On a conjecture of Schinzel)*, Acta Arith. **72** (1995), no. 3, 201–210.

[22] E. V. Flynn, *Large rational torsion on abelian varieties*, J. Number Theory **36** (1990), no. 3, 257–265.

[23] ———, *Sequences of rational torsions on abelian varieties*, Invent. Math. **106** (1991), no. 2, 433–442.

[24] S. Hernández and F. Luca, *Divisibility of exponents of class groups of pure cubic number fields*, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 237–244.
[25] C. S. Herz, *Seminar on complex multiplication. VII. Construction of class fields*, Lecture Notes in Mathematics, No. 21, Springer-Verlag, Berlin, 1966.

[26] M. Hindry and J. H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000.

[27] E. W. Howe, F. Leprévost, and B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364.

[28] P. Humbert, *Sur les nombres de classes de certains corps quadratiques*, Comment. Math. Helv. **12** (1940), no. 1, 233–245.

[29] M. Ishida, *On 2-rank of the ideal class groups of algebraic number fields*, J. Reine Angew. Math. **273** (1975), 165–169.

[30] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237.

[31] S. Kuroda, *On the class number of imaginary quadratic number fields*, Proc. Japan Acad. **40** (1964), 365–367.

[32] F. Leprévost, *Famille de courbes de genre 2 munies d’une classe de diviseurs rationnels d’ordre 13*, C. R. Acad. Sci. Paris Sér. I Math. **313** (1991), no. 7, 451–454.

[33] ———, *Familles de courbes de genre 2 munies d’une classe de diviseurs rationnels d’ordre 15, 17, 19 ou 21*, C. R. Acad. Sci. Paris Sér. I Math. **313** (1991), no. 11, 771–774.

[34] ———, *Torsion sur des familles de courbes de genre g*, Manuscripta Math. **75** (1992), no. 3, 303–326.

[35] ———, *Famille de courbes hyperelliptiques de genre g munies d’une classe de diviseurs rationnels d’ordre 2g^2+4g+1*, Séminaire de Théorie des Nombres, Paris, 1991–92, Progr. Math., vol. 116, Birkhäuser Boston, Boston, MA, 1993, pp. 107–119.

[36] ———, *Points rationnels de torsion de jacobienne de certaine courbe de genre 2*, C. R. Acad. Sci. Paris Sér. I Math. **316** (1993), no. 8, 819–821.

[37] ———, *Jacobienne de certaines courbes de genre 2: torsion et simplicité*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 283–306, Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[38] ———, *Sur une conjecture sur les points de torsion rationnelles des jacobienennes de courbes*, J. Reine Angew. Math. **473** (1996), 59–68.

[39] ———, *Sur certains sous-groupes de torsion de jacobienennes de courbes hyperelliptiques de genre g ≥ 1*, Manuscripta Math. **92** (1997), no. 1, 47–63.
[40] A. Levin, *Ideal class groups, Hilbert's irreducibility theorem, and integral points of bounded degree on curves*, J. Théor. Nombres Bordeaux 19 (2007), no. 2, 485–499.

[41] F. Luca, *A note on the divisibility of class numbers of real quadratic fields*, C. R. Math. Acad. Sci. Soc. R. Can. 25 (2003), no. 3, 71–75.

[42] J.-F. Mestre, *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, Seminar on Number Theory, 1979–1980 (French), Univ. Bordeaux I, Talence, 1980, pp. Exp. No. 15, 18.

[43] , *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, J. Reine Angew. Math. 343 (1983), 23–35.

[44] , *Groupes de classes d'ideaux non cycliques de corps de nombres*, Seminar on number theory, Paris 1981–82 (Paris, 1981/1982), Progr. Math., vol. 38, Birkhäuser Boston, Boston, MA, 1983, pp. 189–200.

[45] , *Corps quadratiques dont le 5-rang du groupe des classes est ≥ 3*, C. R. Acad. Sci. Paris Sér. I Math. 315 (1992), no. 4, 371–374.

[46] R. Murty, *Exponents of class groups of quadratic fields*, Topics in number theory (University Park, PA, 1997), Math. Appl., vol. 467, Kluwer Acad. Publ., Dordrecht, 1999, pp. 229–239.

[47] T. Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg 1 (1922), 140–150.

[48] , *Collected papers of Trygve Nagell. Vol. 1*, Queen's Papers in Pure and Applied Mathematics, vol. 121, Queen's University, Kingston, ON, 2002.

[49] S. Nakano, *On ideal class groups of algebraic number fields*, Proc. Japan Acad. Ser. A Math. Sci. 60 (1984), no. 2, 74–77.

[50] , *On ideal class groups of algebraic number fields*, J. Reine Angew. Math. 358 (1985), 61–75.

[51] , *Construction of pure cubic fields with large 2-class groups*, Osaka J. Math. 25 (1988), no. 1, 161–170.

[52] H. Ogawa, *Curves of genus 2 with a rational torsion divisor of order 23*, Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), no. 9, 295–298.

[53] P. Roquette and H. Zassenhaus, *A class of rank estimate for algebraic number fields*, J. London Math. Soc. 44 (1969), 31–38.

[54] A. Schinzel, *On Hilbert's irreducibility theorem*, Ann. Polon. Math. 16 (1965), 333–340.
[55] B. Schmithals, Eine Verallgemeinerung der Klassenrangabschätzung für Zahlkörper von Roquette und Zassenhaus, Arch. Math. (Basel) 34 (1980), no. 5, 412–415.

[56] J.-P. Serre, Lectures on the Mordell-Weil theorem, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997.

[57] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, J. London Math. Soc. (2) 61 (2000), no. 3, 681–690.

[58] K. Uchida, Class numbers of cubic cyclic fields, J. Math. Soc. Japan 26 (1974), no. 3, 447–453.

[59] P. J. Weinberger, Real quadratic fields with class numbers divisible by n, J. Number Theory 5 (1973), no. 3, 237–241.

[60] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Osaka J. Math. 7 (1970), 57–76.

[61] G. Yu, A note on the divisibility of class numbers of real quadratic fields, J. Number Theory 97 (2002), no. 1, 35–44.