# Quadratic fields with a class group of large 3-rank

Aaron Levin
Department of Mathematics
Michigan State University
East Lansing, MI 48824, USA
E-mail: adlevin@math.msu.edu

Yan Shengkuan
School of Mathematics and Statistics
Xi'an Jiaotong University
Xi'an, 710049, China
E-mail: sjwijd@stu.xjtu.edu.cn

Luke Wiljanen
Department of Mathematics
Michigan State University
East Lansing, MI 48824, USA
E-mail: wiljane8@msu.edu

## Abstract

We prove that there are $\gg X^{\frac{1}{30}}/\log X$ imaginary quadratic number fields with an ideal class group of 3-rank at least 5 and discriminant bounded in absolute value by $X$. This improves on an earlier result of Craig, who proved the infinitude of imaginary quadratic fields with an ideal class group of 3-rank at least 4. The proofs rely on constructions of Mestre for $j$-invariant 0 elliptic curves of large Mordell-Weil rank, and a method of the first author and Gillibert for constructing torsion in ideal class groups of number fields from rational torsion in Jacobians of curves. We also consider analogous questions concerning rational 3-torsion in hyperelliptic Jacobians.

# 1   Introduction

We study the problem of constructing and counting quadratic number fields with large 3-rank (i.e., with an ideal class group of large 3-rank). Our main result is the following:

**Theorem 1.1.** *There exist* $\gg X^{\frac{1}{30}}/\log X$ *imaginary (resp. real) quadratic number fields $k$ with $|\operatorname{Disc}(k)| < X$ and*

$$\operatorname{rk}_3 \operatorname{Cl}(k) \geq 5$$
$$(resp.\ \operatorname{rk}_3 \operatorname{Cl}(k) \geq 4).$$

In particular, we produce infinitely many imaginary quadratic fields with a class group of 3-rank at least $r = 5$, improving on the best previous result, due to Craig [10], who in 1977 proved the same statement but with $r = 4$. In the real quadratic case, we obtain a quantitative version of a result of Diaz y Diaz [13], who combined Craig's work with Scholz's reflection principle [30] to prove an analogous result giving the infinitude of real quadratic fields with 3-rank at least 4. For smaller 3-ranks, our method also produces new enumerative results (see Corollary 6.2 and the subsequent discussion).

Further families of quadratic fields with a given lower bound for the 3-rank have been investigated previously by a number of authors (e.g., [9], [12], [22]). Examples of imaginary quadratic fields with 3-rank 6 were given by Quer [28], and tables of quadratic fields with large 3-rank have been previously computed [2, 12, 14, 24]. In particular, the smallest imaginary quadratic field with an ideal class group of 3-rank 5 (discovered by Quer) is known from work of Belabas [2].

Our approach to Theorem 1.1 is based on the well-known idea of using $j$-invariant 0 elliptic curves over $\mathbb{Q}$ of large Mordell-Weil rank to construct quadratic fields with large 3-rank. There is an extensive literature detailing (and exploiting) the connection between the 3-rank of the Selmer group attached to 3-isogenies between such curves and the 3-ranks of associated quadratic fields (e.g., [1, 7, 8, 11, 28, 29, 33]). We use a geometric manifestation of this concept, combined with a method of the first author and Gillibert [17], and take advantage of the following chain of constructions, previously exploited in [18]:

(1.1)

Elliptic curve $E$ of large rank over $\mathbb{Q}(t)$ $\xrightarrow{\ p\text{-descent}\ }$ $p$-torsion in associated Picard group

$\xrightarrow[\ \ \ \ \ \ \ \ \ \ \ ]{\ \ G\text{illibert-Levin}\ \ }$ $p$-torsion in ideal class groups.

Using the multiplication-by-$p$ map on $E$, this diagram was used in [18] to produce number fields of degree $p^2 - 1$ having an ideal class group with a large $p$-torsion subgroup. In particular, taking $p = 2$, in [18] it was proven that there are infinitely many cubic number fields whose ideal class group contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{11}$ (see also earlier work of Kulkarni [23]).

We apply these ideas to $j$-invariant 0 elliptic curves over $\mathbb{Q}(t)$ of the form

$$E : y^2 = x^3 + f(t),$$
$$E' : y^2 = x^3 - 27f(t),$$

and use the 3-isogeny over $\mathbb{Q}(t)$ given by

(1.2) $$\lambda : E' \to E$$
$$(x, y) \mapsto \left( \frac{x^3 - 108f(t)}{9x^2}, \frac{(x^3 + 216f(t))y}{27x^3} \right).$$

When $f$ is a nonconstant square-free polynomial of degree $d$, $d \not\equiv 2, 4$ (mod 6), a descent argument yields a homomorphism

(1.3) $$E(\mathbb{Q}(t))/\lambda E'(\mathbb{Q}(t)) \hookrightarrow \mathrm{Jac}(C)[3](\mathbb{Q}),$$

where $\mathrm{Jac}(C)[3](\mathbb{Q})$ is the rational 3-torsion subgroup in the Jacobian of the hyperelliptic curve over $\mathbb{Q}$ given by the affine equation

$$C : y^2 = f(t).$$

Explicitly, the homomorphism (1.3) is induced by the map

$$E(\mathbb{Q}(t)) \to \mathrm{Jac}(C)[3](\mathbb{Q}),$$
(1.4) $$(x_0(t), y_0(t)) \mapsto \frac{1}{3} \mathrm{div}(y - y_0(t)),$$

where $\mathrm{div}(y - y_0(t))$ denotes the principal divisor on $C$ associated to the rational function $y - y_0(t)$. In general, when $f$ is not square-free or $d \equiv 2, 4$ (mod 6), one obtains similar homomorphisms to a suitably generalized Picard group (see [16] and [18]). Thus, we have described the first part of (1.1) in the present context.

Next we use the idea, going back to [17], that rational $p$-torsion in the Jacobian of a hyperelliptic curve gives rise to $p$-torsion in ideal class groups of quadratic number fields. The following quantitative version of this idea was proven in [17], explaining the application of the second map in (1.1):

**Theorem 1.2.** *Let $C$ be a smooth projective hyperelliptic curve over $\mathbb{Q}$ with a rational Weierstrass point, and let $m > 1$ be an integer. Let $g$ denote the genus of $C$. Then there exist $\gg X^{\frac{1}{2g+1}}/\log X$ imaginary (resp. real) quadratic number fields $k$ with $|\operatorname{Disc}(k)| < X$ and*

$$\operatorname{rk}_m \operatorname{Cl}(k) \geq \operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\mathrm{tors}}$$
$$(\text{resp. } \operatorname{rk}_m \operatorname{Cl}(k) \geq \operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\mathrm{tors}} - 1).$$

Combining the above ideas gives a method for using $j$-invariant 0 elliptic curves of large $\mathbb{Q}(t)$-rank to produce infinitely many quadratic fields with an ideal class group of large 3-rank.

We now discuss our practical implementation of the above ideas to obtain infinitely many imaginary quadratic fields with a class group of 3-rank at least 5. To begin, we use a method of Mestre [26] (see also [32, §11]) to construct a nontrivial $j$-invariant 0 elliptic curve $E$ over $\mathbb{Q}(t)$ with 6 explicitly given points $P_1, \ldots, P_6 \in E(\mathbb{Q}(t))$ which are independent in the Mordell-Weil group. The elliptic curve $E$ satisfies the hypotheses giving rise to (1.3) ($f$ is squarefree and $6 | \deg f$ in our case), and thus we can use the explicit map (1.4) to compute the image of $P_1, \ldots, P_6$ in $\operatorname{Jac}(C)[3](\mathbb{Q})$. Using Magma[1][4], we verify that $P_1, \ldots, P_6$ yield divisor classes $[D_1], \ldots, [D_6]$ in $\operatorname{Jac}(C)(\mathbb{Q})$ which generate a subgroup isomorphic to $(\mathbb{Z}/3\mathbb{Z})^5$.[2] Since this computation in $\operatorname{Jac}(C)$ is direct and independent of the above theoretical considerations (except for knowledge of the map (1.4)), we do not discuss or develop the material behind the homomorphism (1.3) further.

Thus, we obtain a hyperelliptic curve $C$ over $\mathbb{Q}$ with $\operatorname{rk}_3 \operatorname{Jac}(C)(\mathbb{Q})_{\mathrm{tors}} \geq 5$. Unfortunately, the curve $C$ obtained does not posses a rational Weierstrass point, and we cannot apply Theorem 1.2. Instead, we use a result inspired by the method developed in [18] (precisely to avoid this difficulty), which relied on finding elliptic curves $E$ over $\mathbb{Q}(t)$ that do not have "universal bad reduction" (see [18]) at any rational prime $p$. In this direction, our primary tool for proving Theorem 1.1 is the following result.

**Theorem 1.3.** *Let $f \in \mathbb{Q}[t]$ be a squarefree nonconstant polynomial of degree $d$ with $6|d$. Let $E$ be the elliptic curve over $\mathbb{Q}(t)$ defined by*

$$E : Y^2 = X^3 + f(t).$$

---

[1]Magma programs verifying the claimed calculations are available at http://users.math.msu.edu/users/adlevin/Magma.html.

[2]This is perhaps a bit surprising; naïvely, one might expect roughly half the points to remain independent in $E(\mathbb{Q}(t))/\lambda E'(\mathbb{Q}(t))$ over $\mathbb{Z}/3\mathbb{Z}$, and we have no theoretical explanation for this advantageous situation.

Let $C$ be the (smooth projective) hyperelliptic curve over $\mathbb{Q}$ defined by $y^2 = f(t)$. Let

$$r = \mathrm{rk}_3\, E(\mathbb{Q}(t))/\lambda E'(\mathbb{Q}(t)) = \mathrm{rk}_3 \operatorname{im}(E(\mathbb{Q}(t)) \to \mathrm{Jac}(C)[3](\mathbb{Q}))$$

be the 3-rank of the image of the map (1.4). In addition, suppose that

1. For every odd prime $p$, there exists $t_p \in \mathbb{Q}$ such that

$$3|\operatorname{ord}_p f(t_p).$$

2. There exists $t_2 \in \mathbb{Q}$ such that $\mathbb{Q}(\sqrt{f(t_2)})$ is a quadratic extension of $\mathbb{Q}$ and the prime 2 does not split in this extension.

Then there exist $\gg X^{\frac{1}{d}}/\log X$ imaginary (resp. real) quadratic number fields $k$ with $|\operatorname{Disc}(k)| < X$ and

$$\mathrm{rk}_3 \operatorname{Cl}(k) \geq r - \delta,$$
$$(\text{resp. } \mathrm{rk}_3 \operatorname{Cl}(k) \geq r - 1),$$

where $\delta = 0$ if $f$ takes negative values on $\mathbb{R}$ and $\delta = 1$ otherwise.

An outline of the paper is as follows. After recalling some basic notation and definitions, in Section 2 we give (a slight variation on) the method of the first author and Gillibert [17] for constructing and counting number fields with an ideal class group of large $p$-rank. Next, we give two results describing how specializations of $\mathbb{Q}(t)$-points on $j$-invariant 0 elliptic curves produce ideals which are almost perfect cubes. In Section 4 we prove Theorem 1.3, which will be combined with constructions of Mestre (Section 5, and Section 6 in the guise of 3-torsion in hyperelliptic Jacobians) to finish the proof of the main theorem (Theorem 1.1) in the final section.

Where possible, we have preferred to give reasonably elementary and self-contained proofs, both to increase the accessibility of the results, and to maintain the spirit of the origins of the work as an undergraduate research project.

## 2  Hilbert's Irreducibility Theorem, torsion subgroups of Jacobians, and ideal class groups

We first fix some notation. Throughout, we let $k$ be a number field and we let $\operatorname{Disc}(k)$ be the (absolute) discriminant of $k$. Let $S$ be a finite set of

places of $k$ containing the archimedean places. We let $S_{\text{fin}}$ denote the subset of finite (nonarchimedean) places in $S$. We let $\mathcal{O}_{k,S}$ denote the ring of $S$-integers of $k$ and let $\mathcal{O}_{k,S}^*$ be the group of $S$-units. If $L$ is a finite extension of $k$, we let $S_L$ be the set of places of $L$ lying above places of $S$, and we use $\mathcal{O}_{L,S}$ or $\mathcal{O}_{L,S_L}$ to denote the ring of $S_L$-integers in $L$. For a place $v$ of $k$ we let $|\cdot|_v$ denote a corresponding absolute value (the specific choice will not be important). For a prime $\mathfrak{p}$ of $\mathcal{O}_k$ we let $\mathrm{ord}_{\mathfrak{p}}$ denote the associated discrete valuation. We let $\mathrm{Cl}(k)$ and $\mathrm{Cl}(\mathcal{O}_{k,S})$ denote the ideal class group of $\mathcal{O}_k$ and $\mathcal{O}_{k,S}$, respectively. For an abelian group $A$ we let $\mathrm{rk}\, A$ denote the free rank of $A$, and if $p$ is a prime and $A$ is finite, we let $\mathrm{rk}_p\, A$ be the dimension of $A/pA$ over $\mathbb{Z}/p\mathbb{Z}$. We let $H(\alpha)$ denote the absolute multiplicative height of an algebraic number $\alpha$. If $\alpha = p/q \in \mathbb{Q}$ is written in reduced form, then $H(p/q) = \max\{\log|p|, \log|q|\}$.

We will use the following version of Hilbert's Irreducibility Theorem, combined with an enumerative result of Dvornicich and Zannier [15], in a form proved by Bilu and Gillibert [3, Th. 3.1].

**Theorem 2.1** (Bilu-Gillibert). *Let $k$ be a number field of degree $\ell$ over $\mathbb{Q}$. Let $C$ be a curve over $k$ and $\phi : C \to \mathbb{P}^1$ a morphism (over $k$) of degree $d$. Let $S$ be a finite set of places of $k$, $\epsilon > 0$, and $\mho$ a thin subset of $k$ [3, §3.1]. Consider the points $P \in C(\bar{k})$ satisfying*

$$\phi(P) \in k \smallsetminus \mho,$$
$$|\phi(P)|_v < \epsilon, \qquad \forall v \in S,$$
$$H(\phi(P)) \leq B.$$

*Then among the number fields $k(P)$, where $P$ satisfies the conditions above, there are $\gg B^{\ell}/\log B$ distinct fields of degree $d$ over $k$.*

Our main tool for constructing and enumerating fields with large ideal class groups is the following result based on [17]. We give a self-contained proof for the convenience of the reader.

**Theorem 2.2.** *Let $C$ be a nonsingular projective curve over $\mathbb{Q}$. Let $\phi \in \mathbb{Q}(C)$ be a nonconstant rational function on $C$ with $\deg \phi = d > 1$ and let $p$ be a prime number. Let $\psi_1, \ldots, \psi_r \in \mathbb{Q}(C)$ be nonconstant rational functions on $C$ whose images in $\overline{\mathbb{Q}}(C)^*/(\overline{\mathbb{Q}}(C)^*)^p$ generate a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^r$. Let $S_0$ and $S$ be finite sets of places of $\mathbb{Q}$ and assume that $S$ contains the archimedean place. Suppose that there exists $\epsilon > 0$ and rational*

*numbers $a_v \in \mathbb{Q}$, $v \in S_0$, such that for all points $P \in C(\overline{\mathbb{Q}})$ satisfying*

(2.1)                                       $\phi(P) \in \mathbb{Q},$

(2.2)                               $|\phi(P) - a_v|_v < \epsilon, \quad \forall v \in S_0,$

*we have the equality of fractional $\mathcal{O}_{\mathbb{Q}(P),S}$-ideals*

$$\psi_j(P)\mathcal{O}_{\mathbb{Q}(P),S} = \mathfrak{a}_{P,j}^p,$$

*for some fractional $\mathcal{O}_{\mathbb{Q}(P),S}$-ideal $\mathfrak{a}_{P,j}$, j=1,..., r. Consider the set $T_B$ of points $P \in C(\overline{\mathbb{Q}})$ satisfying* (2.1), (2.2), *and*

$$H(\phi(P)) \leq B.$$

*Then there are $\gg B/\log B$ distinct number fields $\mathbb{Q}(P)$, $P \in T_B$, satisfying*

$$[\mathbb{Q}(P) : \mathbb{Q}] = d,$$
$$\mathrm{rk}_p \, \mathrm{Cl}(\mathbb{Q}(P)) \geq r + \#S_{\mathrm{fin}} - \mathrm{rk}\, \mathcal{O}_{\mathbb{Q}(P),S}^*.$$

*Proof.* Let $T \subset C(\overline{\mathbb{Q}})$ consist of the set of points $P \in C(\overline{\mathbb{Q}})$ satisfying (2.1) and (2.2). By Kummer theory, the assumptions on $\psi_1, \ldots, \psi_r$ imply the equality

$$[\overline{\mathbb{Q}}(C)\left(\sqrt[p]{\psi_1}, \ldots, \sqrt[p]{\psi_r}\right) : \overline{\mathbb{Q}}(C)] = p^r.$$

Then to the field extension $\mathbb{Q}(C)\left(\sqrt[p]{\psi_1}, \ldots, \sqrt[p]{\psi_r}\right)$ of $\mathbb{Q}(C)$, we can associate a (unique up to isomorphism) nonsingular projective curve $\tilde{C}$ over $\mathbb{Q}$ and a morphism $\pi : \tilde{C} \to C$ with $\deg \pi = p^r$. Let $\tilde{T} = \pi^{-1}(T) \subset \tilde{C}(\overline{\mathbb{Q}})$ and $\tilde{T}_B = \pi^{-1}(T_B)$. Let

$$L = \mathbb{Q}(\zeta_{pN})(\sqrt[p]{q} \mid q \in S_{\mathrm{fin}}) = \mathbb{Q}(\zeta_{pN})(\sqrt[p]{u} \mid u \in \mathcal{O}_{\mathbb{Q},S}^*),$$

where $\zeta_{pN}$ is a primitive $pN$th root of unity and $N = \mathrm{lcm}\{n \in \mathbb{N} \mid \phi(n) \leq d\}$ (so that $L$ contains a $p$th root of every root of unity in every number field of degree $\leq d$). Let $Q \in \tilde{T}$, $P = \pi(Q)$, and $k = \mathbb{Q}(P)$. Assume additionally that $P$ isn't a pole of any $\psi_i$, $i = 1, \ldots, r$.

**Lemma 2.3.** *If $L$ and $\mathbb{Q}(Q)$ are linearly disjoint, then*

$$[\mathbb{Q}(Q) : \mathbb{Q}] \leq dp^{\mathrm{rk}_p \, \mathrm{Cl}(k) + \mathrm{rk}\, \mathcal{O}_{k,S}^* - \#S_{\mathrm{fin}}}.$$

*Proof.* Since $L$ and $\mathbb{Q}(Q)$ are linearly disjoint, $[\mathbb{Q}(Q) : \mathbb{Q}] = [L(Q) : L]$, and it suffices to compute a bound for the latter degree. Since $\deg \phi = d$, we have $[L(P) : L] \leq d$ and it suffices to show that

$$[L(Q) : L(P)] \leq p^{\mathrm{rk}_p \, \mathrm{Cl}(k) + \mathrm{rk}\, \mathcal{O}_{k,S}^* - \#S_{\mathrm{fin}}}.$$

From the construction of $\pi$,

$$(2.3) \qquad L(Q) = L(P)\left(\sqrt[p]{\psi_1(P)}, \ldots, \sqrt[p]{\psi_r(P)}\right).$$

Let $t = \operatorname{rk}_p \operatorname{Cl}(\mathcal{O}_{k,S}) \leq \operatorname{rk}_p \operatorname{Cl}(k)$ and let $\mathfrak{b}_1, \ldots, \mathfrak{b}_t$ be $\mathcal{O}_{k,S}$-ideals whose ideal classes generate the $p$-torsion subgroup of $\operatorname{Cl}(\mathcal{O}_{k,S})$. Then $\mathfrak{b}_i^p = \beta_i \mathcal{O}_{k,S}$ for some $\beta_i \in k$, $i = 1, \ldots, t$. Since $[k : \mathbb{Q}] \leq d$ and $k$ and $L$ are linearly disjoint, the only roots of unity in $k$ are $\pm 1$. Let $t' = \operatorname{rk} \mathcal{O}_{k,S}^*$ and let $u_1, \ldots, u_{t'}$, and $-1$ be generators for $\mathcal{O}_{k,S}^*$. Let

$$M = k\left(\sqrt[p]{\beta_1}, \ldots, \sqrt[p]{\beta_t}, \sqrt[p]{u_1}, \ldots, \sqrt[p]{u_{t'}}, \zeta_{2p}\right),$$
$$M' = k\left(\sqrt[p]{\beta_1}, \ldots, \sqrt[p]{\beta_t}, \sqrt[p]{u_1}, \ldots, \sqrt[p]{u_{t'}}\right),$$

for some choice of the $p$th roots (which we now fix). For every $q \in S_{\mathrm{fin}}$, $q \in \mathcal{O}_{k,S}^*$, and so for some choice of $n_q \in \{0, 1\}$, $(-1)^{n_q} q$ is in the multiplicative group generated by $u_1, \ldots, u_{t'}$. It follows that for some choice of the $p$th roots, $k(\sqrt[p]{(-1)^{n_q}q} \mid q \in S_{\mathrm{fin}}) \subset L(P) \cap M'$ and since $k$ and $L$ are linearly disjoint,

$$[L(P) \cap M' : k] \geq [k(\sqrt[p]{(-1)^{n_q}q} \mid q \in S_{\mathrm{fin}}) : k] = [\mathbb{Q}(\sqrt[p]{(-1)^{n_q}q} \mid q \in S_{\mathrm{fin}}) : \mathbb{Q}] = p^{\#S_{\mathrm{fin}}}.$$

Therefore,

$$[L(P)M : L(P)] = [L(P)M' : L(P)] \leq [M' : L(P) \cap M'] = \frac{[M' : k]}{[L(P) \cap M' : k]}$$
$$\leq p^{t+t'-\#S_{\mathrm{fin}}} \leq p^{\operatorname{rk}_p \operatorname{Cl}(k) + \operatorname{rk} \mathcal{O}_{k,S}^* - \#S_{\mathrm{fin}}}.$$

Then from (2.3) it suffices to show that

$$\sqrt[p]{\psi_i(P)} \in M, \quad i = 1, \ldots, r.$$

By hypothesis,

$$\psi_i(P)\mathcal{O}_{k,S} = \mathfrak{a}_i^p$$

for some fractional $\mathcal{O}_{k,S}$-ideal $\mathfrak{a}_i$, $i = 1, \ldots, r$. Since $\mathfrak{a}_i^p$ is principal, by definition of the $\mathfrak{b}_j$ we can write

$$\mathfrak{a}_i = (\alpha) \prod_{j=1}^t \mathfrak{b}_j^{b_j}$$

for some integers $b_j$ and some element $\alpha \in k$. Therefore, raising both sides to the $p$th power, we find that

$$\psi_i(P)\mathcal{O}_{k,S} = \left(\alpha^p \prod_{j=1}^t \beta_j^{b_j}\right)\mathcal{O}_{k,S},$$

and

$$\psi_i(P) = u\alpha^p \prod_{j=1}^{t} \beta_j^{b_j}$$

for some unit $u \in \mathcal{O}_{k,S}^*$. Since $u = (-1)^{c_0} \prod_{j=1}^{t'} u_j^{c_j}$ for some integers $c_j$, we find that $\sqrt[p]{\psi_i(P)} \in M$, $i = 1, \ldots, r$, as desired. $\square$

Let $\psi = \phi \circ \pi : \tilde{C} \to \mathbb{P}^1$ and let $\mho = \mho_1 \cup \mho_2$, where

$\mho_1 = \{\psi(Q) \mid Q \in \tilde{C}(\overline{\mathbb{Q}}), \psi(Q) \in \mathbb{Q}, [\mathbb{Q}(Q) : \mathbb{Q}] < \deg \psi\}$,

$\mho_2 = \{\psi(Q) \mid Q \in \tilde{C}(\overline{\mathbb{Q}}), \psi(Q) \in \mathbb{Q}, \mathbb{Q}(Q) \text{ is not linearly disjoint from } L\}$.

As in [3, p. 947], $\mho$ is a thin subset of $\mathbb{Q}$. Let $a \in \mathbb{Q}$ be such that

(2.4) $$|a - a_v|_v < \frac{\epsilon}{2}, \quad \forall v \in S_0.$$

Let $\phi' = \phi - a$. Then $\phi(P) \in \mathbb{Q}$ if and only if $\phi'(P) \in \mathbb{Q}$, and in this case, for $v \in S_0$, $|\phi'(P)|_v < \frac{\epsilon}{2}$ implies that $|\phi(P) - a_v|_v < \epsilon$. We now apply Theorem 2.1 to $\phi'$, $k = \mathbb{Q}$, $\mho$, and $\frac{\epsilon}{2}$. Since $\phi$ and $\phi'$ differ by an automorphism of $\mathbb{P}^1$, $H(\phi(P))$ and $H(\phi'(P))$ differ by a bounded function. It follows from the above that there exist $\gg B/\log B$ distinct number fields $\mathbb{Q}(P)$, where $P \in T_B$, such that if $Q \in \tilde{T}_B$, $\pi(Q) = P$, then

$$[L(Q) : L] = [\mathbb{Q}(Q) : \mathbb{Q}] = \deg \psi = (\deg \pi)(\deg \phi) = dp^r.$$

On the other hand, by Lemma 2.3, for such points

$$[\mathbb{Q}(Q) : \mathbb{Q}] \le dp^{\text{rk}_p \, \text{Cl}(\mathbb{Q}(P)) + \text{rk} \, \mathcal{O}_{\mathbb{Q}(P),S}^* - \#S_{\text{fin}}}.$$

Combining these two statements yields the desired result.

$\square$

# 3 Points on $j$-invariant $0$ elliptic curves over $\mathbb{Q}(t)$ and cubes of ideals

In this section, we consider an elliptic curve $E$ over $k(t)$ defined by an equation of the form

$$Y^2 = X^3 + f(t).$$

Under certain conditions on $f$, we first show that if $(X_0(t), Y_0(t)) \in E(k(t))$ is a rational point on $E$, then for all values of $t \in k$, the algebraic number

$\sqrt{f(t)} - Y_0(t)$ is almost a perfect cube in $k(\sqrt{f(t)})$. This is immediate from Weil's "theorem of decomposition" [3, 2.7.15], as from preceding discussions the principal divisor associated to $\sqrt{f(t)} - Y_0(t)$ (viewed as a function on the appropriate hyperelliptic curve) is divisible by 3 in the group of divisors. We give an elementary proof, which also has the advantage of explicitly bounding the deviation from being a cube (i.e., the set $S$ in Theorem 3.1 below is explicitly constructed in the proof; alternatively, and in a more general setting, admissible choices of $S$ are studied in [17, Section 2.4] and related to the primes of bad reduction of the related hyperelliptic curve $y^2 = f(t)$).

**Theorem 3.1.** *Let $k$ be a number field. Let $f \in k[t]$ be a nonconstant squarefree polynomial such that either $\deg f$ is odd or $6 \mid \deg f$. Let $E$ be the elliptic curve over $k(t)$ defined by*

$$E : Y^2 = X^3 + f(t).$$

*Let $(X_0(t), Y_0(t)) \in E(k(t))$. For each $t \in k$, let $y_t = \sqrt{f(t)}$, for some choice of the square root. Then there exists a finite set of places $S$ of $k$, containing the archimedean places, such that for all $t \in k$, we have an equality of fractional $\mathcal{O}_{k(y_t),S}$-ideals*

$$(y_t - Y_0(t))\mathcal{O}_{k(y_t),S} = \mathfrak{a}_t^3,$$

*for some fractional $\mathcal{O}_{k(y_t),S}$-ideal $\mathfrak{a}_t$.*

*Proof.* We may write

$$X_0(t) = \frac{a(t)}{d(t)^2}, \quad Y_0(t) = \frac{b(t)}{d(t)^3},$$

for some polynomials $a(t), b(t), d(t) \in k[t]$ such that $a(t)b(t)$ and $d(t)$ are coprime polynomials. Since $f(t)$ is squarefree, it is also clear that $a(t)$, $b(t)$, and $f(t)$ are pairwise coprime. Thus, there exist polynomials $g(t), h(t) \in k[t]$ such that

(3.1)                    $a(t)g(t) + f(t)h(t) = 1.$

Let $S$ be a finite set of places of $k$ containing the archimedean places such that $a, b, d, f, g, h \in \mathcal{O}_{k,S}[t]$, $2 \in \mathcal{O}_{k,S}^*$, and the leading coefficients of $a, b, d$, and $f$ are $S$-units.

Let $t \in k$ and let $\mathfrak{p}$ be a prime of $\mathcal{O}_{k(y_t)}$ not lying above a prime of $S$. Then we need to show that $3 \mid \operatorname{ord}_{\mathfrak{p}}(y_t - Y_0(t))$. Since $3 \mid \operatorname{ord}_{\mathfrak{p}}(X_0(t)^3)$ and

$$-X_0(t)^3 = f(t) - Y_0(t)^2 = (y_t - Y_0(t))(y_t + Y_0(t)),$$

we find that

$$3|\operatorname{ord}_{\mathfrak{p}}((y_t - Y_0(t))(y_t + Y_0(t)) = \operatorname{ord}_{\mathfrak{p}}(y_t - Y_0(t)) + \operatorname{ord}_{\mathfrak{p}}(y_t + Y_0(t)).$$

From this equality, it clearly suffices to prove that

$$3|\min\{\operatorname{ord}_{\mathfrak{p}}(y_t - Y_0(t)), \operatorname{ord}_{\mathfrak{p}}(y_t + Y_0(t))\}.$$

By hypothesis, $2 \in \mathcal{O}_{k,S}^*$ and so $\operatorname{ord}_{\mathfrak{p}}(2) = 0$. Then it is elementary that

$$\min\{\operatorname{ord}_{\mathfrak{p}}(y_t - Y_0(t)), \operatorname{ord}_{\mathfrak{p}}(y_t + Y_0(t))\} = \min\{\operatorname{ord}_{\mathfrak{p}} y_t, \operatorname{ord}_{\mathfrak{p}} Y_0(t)\}.$$

Moreover,

$$\begin{aligned}
\min\{\operatorname{ord}_{\mathfrak{p}} y_t, \operatorname{ord}_{\mathfrak{p}} Y_0(t)\} &= \frac{1}{2}\min\{\operatorname{ord}_{\mathfrak{p}} y_t^2, \operatorname{ord}_{\mathfrak{p}} Y_0(t)^2\} \\
&= \frac{1}{2}\min\{\operatorname{ord}_{\mathfrak{p}} f(t), \operatorname{ord}_{\mathfrak{p}}(X_0(t)^3 + f(t))\} \\
&= \frac{1}{2}\min\{\operatorname{ord}_{\mathfrak{p}} f(t), \operatorname{ord}_{\mathfrak{p}} X_0(t)^3\} \\
&= \frac{1}{2}\min\{\operatorname{ord}_{\mathfrak{p}} f(t), 3\operatorname{ord}_{\mathfrak{p}} X_0(t)\}.
\end{aligned}$$

Hence it suffices to prove that

$$(3.2) \qquad\qquad 3|\min\{\operatorname{ord}_{\mathfrak{p}} f(t), 3\operatorname{ord}_{\mathfrak{p}} X_0(t)\}.$$

This clearly holds when $\operatorname{ord}_{\mathfrak{p}} f(t) \geq 3\operatorname{ord}_{\mathfrak{p}} X_0(t)$, and so we now assume that

$$(3.3) \qquad\qquad \operatorname{ord}_{\mathfrak{p}} f(t) < 3\operatorname{ord}_{\mathfrak{p}} X_0(t).$$

We consider three cases depending on $\operatorname{ord}_{\mathfrak{p}} t$ and $\deg f$.

**Case 1**: $\operatorname{ord}_{\mathfrak{p}} t \geq 0$.

Since $a, d, f, g, h \in \mathcal{O}_{k,S}[t]$, the quantities $\operatorname{ord}_{\mathfrak{p}} a(t)$, $\operatorname{ord}_{\mathfrak{p}} d(t)$, $\operatorname{ord}_{\mathfrak{p}} f(t)$, $\operatorname{ord}_{\mathfrak{p}} g(t)$, $\operatorname{ord}_{\mathfrak{p}} h(t)$ are all nonnegative. It follows from (3.3) that

$$\operatorname{ord}_{\mathfrak{p}} X_0(t) > 0,$$

and as $X_0(t) = \frac{a(t)}{d(t)^2}$, we also have

$$\operatorname{ord}_{\mathfrak{p}} a(t) = \operatorname{ord}_{\mathfrak{p}} X_0(t) + 2\operatorname{ord}_{\mathfrak{p}} d(t) \geq \operatorname{ord}_{\mathfrak{p}} X_0(t) > 0.$$

Since

$$\operatorname{ord}_{\mathfrak{p}}(a(t)g(t) + f(t)h(t)) = \operatorname{ord}_{\mathfrak{p}} 1 = 0,$$

we must have $\operatorname{ord}_{\mathfrak{p}} f(t) = 0$, proving (3.2).

**Case 2**: $\operatorname{ord}_{\mathfrak{p}} t < 0$ and $3 | \deg f$.

Since $f \in \mathcal{O}_{k,S}[t]$ and the leading coefficient of $f$ is an $S$-unit, $\operatorname{ord}_{\mathfrak{p}} t < 0$ implies that

$$\operatorname{ord}_{\mathfrak{p}} f(t) = (\deg f) \operatorname{ord}_{\mathfrak{p}} t.$$

By hypothesis $3 | \deg f$ and so $3 | \operatorname{ord}_{\mathfrak{p}} f(t)$ as desired.

**Case 3**: $\operatorname{ord}_{\mathfrak{p}} t < 0$ and $2, 3 \nmid \deg f$.

The divisibility assumptions on $\deg f$ imply that $\deg f d^6 \neq \deg b^2$ and $\deg f d^6 \neq \deg a^3$. Since $b^2 = a^3 + f d^6$, it follows that

$$\deg a^3 = \deg b^2 > \deg f d^6.$$

Hence

$$3 \deg a = 2 \deg b > \deg f + 6 \deg d.$$

Since $a, d, f \in \mathcal{O}_{k,S}[t]$, the leading coefficients of $a, d, f$ are $S$-units, and $\operatorname{ord}_{\mathfrak{p}} t < 0$, we have the identities

$$\operatorname{ord}_{\mathfrak{p}} a(t) = (\deg a) \operatorname{ord}_{\mathfrak{p}} t,$$
$$\operatorname{ord}_{\mathfrak{p}} d(t) = (\deg d) \operatorname{ord}_{\mathfrak{p}} t,$$
$$\operatorname{ord}_{\mathfrak{p}} f(t) = (\deg f) \operatorname{ord}_{\mathfrak{p}} t.$$

Hence,

$$3 \operatorname{ord}_{\mathfrak{p}} X_0(t) = (3 \deg a - 6 \deg d) \operatorname{ord}_{\mathfrak{p}} t < (\deg f) \operatorname{ord}_{\mathfrak{p}} t = \operatorname{ord}_{\mathfrak{p}} f(t),$$

contradicting (3.3).

Thus, in all cases we have proven (3.2). □

The next result gives a way to handle the odd primes in $S$ in Theorem 3.1. The hypothesis (3.4) below is closely related to the condition from [18] that $E$ doesn't have "universal bad reduction" at $\mathfrak{p}$ (if $\mathfrak{p}$ doesn't lie above 2 or 3, then in our case $E$ doesn't have universal bad reduction at $\mathfrak{p}$ if and only if there exists $t_{\mathfrak{p}} \in k$ such that $6 | \operatorname{ord}_{\mathfrak{p}} f(t_{\mathfrak{p}}))$.

**Theorem 3.2.** *Let $k$ be a number field. Let $f \in k[t]$ be a nonconstant polynomial. Let $E$ be the elliptic curve over $k(t)$ defined by*

$$E : Y^2 = X^3 + f(t).$$

*Let $(X_0(t), Y_0(t)) \in E(k(t))$. For each $t \in k$, let $y_t = \sqrt{f(t)}$, for some choice of the square root. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_k$ not lying above 2. Suppose that there exists $t_{\mathfrak{p}} \in k$ such that*

(3.4) $$3 | \operatorname{ord}_{\mathfrak{p}} f(t_{\mathfrak{p}}).$$

*Then there exists $\epsilon_{\mathfrak{p}} > 0$ such that if $t \in k$ and $|t - t_{\mathfrak{p}}|_{\mathfrak{p}} < \epsilon_{\mathfrak{p}}$, then for any prime $\mathfrak{q}$ of $k(y_t)$ lying above $\mathfrak{p}$, we have*

$$3 | \operatorname{ord}_{\mathfrak{q}}(y_t - Y_0(t)).$$

*Proof.* By continuity, for all $t \in k$ sufficiently $\mathfrak{p}$-adically close to $t_{\mathfrak{p}}$, we have $\operatorname{ord}_{\mathfrak{p}} f(t) = \operatorname{ord}_{\mathfrak{p}} f(t_{\mathfrak{p}})$ and $3 | \operatorname{ord}_{\mathfrak{p}} f(t)$ (and $3 | \operatorname{ord}_{\mathfrak{q}} f(t)$ for any prime $\mathfrak{q}$ of $k(y_t)$ lying above $\mathfrak{p}$). Since $\mathfrak{p}$ does not lie above 2, the result follows from the equivalence with the condition (3.2) used in the proof of Theorem 3.1.   $\square$

# 4   Proof of Theorem 1.3

We now have all of the tools to prove Theorem 1.3.

*Proof of Theorem 1.3.* Let $P_i = (X_i(t), Y_i(t)) \in E(\mathbb{Q}(t))$, $i = 1, \ldots, r$, be points whose images by the map (1.4) generate a subgroup isomorphic to $(\mathbb{Z}/3\mathbb{Z})^r$ in $\operatorname{Jac}(C)[3](\mathbb{Q})$. Let $S_0$ consist of the prime 2 and the (finite) union of the set of places of $\mathbb{Q}$ given by Theorem 3.1 (with $k = \mathbb{Q}$) applied to $P_1, \ldots, P_r$. By hypothesis, for each odd prime $p \in S_0$, there exists $t_p \in \mathbb{Q}$ such that $3 | \operatorname{ord}_p f(t_p)$. For each such $p$ and $t_p$, let $\epsilon_p > 0$ be as in Theorem 3.2. By hypothesis, there exists $t_2 \in \mathbb{Q}$ such that $\mathbb{Q}(\sqrt{f(t_2)})$ is a quadratic extension of $\mathbb{Q}$ and the prime 2 does not split in this extension. Then for some sufficiently small $\epsilon_2 > 0$, by Krasner's lemma (or elementary arguments in this specific case) if $|t - t_2|_2 < \epsilon_2$ then $\mathbb{Q}(\sqrt{f(t)})$ is a quadratic extension of $\mathbb{Q}$ and the prime 2 does not split in this extension. Let $t_\infty \in \mathbb{Q}$ and $\epsilon_\infty > 0$ be such that $f(t)$ is negative (resp. positive) if $|t - t_\infty| < \epsilon_\infty$. Let $\epsilon = \min_{p \in S_0} \epsilon_p$. Let $S = \{2, \infty\}$. Consider the rational functions $\psi_i = y - Y_i(t) \in \mathbb{Q}(t, y) = \mathbb{Q}(C)$, $i = 1, \ldots, r$. By Theorem 3.1 and Theorem 3.2, if $P \in C(\overline{\mathbb{Q}})$, $t = t(P) \in \mathbb{Q}$ and $|t - t_p|_p < \epsilon$ for all $p \in S_0$, then $\psi_i(P) = \sqrt{f(t)} - Y_i(t)$ generates the cube of a fractional ideal outside 2, i.e., $\psi_i(P)\mathcal{O}_{\mathbb{Q}(P),S} = \mathfrak{a}_{P,i}^3$ for some fractional $\mathcal{O}_{\mathbb{Q}(P),S}$-ideal $\mathfrak{a}_{P,i}$, $i = 1, \ldots, r$. Furthermore, from our assumptions at $p = 2, \infty$, $\mathbb{Q}(P)$ is an imaginary (resp. real) quadratic field in which 2 does not split. Note also that if $t \in \mathbb{Q}$ and $H(t) < B$, then the discriminant of $\mathbb{Q}(\sqrt{f(t)})$ is $\ll B^d$ (we use here that $d$ is even). By our hypotheses and the form of the map (1.3), the functions $\psi_1, \ldots, \psi_r$ generate a subgroup isomorphic to $(\mathbb{Z}/3\mathbb{Z})^r$ in $\overline{\mathbb{Q}}(C)^*/(\overline{\mathbb{Q}}(C)^*)^3$. Let $\phi = t$, a rational function of degree 2 on $C$. Combining all of the above, Theorem 2.2 gives that there are $\gg X^{\frac{1}{d}}/\log X$ distinct imaginary (resp. real) quadratic number fields $k$ with $|\operatorname{Disc}(k)| < X$

satisfying

$$\mathrm{rk}_3\,\mathrm{Cl}(\mathbb{Q}(P)) \geq r + \#S_{\mathrm{fin}} - \mathrm{rk}\,\mathcal{O}^*_{\mathbb{Q}(P),S}.$$

Since $S = \{2, \infty\}$, $\#S_{\mathrm{fin}} = 1$, and since there is a single prime lying above 2 in $\mathcal{O}_{\mathbb{Q}(P)}$, we have $\mathrm{rk}\,\mathcal{O}^*_{\mathbb{Q}(P),S} = 1$ (resp. $\mathrm{rk}\,\mathcal{O}^*_{\mathbb{Q}(P),S} = 2$). This gives the desired result when $f$ takes both negative and positive values on $\mathbb{R}$. Otherwise, we obtain the appropriate result for either real or imaginary quadratic fields, and the full theorem follows from Scholz's reflection principle [30]: if $d$ is a positive integer, then $\mathrm{rk}_3\,\mathrm{Cl}(\sqrt{-3d}) - \mathrm{rk}_3\,\mathrm{Cl}(\sqrt{d}) \in \{0, 1\}$.                     $\square$

# 5 Mestre's construction of a $j$-invariant $0$ elliptic curve over $\mathbb{Q}(t, u)$ of rank at least $6$

We recall a construction of Mestre [26, 27] which yields a $j$-invariant $0$ elliptic curve over $\mathbb{Q}(t, u)$ of rank at least 6 (and after a specialization, a $j$-invariant $0$ elliptic curve over $\mathbb{Q}(t)$ of rank at least 7).

Let $K$ be a field of characteristic 0 and let $x_1, \ldots, x_5 \in K$. Let

$$\begin{aligned}
x_6 &= -(x_1 + \cdots + x_5), \\
p(X) &= (X - x_1) \cdots (X - x_6) \\
&= X^6 + a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X + a_0,
\end{aligned}$$

and

$$g(X) = X^2 + a_4/3.$$

Then

$$g(X)^3 - p(X) = -a_3 X^3 + \left(\frac{a_4^2}{3} - a_2\right) X^2 - a_1 X + \left(\frac{a_4}{3}\right)^3 - a_0,$$

and the cubic curve $C : Y^3 = g(X)^3 - p(X)$ will generically be a genus 1 curve of $j$-invariant 0 possessing the six $K$-rational points $P_i = (x_i, g(x_i))$, $i = 1, \ldots, 6$. To obtain a further point when $K = \mathbb{Q}(t, u)$, Mestre shows

that if

$$x_1 = \frac{1 - u^3}{4u} + t,$$

$$x_2 = \frac{1 - u^3}{4u} - t,$$

$$x_3 = -\frac{u^3 + 3}{4u} + t,$$

$$x_4 = \frac{u^6 - 6u^3 - 3}{4(u^4 - u)} - t,$$

$$x_5 = \frac{u^9 - u^6 + 15u^3 + 1}{4(u^7 - u)} + t,$$

$$x_6 = -(x_1 + \cdots + x_5) = \frac{u^6 + 8u^3 - 1}{4(u^4 + u)} - t,$$

then $a_3 = -1$. Then since the leading coefficient of $g(X)^3 - p(X)$ is a perfect cube, the curve $C$ has a 7th rational point $P_7$ at infinity. Setting, say, $P_7$ as the origin, one easily finds (by a specialization and explicit computation) that the other 6 points are independent in the Mordell-Weil group of the resulting elliptic curve over $\mathbb{Q}(t, u)$. Mestre goes further and uses this construction to find an elliptic curve of rank at least 7 over $\mathbb{Q}(t)$. However, putting the curve in Weierstrass form, the extra point constructed has the same $y$-coordinate as a previous point, and so the new point does not produce any extra 3-torsion (via the map (1.3)).

# 6 3-torsion in hyperelliptic Jacobians

Let $p$ be an odd prime. As a function field analogue of constructing quadratic fields with an ideal class group of large $p$-rank, it is an interesting problem in its own right to construct hyperelliptic curves $C$ over $\mathbb{Q}$ such that $\mathrm{rk}_p \mathrm{Jac}(C)[p](\mathbb{Q})$ is large. For a given $p$-rank, it is further interesting to minimize the genus of the curve $C$ involved, both for intrinsic reasons and for applications to the enumerative problem of counting quadratic fields with interesting ideal class groups. Since $\mathbb{Q}$ doesn't contain a primitive $p$th root of unity, a well-known argument using the Weil pairing gives the bound (for any smooth projective curve $C$)

$$\mathrm{rk}_p \mathrm{Jac}(C)[p](\mathbb{Q}) \leq g(C),$$

where $g(C)$ denotes the genus of $C$.

We now restrict to the case $p = 3$. Using the constructions of the previous section we prove the following result.

**Theorem 6.1.** *There exists a hyperelliptic curve $C : y^2 = f(t)$ over $\mathbb{Q}$ of genus $g$, $\deg f = d$, and $\mathrm{rk}_3 \mathrm{Jac}(C)[3](\mathbb{Q}) \geq r$ for the following values of $r$, $d$, and $g = g(C)$:*

| $r$ | $d$ | $g$ |
|-----|-----|-----|
| 1 | 3 | 1 |
| 2 | 5 | 2 |
| 3 | 9 | 4 |
| 4 | 10 | 4 |
| 5 | 30 | 14 |

*Explicitly, the last three entries are realized by the hyperelliptic curves*

$$C_r : y^2 = f_r(t), \quad r = 3, 4, 5,$$

*with generators for $\mathrm{Jac}(C)[3](\mathbb{Q})$ given by the classes of*

$$D_{r,i} = \begin{cases} \frac{1}{3}\,\mathrm{div}(y - y_{r,i}(t)), & \text{if } r = 3, 5 \\ \frac{1}{3}\,\mathrm{div}(y - y_{r,i}(t)) - \frac{1}{3}\,\mathrm{div}(y - y_{r,5}(t)), & \text{if } r = 4 \end{cases}$$

*for $i = 1, \ldots, r$, where*

$$f_3(t) = t^9 + 2973t^6 - 369249t^3 + 11764900$$

$$y_{3,1}(t) = t^6 - 106t^3 + 3430$$

$$y_{3,2}(t) = \frac{1}{64}t^6 + \frac{269}{4}t^3 + 3430$$

$$y_{3,3}(t) = t^6 + 36t^5 + 486t^4 + 3350t^3 + 13914t^2 + 33264t + 40474$$

$$\begin{aligned}
f_4(t) =\ & 1273586291881530173431126946654244t^{10} - 144767265584415422595009805935829000t^9 \\
& + 7675409498430949648595073591624843211t^8 - 232279490111578558717503021611493180600t^7 \\
& + 4869337393859474196212065079200095373500t^6 - 8471956828413213486742748322179256745500t^5 \\
& + 13966552815344828853111870565028713666389900t^4 - 150980036450631929144153112446207907104172000t^3 \\
& + 1459774319726346792718147450304690725197946200t^2 - 13500425943365568652182653206136090492791068000t \\
& + 543592155691663960065241800360826161610140961
\end{aligned}$$

$$\begin{aligned}
y_{4,1}(t) =\ & 11285328049647162t^5 - 612703879315493343t^4 + 11259180860536474740t^3 + 124175441794992816207t^2 \\
& - 289418513692462490000 28t + 233150239731294170088 93
\end{aligned}$$

$$\begin{aligned}
y_{4,2}(t) =\ & 11285328049647162t^5 - 637837872300913137t^4 + 15898504501345253760t^3 - 133140352448943347487t^2 \\
& + 2895345088136314829232t - 23315023973129417008893
\end{aligned}$$

$$\begin{aligned}
y_{4,3}(t) =\ & 11285328049647162t^5 - 641395912765696179t^4 + 15779426445792454284t^3 - 132367737077167916373t^2 \\
& + 2891689893601551455028t - 23295069079544963156463
\end{aligned}$$

$$\begin{aligned}
y_{4,4}(t) =\ & 11285328049647162t^5 - 787772412770249571t^4 + 14665379977955069244t^3 - 219254957235699134757t^2 \\
& + 2621647313739427449588t - 35358708563462647994607
\end{aligned}$$

$$\begin{aligned}
y_{4,5}(t) =\ & 11285328049647162t^5 + 2985212511317920527t^4 + 74598289369102611840t^3 + 1831498005344531215377t^2 \\
& + 17007935557191258869 4272t + 18312273088496078252 2323
\end{aligned}$$

*and*

$$f_5(t) = f_4(t^3),$$
$$y_{5,i}(t) = y_{4,i}(t^3), \quad i = 1, \ldots, 5.$$

We note that, in terms of the genus, the results for $r = 1, 2, 4$ are sharp. We do not know if there exists a hyperelliptic curve with $(r, g) = (3, 3)$. However, it was shown in [21] that there exist (non-hyperelliptic) curves $C$ of genus 3 with $\mathrm{rk}_3 \mathrm{Jac}(C)[3](\mathbb{Q}) = 3$.

Combined with Theorem 1.2, the result for $r = 3$ immediately gives:

**Corollary 6.2.** *There exist* $\gg X^{\frac{1}{9}} / \log X$ *imaginary quadratic number fields* $k$ *with* $|\mathrm{Disc}(k)| < X$ *and*

$$\mathrm{rk}_3 \mathrm{Cl}(k) \geq 3.$$

With further work (as in the next section) the result for $r = 4$ should also lead to new enumerative results, although we did not pursue this. For smaller 3-rank, the best enumerative results for ideal class groups of quadratic fields are due to Heath-Brown [20, 19] (rank 1, i.e., class number divisible by 3) and Luca and Pacelli [25] (rank 2), with many earlier results by other authors (e.g., [5], [6], [31]).

*Proof of Theorem 6.1.* The first two entries in the table are well-known. For any value of $a \in \mathbb{Q} \setminus \{0, \frac{1}{27}\}$, the elliptic curve $y^2 = t^3 + (t + a)^2/4$ has the 3-torsion point $(0, a/2)$. For any value of $a, b \in \mathbb{Q}$, $a^2 - 4b^2 \neq 0, b \neq 0$, the genus two curve $C_{a,b} : y^2 = t^6 + at^3 + b^2$ satisfies $\mathrm{rk}_3 \mathrm{Jac}(C_{a,b})[3](\mathbb{Q}) = 2$, with generators for $\mathrm{Jac}(C_{a,b})[3](\mathbb{Q})$ given by the classes of $\frac{1}{3} \mathrm{div}(y - t^3 \pm b)$ (more generally, see [17, Lemma 3.3]). For appropriate choices of $a$ and $b$, $C_{a,b}$ possesses a rational Weierstrass point, and hence also admits a quintic Weierstrass model over $\mathbb{Q}$.

In the case $r = 3$, we consider Mestre's construction in Section 5 with the parameters

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (2, 3, -5, 0, t, -t).$$

This yields a genus one curve $Y^3 = r(X)$ over $\mathbb{Q}(t)$ with (at least) 6 $\mathbb{Q}(t)$-rational points $(x_i, g(x_i))$, $i = 1, \ldots, 6$. Choosing, say, the first point as the origin, one finds the elliptic curve

$$\tilde{E}_3 : y^2 = x^3 + f_3(t^2)$$

and 5 points $\tilde{P}_1, \ldots, \tilde{P}_5 \in \tilde{E}_3(\mathbb{Q}(t))$ (the curve $\tilde{E}_3$ also appears in [32]). The points $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3, \tilde{P}_4 + \tilde{P}_5 \in \tilde{E}_3(\mathbb{Q}(t))$ have coordinates that are rational functions in $t^2$, and thus we find 4 corresponding points, call them $P_1, \ldots, P_4$, on the elliptic curve

$$E_3 : y^2 = x^3 + f_3(t).$$

Let $y_{3,i}(t) = y(P_i) \in \mathbb{Q}(t)$ be the $y$-coordinates of the 4 points. Abusing no-tation, we also view $y_{3,i}(t) \in \mathbb{Q}(C_3) = \mathbb{Q}(t, y)$ and consider the rational func-tion $y - y_{3,i}(t)$ on the hyperelliptic curve $C_3$. By explicit computation, one verifies that $\operatorname{div}(y - y_{3,i}(t)) = 3D_{3,i}$ for some divisor $D_{3,i}$ on $C_3$, $i = 1, \ldots, 4$. Thus, the divisors $D_{3,i}$ yield 3-torsion classes $[D_{3,i}] \in \operatorname{Jac}(C_3)[3](\mathbb{Q})$, $i = 1, \ldots, 4$. By explicit computation (with Magma), one finds that $[D_{3,1}], [D_{3,2}]$, and $[D_{3,3}]$ are independent (over $\mathbb{Z}/3\mathbb{Z}$), while $[D_{3,1}] + \cdots + [D_{3,4}] = 0$. There-fore $\operatorname{rk}_3 \operatorname{Jac}(C_3)[3](\mathbb{Q}) \geq 3$, giving the 3rd entry in the table.

Finally, we describe the (related) constructions for $r = 4, 5$. The con-struction from Section 5 yields an elliptic curve over $\mathbb{Q}(t, u)$ with 6 $\mathbb{Q}(t, u)$-points that are independent in the Mordell-Weil group. Specializing to $u = 2$ and rescaling $t$ (to simplify the resulting polynomials) we find the elliptic curve

$$E_4 : y^2 = x^3 + f_4(t),$$

with six corresponding points $P_1, \ldots, P_6 \in E_4(\mathbb{Q}(t))$ (the sixth point turns out not to give new torsion). We set $y_{4,i}(t) = y(P_i) \in \mathbb{Q}(t)$ , $i = 1, \ldots, 5$, and view $y_i(t) \in \mathbb{Q}(C_4) = \mathbb{Q}(t, y)$. Define the divisors

$$D_{4,i} = \frac{1}{3} \operatorname{div}(y - y_{4,i}(t)) - \frac{1}{3} \operatorname{div}(y - y_{4,5}(t)), \quad i = 1, \ldots, 4$$

on $C_4$. Using Magma, one verifies that the divisor classes $[D_{4,1}], \ldots, [D_{4,4}]$ are independent over $\mathbb{Z}/3\mathbb{Z}$. Therefore $\operatorname{rk}_3 \operatorname{Jac}(C_4)[3](\mathbb{Q}) \geq 4$. Finally, with

$$
\begin{aligned}
f_5(t) &= f_4(t^3), \\
y_{5,i}(t) &= y_{4,i}(t^3), & i &= 1, \ldots, 5 \\
D_{5,i} &= \frac{1}{3} \operatorname{div}(y - y_{5,i}(t)), & i &= 1, \ldots, 5,
\end{aligned}
$$

a calculation in Magma with $[D_{5,1}], \ldots, [D_{5,5}]$ shows that $\operatorname{rk}_3 \operatorname{Jac}(C_5)[3](\mathbb{Q}) \geq 5$. $\qquad \square$

# 7 Proof of Theorem 1.1

The proof of Theorem 1.1 is based on Theorem 1.3 and a slight modification of the construction from last section when $r = 5$ (so that the hypotheses of Theorem 1.3 are appropriately satisfied).

*Proof of Theorem 1.1.* We use Mestre's construction from Section 5, with an appropriately chosen specialization so that (1) and (2) of Theorem 1.3 hold and $f$ takes negative values on $\mathbb{R}$. For this purpose, letting $u = -\frac{9}{5}$ and replacing $t$ by $t^3$ in the constructions of Section 5, we find an elliptic curve

$$E : y^2 = x^3 + f(t),$$

with $f \in \mathbb{Z}[t]$, $\deg f = 30$, and six points $P_1, \ldots, P_6 \in E(\mathbb{Q}(t))$. Let $y_i(t) = y(P_i) \in \mathbb{Q}(t)$ , $i = 1, \ldots, 6$. Let $C$ be the hyperelliptic curve $y^2 = f(t)$ and view $y_i(t) \in \mathbb{Q}(C) = \mathbb{Q}(t, y)$. Using Magma, one verifies that $\operatorname{div}(y - y_i(t)) = 3D_i$ for some divisor $D_i$ on $C$, $i = 1, \ldots, 6$, and that $[D_1], \ldots, [D_5]$ generate a subgroup $(\mathbb{Z}/3\mathbb{Z})^5$ in $\operatorname{Jac}(C)(\mathbb{Q})$. Moreover, the leading coefficient of $f$ is positive, $f(0)$ is negative, 2 and 5 are the only prime factors of $\gcd(f(0), f(1))$, $\operatorname{ord}_2(f(0)) = 3$ and $\operatorname{ord}_5(f(0)) = 12$. Then (1) of Theorem 1.3 holds (for some choice of $t_p \in \{0, 1\}$ for every odd prime $p$), and (2) holds as 2 ramifies in $\mathbb{Q}(\sqrt{f(0)})$. Since $\deg f = d = 30$ and $f$ takes negative values on $\mathbb{R}$, the conclusion of Theorem 1.3 gives the desired statement. $\quad\square$

## Acknowledgements

## References

[1] A. Bandini, *3-Selmer groups for curves $y^2 = x^3 + a$*, Czechoslovak Math. J. 58 (133) (2008), no. 2, 429–445.

[2] K. Belabas, *On quadratic fields with large 3-rank*, Math. Comp. 73 (2004), no. 248, 2061–2074.

[3] Y. Bilu and J. Gillibert, *Chevalley-Weil theorem and subgroups of class groups*, Israel J. Math. 226 (2018), no. 2, 927–956.

[4] 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).

[5] D. Byeon and E. Koh, *Real quadratic fields with class number divisible by 3*, Manuscripta Math. 111 (2003), no. 2, 261–263.

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

[7] Y.-M. J. Chen, *The Selmer groups of elliptic curves and the ideal class groups of quadratic fields*, Comm. Algebra 25 (1997), no. 7, 2157–2167.

[8] H. Cohen and F. Pazuki, *Elementary 3-descent with a 3-isogeny*, Acta Arith. 140 (2009), no. 4, 369–404.

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

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

[11] M. Delong, *Using elliptic curves to produce quadratic number fields of high three-rank*, Rocky Mountain J. Math. 34 (2004), no. 2, 599–618.

[12] F. Diaz y Diaz, *On some families of imaginary quadratic fields*, Math. Comp. 32 (1978), no. 142, 637–650.

[13] 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.

[14] F. Diaz y Diaz, D. Shanks, and H. C. Williams, *Quadratic fields with 3-rank equal to 4*, Math. Comp. 33 (1979), no. 146, 836–840.

[15] 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.

[16] J. Gillibert, E. Hallouin, and A. Levin, *Integral points on elliptic curves with j-invariant 0 over k(t)*, (in prepration).

[17] J. Gillibert and A. Levin, *Pulling back torsion line bundles to ideal classes*, Math. Res. Lett. 19 (2012), no. 6, 1171–1184.

[18] J. Gillibert and A. Levin, *Elliptic surfaces over $\mathbb{P}^1$ and large class groups of number fields*, Int. J. Number Theory 15 (2019), no. 10, 2151–2162.

[19] D. R. Heath-Brown, *Quadratic class numbers divisible by 3*, Funct. Approx. Comment. Math. 37 (2007), part 1, 203–211.

[20] D. R. Heath-Brown, *Corrigendum to the paper "Quadratic class numbers divisible by 3"*, Funct. Approx. Comment. Math. 43 (2010), part 2, 227.

[21] 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.

[22] Y. Kishi and T. Komatsu, *Imaginary quadratic fields whose ideal class groups have 3-rank at least three*, J. Number Theory 170 (2017), 46–54.

[23] A. Kulkarni, *An explicit family of cubic number fields with large 2-rank of the class group*, Acta Arith. 182 (2018), no. 2, 117–132.

[24] P. Llorente and J. Quer, *On the 3-Sylow subgroup of the class group of quadratic fields*, Math. Comp. 50 (1988), no. 181, 321–333.

[25] F. Luca and A. M. Pacelli, *Class groups of quadratic fields of 3-rank at least 2: effective bounds*, J. Number Theory 128 (2008), no. 4, 796–804.

[26] J.-F. Mestre, *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris Sér. I Math. 314 (1992), no. 12, 919–922.

[27] J.-F. Mestre, *Rang de courbes elliptiques d'invariant nul*, C. R. Acad. Sci. Paris Sér. I Math. 321 (1995), no. 9, 1235–1236.

[28] J. Quer, *Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12*, C. R. Acad. Sci. Paris Sér. I Math. 305 (1987), no. 6, 215–218.

[29] P. Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory 23 (1986), no. 3, 294–317.

[30] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math. 166 (1932), 201–203.

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

[32] C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. 8 (1995), no. 4, 943–973.

[33] J. Top, *Descent by 3-isogeny and 3-rank of quadratic fields*, Advances in number theory (Kingston, ON, 1991), Oxford Sci. Publ., Oxford Univ. Press, New York, 1993, pp. 303–317.