HILBERT'S IRREDUCIBILITY THEOREM AND IDEAL CLASS GROUPS OF QUADRATIC FIELDS

KAIVALYA R. KULKARNI AND AARON LEVIN

Abstract. We prove a version of Hilbert's Irreducibility Theorem in the quadratic case, giving a quantitative improvement to a result of Bilu-Gillibert in this restricted setting. As an application, we give improvements to several quantitative results counting quadratic fields with certain types of ideal class groups. The proof of the main theorem is based on a result of Stewart and Top on values of binary forms modulo squares.

1. Introduction

The Hilbert Irreducibility Theorem plays a key role in recent approaches to constructing and counting number fields with a large ideal class group (originating in work of the second author [13] and joint work of the second author with Gillibert [9]). Recent applications of these techniques to study ideal class groups include work of Bilu-Gillibert [1], A. Kulkarni [12], work of the second author with Gillibert [10], and work of the second author with Wiljanen and Yan [14].

Let $H(\alpha)$ denote the absolute multiplicative height of an algebraic number α. If $\alpha = p/q \in \mathbb{Q}$ is written in reduced form, then $H(p/q) = \max\{|p|, |q|\}$. Partially in pursuit of applications to ideal class groups, Bilu and Gillibert [1, Th. 3.1] proved the following version of Hilbert's Irreducibility Theorem (building on an enumerative result of Dvornicich and Zannier [8]):

Theorem 1.1 (Bilu-Gillibert [1, Th. 3.1]). *Let k be a number field of degree ℓ 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* [1, §3.1]. *Then there exist constants B_0 and c such that for all $B \geq B_0$, among the number fields $k(P)$, where the point $P \in C(\bar{k})$ satisfies*

$$\begin{aligned} \phi(P) &\in k \setminus \mho, \\ |\phi(P)|_v &< \epsilon, \qquad \forall v \in S, \\ H(\phi(P)) &\leq B, \end{aligned}$$

there exist at least $cB^\ell / \log B$ distinct fields of degree d over k.

2020 *Mathematics Subject Classification.* Primary 11R29; Secondary 12E25.

Key words and phrases. Ideal class groups, Hilbert's Irreducibility Theorem.

It was remarked by Bilu and Gillibert [1, Rem. 3.2] that Theorem 1.1 likely holds with a lower bound of the form $cB^{2\ell}/(\log B)^A$ for some $A > 0$. Our main result shows that this predicted lower bound holds (with $A = 2$) when $k = \mathbb{Q}, \ell = 1$, and $d = 2$:

Theorem 1.2. *Let C be a curve over $\mathbb{Q}$ and $\phi : C \to \mathbb{P}^1$ a morphism of degree 2. Let S be a finite set of places of $\mathbb{Q}$, $\epsilon > 0$, and $\mho$ a thin subset of $\mathbb{Q}$. Then there exist constants B_0 and c such that for all $B \geq B_0$, among the number fields $\mathbb{Q}(P)$, where the point $P \in C(\overline{\mathbb{Q}})$ satisfies*

$$\begin{aligned} \phi(P) &\in \mathbb{Q} \setminus \mho, \\ |\phi(P)|_v &< \epsilon, \qquad \forall v \in S, \\ H(\phi(P)) &\leq B, \end{aligned}$$

there exist at least $cB^2/(\log B)^2$ distinct quadratic fields over $\mathbb{Q}$.

Using Theorem 1.2 in place of Theorem 1.1 allows us to recover and improve on several enumerative results involving ideal class groups of quadratic number fields. Given an integer $m > 1$, it has been known since Nagell [17] that there are infinitely many imaginary quadratic number fields with class number divisible by m, and the analogous result for real quadratic fields was proved independently by Yamamoto [22] and Weinberger [21]. Quantitative results giving a lower bound for the number of such fields were given by Murty [16], Soundararajan [19], and Yu [23].

More generally, one can study the m-rank of the ideal class group. If A is a finitely generated abelian group, we define the m-rank of A, $\operatorname{rk}_m A$, to be the largest integer r such that A has a subgroup isomorphic to $(\mathbb{Z}/m\mathbb{Z})^r$. For a number field k, we let $\operatorname{Cl}(k)$ denote its ideal class group and let d_k denote its (absolute) discriminant.

As an application of Theorem 1.2, we first state a general result counting quadratic number fields with a large class group generated, via the technique of [9], from a hyperelliptic curve with a rational Weierstrass point and a large rational torsion subgroup in its Jacobian. The result is identical to [9, Cor. 3.2], except that we improve the lower bound for an asymptotic count of such fields, by discriminant, from $X^{\frac{1}{2g+1}}/\log X$ to $X^{\frac{1}{g+1}}/(\log X)^2$ (up to a constant factor).

Theorem 1.3. *Let C be a smooth projective hyperelliptic curve over $\mathbb{Q}$ with a $\mathbb{Q}$-rational Weierstrass point. Let g denote the genus of C and let $\operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}}$ denote the rational torsion subgroup of the Jacobian of C. Let $m > 1$ be an integer. Then there exist $\gg \frac{X^{\frac{1}{g+1}}}{(\log X)^2}$ imaginary quadratic number fields k with*

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

and $\gg \frac{X^{\frac{1}{g+1}}}{(\log X)^2}$ real quadratic number fields k with

$$\operatorname{rk}_m \operatorname{Cl}(k) \geq \operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}} - 1, \quad d_k < X.$$

We let $\mathcal{N}^-(m^r;X)$ and $\mathcal{N}^+(m^r;X)$ denote the number of imaginary quadratic and real quadratic number fields k, respectively, with discriminant d_k satisfying $|d_k| \leq X$ and such that $\operatorname{rk}_m \operatorname{Cl}(k) \geq r$.

By noting (see [9, Lemma 3.3]) that for $c \in \mathbb{Q} \setminus \{0, \pm 1\}$, the smooth projective hyperelliptic curve C with affine equation

$$y^2 = x^{2m} - (1+c^2)x^m + c^2$$

has genus $m-1$, a rational Weierstrass point, and $\operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}} \geq 2$, we find as a corollary:

Corollary 1.4. *Let $m > 1$ be an integer. Then*

$$\mathcal{N}^-(m^2;X) \gg X^{\frac{1}{m}}/(\log X)^2,$$
$$\mathcal{N}^+(m;X) \gg X^{\frac{1}{m}}/(\log X)^2.$$

When m is odd, this yields a small improvement to results of Byeon [2] and Yu [23] (following results of Murty [16]), who proved $\mathcal{N}^-(m^2;X) \gg X^{\frac{1}{m}-\epsilon}$ and $\mathcal{N}^+(m;X) \gg X^{\frac{1}{m}-\epsilon}$, respectively. When m is even, in the real quadratic case Chakraborty, Luca, and Mukhopadhyay [6] (see also [15]) proved the logarithmically better bound $\mathcal{N}^+(m;X) \gg X^{\frac{1}{m}}$. When m is even and k is imaginary quadratic, Corollary 1.4 appears to be new and fills a gap in the literature, bringing this case in line with the other known results.

For small values of m better results are known (see results of Byeon [3, 4] for $m = 5, 7$). We discuss the case $m = 3$, where Theorem 1.2 again allows us to make quantitative improvements to some of the known results. In the case of class number divisibility by 3, Heath-Brown [11] showed $\mathcal{N}^\pm(3;X) \gg X^{\frac{9}{10}-\epsilon}$, improving on [5, 7, 23]. For 3-rank 2, Luca and Pacelli proved $\mathcal{N}^\pm(3^2;X) \gg X^{\frac{1}{3}}$, and recently Yu [24] improved this in the imaginary quadratic case, finding $\mathcal{N}^-(3^2;X) \gg X^{\frac{1}{2}-\epsilon}$.

For higher 3-rank, it was shown by the second author and Wiljanen and Yan [14] that $\mathcal{N}^-(3^3;X) \gg X^{\frac{1}{9}}/\log X$, $\mathcal{N}^+(3^4;X) \gg X^{\frac{1}{30}}/\log X$, and $\mathcal{N}^-(3^5;X) \gg X^{\frac{1}{30}}/\log X$. Using Theorem 1.2, we are able to improve these results.

Theorem 1.5. *We have*

$$\mathcal{N}^-(3^3;X) \gg \frac{X^{\frac{1}{5}}}{(\log X)^2},$$
$$\mathcal{N}^+(3^4;X) \gg \frac{X^{\frac{1}{15}}}{(\log X)^2},$$
$$\mathcal{N}^-(3^5;X) \gg \frac{X^{\frac{1}{15}}}{(\log X)^2}.$$

The proof of our main theorem (Theorem 1.2), given in Section 3, is based on a result of Stewart and Top [20] on the squarefree part of values of binary forms, which we describe in the next section. In the final section we briefly describe the proofs of the applications to ideal class groups (Theorem 1.3 and Theorem 1.5).

2. Values of binary forms modulo kth powers

For a positive integer k and integer n, we say that n is k-free if n is not divisible by the kth power of a prime. The main tool in proving Theorem 1.2 is a slight variation of a result of Stewart and Top [20, Th. 2].

Theorem 2.1 (Stewart-Top)**.** *Let A, B, M, and k be integers with $M \geq 1$ and $k \geq 2$. Let F be a binary form with integer coefficients and degree r which is not a constant multiple of a power of a linear form and which is not divisible over $\mathbb{Q}$ by the kth power of a non-constant binary form. Let*

$$C(x) := \{(a,b) \in \mathbb{N} \times \mathbb{N} | \ 0 < a, b \leq x^{1/r} \text{ and } (a,b) \equiv (A,B) \bmod M\}.$$

Let $S_k(x)$ denote the number of k-free integers t such that $|t| \leq x$ and $F(a,b) = tz^k$ for some $z \in \mathbb{Z}, (a,b) \in C(x)$. Then,

$$S_k(x) \gg \frac{x^{\frac{2}{r}}}{(\log x)^2}.$$

Stewart and Top's original result did not require the integers a and b to be positive, and did not place a bound on a and b. Since the proof of Theorem 2.1 only requires slight modifications to their original proof, we give a sketch of the proof highlighting the necessary changes.

Proof. Following Stewart and Top, we may write F as a product $F_1 F_2 \cdots F_l$ of binary forms with integer coefficients, such that F_{i+1} divides F_i for all $1 \leq i \leq l-1$, and F_i has nonzero discriminant for $i = 1, \ldots, l$. Then F_1 may be written as a product of nonconstant forms $G_1 \cdots G_m$ where G_i is irreducible in $\mathbb{Q}[x,y]$ for all i.

The proof of Theorem 2 in [20] is divided into three cases: (1) some G_i is nonlinear, (2) $G_1, \ldots, G_m$ are linear and $m \geq 3$, and (3) $G_1, \ldots, G_m$ are linear and $m = 2$. In each case, we claim that the constructions used in [20] may be modified so that the integers a and b used are positive.

In Case (1), a and b are positive integral linear combinations of integers r_0, s_0, r_1, s_1, where for a certain given lattice $\Lambda_p \subset \mathbb{Z}^2$, $(r_0, s_0) \in \Lambda_p$ is chosen such that $\max\{|r_0|, |s_0|\}$ is minimal, and (r_1, s_1) is chosen such that $v_0 = (r_0, s_0), v_1 = (r_1, s_1)$ is a basis of Λ_p and $\max\{|r_1|, |s_1|\}$ is minimal. Then we use the following lemma:

Lemma 2.2. *Let $\Lambda \subset \mathbb{Z}^2$ be a lattice of rank 2. Let $(r_0, s_0) \in \Lambda$ be chosen such that $\max\{|r_0|, |s_0|\}$ is minimal, and (r_1, s_1) chosen such that $v_0 = (r_0, s_0), v_1 = (r_1, s_1)$ is a basis of Λ and $\max\{|r_1|, |s_1|\}$ is minimal. Let $M = \max\{|r_0|, |s_0|, |r_1|, |s_1|\}$. Then there exists a basis $v_0' = (r_0', s_0'), v_1' = (r_1', s_1') \in \Lambda$ with $r_0', s_0', r_1', s_1 \geq 0$ such that*

$$\max\{|r_0'|, |s_0'|, |r_1'|, |s_1'|\} \leq 3\max\{|r_0|, |s_0|, |r_1|, |s_1|\} = 3M. \tag{2.1}$$

Proof. Suppose first that r_0 and s_0 have the same sign or that $r_0s_0 = 0$. Then after possibly replacing v_0 by $-v_0$ and v_1 by $-v_1$, and after possibly interchanging the coordinates, we may assume that $r_0 \geq s_0 \geq 0$ and $r_1 \geq 0$. If $s_1 \geq 0$, then clearly we may take $v_0' = v_0$ and $v_1' = v_0$. So we may assume $s_1 < 0$.

Note that $r_0 \neq 0$ and let $n = \lceil r_1/r_0 \rceil$. Let $v_0' = v_0$ and $v_1' = nv_0 - v_1 = (nr_0 - r_1, ns_0 - s_1)$. Then v_0', v_1' are a basis of Λ. Since $r_1/r_0 \leq n < r_1/r_0 + 1$ and $r_0 \geq s_0$, we have

$$0 \leq nr_0 - r_1 < r_0 \leq M$$

and

$$0 \leq ns_0 - s_1 < r_1 + s_0 + |s_1| \leq 3M.$$

Thus, we see that v_0', v_1' satisfy the conclusions of the theorem. The same proof, with the indices interchanged, works if r_1 and s_1 have the same sign or if $r_1s_1 = 0$.

Suppose now that $r_0r_1s_0s_1 \neq 0$ and the coordinates of v_i have opposite signs for $i = 1, 2$. Then after possibly replacing v_0 by $-v_0$ and v_1 by $-v_1$, we may assume that $r_0, r_1 > 0$ and $s_0, s_1 < 0$. Then $v_1 - v_0 = (r_1 - r_0, s_1 - s_0)$ and $|r_1 - r_0| < M$, $|s_1 - s_0| < M$. Since $v_0, v_1 - v_0$ is a basis of Λ, this contradicts the minimality of v_0 and v_1, and this case is impossible. □

Then in Case (1), modifying the construction to use the nonnegative integers r_0', s_0', r_1', s_1' in place of r_0, s_0, r_1, s_1 preserves the conclusions in this case (with possibly slightly smaller constants).

In Case (2), the construction in [20] already uses positive integers a and b.

In Case (3), $a = A + kM, b = B + lcM$, and the parameters A, B, c, l, M, t in the proof may all clearly be taken to be nonnegative. It only remains to show that the parameter k in the proof may be constructed to be positive. If $d \leq 0$ then the existing proof already gives $k = t - dl > 0$. If $d > 0$ then we may replace $k = t - dl$ with $k = t + idl$ for some $i \in \{0, 1\}$ satisfying $cf + ide \neq 0$, and the remainder of the proof remains substantially unchanged.

Finally, we note that all of the constructions produce integers a and b such that $\max\{|a|, |b|\} \ll x^{1/r}$. Then replacing x by cx for an appropriately small constant $c > 0$, we see that we may choose $\max\{|a|, |b|\} \leq x^{1/r}$ in the constructions and, by the remainder of the proof in [20],

$$S_k(x) \gg \frac{(cx)^{\frac{2}{r}}}{(\log cx)^2} \gg \frac{x^{\frac{2}{r}}}{(\log x)^2}.$$

□

3. Proof of Theorem 1.2

We need the following lemma for the proof of Theorem 1.2.

Lemma 3.1. *Let S be a finite set of places of $\mathbb{Q}$, and let $\epsilon > 0$. Then there exists an invertible linear fractional transformation $\psi \in \mathbb{Q}(t)$ and integers M, A, and B such that whenever $\psi(t) = a/b$, $a, b > 0$, $a \equiv A \pmod{M}, b \equiv B \pmod{M}$, we have $|t|_v < \epsilon$ for all $v \in S$.*

Proof. If S doesn't contain the (unique) archimedean place ∞ of $\mathbb{Q}$, then this is straightforward (with ψ the identity). If S contains the archimedean place, let N be an integer such that $N > 1/\epsilon$ and let

$$\psi(t) = \frac{1 - Nt}{1 + Nt}.$$

Then it is easily verified that the inverse image of the real interval $(0, +\infty)$ under ψ is $(-1/N, 1/N) \subset (-\epsilon, \epsilon)$ and so if $\psi(t) = a/b > 0$, then $|t|_\infty < \epsilon$. Since $\psi^{-1}(1) = 0$, taking $A = B = 1$ and M divisible by sufficiently large powers of the (finite) primes in S, we see that if $a \equiv A \pmod{M}, b \equiv B \pmod{M}$ and $\psi(t) = a/b$, then $|t|_v < \epsilon$ for all finite places v in S. □

We also need the following fact about thin sets [18, p. 133]:

Lemma 3.2. *Let $\mho \subset \mathbb{Q}$ be a thin set. Then for $x > 0$, there exist at most $O(x)$ rational numbers α such that $\alpha \in \mho$ and $H(\alpha) < x$.*

We now prove Theorem 1.2.

Proof of Theorem 1.2. Let $C, \phi, S, \mho$, and ϵ be as in the statement of the theorem. Then ϕ induces a quadratic extension of function fields $\mathbb{Q}(C)/\mathbb{Q}(t)$ and we may write $\mathbb{Q}(C) = \mathbb{Q}(\sqrt{f(t)})$ for some nonconstant squarefree polynomial $f(t) \in \mathbb{Q}[t]$. Then C may be taken to have affine equation $y^2 = f(t)$, where ϕ is induced by the projection onto the t-coordinate.

Let ψ, A, B, and M be as in Lemma 3.1 (with respect to ϵ and S). Let $\tau = \psi^{-1}$ and write $f(\tau(X/Y)) = F(X, Y)R(X, Y)^2$ for some rational function $R(X, Y) \in \mathbb{Q}(X, Y)$ and squarefree homogeneous polynomial $F \in \mathbb{Z}[X, Y]$. Since f is nonconstant squarefree, F is nonconstant, and looking at degrees it follows easily that $\deg F$ is even. Thus, $\deg F \geq 2$. Then F satisfies the hypotheses of Theorem 2.1 (with $k = 2$).

Let x be a positive real number. Let $T(x)$ be the set of squarefree (i.e., 2-free) integers t for which there exist positive integers $a \leq x$ and $b \leq x$ satisfying $a \equiv A \pmod{M}, b \equiv B \pmod{M}$, and $F(a, b) = tz^2$ for some integer z. Note that $S_2(x^{\deg F})$ gives a lower bound for the number of elements of $T(x)$. For each $t \in T(x)$, let (a_t, b_t) be a pair of positive integers satisfying the conditions in the definition of $t \in T(x)$, and let $T'(x) = \{(a_t, b_t) \mid t \in T(x)\}$. Let

$$R(x) = \{P \in C(\overline{\mathbb{Q}}) \mid \psi(\phi(P)) = a/b, (a, b) \in T'(x), \phi(P) \notin \mho\}.$$

Let $P \in R(x)$. Then $\psi(\phi(P)) = a_t/b_t = a/b$, for some $(a_t, b_t) = (a, b) \in T'(x)$ and $t \in T(x)$. By construction, we have

$$\phi(P) = \tau(a/b) \in \mathbb{Q} \setminus \mho, \tag{3.1}$$

and by Lemma 3.1, we have

$$|\phi(P)|_v < \epsilon \tag{3.2}$$

for all $v \in S$. Note also that

$$\begin{aligned}\mathbb{Q}(P) &= \mathbb{Q}(\sqrt{f(\phi(P))}) = \mathbb{Q}(\sqrt{f(\tau(a_t/b_t))}) = \mathbb{Q}(\sqrt{F(a_t,b_t)R(a_t,b_t)^2}) \\ &= \mathbb{Q}(\sqrt{F(a_t,b_t)}) = \mathbb{Q}(\sqrt{t}).\end{aligned}$$

It follows that the fields $\mathbb{Q}(P)$, $P \in R(x)$, are all distinct. By elementary properties of heights, for some positive constant c depending only on ψ,

$$H(\phi(P)) \le cH(\psi(\phi(P)))$$

and $H(\psi(\phi(P))) = \max\{|a|,|b|\} \le x$. Rescaling, if $P \in R(c^{-1}x)$ then $H(\phi(P)) \le x$ (and (3.1) and (3.2) hold). To finish the proof, it remains to count the elements in $R(c^{-1}x)$.

Let $\mho(x) = \{\alpha \in \mho \mid H(\alpha) < x\}$. By Lemma 3.2,

$$|\mho(x)| \ll x.$$

Then by Theorem 2.1,

$$|R(c^{-1}x)| \ge |T'(c^{-1}x)| - 2|\mho(x)| \ge S_2((c^{-1}x)^{\deg F}) - 2|\mho(x)| \gg \frac{x^2}{(\log x)^2},$$

completing the proof.

□

4. Proof of Theorem 1.3 and Theorem 1.5

We take the following result from the proof of [9, Cor. 2.11]:

Theorem 4.1. *Let C be a smooth projective curve over $\mathbb{Q}$, and let $m > 1$. Let S be the set of primes of bad reduction of C. Let $\phi : C \to \mathbb{P}^1$ be a nonconstant morphism. Then there exists a thin set $\mho \subset \mathbb{Q}$ such that if $P \in C(\overline{\mathbb{Q}})$ and $\phi(P) \in \mathbb{Q} \setminus \mho$, then $[\mathbb{Q}(P) : \mathbb{Q}] = \deg \phi$ and*

$$\operatorname{rk}_m \operatorname{Cl}(\mathbb{Q}(P)) \ge \operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\mathrm{tors}} + \#S - \operatorname{rk} \mathcal{O}^*_{\mathbb{Q}(P),S},$$

Here, $\mathcal{O}^*_{\mathbb{Q}(P),S}$ denotes the group of S'-units of $\mathbb{Q}(P)$, where S' consists of the set of places of $\mathbb{Q}(P)$ lying above S along with the archimedean places. We now prove Theorem 1.3.

Proof of Theorem 1.3. Since C has a rational Weierstrass point, C is birational to an affine curve given by an equation $y^2 = f(x)$ with $f \in \mathbb{Z}[x]$ monic and $\deg f = d$ odd. Let S be the set of primes of bad reduction of C and let $M = \prod_{p \in S} p$. Let N be a large enough positive integer such that $f(x) > 0$ if $|x - N/M| < 1$ and such that $(M,N) = 1$. Let $\phi : C \to \mathbb{P}^1$ be the morphism induced by $(x,y) \mapsto x - N/M$ and let $\mho$ be the thin set from Theorem 4.1 (for C, ϕ, and m). Let $P \in C(\overline{\mathbb{Q}})$ with $\phi(P) \in \mathbb{Q} \setminus \mho, |\phi(P)|_v < 1$ for all $v \in S \cup \{\infty\}$, and $H(\phi(P)) \le B$. Let $P = (x_0, y_0)$. Since $\phi(P) \in \mathbb{Q}$, we have $x_0 \in \mathbb{Q}$. For $p \in S$, by assumption $|x_0 - N/M|_p < 1$, and so

$\operatorname{ord}_p x_0 = \operatorname{ord}_p N/M = -1$. Since $f \in \mathbb{Z}[x]$ is monic, this implies that $\operatorname{ord}_p f(x_0) = -d$ is odd and p ramifies in $\mathbb{Q}(P) = \mathbb{Q}(y_0) = \mathbb{Q}(\sqrt{f(x_0)})$. By the choice of N, $|\phi(P)|_\infty < 1$ implies that $f(x_0) > 0$ and $\mathbb{Q}(P)$ is a real quadratic field. Therefore, by Dirichlet's unit theorem,

$$\#S - \operatorname{rk} \mathcal{O}^*_{\mathbb{Q}(P),S} = -\operatorname{rk} \mathcal{O}^*_{\mathbb{Q}(P)} = -1.$$

Since $\phi(P) \in \mathbb{Q} \setminus \mho$, by Theorem 4.1,

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

We now bound the discriminant of $\mathbb{Q}(P)$. First note that $H(\phi(P)) \leq B$ implies $H(x_0) \leq cB$ for some constant c (depending on M and N). If $x_0 = a/b$, then $\mathbb{Q}(\sqrt{f(x_0)}) = \mathbb{Q}(\sqrt{b^{d+1} f(a/b)})$, where $b^{d+1} f(a/b)$ is a homogeneous polynomial of degree $d+1 = 2g+2$ in a and b. It follows that $d_{\mathbb{Q}(P)} \leq c' B^{2g+2}$ for some constant c' depending on f, M, and N. Setting $B = (X/c')^{\frac{1}{2g+2}}$ and using Theorem 1.2, we find $\gg \frac{X^{\frac{1}{g+1}}}{(\log X)^2}$ distinct real quadratic fields $k = \mathbb{Q}(P)$ with $d_k < X$ and $\operatorname{rk}_m \operatorname{Cl}(k) \geq \operatorname{rk}_m \operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}} - 1$. Finally, choosing N to be a large enough positive integer such that $f(x) < 0$ if $|x + N/M| < 1$ (and $(M, N) = 1$), and taking $\phi = x + N/M$, the same proof yields the result for imaginary quadratic fields (with the improvement over the real quadratic case coming from the difference in the ranks of the unit groups $\mathcal{O}^*_{\mathbb{Q}(P)}$). □

Finally, we give the proof of Theorem 1.5.

Proof of Theorem 1.5. By [14, Th. 6.1], the genus 4 hyperelliptic curve

$$C : y^2 = t^9 + 2973t^6 - 369249t^3 + 11764900$$

satisfies $\operatorname{rk}_3 \operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}} \geq 3$. Then the statement for $\mathcal{N}^-(3^3; X)$ follows immediately from the existence of this curve and Theorem 1.3. The proof of the statements involving $\mathcal{N}^+(3^4; X)$ and $\mathcal{N}^-(3^5; X)$ are identical to the proof of the main theorem in [14], except that one replaces the use of Theorem 1.1 in that proof with Theorem 1.2, providing the improvement in the bounds. □

Acknowledgments. The second author was supported in part by NSF grant DMS-2001205. We would like to thank the referee for several helpful comments.

References

[1] Y. Bilu and J. Gillibert, *Chevalley-Weil theorem and subgroups of class groups*, Israel J. Math. **226** (2018), no. 2, 927–956. MR 3819714

[2] D. Byeon, *Imaginary quadratic fields with noncyclic ideal class groups*, Ramanujan J. **11** (2006), no. 2, 159–163. MR 2267671

[3] ———, *Real quadratic fields with class number divisible by 5 or 7*, Manuscripta Math. **120** (2006), no. 2, 211–215. MR 2234249

[4] ———, *Quadratic fields with noncyclic 5- or 7-class groups*, Ramanujan J. **19** (2009), no. 1, 71–77. MR 2501238

[5] D. Byeon and E. Koh, *Real quadratic fields with class number divisible by 3*, Manuscripta Math. **111** (2003), no. 2, 261–263. MR 1989426

[6] K. Chakraborty, F. Luca, and A. Mukhopadhyay, *Exponents of class groups of real quadratic fields*, Int. J. Number Theory **4** (2008), no. 4, 597–611.

[7] 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. MR 1929021

[8] 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. MR 1310635

[9] J. Gillibert and A. Levin, *Pulling back torsion line bundles to ideal classes*, Math. Res. Lett. **19** (2012), no. 6, 1171–1184. MR 3091601

[10] ———, *Elliptic surfaces over $\mathbb{P}^1$ and large class groups of number fields*, Int. J. Number Theory **15** (2019), no. 10, 2151–2162. MR 4033251

[11] D. R. Heath-Brown, *Quadratic class numbers divisible by 3*, Funct. Approx. Comment. Math. **37** (2007), no. part 1, 203–211. MR 2357319

[12] 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. MR 3749365

[13] 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. MR 2394898

[14] A. Levin, S. Yan, and L. Wiljanen, *Quadratic fields with a class group of large 3-rank*, Acta Arith. **197** (2021), no. 3, 275–292. MR 4194947

[15] 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. MR MR1999181 (2004g:11099)

[16] M. Ram 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. MR 1691322

[17] T. Nagel, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **1** (1922), no. 1, 140–150. MR 3069394

[18] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. MR 1757192

[19] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. (2) **61** (2000), no. 3, 681–690. MR 1766097

[20] 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. MR 1290234

[21] P. J. Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory **5** (1973), 237–241. MR 335471

[22] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka Math. J. **7** (1970), 57–76. MR 266898

[23] G. Yu, *A note on the divisibility of class numbers of real quadratic fields*, J. Number Theory **97** (2002), no. 1, 35–44. MR MR1939135 (2003m:11187)

[24] ———, *Imaginary quadratic fields with class groups of 3-rank at least 2*, Manuscripta Math. **163** (2020), no. 3-4, 569–574. MR 4159812

Department of Mathematics, Michigan State University, East Lansing, MI 48824, USA

Email address: kaivalya.r.kulkarni@gmail.com

Email address: adlevin@math.msu.edu