JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Aaron LEVIN

Ideal class groups, Hilbert's irreducibility theorem, and integral points of bounded degree on curves

Tome 19, n° 2 (2007), p. 485-499.

<http://jtnb.cedram.org/item?id=JTNB_2007__19_2_485_0>

© Université Bordeaux 1, 2007, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/), implique l'accord avec les conditions générales d'utilisation (http://jtnb.cedram.org/legal/). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Journal de Théorie des Nombres
de Bordeaux **19** (2007), 485-499

Ideal class groups, Hilbert's irreducibility theorem, and integral points of bounded degree on curves

par Aaron LEVIN

Résumé. Nous étudions la construction et le comptage, pour tout couple d'entiers $m, n > 1$, des corps de nombres de degré n dont le groupe des classes possède un "grand" m-rang. Notre technique repose essentiellement sur le théorème d'irréductibilité de Hilbert et sur des résultats concernant les points entiers de degré borné sur des courbes.

Abstract. We study the problem of constructing and enumerating, for any integers $m, n > 1$, number fields of degree n whose ideal class groups have "large" m-rank. Our technique relies fundamentally on Hilbert's irreducibility theorem and results on integral points of bounded degree on curves.

1. Introduction

In 1922, Nagell [20, 21] proved that for any integer m, there exist infinitely many imaginary quadratic number fields with class number divisible by m. This result has since been reproved by a number of different authors (e.g., [1], [13], [16]). Nearly fifty years later, working independently, Yamamoto [31] and Weinberger [30] extended Nagell's class number divisibility result to real quadratic fields. Soon after, Uchida [28] proved the analogous result for cubic cyclic fields. The class number divisibility problem for number fields of arbitrary degree was resolved in 1984 by Azuhata and Ichimura [2]. 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

$$\operatorname{rk}_m \operatorname{Cl}(k) \geq r_2, \tag{1.1}$$

where $\operatorname{Cl}(k)$ is the ideal class group of k and $\operatorname{rk}_m \operatorname{Cl}(k)$ denotes the largest integer such that $(\mathbb{Z}/m\mathbb{Z})^{\operatorname{rk}_m \operatorname{Cl}(k)}$ is a subgroup of $\operatorname{Cl}(k)$. The right-hand side of (1.1) was later improved to r_2+1 by Nakano [22, 23]. Choosing r_2 as

Manuscrit reçu le 2 août 2006.

large as possible, we thus obtain, for any m, infinitely many number fields k of degree $n > 1$ with

$$\operatorname{rk}_m \operatorname{Cl}(k) \geq \left\lfloor \frac{n}{2} \right\rfloor + 1, \tag{1.2}$$

where $\lfloor \cdot \rfloor$ denotes the greatest integer function. Furthermore, improving on previous work of Ishida [15] and Ichimura [14], Nakano proved the existence of infinitely many number fields k of degree $n > 1$ with

$$\operatorname{rk}_2 \operatorname{Cl}(k) \geq n. \tag{1.3}$$

Recently, progress has been made on obtaining quantitative results on counting the number fields in the above results. Let

$$\mathcal{N}_{m,n,s}(X) = \#\{k \subset \bar{\mathbb{Q}} \mid [k : \mathbb{Q}] = n, \operatorname{rk}_m \operatorname{Cl}(k) \geq s, |\operatorname{Disc}_{k/\mathbb{Q}}| < X\}.$$

Before the present paper, general results seem to have been proven only for $s = 1$ (of course, for m square-free, $\mathcal{N}_{m,n,1}(X)$ just counts number fields of degree n with class number divisible by m). The first such result, due to Murty [19], is that $\mathcal{N}_{m,2,1}(X) \gg X^{\frac{1}{2}+\frac{1}{m}}$. He also proved a result for real quadratic fields (in this direction see also [8], [18], and [32]). Soundararajan [26] improved Murty's result to $\mathcal{N}_{m,2,1}(X) \gg X^{\frac{1}{2}+\frac{2}{m}-\epsilon}$ if $m \equiv 0 \mod 4$ and $\mathcal{N}_{m,2,1}(X) \gg X^{\frac{1}{2}+\frac{3}{m+2}-\epsilon}$ if $m \equiv 2 \mod 4$, $m \neq 2$. For cubic fields, Hernández and Luca [12] proved $\mathcal{N}_{m,3,1}(X) \gg X^{\frac{1}{6m}}$. Bilu and Luca [4] improved on this, as the special case $n = 3$, giving the first result for every $n > 1$,

$$\mathcal{N}_{m,n,1}(X) \gg X^{\frac{1}{2m(n-1)}}. \tag{1.4}$$

In this paper we prove the following result.

Theorem 1.1. *Let $m, n > 1$ be positive integers. Let*

$$s_1 = \left\lfloor \frac{n}{2} \right\rfloor,$$
$$s_2 = \left\lceil \left\lfloor \frac{n+1}{2} \right\rfloor + \frac{n}{m-1} - m \right\rceil,$$

where $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$ are the greatest and least integer functions, respectively. Then

$$\mathcal{N}_{m,n,s_1}(X) \gg \frac{X^{\frac{1}{m(n-1)}}}{\log X}, \tag{1.5}$$

$$\mathcal{N}_{m,n,s_2}(X) \gg \frac{X^{\frac{1}{(m+1)n-1}}}{\log X}, \qquad \text{if } n > (m-1)^2. \tag{1.6}$$

The implied constants in Theorem 1.1 can, in principle, be effectively determined. Note that in (1.5), we improve on the exponent in Bilu and Luca's result (1.4) by essentially a factor of two, while enumerating number fields whose class groups have (provable) m-ranks as large as those of Azuhata and Ichimura. Furthermore, fixing m, for $n \gg 0$, (1.6) gives infinitely many number fields k of degree n with

$$\mathrm{rk}_m \mathrm{Cl}(k) \geq \frac{n}{2} + \frac{n}{m-1} + O(1).$$

For $m = 2$, we obtain infinitely many number fields k of degree $n > 1$ with

$$\mathrm{rk}_2 \mathrm{Cl}(k) \geq \frac{3n}{2} - 2.$$

So we obtain, for large enough n, an improvement on Nakano's inequalities (1.2) and (1.3).

Our proof of Theorem 1.1 relies on Hilbert's irreducibility theorem. We also give an alternative approach (yielding slightly different results) based on Diophantine finiteness results concerning integral points of bounded degree on curves. We now give a quick sketch of our technique. We start with a certain superelliptic curve C possessing a rational function ψ of degree n. Then we construct a curve Y and a covering $\pi : Y \to C$ that has the property that if $\pi(Q) = P$, $\psi(P) \in \mathbb{Z}$, then $[\mathbb{Q}(Q) : \mathbb{Q}]$ is bounded by a number depending only on $\mathrm{rk}_m \mathrm{Cl}(\mathbb{Q}(P))$. On the other hand, by Hilbert's irreducibility theorem, for most points $Q \in (\psi \circ \pi)^{-1}(\mathbb{Z})$, $[\mathbb{Q}(Q) : \mathbb{Q}] = \deg \psi \circ \pi$. Thus, combining these two statements, we obtain lower bounds on $\mathrm{rk}_m \mathrm{Cl}(\mathbb{Q}(P))$ for many points $P \in \psi^{-1}(\mathbb{Z})$. A similar argument, but using finiteness results on integral points of bounded degree on curves, yields a (weaker) lower bound on $\mathrm{rk}_m \mathrm{Cl}(\mathbb{Q}(P))$ for all but finitely many $P \in \psi^{-1}(\mathbb{Z})$.

2. Hilbert's irreducibility theorem and integral points of bounded degree on curves

The classical Hilbert irreducibility theorem states that for a number field k and an absolutely irreducible polynomial $f \in k[x, y]$, there exist infinitely many specializations $y_0 \in \mathbb{Z}$ such that $f(x, y_0)$ is irreducible over k. A quantitative geometric formulation of the theorem sufficient for our needs is as follows.

Theorem 2.1 (Hilbert irreducibility theorem)**.** *Let C be an irreducible nonsingular projective curve defined over a number field k. Let $f : C \to \mathbb{P}^1$ be a morphism defined over k. Then there exists $\epsilon > 0$ such that for all but $O(N^{1-\epsilon})$ values $n = 1, \ldots, N$, if $P \in f^{-1}(n)$ then $[k(P) : k] = \deg f$.*

In fact, it is known that one can take $\epsilon = \frac{1}{2}$ in Theorem 2.1 and that the constant in the $O(N^{1-\epsilon})$ in the theorem is effective and can be given quite

explicitly for $\epsilon < \frac{1}{2}$ (for these and more general and precise statements of Hilbert's irreducibility theorem, see [25, Ch. 9] and [9]).

With the hypotheses of Theorem 2.1, for each integer i let $P_i \in f^{-1}(i)$. Dvornicich and Zannier [10, 11] studied the degree of the field extension $\mathbb{Q}(P_1, \dots, P_N)$. Their results imply in particular a useful result on the number of isomorphism classes of number fields in the set $\{\mathbb{Q}(P_1), \dots, \mathbb{Q}(P_N)\}$.

Theorem 2.2 (Dvornicich, Zannier)**.** *Let C be an irreducible nonsingular projective curve defined over a number field k. Let $f : C \to \mathbb{P}^1$ be a morphism defined over k. For each integer i, let $P_i \in f^{-1}(i)$. Let $g(N)$ denote the number of isomorphism classes of number fields in the set $\{\mathbb{Q}(P_1), \dots, \mathbb{Q}(P_N)\}$. Then $g(N) \gg \frac{N}{\log N}$.*

An analysis of the proof in [10] shows that furthermore the implied constant in Theorem 2.2 is effective (for this one makes use of effective versions of Hilbert's irreducibility theorem, as mentioned above, and the prime number theorem).

Hilbert's irreducibility theorem is closely related to finiteness results on integral points on curves. We now recall two such results concerning integral points of bounded degree. Let C be an irreducible nonsingular projective curve defined over a number field k. Let ψ be a rational function on C defined over k. If $L \supset k$, there is a natural action of the Galois group $\mathrm{Gal}(\bar{L}/L)$ on the set of poles of ψ. Let Σ_L denote the set of orbits under this action. So $\Sigma_{\bar{k}}$ is just the set of poles of ψ. We denote by $\mathcal{O}_L$ the ring of integers of L. More generally, for a finite set of places S of L containing the archimedean places, we denote by $\mathcal{O}_{L,S}$ the ring of S-integers of L. A classical method of Runge allows one to effectively determine the S-integral points in $C(L)$ with respect to ψ if $|S| < |\Sigma_L|$. As noticed by Bombieri [5] (a related result had previously been proven by Sprindžuk [27]), in Runge's method one can even allow the field L and set of places S to vary. This yields the following theorem (this formulation is taken from [3]).

Theorem 2.3 (Bombieri, Runge, Sprindžuk)**.** *The set of points*

$$\bigcup_{\substack{L,S \\ |S|<|\Sigma_L|}} \{P \in C(L) \mid \psi(P) \in \mathcal{O}_{L,S}\}$$

is finite and can be effectively determined.

If S is the set of archimedean places of L, then $|S| \leq [L : \mathbb{Q}]$, and so Theorem 2.3 implies, for instance, that the set

$$\{P \in C(\bar{k}) \mid [\mathbb{Q}(P) : \mathbb{Q}] < |\Sigma_{\mathbb{Q}}|, \psi(P) \in \mathcal{O}_{\mathbb{Q}(P)}\}$$

is finite and can be effectively determined.

In [29], Vojta proved an inequality in Diophantine approximation which has as consequences both Falting's theorem on rational points on curves and

the Roth-Wirsing theorem in Diophantine approximation. Among further consequences of Vojta's inequality (see [17]), we have a result on integral points of bounded degree on curves.

Theorem 2.4 (Vojta)**.** *Let S be a finite set of places of k containing the archimedean places. If L is a finite extension of k, denote by S_L the set of places of L lying above places in S. The set of points*

$$\bigcup_{\substack{L\supset k\\ 2[L:k]<|\Sigma_{\bar{k}}|}} \{P\in C(L)\mid \psi(P)\in \mathcal{O}_{L,S_L}\}$$

is finite.

The finite set in Theorem 2.4 cannot, at present, be effectively determined. Since only the degree $[L:k]$, and not $|S|$, enters into Theorem 2.4, and since we can also take $k\neq\mathbb{Q}$ in the theorem, in general Theorem 2.4 will give better results than Theorem 2.3, at the loss of effectivity.

3. Proof of Theorem 1.1

We begin with a slightly more precise version of inequality (1.6) of Theorem 1.1.

Theorem 3.1. *Let $m,n>1$ be integers. Let $r>n$ be an integer such that $r-\lfloor\frac{r}{m}\rfloor\leq n$ and $(r,m)=1$. Then there exist effective constants $c_1,c_2>0$ such that if $X>c_1$, there are at least $c_2X^{\frac{1}{r(m-1)+n-1}}/\log X$ pairwise nonisomorphic number fields k with $[k:\mathbb{Q}]=n$, $|\operatorname{Disc}_{k/\mathbb{Q}}|<X$, and*

$$\operatorname{rk}_m \operatorname{Cl}(k)\geq r-\left\lfloor\frac{n+1}{2}\right\rfloor-\delta(m,n), \tag{3.1}$$

where $\delta(m,n)=1$ if m and n are both even, and $\delta(m,n)=0$ otherwise.

It is easy to see that for any $m,n>1$, there always exists $r\geq n+\frac{n}{m-1}-m+1$ such that $r-\lfloor\frac{r}{m}\rfloor\leq n$ and $(r,m)=1$. Note also that $n+\frac{n}{m-1}-m+1>n$ if $n>(m-1)^2$ and that $r-\lfloor\frac{r}{m}\rfloor\leq n$ implies $r(m-1)+n-1\leq(m+1)n-1$. Using these facts, (1.6) follows easily from Theorem 3.1.

The next lemma gives certain integers that will be needed in the proof of Theorem 3.1.

Lemma 3.1. *Let m and r be positive integers. Let T be the set of primes less than $mr+1$. There exist positive integers $a_1,\dots,a_r$ such that*

$$a_i\equiv 1 \mod p,\quad \forall p\in T, \tag{3.2}$$

and

$$\left(a_i, \prod_{j=2}^{r}(a_1^m + a_j^m) \prod_{2\le k<l\le r}(a_k^m - a_l^m)\right) = 1,$$

for $i = 1, \dots, r$.

Proof. We prove by induction that for $1 \le r' \le r$, there exist positive integers $a_1, \dots, a_{r'}$ satisfying (3.2) and

$$\left(a_i, \prod_{j=2}^{r'}(a_1^m + a_j^m) \prod_{2\le k<l\le r'}(a_k^m - a_l^m)\right) = 1$$

for all i. This is trivial for $r' = 1$. Suppose that we have constructed positive integers $a_1, \dots, a_{r'}$, $r' < r$, as above. We construct $a_{r'+1}$ as follows. Let T' be the set of primes dividing $\prod_{i=1}^{r'} a_i$ and T'' the set of primes dividing $\prod_{j=2}^{r'}(a_1^m + a_j^m)\prod_{2\le k<l\le r'}(a_k^m - a_l^m)$. Let $p \in T'$. By (3.2), we have $p > mr$. Since $r' < r$, it follows that there exists an integer b_p such that $b_p^m \not\equiv -a_1^m \mod p$ and $b_p^m \not\equiv a_i^m \mod p$ for $i = 2, \dots, r'$ (note also that $b_p \not\equiv 0 \mod p$). Now we simply choose $a_{r'+1} > 0$ so that $a_{r'+1} \equiv 1 \mod p$ for all $p \in T$, $a_{r'+1} \equiv b_p \mod p$ for all $p \in T'$, and $a_{r'+1} \equiv 1 \mod p$ for all $p \in T'' \setminus T'$. Then it is easily verified that $a_1, \dots, a_{r'+1}$ have the desired properties. □

We now define the curves and maps that are central to the proofs of Theorem 3.1 and later results. Let m, n, and r be as in Theorem 3.1. Let

$$h(x) = -(x - a_1^m)\prod_{i=2}^{r}(x + a_i^m),$$

with $a_1, \dots, a_r$ as in Lemma 3.1. Let C be the nonsingular affine plane curve defined by

$$y^m = h(x).$$

Let $\tilde{C}$ be a nonsingular projective closure of C. It follows from the condition $(r, m) = 1$ that there is a unique point in $\tilde{C} \setminus C$, which we will denote by ∞. Let $f(x)$ be the Taylor series for $\sqrt[m]{h(x)}$ at $x = 0$ truncated to degree $\lfloor \frac{r}{m} \rfloor - 1$ with $f(0) = \prod_{i=1}^{r} a_i$. Then $f(x)$ is defined over $\mathbb{Q}$ and

$$\operatorname{ord}_x\left(f(x)^m - h(x)\right) \ge \left\lfloor \frac{r}{m} \right\rfloor \ge r - n. \tag{3.3}$$

Let b be the lowest common denominator of the coefficients of f. Let ψ be the rational function on $\tilde{C}$ induced by the rational function

$$\frac{b(y - f)}{x^{r-n}}$$

on C.

Let Y be the nonsingular curve in $\mathbb{A}^r$ (with coordinates $x_1, \dots, x_r$) defined by

$$x_1^m + x_i^m = a_1^m + a_i^m, \quad 2 \le i \le r,$$
$$x_i^m - x_j^m = a_i^m - a_j^m, \quad 2 \le i < j \le r.$$

We have a covering of C by Y, $\pi : Y \to C$, given by

$$(x_1, \dots, x_r) \mapsto \left(-x_1^m + a_1^m, \prod_{i=1}^{r} x_i \right).$$

For our purposes, the key property of this covering is that, under appropriate conditions, for a point $P \in C(\bar{\mathbb{Q}})$, the degree $[\mathbb{Q}(Q) : \mathbb{Q}]$ for a point $Q \in \pi^{-1}(P)$ is controlled by the m-rank of the class group of $\mathbb{Q}(P)$.

For notational convenience, let $t_1 = -a_1^m$ and $t_i = a_i^m$ for $i = 2, \dots, r$.

Lemma 3.2. *Let $P = (x, y) \in C(k)$, for some number field k. Suppose that for all i,*

$$(x + t_i)\,\mathcal{O}_k = \mathfrak{a}_i^m \tag{3.4}$$

for some fractional ideal $\mathfrak{a}_i$ of $\mathcal{O}_k$. Let r_1 and r_2 be the number of real and complex places, respectively, of k. Let ζ be a generator for the group of roots of unity in k. Let $s = \operatorname{rk}_m \operatorname{Cl}(k)$. Let $Q \in \pi^{-1}(P)$. Then for some prime p dividing m,

$$[k(Q) : k] \le [k(\sqrt[p]{\zeta}) : k] m^{r-1} p^{r_1 + r_2 + s - r}$$

and $k(Q)$ has at most $\frac{1}{2}[k(\sqrt[p]{\zeta}) : \mathbb{Q}] m^{r-1} p^{r_1+r_2+s-r}$ archimedean places.

Proof. Let $\operatorname{ord}_p m$ denote the largest power of p dividing m. Let p be a prime dividing m such that $\operatorname{rk}_{p^{\operatorname{ord}_p m}} \operatorname{Cl}(k) = \operatorname{rk}_m \operatorname{Cl}(k) = s$. Let $G = \{[\mathfrak{a}]^{\frac{m}{p}} \mid [\mathfrak{a}] \in \operatorname{Cl}(k), [\mathfrak{a}]^m = 1\}$, a subgroup of $\operatorname{Cl}(k)$. Clearly, $G \cong (\mathbb{Z}/p\mathbb{Z})^s$. Let $\mathfrak{b}_i$, $i = 1, \dots, s$, be ideals whose ideal classes generate G. Then for each i, $\mathfrak{b}_i^p = (\beta_i)$ for some $\beta_i \in k$. Let $u_1, \dots, u_{r_1+r_2-1}, \zeta$ be generators for $\mathcal{O}_k^*$. Let $L = k(\sqrt[p]{\beta_1}, \dots, \sqrt[p]{\beta_s}, \sqrt[p]{u_1}, \dots, \sqrt[p]{u_{r_1+r_2-1}}, \sqrt[p]{\zeta})$. Let $Q = (x_1 \dots, x_r)$ with $\pi(Q) = P$. Note that

$$[L : k] \le [k(\sqrt[p]{\zeta}) : k] p^{r_1+r_2+s-1}$$

and L is totally imaginary. If $x_i^{\frac{m}{p}} \in L$ for all i, then $[L(Q) : L] \le \left(\frac{m}{p}\right)^{r-1}$ (note that $\prod_{i=1}^r x_i = y \in k \subset L$). Thus, to prove the lemma it suffices to show that $x_i^{\frac{m}{p}} \in L$ for all i.

It follows from the defining equations for Y and the definition of π that $x_1^m = -(x + t_1)$ and $x_i^m = x + t_i$ for $i \ge 2$. By hypothesis, $(x_i^m) = (x + t_i) = \mathfrak{a}_i^m$. Since $[\mathfrak{a}_i]^{\frac{m}{p}} \in G$,

$$\mathfrak{a}_i^{\frac{m}{p}} = (\alpha) \prod_{j=1}^{s} \mathfrak{b}_j^{c_j}$$

for some integers c_j and some element $\alpha \in k$. Therefore,

$$(x_i^m) = \left(\mathfrak{a}_i^{\frac{m}{p}}\right)^p = (\alpha^p) \prod_{j=1}^{s} \left(\beta_j^{c_j}\right).$$

So $x_i^m = u\alpha^p \prod_{j=1}^s \beta_j^{c_j}$ for some unit $u \in \mathcal{O}_k^*$. Therefore, $x_i^{\frac{m}{p}} = \alpha \sqrt[p]{u} \prod_{j=1}^s \sqrt[p]{\beta_j^{c_j}}$ for some choice of the p-th roots. So $x_i^{\frac{m}{p}} \in L$ for all i as desired. □

The condition (3.4) of Lemma 3.2 is satisfied for a large class of points of C. Let $\Delta(h) = \prod_{1 \le i < j \le r} (t_i - t_j)^2$ and let $\Delta(h)_0$ be the product of the primes dividing $\Delta(h)$.

Lemma 3.3. *There exists an integer c_0 such that if $c \in \mathbb{Z}$, $c \equiv c_0 \mod \Delta(h)_0$, and $(x, y) \in \psi^{-1}(c)$, then for all i, $(x + t_i)\,\mathcal{O}_{\mathbb{Q}(x)} = \mathfrak{a}_i^m$ for some fractional ideal $\mathfrak{a}_i$ of $\mathcal{O}_{\mathbb{Q}(x)}$.*

Proof. Let $\tilde{f} = bf \in \mathbb{Z}[x]$. We first claim that there exists a c_0 such that

$$(-t_i)^{r-n} c_0 \not\equiv -\tilde{f}(-t_i) \mod p \tag{3.5}$$

for $i = 1, \dots, r$ and all primes p dividing $\Delta(h)_0$. For $p < r + 1$, by (3.2) we have $a_i \equiv 1 \mod p$ for all i, and so for such p the condition (3.5) becomes $c_0 \not\equiv (-1)^{r-n+1}\tilde{f}(-1), -\tilde{f}(1) \mod p$. For $p < r + 1$, let b_p be such that $b_p \not\equiv (-1)^{r-n+1}\tilde{f}(-1), -\tilde{f}(1) \mod p$ (note that for $p = 2$, this is possible because $(-1)^{r-n+1}\tilde{f}(-1) \equiv -\tilde{f}(1) \bmod 2$). If $p > r$ and $p | \Delta(h)_0$, then by the pigeon-hole principle, there exists b_p such that $b_p \not\equiv -(-t_i)^{n-r}\tilde{f}(-t_i) \mod p$ for $i = 1, \dots, r$ (by construction, $p \nmid t_i$, so t_i is invertible mod p). Thus, we choose c_0 such that $c_0 \equiv b_p \mod p$ for all primes p dividing $\Delta(h)_0$.

We now show that this choice of c_0 works in the lemma. Suppose that $\psi(x_c, y_c) = c \equiv c_0 \mod \Delta(h)_0$. Note that by (3.3),

$$y_c^m + \prod_{i=1}^{r}(x_c + t_i) = \frac{\left(\tilde{f}(x_c) + cx_c^{r-n}\right)^m + b^m \prod_{i=1}^r (x_c + t_i)}{b^m} = \frac{x_c^{r-n}}{b^m} g_c(x_c) = 0, \tag{3.6}$$

where $g_c(x) \in \mathbb{Z}[x]$ and $\deg g_c = n$. So either $x_c = 0$, in which case the conclusion of the lemma is trivially true, or x_c satisfies $g_c(x_c) = 0$. If $g_c(x_c) = 0$, then $x = x_c + t_i$ satisfies $g_c(x - t_i) = 0$. From (3.6), the constant term of $g_c(x - t_i)$ is

$$g_c(-t_i) = \frac{1}{(-t_i)^{r-n}} \left(\tilde{f}(-t_i) + c(-t_i)^{r-n}\right)^m.$$

By our choice of c_0 and that $c \equiv c_0 \mod \Delta(h)_0$, it follows that $p \nmid g_c(-t_i)$ for all $p | \Delta(h)_0$. This obviously implies that $v_{\mathfrak{p}}(x_c + t_i) \le 0$ for all i and all

primes $\mathfrak{p}$ of $\mathcal{O}_k$ dividing $\Delta(h)_0$, where $k = \mathbb{Q}(x_c) = \mathbb{Q}(x_c, y_c)$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_k$ such that $v_\mathfrak{p}(x_c) < 0$. Then $v_\mathfrak{p}(x_c) = v_\mathfrak{p}(x_c + t_i)$ for all i. Thus $mv_\mathfrak{p}(y_c) = rv_\mathfrak{p}(x_c)$ and since $(r, m) = 1$, we have $m | v_\mathfrak{p}(x_c + t_i)$ for all i. Now let $\mathfrak{p}$ be a prime of $\mathcal{O}_k$ such that $v_\mathfrak{p}(x_c + t_j) > 0$ for some j. From the above, $\mathfrak{p} \nmid \Delta(h)_0$. If $i \neq j$ and $v_\mathfrak{p}(x_c + t_i) > 0$, then $\mathfrak{p} | (t_i - t_j)$, a contradiction. Since $y_c^m = -\prod_{i=1}^r (x_c + t_i)$, clearly we must have $m | v_\mathfrak{p}(x_c + t_j)$. It follows that for all i, $(x_c + t_i)\,\mathcal{O}_k = \mathfrak{a}_i^m$ for some fractional ideal $\mathfrak{a}_i$ of $\mathcal{O}_k$. □

We now compute the discriminants and numbers of real and complex places of the fields $\mathbb{Q}(P)$, $P \in \psi^{-1}(c)$, appearing in Lemma 3.3.

Lemma 3.4. *There exists a constant c' such that for $c > c'$, $c \in \mathbb{Z}$, if $P \in \psi^{-1}(c)$ then $\mathbb{Q}(P)$ has at most one real place if n is odd, at most two real places if m and n are even, and no real places in all other cases. Furthermore, for $P \in \psi^{-1}(c)$, $\mathrm{Disc}_{\mathbb{Q}(P)/\mathbb{Q}} = O(c^{r(m-1)+n-1})$.*

Proof. Let $\tilde{f}$ and g_c be as in the proof of Lemma 3.3. For $P = (x_c, y_c) \in \psi^{-1}(c)$, since $y_c = f(x_c) + \frac{c}{b} x_c^{r-n}$, $\mathbb{Q}(P) = \mathbb{Q}(x_c)$. Therefore, it suffices to study the roots of $g_c(x)$. Let

$$q_c(x) = \left(\tilde{f}(x) + cx^{r-n}\right)^m + b^m (x - a_1^m) \prod_{i=2}^r (x + a_i^m) = x^{r-n} g_c(x).$$

Looking at the expansion of q_c (note also that $r - m(r-n) > 0$), it is easy to see that

$$\lim_{c \to \infty} \frac{q_c\left(c^{\frac{m}{r-m(r-n)}} x\right)}{c^{\frac{mr}{r-m(r-n)}}} = b^m x^r + x^{m(r-n)}.$$

Therefore, using the continuity of the roots of a polynomial in terms of the coefficients, we see that $g_c(x)$ has roots $c^{\frac{m}{r-m(r-n)}} \alpha_i$ for $i = 1, \ldots, r - m(r-n)$, where each α_i tends to a different root of $b^m x^{r-m(r-n)} + 1$ as $c \to \infty$. In particular, for large enough c, at most one α_i is real if $r - m(r-n)$ is odd, and none of the α_i are real if $r - m(r-n)$ is even.

Recall that $\tilde{f}(0) = b \prod_{i=1}^r a_i$. A straightforward calculation shows that

$$\lim_{c \to \infty} g_c\left(\frac{1}{c^{\frac{1}{r-n}} x}\right) \frac{x^n}{c} = x^{r-m(r-n)} \left[\left(1 + bx^{r-n} \prod_{i=1}^r a_i\right)^m - b^m x^{m(r-n)} \prod_{i=1}^r a_i^m\right].$$

Arguing as before, $g_c(x)$ has roots $\frac{1}{c^{\frac{1}{r-n}} \beta_i}$ for $i = 1, \ldots, (m-1)(r-n)$, where each β_i tends to a different root of

$$\left(1 + bx^{r-n} \prod_{i=1}^r a_i\right)^m - b^m x^{m(r-n)} \prod_{i=1}^r a_i^m \tag{3.7}$$

as $c \to \infty$. Explicitly, the roots of (3.7) are given by the $(m-1)(r-n)$ values of

$$\left(\frac{1}{b(\zeta_m^j - 1)\prod_{i=1}^r a_i}\right)^{\frac{1}{r-n}}$$

for $j = 1, \dots, m-1$, where ζ_m is a primitive m-th root of unity. Therefore, for large enough c, at most one of the β_i is real if $r-n$ is odd and m is even, and otherwise none of the β_i are real. Note that $r - m(r-n) + (m-1)(r-n) = n$. Therefore, for large c, we have described all n roots of $g_c(x)$. The statement about the real places of $\mathbb{Q}(P)$ follows.

As for the statement on $\mathrm{Disc}_{\mathbb{Q}(P)/\mathbb{Q}}$, let $x_1, \dots, x_n$ be the n roots of $g_c(x)$. Then the above calculations show that in the product $\prod_{1 \le i < j \le n}(x_i - x_j)^2$, there are $2\binom{(m-1)(r-n)}{2}$ factors of order $O(c^{\frac{1}{n-r}})$, and the remaining $2\binom{n}{2} - 2\binom{(m-1)(r-n)}{2}$ of the factors are $O(c^{\frac{m}{r-m(r-n)}})$. We have

$$\frac{2}{n-r}\binom{(m-1)(r-n)}{2} + \frac{2m}{r-m(r-n)}\left(\binom{n}{2} - \binom{(m-1)(r-n)}{2}\right) = r(m-1) + n - 1.$$

Since $m(r-n) < r$, the leading coefficient of $g_c(x)$ does not depend on c. It follows that for $P \in \psi^{-1}(c)$, $\mathrm{Disc}_{\mathbb{Q}(P)/\mathbb{Q}} = O(c^{r(m-1)+n-1})$. □

Let $\tilde{Y}$ be a nonsingular projective closure of Y.

Lemma 3.5. *Let $P_i = (0, \zeta_m^i \prod_{j=1}^r a_j) \in C \subset \tilde{C}$ for $i = 0, \dots, m-1$, where ζ_m is a primitive m-th root of unity. Then the divisor of poles of ψ is given by*

$$(r - m(r-n))\,\infty + \sum_{i=1}^{m-1}(r-n)P_i.$$

In particular, $\deg \psi = n$. *The rational function $\psi \circ \pi$ has degree nm^{r-1} and m^r distinct poles on $\tilde{Y}$, all defined over $\mathbb{Q}(\zeta_{2m})$, where ζ_{2m} is a primitive $2m$-th root of unity.*

Proof. Indeed, since $(y-f)(P_i) \neq 0$ for $i = 1, \dots, m-1$, plainly ψ has a pole of order $r-n$ at P_i for $i = 1, \dots, m-1$. Using the identity

$$\frac{b(y-f)}{x^{r-n}} = \frac{\sum_{i=0}^{m-1} f^i y^{m-1-i}}{\sum_{i=0}^{m-1} f^i y^{m-1-i}} \cdot \frac{b(y-f)}{x^{r-n}} = \frac{b(h-f^m)}{x^{r-n}\sum_{i=0}^{m-1} f^i y^{m-1-i}},$$

and Eq. (3.3), we see that ψ doesn't have a pole at P_0. A similar calculation shows that $\mathrm{ord}_\infty x = -m$ and $\mathrm{ord}_\infty y = -r$. Since $\deg f = \lfloor \frac{r}{m} \rfloor - 1$ and $m(\lfloor \frac{r}{m} \rfloor - 1) < r$,

$$\mathrm{ord}_\infty \frac{b(y-f)}{x^{r-n}} = \mathrm{ord}_\infty \frac{y}{x^{r-n}} = -(r - m(r-n)).$$

So ψ has a pole of order $r - m(r-n)$ at ∞.

For the last assertion, it suffices to show that each of the $m-1$ points P_i, $i = 1, \dots m-1$, and the point at ∞ on $\tilde{C}$ pull back by π to m^{r-1} distinct points on $\tilde{Y}$, all defined over $\mathbb{Q}(\zeta_{2m})$. Explicitly, $P_1, \dots, P_{m-1}$ pull back to the $(m-1)m^{r-1}$ points $(\mu_1 a_1, \dots, \mu_r a_r) \in Y \subset \tilde{Y}$ with $\mu_i^m = 1$ for all i and $\prod_{i=1}^r \mu_i \neq 1$. The point at infinity on $\tilde{C}$ pulls back to the m^{r-1} points at infinity in $\tilde{Y} \setminus Y$ (which are all defined over $\mathbb{Q}(\zeta_{2m})$). □

We now have all of the ingredients to prove Theorem 3.1. Let c_0 and c' be as in Lemmas 3.3 and 3.4. Let L be the field over $\mathbb{Q}$ generated by all roots of unity appearing in any number field of degree n over $\mathbb{Q}$. Let

$$\mathcal{C} = \{c \in \mathbb{Z} \mid c > c', c \equiv c_0 \bmod \Delta(h)_0, [L(P) : L] = n, \forall P \in \psi^{-1}(c)\}$$

and let

$$\mathcal{C}(M) = \{c \in \mathcal{C} \mid c < M\}.$$

Proof of Theorem 3.1. By Lemma 3.5, $\psi \circ \pi$ gives a rational function of degree nm^{r-1} on $\tilde{Y}$. By Hilbert's irreducibility theorem, for all but $O(M^{1-\epsilon})$ values $c \in \mathcal{C}(M)$, if $\psi(\pi(Q)) = c$, then $[\mathbb{Q}(\zeta_{2m})(Q) : \mathbb{Q}(\zeta_{2m})] = nm^{r-1}$. Furthermore, if $P = \pi(Q)$, note that ± 1 are the only roots of unity in $\mathbb{Q}(P)$ and $[\mathbb{Q}(P) : \mathbb{Q}] = n$. Therefore, by Lemmas 3.2, 3.3, and 3.4, if $\psi(\pi(Q)) = c$, $P = \pi(Q)$, $c \in \mathcal{C}$, then $\mathbb{Q}(P)$ has $\left\lfloor \frac{n+1}{2} \right\rfloor + \delta(m,n)$ archimedean places and

$$[\mathbb{Q}(\zeta_{2m})(Q) : \mathbb{Q}(\zeta_{2m})] \leq nm^{r-1} p^{\mathrm{rk}_m \mathrm{Cl}(\mathbb{Q}(P)) + \left\lfloor \frac{n+1}{2} \right\rfloor + \delta(m,n) - r}$$

for some prime p dividing m. Therefore, for all but $O(M^{1-\epsilon})$ values $c \in \mathcal{C}(M)$, if $\psi(P) = c$, then $\mathrm{rk}_m \mathrm{Cl}(\mathbb{Q}(P)) \geq r - \left\lfloor \frac{n+1}{2} \right\rfloor - \delta(m,n)$.

It remains only to count the number of isomorphism classes of number fields in the set

$$F(M) = \{\mathbb{Q}(P) \mid P \in C, \psi(P) = c, c \in \mathcal{C}(M)\}.$$

Since ψ has degree n by Lemma 3.5, by Hilbert's irreducibility theorem, the set $\mathcal{C}(M)$ has cardinality $\frac{1}{\Delta(h)_0} M + O(M^{1-\epsilon})$. Furthermore, by Theorem 2.2 (applied to ψ composed with an appropriate automorphism of $\mathbb{P}^1$) there are $\gg \frac{M}{\log M}$ isomorphism classes of number fields in $F(M)$. By Lemma 3.4, the fields in $F(M)$ have discriminant $O(M^{r(m-1)+n-1})$. Thus, letting $M = X^{\frac{1}{r(m-1)+n-1}}$ gives the enumerative statement in the theorem. □

Alternatively, we can prove a result along the lines of Theorem 3.1 using results on integral points of bounded degree on curves. Let

$$R_s = \{P \in Y \mid \psi(\pi(P)) = c, c \in \mathcal{C}, \mathrm{rk}_m \mathrm{Cl}(\mathbb{Q}(\pi(P))) < s\}.$$

The proof of Theorem 3.1 using Hilbert's irreducibility theorem shows that if $s = r - \left\lfloor \frac{n+1}{2} \right\rfloor - \delta(m,n)$, then R_s does not contain many elements (of bounded height, say) relative to R_∞. If

$$s = r - \left\lfloor \frac{n+1}{2} \right\rfloor - \max_{\substack{p \mid m \\ p \text{ prime}}} \log_p \frac{n\phi(2m)}{2m} - \delta(m,n), \tag{3.8}$$

then we show that in fact R_s is finite. Here ϕ is Euler's totient function and $\log_p$ denotes the logarithm to base p.

Theorem 3.2. *Let s be as in* (3.8)*. Then R_s is finite and can be effectively determined.*

Proof. As in the proof of Theorem 3.1, by Lemmas 3.2, 3.3, and 3.4, for all $P \in R_s$,

$$[\mathbb{Q}(\zeta_{2m})(P) : \mathbb{Q}] < \phi(2m) n m^{r-1} \max_{\substack{p \mid m \\ p \text{ prime}}} p^{s + \left\lfloor \frac{n+1}{2} \right\rfloor + \delta(m,n) - r}$$

and $\mathbb{Q}(\zeta_{2m})(P)$ has strictly less than

$$\frac{\phi(2m)n}{2} m^{r-1} \max_{\substack{p \mid m \\ p \text{ prime}}} p^{s + \left\lfloor \frac{n+1}{2} \right\rfloor + \delta(m,n) - r}$$

archimedean places. By Lemma 3.5, $\psi \circ \pi$ has m^r distinct poles, all defined over $\mathbb{Q}(\zeta_{2m})$. Note also that R_s is a set of integral points with respect to $\psi \circ \pi$. Therefore, by Theorem 2.3 (applied to $\tilde{Y}$ and $\psi \circ \pi$), we see that R_s will be finite and effectively determinable if

$$m^r \geq \frac{\phi(2m)n}{2} m^{r-1} \max_{\substack{p \mid m \\ p \text{ prime}}} p^{s + \left\lfloor \frac{n+1}{2} \right\rfloor + \delta(m,n) - r},$$

or equivalently, if

$$s \leq r - \left\lfloor \frac{n+1}{2} \right\rfloor - \max_{\substack{p \mid m \\ p \text{ prime}}} \log_p \frac{n\phi(2m)}{2m} - \delta(m,n).$$

□

To obtain an effective result, we applied Theorem 2.3 in Theorem 3.2. If instead we had used Vojta's Theorem 2.4 (with $k = \mathbb{Q}(\zeta_{2m})$), at the loss of effectivity, the $\log_p \frac{n\phi(2m)}{2m}$ term in (3.8) could be replaced by $\log_p \frac{2n}{m}$ (giving a minor improvement in some cases). A similar statement applies to Theorem 3.4.

To finish the proof of Theorem 1.1, it remains to prove inequality (1.5). The proof is similar to the proof of Theorem 3.1, so we will only note the differences.

Theorem 3.3. *Let $m, n > 1$ be integers. Then there exist effective constants $c_1, c_2 > 0$ such that if $X > c_1$, there are at least $c_2 X^{\frac{1}{m(n-1)}} / \log X$ pairwise nonisomorphic number fields k with $[k : \mathbb{Q}] = n$, $|\operatorname{Disc}_{k/\mathbb{Q}}| < X$, and*

$$\operatorname{rk}_m \operatorname{Cl}(k) \geq \left\lfloor \frac{n}{2} \right\rfloor. \tag{3.9}$$

Proof. The proof follows the proof of Theorem 3.1 with $r = n$, $\psi = y$, and $f = 0$, with the following differences. The main point is that the condition $(r, m) = 1$ of Theorem 3.1 can be dropped in this case. The condition $(r, m) = 1$ was used only at the end of the proof of Lemma 3.3 in the case where $v_{\mathfrak{p}}(x_c) < 0$. If $\psi = y$ and $(x_c, y_c) \in \psi^{-1}(c)$, $c \in \mathbb{Z}$, then x_c satisfies $h(x) - c^m$ and is therefore an algebraic integer. But now the part of the proof of Lemma 3.3 where $v_{\mathfrak{p}}(x_c) < 0$ is unnecessary, and so we no longer need the condition $(r, m) = 1$. The other differences are that the δ term in (3.1) is no longer necessary and the correct change in the discriminant bound in Lemma 3.4 is $\operatorname{Disc}_{\mathbb{Q}(P)/\mathbb{Q}} = O(c^{m(n-1)})$ (these two statements are easy to directly verify). □

As a final application of our technique, we prove a theorem which implies, in particular, that there are number fields k of degree n with $\operatorname{rk}_n \operatorname{Cl}(k)$ arbitrarily large. To obtain a cofiniteness result, we use the integral points approach of Theorem 3.2.

Theorem 3.4. *Let $n > 1$ be a positive integer. Let $f(x) = \pm \prod_{i=1}^{r} (x - a_i)$ be a polynomial with $a_1, \ldots, a_r$ distinct integers. Let*

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

For $x \in T$, let $r_1(x)$ denote the number of real places of $\mathbb{Q}\left(\sqrt[n]{f(x)}\right)$. Then for all but finitely many (effectively determinable) $x \in T$,

$$\operatorname{rk}_n \operatorname{Cl}\left(\mathbb{Q}\left(\sqrt[n]{f(x)}\right)\right) \geq r - \frac{n + r_1(x)}{2} - \max_{\substack{p \mid n \\ p \text{ prime}}} \log_p \frac{n\phi(2m)}{2}.$$

Proof. Apply the proof of Theorem 3.2 (with appropriate minor changes) to the curve $y^n = f(x)$ with the rational function $\psi = x$ and the set $\mathcal{C} = T$. □

The set T in Theorem 3.4 can be infinite or empty depending on f. For general monic f, one can similarly prove a result about $\operatorname{rk}_n \operatorname{Cl}\left(k\left(\sqrt[n]{f(x)}\right)\right)$, where k is the splitting field of f. Theorem 3.4 fits into a series of general results [7, 6, 24] giving information on $\operatorname{Cl}(k)$ in terms of the ramification behavior of primes in $\mathcal{O}_k$.

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] F. Beukers and S. Tengely, *An implementation of Runge's method for Diophantine equations*. Preprint.

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

[5] E. Bombieri, *On Weil's "théorème de décomposition"*. Amer. J. Math. **105** (1983), no. 2, 295–308.

[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] 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).

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

[10] 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.

[11] R. Dvornicich and U. Zannier, *Fields containing values of algebraic functions. II. (On a conjecture of Schinzel)*. Acta Arith. **72** (1995), no. 3, 201–210.

[12] 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.

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

[14] H. Ichimura, *On* 2*-rank of the ideal class groups of totally real number fields*. Proc. Japan Acad. Ser. A Math. Sci. **58** (1982), no. 7, 329–332.

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

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

[17] A. Levin, *Vojta's inequality and rational and integral points of bounded degree on curves*. Compos. Math. **143** (2007), no. 1, 73–81.

[18] 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.

[19] 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.

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

[21] T. Nagell, *Collected papers of Trygve Nagell. Vol. 1*. Queen's Papers in Pure and Applied Mathematics, vol. 121, Queen's University, Kingston, ON, 2002.

[22] S. Nakano, *On the construction of certain number fields*. Tokyo J. Math. **6** (1983), no. 2, 389–395.

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

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

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

[26] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*. J. London Math. Soc. (2) **61** (2000), no. 3, 681–690.
[27] V. G. Sprindžuk, *Reducibility of polynomials and rational points on algebraic curves*. Dokl. Akad. Nauk SSSR **250** (1980), no. 6, 1327–1330.
[28] K. Uchida, *Class numbers of cubic cyclic fields*. J. Math. Soc. Japan **26** (1974), no. 3, 447–453.
[29] P. Vojta, *A generalization of theorems of Faltings and Thue-Siegel-Roth-Wirsing*. J. Amer. Math. Soc. **5** (1992), no. 4, 763–804.
[30] P. J. Weinberger, *Real quadratic fields with class numbers divisible by n*. J. Number Theory **5** (1973), no. 3, 237–241.
[31] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*. Osaka J. Math. **7** (1970), 57–76.
[32] G. Yu, *A note on the divisibility of class numbers of real quadratic fields*. J. Number Theory **97** (2002), no. 1, 35–44.

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