EXPONENTS OF CLASS GROUPS OF QUADRATIC FIELDS

M. Ram Murty[1]

Dedicated to the memory of Sarvadaman Chowla

Abstract

Given a positive integer $g \geq 2$, we would like to study the number of real and imaginary quadratic fields that have an element of order g in their ideal class group. Conjectures of Cohen and Lenstra predict a positive probability for such an event. Our goal here is to derive quantitative results in this direction. We establish for $g \geq 3$, the number of imaginary quadratic fields whose absolute discriminant is $\leq x$ and whose class group has an element of order g is $\gg x^{\frac{1}{2}+\frac{1}{g}}$. For g odd we show that the number of real quadratic fields whose discriminant is $\leq x$ and whose class group has an element of order g is $\gg x^{1/2g-\epsilon}$ for any $\epsilon > 0$. (The implied constant may depend on ϵ.)

Introduction. Given a positive integer $g \geq 2$, we would like to study the number of real and imaginary quadratic fields that have an element of order g in their ideal class group. Conjectures of Cohen and Lenstra [CL] predict a positive probability for such an event. Indeed, if $g = p$ is an odd prime, then in the case of imaginary quadratic fields, they forecast that

$$1 - \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^i}\right)$$

as the probability that an imaginary quadratic field has an element of order p in the class group. In the real quadratic case, their prediction is

$$1 - \prod_{i=2}^{\infty} \left(1 - \frac{1}{p^i}\right)$$

as the corresponding probability.

Qualitative results in this line of thought have a long history. The case $g = 2$ is classical work of Gauss. The case $g = 3$ was studied by Davenport and Heilbronn [DH]. Earlier, Nagell [N], Honda [H], Ankeny and Chowla [AC], Hartung [Ha], Yamamoto [Y] and Weinberger [W] derived the infinitude of such fields, for any given g.

[1] *Research partially supported by NSERC.*
AMS Classification. 11R29 11R11 11N36

Our goal here is to derive quantitative results in this direction. In an earlier paper [RM], we indicated how one can use the ABC conjecture to show that at least $\gg x^{1/g-\epsilon}$ imaginary quadratic fields with absolute discriminant $\leq x$ have an element of order g in their class group. In the real quadratic case, we obtained a lower bound of $\gg x^{1/2g-\epsilon}$ for the number of such fields.

In this paper, we will establish stronger results *without* the ABC conjecture. We will prove:

Theorem 1. *Let $g \geq 3$. The number of imaginary quadratic fields whose absolute discriminant is $\leq x$ and whose class group has an element of order g is $\gg x^{\frac{1}{2}+\frac{1}{g}}$.*

Theorem 2. *Let g be odd. The number of real quadratic fields whose discriminant is $\leq x$ and whose class group has an element of order g is $\gg x^{1/2g-\epsilon}$ for any $\epsilon > 0$. (The implied constant may depend on ϵ.)*

Theorem 2 is still valid if g is even and not divisible by 4 and we briefly indicate how to derive this at the end of the proof of Theorem 2. If g is divisible by 4, the argument of Theorem 2 gives us $\gg x^{1/4g-\epsilon}$ real quadratic fields with discriminant $< x$ and whose class group contains an element of exponent g.

A lot of work has centered around the complementary question of finding class groups not divisible by g. For example, the recent work of Kohnen and Ono [KO] and Ono [O] shows that for all odd primes ℓ, there are $\gg \sqrt{x}/\log x$ imaginary quadratic fields with discriminants $|D| \leq x$ with $\ell \not| h(D)$ where $h(D)$ denotes the class number of the field.

Here is a brief outline of the method. In the imaginary quadratic case, our strategy is to consider numbers of the form

$$m^g - n^2$$

with $2X^{1/g} < m < 3X^{1/g}$ and $X^{1/2} < n < 2X^{1/2}$. Then,

$$3^g X > m^g - n^2 > 2^g X - 4X \geq 4X$$

since $g \geq 3$. Since the probablity that a random number is squarefree is $6/\pi^2$, one expects a positive proportion of such (m, n) with m and n in the stated range. This idea is made precise using the sieve of Eratosthenes in section 2. Hence, it is therefore reasonable to expect $\gg X^{1/2+1/g}$ numbers of the form

$$d = m^g - n^2$$

which are squarefree. It is then not difficult to show that in $\mathbb{Q}(\sqrt{-d})$, the ideal $(n+\sqrt{-d})$ is the g-th power of an ideal which has order g in the ideal class group of that field. Finally, we make a count of how many distinct numbers d arise in this fashion and show there are not too many repetitions. This is how Theorem 1 is derived.

For the real quadratic case, the strategy is different. We modify an argument of Weinberger to first establish that if $D = n^{2g} + 4$ and $n > g$ is prime, then with suitable restrictions, the ideal $(n^2, 2+\sqrt{D})$ has order g or $g/2$ in the ideal class group of $\mathbb{Q}(\sqrt{D})$. One then counts the number of distinct real quadratic fields that arise in this way by making use of a classical result of Sprindzuk on the number of integral points on certain hyper-elliptic curves.

2. Squarefree values of quadratic polynomials.

Let $f(n) = n^2 + c$ with c an integer. We will need the following elementary lemma.

Lemma 1. *Let p be an odd prime. If $p \not| c$, then the congruence $n^2 + c \equiv 0 (\mod p^2)$ has at most 2 solutions. If $p|c$, and $p^2 \not| c$, there are no solutions. If $p^2|c$, then $p|n$, so there are p solutions mod p^2. If $p = 2$, there are either 2 solutions or no solutions according as $c \equiv 0, -1 (\mod 4)$ or not.*

Proof. The congruence $n^2 + c \equiv 0 (\mod p)$ has at most two solutions mod p. If n_0 mod p is a solution, then we begin by counting how many lifts it has to mod p^2. Indeed, suppose

$$(n_0 + tp)^2 \equiv -c (\mod p^2)$$

then,

$$\frac{n_0^2 + c}{p} + 2n_0 t \equiv 0 (\mod p).$$

This has a unique solution $t (\mod p)$ provided $p \not| 2c$. Therefore, if $p \not| 2c$, then there are at most 2 solutions to the congruence $n_0^2 + c \equiv 0 (\mod p^2)$. The last three assertions are obvious.

Lemma 2. *Let d be an odd squarefree number and denote by $\rho_c(d^2)$ the number of solutions of the congruence $n^2 + c \equiv 0 (\mod d^2)$. Then*

$$\rho_c(d^2) \leq 2^{\nu(d)} \gamma(c)$$

where $\nu(d)$ denotes the number of distinct prime divisors of d and $\gamma(c)$ is the product of the distinct primes dividing c.

Proof. By the Chinese remainder theorem, $\rho_c(m)$ is a multiplicative function of m. By Lemma 1, $\rho_c(p^2) \leq 2$ if $p \not| 2c$. If $p|c$, then $\rho_c(p^2) \leq p$ again by Lemma 1. Therefore,

$$\rho_c(d^2) \leq 2^{\nu(d)}\gamma(c),$$

as desired.

Lemma 3. *Let $\nu(m)$ denote the number of distinct prime divisors of m. Then,*

$$\sum_{m<T} \nu(m) = T \log\log T + O(T).$$

Proof. The sum is clearly bounded by

$$\sum_{p<T} \frac{T}{p}$$

and by the elementary formula

$$\sum_{p<T} \frac{1}{p} = \log\log T + \mathrm{O}(1)$$

the result is now immediate.

Let $S(x, y; c)$ enumerate the number of $x < n < y$ such that $f(n) = n^2 + c$ is squarefree. For each squarefree d, let $\rho_c(d)$ be the number of solutions of the congruence

$$n^2 + c \equiv 0(\bmod d).$$

We will also introduce

$$P(z) = \prod_{p \leq z} p,$$

where the product is over primes less than or equal to z. Observe that by elementary number theory, namely Chebychev's theorem, we have

$$P(z) < e^{\kappa z},$$

for some constant κ.

Theorem 3. *If $|c| < y$, then*

$$S(x,y;c) \geq (y-x)\frac{\phi(c)}{c}\prod_{p}\Big(1-\frac{2}{p^2}\Big) + \mathrm{O}\Big(\frac{y\nu(c)}{\log y}\Big),$$

where ϕ denotes Euler's function.

Proof. It is clear that

$$S(x,y;c) \leq \sum_{x<n<y}\sum_{d^2|(n^2+c,P(z)^2)}\mu(d).$$

On the other hand, let $N_p(x,y;c)$ to be the number of n satisfying $x<n<y$ and $p^2|n^2+c$. Then,

$$S(x,y;c) \geq \sum_{x<n<y}\sum_{d^2|(n^2+c,P(z)^2)}\mu(d) - \sum_{z<p<y+|c|}N_p(x,y;c).$$

By Lemma 1, we know that

$$N_p(x,y;c) \leq 2\Big(\frac{y}{p^2}+1\Big)$$

if $p\not|\,2c$. Again by Lemma 1, we have

$$N_p(x,y;c) \leq \frac{y}{p}$$

if $p|c$. Therefore (for $z \geq 2$),

$$\sum_{z<p<y+|c|}N_p(x,y;c) \ll \sum_{z<p<y+|c|,p\not|\,c}\Big(\frac{y}{p^2}+1\Big) + \sum_{z<p<y+|c|,p|c}\frac{y}{p}.$$

Observe that

$$\sum_{z<p<y+|c|,p|c}\frac{y}{p} \leq \frac{y}{z}\nu(c)$$

and that

$$\sum_{z<p<y+|c|,p\not|\,c}\Big(\frac{y}{p^2}+1\Big) \ll \frac{y}{z}+\frac{y}{\log y}.$$

Therefore, for $|c|<y$, we have

$$\begin{aligned}
S(x,y;c) &\geq \sum_{x<n<y}\sum_{d^2|(n^2+c,P(z)^2)}\mu(d) - \sum_{z<p<y+|c|}N_p(x,y;c)\\
&\geq \sum_{d|P(z)}\mu(d)\sum_{\substack{x<n<y\\ n^2+c\equiv 0 \pmod{d^2}}} 1 + \mathrm{O}(y\nu(c)/z) + \mathrm{O}(y/\log y)\\
&= \sum_{d|P(z)}\mu(d)\Big\{\frac{y-x}{d^2}\rho_c(d^2) + O(\rho_c(d^2))\Big\} + \mathrm{O}(y\nu(c)/z + y/\log y).
\end{aligned}$$

We will choose $z = \kappa \log y$ for some appropriate constant $\kappa > 0$. Then the error term above is $\mathrm{O}(y\nu(c)/\log y)$. Since $\rho_c(d^2) \le \gamma(c)2^{\nu(d)}$ by Lemma 2, we find

$$\sum_{d|P(z)} \rho_c(d^2) \le \gamma(c) \sum_{d \le P(z)} 2^{\nu(d)}.$$

The elementary estimate

$$\sum_{d \le w} 2^{\nu(d)} \ll w \log w$$

yields the result

$$S(x,y;c) \ge (y-x) \sum_{d|P(z)} \frac{\mu(d)}{d^2} \rho_c(d^2) + O(y^{\kappa(1+\epsilon)}) + \mathrm{O}(y\nu(c)/\log y).$$

We will choose κ sufficiently small, so that this quantity is

$$\ge (y-x) \sum_{d|P(z)} \frac{\mu(d)}{d^2} \rho_c(d^2) + O(y\nu(c)/\log y).$$

The sum can be written as a product:

$$\sum_{d|P(z)} \frac{\mu(d}{d^2} \rho_c(d^2) = \prod_{p \le z} \Big(1 - \frac{\rho_c(p^2)}{p^2}\Big) \ge \frac{\phi(c)}{c} \prod_p \Big(1 - \frac{2}{p^2}\Big)$$

by an application of Lemma 2. This completes the proof of Theorem 3.

We now apply Theorem 3 to $c = -m^g$, m odd and consider those m, n satisfying

$$X^{1/2} < n < 2X^{1/2}, \quad 2X^{1/g} < m < 3X^{1/g}$$

so that the number of squarefree values in the sequence

$$m^g - n^2$$

is

$$\gg X^{1/2} \sum_{\substack{2X^{1/g} < m < 3X^{1/g} \\ m \ odd}} \frac{\phi(m)}{m} + O(\frac{X^{\frac{1}{g}+\frac{1}{2}} \log\log X}{\log X}),$$

by an application of Lemma 3 in estimating the error term. Since

$$\sum_{m \le T, m \ odd} \frac{\phi(m)}{m} = \sum_{d \le T, d \ odd} \frac{\mu(d)}{d} \Big[\frac{T}{d}\Big] = \sum_{d \le T, d \ odd} \frac{\mu(d)}{d} \Big(\frac{T}{d} + \mathrm{O}(1)\Big) = \frac{8}{\pi^2} T + \mathrm{O}(\log T),$$

we deduce that there are $\gg X^{1/2+1/g}$ squarefree values $\leq X$ that are of the form $m^g - n^2$ with m, n in the specified ranges and m odd. Let us signal for future use the important fact that for these m, n, we have $4X \leq (2^g - 4)X \leq m^g - n^2 \leq (3^g - 1)X$.

3. Proof of Theorem 1.

For each of the $\gg X^{1/2+1/g}$ squarefree values of $m^g - n^2$ produced in the previous section, we consider the factorization

$$m^g = (n + \sqrt{-d})(n - \sqrt{-d})$$

in $\mathbb{Q}(\sqrt{-d})$. Recall that in the construction of the previous section, m is odd. Since d is squarefree, m and n are coprime for otherwise the square of a prime will divide $m^g - n^2$ and hence d. Also, if the ideals $(n + \sqrt{-d})$ and $(n - \sqrt{-d})$ are not coprime, then any common factor must divide 2 which implies m is even, which is not the case, by construction. Therefore, each of the ideals $(n + \sqrt{-d})$ and $(n - \sqrt{-d})$ must be a perfect g-th power. Thus,

$$\mathfrak{a}^g = (n + \sqrt{-d})$$

for some ideal $\mathfrak{a}$ of norm m. If $\mathfrak{a}$ has order $r \leq g - 1$ (say), then

$$\mathfrak{a}^r = (u + v\sqrt{-d}) \quad \text{or} \quad (\frac{u + v\sqrt{-d}}{2}).$$

Observe that $v \neq 0$ for otherwise $\mathfrak{a}$ and $\mathfrak{a}'$, the conjugate ideal would have a common factor, which is not the case. Hence, taking norms of both sides of the above equation,

$$3^{g-1} X^{(g-1)/g} \geq m^{g-1} \gg d = m^g - n^2 \geq 4X$$

a contradiction for sufficiently large X. This produces an element of order g in the ideal class group.

We now count the number of distinct squarefree numbers in the enumeration above. Indeed, let S be the set of squarefree d's counted above which appear twice in the list. Then we have for each $d \in S$,

$$d = m_1^g - n_1^2 = m_2^g - n_2^2$$

for $(m_1, n_1) \neq (m_2, n_2)$. This means

$$m_1^g - m_2^g = n_1^2 - n_2^2 = (n_1 - n_2)(n_1 + n_2).$$

For fixed m_1, m_2, the choices for n_1 and n_2 are derived from the divisors of $m_1^g - m_2^g$. It is an elementary fact of number theory that the number of divisors of a number n is $O(n^\epsilon)$. Thus, the number of divisors of $m_1^g - m_2^g$ cannot exceed $O(X^\epsilon)$. The number of possible values of m_1 and m_2 are $O(X^{2/g})$ and therefore the total number of elements in S cannot exceed $O(X^{2/g+\epsilon})$. The final enumeration gives

$$\gg X^{1/2+1/g} - O(X^{2/g+\epsilon})$$

distinct squarefree values of $d < X$ such that the class group of $\mathbb{Q}(\sqrt{-d})$ has an element of order g. Since $g \geq 3$, this completes the proof of Theorem 1.

4. An effective version of Weinberger's theorem.

We will begin by making a result of Weinberger effective. In [W], it is proved that:

Proposition. Let $D = n^{2g} + 4$.

(i) If $n > g$ is prime and $\mathbb{Q}(\sqrt{D}) \neq \mathbb{Q}(\sqrt{5})$, then the fundamental unit of $\mathbb{Q}(\sqrt{D})$ is $(n^g + \sqrt{D})/2$.

(ii) Suppose that the polynomial $T^k - 4$ is irreducible mod n for every divisor k of g. Then, the ideal $\mathfrak{a} = (n^2, 2 + \sqrt{D})$ has order g if g is odd, or $g/2$ if g is even, in the ideal class of group of $\mathbb{Q}(\sqrt{D})$.

For the sake of completeness, we will indicate the proof of the Proposition. Let r and s be integers and ρ_1, ρ_2 the roots of

$$T^2 - rT - s = 0.$$

Define $c_j(r,s) = \rho_1^j + \rho_2^j$. Let

$$\alpha = \frac{n^g + \sqrt{D}}{2}.$$

Then, $N(\alpha) = -1$ and $\alpha > 1$. If $\epsilon > 1$ denotes the fundamental unit of $\mathbb{Q}(\sqrt{D})$, then $\alpha = \epsilon^j$ for some odd j. Since $\epsilon > 1$, we have $r = Tr(\epsilon) = \epsilon + \epsilon^{-1} > 0$ and the minimal polynomial of ϵ is

$$T^2 - rT - 1, \quad r > 0.$$

Then

$$n^g = Tr(\alpha) = Tr(\epsilon^j) = \rho_1^j + \rho_2^j = c_j(r,1)$$

where ρ_1 and ρ_2 are zeros of $T^2 - rT - 1 = 0$. Thus,

$$c_j(r,1) - n^g = 0.$$

It is not difficult to see that

$$c_j(r,s) = \sum_{\nu=0}^{j/2} f_\nu r^{j-2\nu} s^\nu$$

for integers f_ν. Moreover, when j is odd, $f_{(j-1)/2} = j$ and $f_0 = 1$. In addition, let us observe that if $r, s > 1$, then $c_j(r,s) > r^j$ as an easy computation shows. Thus, $r | c_j(r,1)$ and so $r | n^g$. If $r = 1$, then $\epsilon = (1+\sqrt{5})/2$ contrary to hypothesis. Since n is prime, $r = n^k$ for some $k \leq g$. By the observation above, $n^g = c_j(r,1) \geq r^j = n^{jk}$ and so $jk \leq g$. Since $n > g$ is prime, it follows that $(j,n) = 1$ since $j \leq g$. As j is odd, $c_j(r,1)/r \equiv j (\mod n)$ by what we have said above. We conclude that $c_j(r,1)/r$ is coprime to n so that $n^{g-k} = 1$. Thus, $g = k$ and $j = 1$ as desired. This proves (i).

To prove (ii), we consider the ideal

$$\mathfrak{a} = (n^2, 2 + \sqrt{D}).$$

Now,

$$\mathfrak{a}^g = (n^{2g}, n^{2g-2}(2+\sqrt{D}), \cdots, (2+\sqrt{D})^g)$$

which is easily seen to be

$$(\sqrt{D}+2)(\sqrt{D}-2, n^{2g-2}, \cdots, (\sqrt{D}+2)^{g-1}).$$

This means that $\mathfrak{a}^g \subseteq (2+\sqrt{D})$ while $N(\mathfrak{a}^g) = n^{2g} = N((2+\sqrt{D})$. Hence, $\mathfrak{a}^g = (2+\sqrt{D})$. It is then not difficult to show that in fact, the order of $\mathfrak{a}$ in the ideal class group is g when g is odd and $g/2$ when g is even whenever n is prime and the polynomial $T^k - 4$ is irreducible mod n for every divisor k of g.

5. Proof of Theorem 2.

We will now prove Theorem 2. We will need the following lemma.

Lemma. *The number of primes $p < x$ such that the polynomial $T^k - 4$ is irreducible mod p is $\gg x/\log x$.*

Proof. Let K be the splitting field of the polynomial T^k-4. Let $L=\mathbb{Q}(\zeta_k)$ and consider the Galois extension K/L. By the Chebotarev density theorem, there are $\gg x/\log x$ prime ideals $\mathfrak{p}$ of first degree with absolute norm $\leq x$ in L such that T^k-4 is irreducible mod $\mathfrak{p}$. This completes the proof.

Now suppose g is odd. To apply the effective Weinberger theorem, we must ensure that n is a prime such that T^k-4 is irreducible mod n for every $k|g$. Using the Chebotarev density theorem, one can show that the number of $n<X^{1/2g}$ such that $T^{2g}-4$ is irreducible mod n is $\gg X^{1/2g}/\log X$. This immediately implies that T^k-4 is irreducible mod n for every $k|2g$. Thus, for each of these values of n, the class group of $\mathbb{Q}(\sqrt{n^{2g}+4})$ has an element of order g provided $\mathbb{Q}(\sqrt{n^{2g}+4})\neq\mathbb{Q}(\sqrt{5})$. First, let us observe that the number of integral solutions of

$$5y^2=x^{2g}+4$$

is absolutely bounded (by a classical theorem of Siegel). This eliminates only a finite set of values of n from our consideration. We now need to count the number of distinct quadratic fields obtained in this way. This means, for a fixed d, we need to count the number of integral solutions of $dy^2=n^{2g}+4$ which is a hyper-elliptic curve. By a result of Sprindzuk [S] or Evertse - Silverman [ES], we find that the number of such n cannot exceed $C^{\nu(d)}$ for some absolute constant C, where $\nu(d)$ denotes the number of prime factors of d. Since the number of prime factors of d cannot exceed

$$\ll\frac{\log d}{\log\log d}$$

by a classical estimate of Ramanujan, we immediately deduce that the number of distinct quadratic fields among $\mathbb{Q}(\sqrt{n^{2g}+4})$ is $\gg X^{1/2g-\epsilon}$. This completes the proof of Theorem 2.

We remark that the above theorem is also valid if $g=2r$ with r odd. Indeed, if $g/2$ is odd then, the argument of Weinberger used above gives us an element of order g or $g/2$. If a positive proportion of the fields we have above have an element of order g then we are done. Otherwise, let us suppose that we have $\gg X^{1/2g}/\log X$ fields with an element of order $g/2$. If the discriminant of a quadratic field is not prime, we have (by genus theory) an element of order 2 in the class group which we can multiply to an element of order $g/2$ which is odd, to get an element of order g. By an elementary sieve estimate, we know that the number of $n<X^{1/2g}$ with n prime and $n^{2g}+4$ a prime power is $\ll X^{1/2g}/\log^2 X$.

Since this is negligible compared to the number of fields we have, namely $\gg X^{1/2g}/\log X$, we can now proceed as above and derive our estimate.

If g is divisible by 4, then it is clear that our argument produces at least $\gg X^{1/4g-\epsilon}$ real quadratic fields with an element of exponent g in the class group.

6. Concluding remarks.

All of the above results can be generalized to the function field case with better results in the analogue of the real quadratic case and this work will appear in the joint paper [CM]. Even sharper results can be obtained if one only considers quadratic extensions of $\mathbb{F}_p$ generated by the square root of either cubic or quartic polynomials. This is because of the obvious connection to elliptic curves. In fact, the connection beautifully intertwines the Lang-Trotter conjectures for primitive points of elliptic curves over function fields over finite fields with the Cohen-Lenstra conjectures. This work will appear jointly with Rajiv Gupta in [GM]. Finally we mention related work of Jiang Yu [Yu] which establishes the Cohen-Lenstra conjecture as $p\to\infty$ and fixed discriminantal degree. We are of course interested in the orthogonal direction, namely with p fixed and the discriminantal degree tending to ∞.

REFERENCES

[AC] N. Ankeny and S. Chowla, On the divisibility of the class numbers of quadratic fields, *Pacific Journal of Math.,* **5** (1955) p. 321-324.

[CL] H. Cohen and H.W. Lenstra Jr., Heuristics on class groups of number fields, *Springer Lecture Notes,* **1068** in Number Theory Noordwijkerhout 1983 Proceedings.

[CM] D. Cardon and M. Ram Murty, Exponents of class groups of quadratic fields of function fields over finite fields, in preparation.

[DH] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Royal Soc., A* **322** (1971) p. 405 - 420.

[ES] J.-H. Evertse and J.H. Silverman, Uniform bounds for the number of solutions to $Y^n = f(x)$, *Math. Proc. Camb. Phil. Soc.,* **100** (1986) p. 237-248.

[GM] R. Gupta and M. Ram Murty, Class groups of quadratic function fields, in preparation.

[Ha] P. Hartung, Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3, *J. Number Theory,* **6**(1974), 276-278.

[H] T. Honda, A few remarks on class numbers of imaginary quadratic fields, *Osaka J. Math.,* **12** (1975), 19-21.

[Ho] C. Hooley, Applications of sieve methods, *Cambridge Tracts in Mathematics,* 1976.

[KO] W. Kohnen and K. Ono, Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication, to appear in *Inventiones Math.*

[MMS] M. Ram Murty, V. Kumar Murty and N. Saradha, Modular forms and the Chebotarev density theorem, *Amer. J. Math.,* **110** (1988), no. 2, p. 253-281.

[RM] M. Ram Murty, The ABC conjecture and exponents of quadratic fields, *Contemporary Math.***210,** (1997) pp. 85-95, in Number Theory, edited by V. Kumar Murty and Michel Waldschmidt, Amer. Math. Soc., Providence.

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

[O] K. Ono, Indivisibility of class numbers of real quadratic fields, preprint.

[S] V.G. Sprindzuk, On the number of solutions of the Diophantine equation $x^3 = y^2 + A$ (in Russian), *Dokl. Akad. Nauk. BSSR* **7** (1963) p. 9-11.

[W] P. Weinberger, Real Quadratic Fields with Class Numbers Divisible by n, *Journal of Number Theory,* **5** (1973) p. 237-241.

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

[Yu] Jiu-Kang Yu, Toward the Cohen-Lenstra conjecture in the function field case, preprint.

Department of Mathematics,
Queen's University,
Kingston, Ontario,
K7L 3N6, Canada
murty@mast.queensu.ca