Journal of Number Theory **97**, 35–44 (2002)
doi:10.1006/jnth.2001.2773

A Note on the Divisibility of Class Numbers of Real Quadratic Fields

Gang Yu

Department of Mathematics, The University of Michigan, Ann Arbor, Michigan 48109
E-mail: gyu@math.lsa.umich.edu

Communicated by D. Goss

Received April 4, 2001

Suppose $g > 2$ is an odd integer. For real number $X > 2$, define $S_g(X)$ the number of squarefree integers $d \leqslant X$ with the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ being divisible by g. By constructing the discriminants based on the work of Yamamoto, we prove that a lower bound $S_g(X) \gg X^{1/g-\varepsilon}$ holds for any fixed $\varepsilon > 0$, which improves a result of Ram Murty.

Key Words: quadratic fields; class numbers; binary forms.

1. INTRODUCTION

In this note, we prove a quantitative result concerning the divisibility of class numbers of real quadratic fields. More precisely, let $g \geqslant 2$ be a positive integer, and $X > 3$ a real number, we shall give a lower bound for the number of fundamental discriminants $D \leqslant X$, with the class group of $\mathbb{Q}(\sqrt{D})$ having an element of order g.

There have been numerous qualitative results about divisibility of class numbers of quadratic fields (cf. [7], [1], [3], etc.). In particular, for the real quadratic field case, Weinberger [10] and Yamamoto [11] independently showed that, for any $g \geqslant 2$, there are infinitely many real quadratic fields with class number divisible by g. For the complementary question, Ono [8] proved that, for p a prime, $3 < p < 5000$, there are $\gg \sqrt{X}(\log X)^{-1}$ fundamental discriminants $D \leqslant X$ such that p does not divide the class number of $\mathbb{Q}(\sqrt{D})$.

For prime p, the "Cohen–Lenstra Heuristics" [2] suggests that the probability that the class number of a real quadratic field is divisible by p is

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

This implies that a positive proportion of real quadratic fields contain a non-trivial p-part in the class group. The probabilistic model also suggests that,

0022-314X/02 $35.00

for any fixed positive integer g, a positive proportion of real quadratic fields have a subgroup of order g in the class group.

Murty [5, 6] considered the quantitative version of this problem. He proved the following theorem.

THEOREM 1 (Murty [6]). *Let g be odd. The number of real quadratic fields whose discriminant is $\leqslant X$ and whose class group has an element of order g is $\gg x^{1/2g-\varepsilon}$ for any $\varepsilon > 0$.*

Murty proved the above theorem based on Weinberger's construction of discriminants. To get a better quantitative result, one would expect to make use of a construction similar to that of Soundararajan [9] in dealing with the imaginary quadratic fields case. Some invincible difficulty, however, arises in this case due to lack of control over the size of the fundamental unit.

Yamamoto [11] constructed the discriminant in a different way. To make the role of the fundamental unit implicit, every discriminant is requested to have two different representations by a special binary polynomial. Although this may not be a natural method, it enables us to prove a better quantitative result.

THEOREM 2. *Let g be odd. For any $\varepsilon > 0$, the number of real quadratic fields with discriminant $\leqslant X$ and class number divisible by g is $\gg X^{1/g-\varepsilon}$ for any $\varepsilon > 0$.*

Henceforth, we suppose $\varepsilon < 10^{-2}$ is a fixed positive real number. As usual, for real number t, $\{t\}$ denotes the fractional part of t and $||t|| \coloneqq \min\{\{t\}, 1-\{t\}\}$; $e(t) = \exp(2\pi i t)$; for integer k, we write $\tau(k)$ to denote the usual divisor function.

2. PRELIMINARY LEMMAS

Throughout this section, g is an odd integer with factorization

$$g = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k},$$

where $p_1, p_2, \ldots, p_k$ are distinct primes and $\delta_j \geqslant 1$ for $1 \leqslant j \leqslant k$. For every j $(1 \leqslant j \leqslant k)$, we fix two distinct primes l_j and l_j' such that $l_j \equiv l_j' \equiv 1 \pmod{p_j}$.

Before we construct our discriminant, we state a result of Yamamoto [11].

LEMMA 3. *Let y, z, y', z' be a non-trivial solution of the Diophantine equation*

$$Y^2 - 4Z^g = Y'^2 - 4Z'^g \tag{2.1}$$

such that

(i) $(y, z) = (y', z') = 1$;
(ii) $l_j \mid z$ *and* $l'_j \mid z'$;
(iii) y (*resp.* y') *is not a* p_j*th power residue modulo* l_j, (*resp.* l'_j), $(1 \leqslant j \leqslant k)$;
(iv) $\frac{y+y'}{2}$ *is a* p_j*th power residue modulo* l_j, $(1 \leqslant j \leqslant k)$.

Then the ideal class group of the field

$$F := \mathbb{Q}(\sqrt{y^2 - 4z^g})$$

has a subgroup N *such that*

$$N \cong \begin{cases} \mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/g\mathbb{Z} & \text{if } D < -4, \\ \mathbb{Z}/g\mathbb{Z} & \text{if } D > 0, \end{cases}$$

where D *is the discriminant of* F.

With Lemma 3, we shall consider a family of special quadratic fields. First of all, for any prime factor p_j of g, we notice that there are infinitely many primes $l_j \equiv 1 \pmod{p_j}$ such that 2 is a p_jth power residue modulo l_j and 3 is not. For each p_j $(1 \leqslant j \leqslant k)$, we fix two such primes l_j, l'_j such that we have $2k$ distinct primes $\{l_1, \ldots, l_k, l'_1, \ldots, l'_k\}$.

Set

$$\alpha := \prod_{j=1}^{k} l_j, \quad \beta := \prod_{j=1}^{k} l'_j \quad \text{and} \quad \Omega := 4\alpha\beta. \tag{2.2}$$

Suppose we have the fixed triplet (α, β, Ω).

LEMMA 4. *For* a, b *two positive integers satisfying*

$$a \equiv \alpha \pmod{\Omega}, \qquad b \equiv \beta \pmod{\Omega}, \tag{2.3}$$

let

$$d := \tfrac{3}{4}(3a^g + b^g)(a^g + 3b^g). \tag{2.4}$$

Then the class number of $\mathbb{Q}(\sqrt{d})$ *is divisible by* g.

Proof. Suppose $(a, b) = t$, and we write

$$a' = \frac{a}{t}, \quad b' = \frac{b}{t}, \quad d' = \frac{d}{t^{2g}}.$$

Then we have

$$\begin{aligned} d' &= (2(a'^g + b'^g) + (a'^g - b'^g)/2)^2 - 4a'^{2g} \\ &= (2(a'^g + b'^g) - (a'^g - b'^g)/2)^2 - 4b'^{2g}. \end{aligned} \tag{2.5}$$

Write

$$\begin{aligned} y &= 2(a'^g + b'^g) + (a'^g - b'^g)/2, \\ y' &= 2(a'^g + b'^g) - (a'^g - b'^g)/2, \\ z &= a'^2, \quad z' = b'^2. \end{aligned}$$

Then from (2.5), (y, z, y', z') gives a non-trivial solution of the Diophantine equation (2.1). We note that $(y, z) = (y', z') = 1$, that

$$l_1 l_2 \cdots l_k \mid z. \quad l'_1 l'_2 \cdots l'_k \mid z'$$

from $(t, \Omega) = 1$, also that, for any j $(1 \leqslant j \leqslant k)$, we have

$$y \equiv \tfrac{3}{2} b'^g \pmod{l_j}, \qquad y' \equiv \tfrac{3}{2} a'^g \pmod{l'_j}$$

and

$$\frac{y + y'}{2} \equiv 2b'^g \pmod{l_j}.$$

Thus, according to our choice of $\{l_j\}$, $\{l'_j\}$, all the conditions in Lemma 3 are satisfied, whence the class number of $\mathbb{Q}(\sqrt{d'})(= \mathbb{Q}(\sqrt{d}))$ is divisible by g. ∎

Before we end this section, we introduce an estimate of Greaves [4] about lattice point distribution. For any pair of integers (s, t), we denote

$$||(s, t)|| := \max\{|s|, |t|\}. \tag{2.6}$$

For integer r and $\omega \in (\mathbb{Z}/r\mathbb{Z})^\times$, we denote

$$M_0 = M_0(r, \omega) := \min_{\substack{a \equiv \omega b \pmod r \\ a \neq 0}} ||(a, b)||. \tag{2.7}$$

A simple argument with the Box Principle shows that $M_0(r, \omega) \leqslant \sqrt{r}$.

LEMMA 5. *The number $N_\omega(r; S, T)$ of pairs (s, t) for which*

$$s \leqslant S, \quad t \leqslant T$$

and

$$s \equiv \omega t \pmod{r}$$

satisfies

$$N_\omega(r; S, T) \leqslant \frac{ST}{r} + O\left(\frac{S+T}{M_0(r,\omega)}\right).$$

Proof. This is Lemma 1 of Greaves [4].

3. TWO ESTIMATES

Throughout this section, P is a sufficiently large real number, $M = P^{2-(3/2)\varepsilon}$. Also, $f(a,b)$ and $F(a,b)$ are the binary forms defined by

$$f(a,b) \coloneqq (3a^g + b^g), \qquad F(a,b) \coloneqq f(a,b)f(b,a). \tag{3.1}$$

We shall estimate the number of integers representated by $F(a,b)$ in a range which satisfy some additional restrictions.

We note that, from Chebotarev's density theorem, the subset of primes q for which 3 is a gth power residue constitutes a positive proportion of all primes. Thus there exist $\gg P^{2-(3/2)\varepsilon}(\log P)^{-3}$ integers m satisfying

$$M < m = q_1 q_2 q_3 \leqslant 8M, \tag{3.2}$$

where q_1, q_2 and q_3 are primes subject the condition

$$P^{2/3-(1/2)\varepsilon} < q_1 < q_2 < q_3 \leqslant 2P^{2/3-(1/2)\varepsilon} \tag{3.3}$$

and also satisfying the condition that 3 be a gth power residue modulo q_j, $j = 1, 2, 3$.

Henceforth, the letter m always stands for an integer satisfying the above conditions. By $r(m)$ we denote the number of pairs (a,b) with $\Omega P < a, b \leqslant 2\Omega P$, for which $F(a,b)$ is divisible by m, and for which (2.3) is satisfied. We also write

$$S_1(P) \coloneqq \sum_{M < m \leqslant 8M} r(m),$$

and

$$S_2(P) \coloneqq \sum_{M < m \leqslant 8M} r^2(m).$$

LEMMA 6. *One has*

$$S_2(P) \ll P^{2+2\varepsilon}.$$

Proof. From Lemma 5, we have

$$\begin{aligned} S_2(P) &= \sum_{M<m\leqslant 8M} \left(\sum_{\substack{\Omega P<a,b\leqslant 2\Omega P \\ (a,b)\equiv(\alpha,\beta) \pmod{\Omega} \\ F(a,b)\equiv 0 \pmod{m}}} 1 \right)^2 \\ &\ll \sum_{M<m\leqslant 8M} \sum_{f(\omega,1)\equiv 0 \pmod{m}} N^2_{-\omega}(m;\Omega P,\Omega P) \\ &\ll \sum_{M<m\leqslant 8M} \sum_{f(\omega,1)\equiv 0 \pmod{m}} \left(\frac{P^4}{m^2} + \frac{P^2}{M_0^2(m,-\omega)} \right) \\ &\ll \sum_{M<m\leqslant 8M} \sum_{f(\omega,1)\equiv 0 \pmod{m}} \frac{P^2}{M_0^2(m,-\omega)} + \frac{P^4}{M}. \end{aligned} \tag{3.4}$$

Note from the definition of $M_0(m,\omega)$, we have

$$\begin{aligned} &\sum_{M<m\leqslant 8M} \sum_{f(\omega,1)\equiv 0 \pmod{m}} \frac{P^2}{M_0^2(m,-\omega)} \\ &\ll P^2 \sum_{M<m\leqslant 8M} \sum_{f(\omega,1)\equiv 0 \pmod{m}} \sum_{s\leqslant\sqrt{M}} \frac{1}{s^2} \sum_{\substack{|r|\leqslant s \\ (r+\omega s)(s+\omega r)\equiv 0 \pmod{m}}} 1 \\ &\ll P^2 \sum_{M<m\leqslant 8M} \sum_{s\leqslant\sqrt{M}} \frac{1}{s^2} \sum_{\substack{|r|\leqslant s \\ F(r,s)\equiv 0 \pmod{m}}} 1 \\ &\ll P^{2+\varepsilon} \sum_{s\leqslant\sqrt{M}} \frac{1}{s^2} \sum_{|r|\leqslant s} 1 \ll P^{2+2\varepsilon}, \end{aligned} \tag{3.5}$$

which, along with (3.4), proves the lemma. ∎

LEMMA 7. *One has*

$$S_1(P) \gg P^2(\log P)^{-3}.$$

Proof. First, we note that

$$S_1(P) \geqslant \sum_{M<m\leqslant 8M} \sum_{\omega^g\equiv 3 \pmod m} \sum_{\substack{\Omega P<a,b\leqslant 2\Omega P \\ (a,b)\equiv(\alpha,\beta) \pmod\Omega \\ a+\omega b\equiv 0 \pmod m}} 1. \tag{3.6}$$

By abuse of notation, we replace a and b in the sum, respectively, by $a\Omega+\alpha$ and $b\Omega+\beta$ to get rid of the restriction $(a,b)\equiv(\alpha,\beta) \pmod\Omega$. Then we have

$$S_1(P) \geqslant \sum_{M<m\leqslant 8M} \sum_{\omega^g\equiv 3 \pmod m} \sum_{P<b<2P} \sum_{\substack{P<a<2P \\ a\equiv -\omega b-\bar{\Omega}(\alpha+\omega\beta) \pmod m}} \phi(a), \tag{3.7}$$

where, for convenience, we have added a sufficiently smooth weight function $\phi(a)$ supported on $[P,2P]$ such that

$$0\leqslant\phi(\xi)\leqslant 1 \quad \text{on } [P,2P] \quad \text{and} \quad \phi(t)=1 \quad \text{on } [P/2,3P/2], \tag{3.8}$$

$$\phi^{(j)}(t) \ll_j P^{-j}, \quad j=1,2,3,\ldots, \tag{3.9}$$

and

$$\phi^{(j)}(P)=\phi^{(j)}(2P)=0, \quad j=0,1,2,\ldots,K_\varepsilon \tag{3.10}$$

for some sufficiently large K_ε. Now from (3.7) and Poisson's summation formula, we have

$$\begin{aligned} S_1(P) \geqslant & \sum_{M<m\leqslant 8M} \sum_{\omega^g\equiv 3 \pmod m} \sum_{P<b<2P} \frac{1}{m} \\ & \times \sum_h \hat{\phi}\left(\frac{h}{m}\right) e\left(\frac{h(\omega b+\bar{\Omega}(\alpha+\omega\beta))}{m}\right), \end{aligned} \tag{3.11}$$

where $\hat{\phi}$ is the Fourier transform of ϕ. It is easy to see that the contribution of the terms with $h=0$ is

$$\gg P\hat{\phi}(0) \sum_m \frac{1}{m} \gg P^2(\log P)^{-3}. \tag{3.12}$$

Thus, to prove the lemma, it suffices to show that the other terms gives a contribution of $O(P^2(\log P)^{-4})$. Let

$$H := MP^{-1+\varepsilon/3}.$$

We first note that, from (3.8) to (3.10), integrating by parts, the terms with $|h| > H$ give a negligible contribution. Hence, to prove the lemma, it suffices to show that the sum

$$\Sigma_2(P) := \sum_{M<m\leqslant 8M} \frac{1}{m} \times \sum_{\omega^g\equiv 3 \pmod m} \sum_{P<b<2P} \sum_{0<|h|\leqslant H} \hat{\phi}\left(\frac{h}{m}\right) e\left(\frac{h(\omega b + \bar{\Omega}(\alpha+\omega\beta))}{m}\right) \quad (3.13)$$

is bounded by $O(P^2(\log P)^{-4})$.

Summing over b, we see that

$$\begin{aligned}\Sigma_2(P) &\ll \frac{P}{M} \sum_{m,\omega} \sum_{0<|h|\leqslant H} \min\left\{P, \frac{1}{||h\omega/m||}\right\} \\ &\ll \frac{P^2}{M} \sum_{m,\omega} \sum_{\substack{0<|h|\leqslant H \\ ||h\omega/m||<P^{-1}}} 1 + \frac{P}{M} \sum_{m,\omega} \sum_{\substack{0<|h|\leqslant H \\ ||h\omega/m||\geqslant P^{-1}}} \frac{1}{||h\omega/m||} \\ &= \Sigma_{21}(P) + \Sigma_{22}(P) \qquad \text{say.} \end{aligned} \quad (3.14)$$

From Lemma 5, we have

$$\begin{aligned}\Sigma_{21}(P) &\ll \frac{P^2}{M} \sum_{m,\omega} \sum_{0<|h|\leqslant H} \sum_{\substack{|c|\leqslant 8M/P \\ c\equiv\omega h \pmod m}} 1 \\ &\ll \frac{P^2}{M} \sum_{m,\omega} \left(\frac{MH}{mP} + \frac{MP^{-1}+H}{M_0(m,\omega)}\right) \\ &\ll HP \sum_m \frac{1}{m} + \frac{HP^2}{M} \sum_{|s|<3\sqrt{M}} \frac{1}{|s|} \sum_{|r|\leqslant s} \tau(F(r,s)) \\ &\ll P^{2-\varepsilon/4}. \end{aligned} \quad (3.15)$$

Again, from Lemma 5, we have

$$\begin{aligned}\Sigma_{22}(P) &\ll \frac{P}{M} \sum_{m,\omega} \sum_{mP^{-1}<c\leqslant m/2} \frac{m}{c} \sum_{\substack{0<|h|\leqslant H \\ c\equiv\omega h \pmod m}} 1 \\ &\ll P \sum_{MP^{-1}<C=2^j\leqslant 4M} \frac{1}{C} \sum_{m,\omega} N_\omega(m; H, 2C) \end{aligned} \quad (3.16)$$

$$\ll P \sum_{MP^{-1} < C = 2^j \leqslant 4M} \frac{1}{C} \sum_{m,\omega} \left(\frac{HC}{m} + \frac{H + C}{M_0(m, \omega)} \right)$$

$$\ll HP(\log P)^{-2} + \frac{HP^2 \log P}{M} \sum_{m,\omega} \frac{1}{M_0(m, \omega)}$$

$$\ll P^{2-\varepsilon} + P^{1+\varepsilon/2} \sqrt{M} \ll P^{2-\varepsilon/2}.$$

By combining estimates (3.15) and (3.16), we have completed the proof. ∎

4. PROOF OF THE THEOREM

From Lemmas 6 and 7, we have

$$\binom{3g+1}{3}^{-1} \sum_{\substack{M < m \leqslant 8M \\ r(m) > 0}} \frac{1}{r(m)} \gg \frac{S_1(P)^3}{S_2(P)^2} \gg P^{2-5\varepsilon}. \tag{4.1}$$

We note that, from our construction of the integers m, the left-hand side of (4.1) gives a lower bound for the cardinality of a set $\mathscr{D}(P)$ which satisfies:

(1) $\mathscr{D}(P) \in [12P^{2g}, 12(2P)^{2g}]$;
(2) every $d \in \mathscr{D}(P)$ is divisible by some m and is given by the form (2.4) for some a, b satisfying (2.3);
(3) if $d_1, d_2 \in \mathscr{D}(P)$ are distinct, then g.c.d.(d_1, d_2) is not divisible by any m.

For every $d \in \mathscr{D}(P)$, we write $d = d_0 f^2$ such that d_0 is squarefree. Suppose $\mathscr{D}'(P)$ is the subset of $\mathscr{D}(P)$ consist of the elements d with d_0 divisible by some m. Then, from our constructions (3.2) and (3.3), it is easy to see that

$$|\mathscr{D}'(P)| = |\mathscr{D}(P)| + O(P^{4/3+\varepsilon}) \gg P^{2-5\varepsilon}. \tag{4.2}$$

We conclude that, up to $12(2P)^{2g}$, there are $\gg P^{2-5\varepsilon}$ integers d, with distinct squarefree part, satisfying the conditions of Lemma 4. Setting

$$P = \frac{1}{2}\left(\frac{X}{12}\right)^{1/2g},$$

we have proved Theorem 2.

ACKNOWLEDGMENTS

The greatest gratitude goes to Professor Trevor Wooley for his encouragement and several valuable conversations with the author.

REFERENCES

1. N. Ankeny and S. Chowla, On the divisibility of the class numbers of quadratic fields, *Pacific J. Math.* **5** (1955), 321–324.
2. H. Cohen and H. W. Lenstra, "Heuristics on Class Groups of Number Fields," Springer Lecture Notes, *in* Number Theory Noordwijkerhout 1983 Proceedings, Vol. 1068, Springer, Berlin.
3. H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc.* A **322** (1971), 405–420.
4. G. Greaves, Power-free values of binary forms, *Quart. J. Math. Oxford* (2) **43** (1992), 45–65.
5. M. R. Murty, The *ABC* conjecture and exponents of quadratic fields, *Contemp. Math.* **210,** (1997), 85–95; *in* "Number Theory," (V. K. Murty and M. Waldschmidt Eds.), Amer. Math. Soc., Providence, RI.
6. M. R. Murty, Exponents of class groups of quadratic fields, *in* "Topics in Number Theory, (University Park, PA, 1997)," pp. 229–239, Mathematical Applications, Vol. 467, Kluwer Acad. Publ., Dordrecht, 1999.
7. T. Nagell, Über die Klassenzahl imaginar quadratischer Zahlkörper, *Abh. Math. Seminar Univ. Hamburg* **1** (1922), 140–150.
8. K. Ono, Indivisibility of class numbers of real quadratic fields, *Compositio Math.* **119,** no. 1, (1999), 1–11.
9. K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc.* (2) **61** (2000), 681–690.
10. P. Weinberger, Real quadratic fields with class numbers divisible by n, *J. Number Theory* **5** (1973), 237–241.
11. Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* **7** (1970), 57–76.