Imaginary quadratic fields with noncyclic ideal class groups

Dongho Byeon

School of Mathematical Sciences, Seoul National University, Seoul, Korea
e-mail: dhbyeon@math.snu.ac.kr

Abstract. Let g be an odd positive integer and X be a positive real number. We shall show that for any $\epsilon > 0$, the number of imaginary quadratic fields with discriminant $\geq -X$ and ideal class group having a subgroup isomorphic to $\mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/g\mathbb{Z}$ is $\gg X^{1/g-\epsilon}$.

Key words: Imaginary quadratic fields, noncyclic ideal class group

2000 Mathematics Subject Classification: 11R11, 11R29

1 Introduction and statement of result

Numerous results about divisibility of class numbers of quadratic fields are known by many authors (cf. [1], [4], [7], [8], [9], [10], [11], [12]). The best known quantitative result for imaginary quadratic fields is;

> (Soundararajan [9]) *If $g \geq 3$ is an odd positive integer, then the number of imaginary quadratic fields whose absolute discriminant is $\leq X$ and whose ideal class group has an element of order g is $\gg X^{\frac{1}{2}+\frac{1}{g}-\epsilon}$, for any $\epsilon > 0$.*

and for real quadratic fields is;

> (Yu [12]) *If $g \geq 3$ is an odd positive integer, then the number of real quadratic fields whose absolute discriminant is $\leq X$ and whose ideal class group has an element of order g is $\gg X^{\frac{1}{g}-\epsilon}$, for any $\epsilon > 0$.*

Under the assumption that ideal class group of quadratic field is quite rarely noncyclic, Cohen and Lenstra [2] predict a postive probability of such an event.

On the other hand, Yamamoto [11] proved that for any odd positive integer $g \geq 3$, there are infinitely many imaginary quadratic fields with ideal class group having a subgroup isomorphic to $\mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/g\mathbb{Z}$. For real quadratic fields, less is known except the case $g = 3$, 5, 7 due to Craig [3] and Mestre [5] [6].

However it seems that there is no known quantitative result about the number of quadratic fields whose ideal class groups is not cyclic. The aim of this note is to give a lower bound for this number.

Theorem *Let g be an odd positive integer and X be a positive real number. For any $\epsilon > 0$, the number of imaginary quadratic fields with discriminant $\geq -X$ and ideal class group having a subgroup isomorphic to $\mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/g\mathbb{Z}$ is $\gg X^{1/g-\epsilon}$.*

The theorem will be obtained by a straightforward modification of Yu's construction in [12]. Thus mainly we shall follow the paper of Yu.

2 Preliminaries

Let g be an odd positive integer with factorization

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

where p_1,p_2, $\cdots$, p_k are distinct primes and $\delta_j \geq 1$ for $1 \leq j \leq k$. For every j, we fix two distinct primes l_j and l'_j such that $l_j \equiv l'_j \equiv 1 \pmod{p_j}$.

Lemma 1(Yamamoto [11]) *let y, z, y', z' be a non-trivial solution of the Diophantine equation*

$$Y^2 - 4Z^g = Y'^2 - 4Z'^g$$

such that

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

Then the ideal class group of the field

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

has a subgroup N *such that*

$$N \cong \left\{ \begin{array}{ll} \mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/g\mathbb{Z} & \textit{if } D < -4, \\ \mathbb{Z}/g\mathbb{Z} & \textit{if } D > 0, \end{array} \right.$$

where D *is the discriminant of* F*.*

From the Chebotarev density theorem, we note that, for any prime factor p_j of g 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 (cf. [Lemma 3, 11]). For each p_j $(1 \leq j \leq k)$, we fix two such primes l_j, l'_j such that we have $2k$ distinct primes $\{l_1, \cdots, l_k, l'_1, \cdots l'_k\}$. Set

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

Lemma 2(Yu [12]) *Suppose we have the fixed triplet* (α, β, Ω)*. For* a*,* b *two integers satisfying*

$$a \equiv \alpha \ \textit{(mod } \Omega\textit{)}, \qquad b \equiv \beta \ \textit{(mod } \Omega\textit{)},$$

let

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

Then the ideal class group of $\mathbb{Q}(\sqrt{d})$ *has a subgroup* N *such that*

$$N \cong \left\{ \begin{array}{ll} \mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/g\mathbb{Z} & \textit{if } D < -4, \\ \mathbb{Z}/g\mathbb{Z} & \textit{if } D > 0. \end{array} \right.$$

Proof: In [12], Yu considered only the case that a, b are positive. But it is clear that Lemma 2 holds for negative or positive integers a, b. □

3 Proof of Theorem

Lemma 3 *Let P be a positive real number. Suppose*

$$a := -A \text{ and } b := B \text{ where } \Omega P < A, B < 2^{\frac{1}{g}}\Omega P,$$

satisfy the condition in Lemma 2. Then

$$d = -\frac{3}{4}(3A^g - B^g)(3B^g - A^g) < 0$$

and the ideal class group of the imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ has a subgroup N isomorphic to $\mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/g\mathbb{Z}$.

Proof: Note that $3\Omega^g P^g < 3A^g < 6\Omega^g P^g$ and $\Omega^g P^g < B^g < 2\Omega^g P^g$. So we have

$$\Omega^g P^g < 3A^g - B^g < 5\Omega^g P^g.$$

Similarly we have

$$\Omega^g P^g < 3B^g - A^g < 5\Omega^g P^g.$$

Thus $d < 0$ and Lemma 3 follows from Lemma 2. □

Let P be a sufficiently large positive real number and $M = P^{2-(3/2)\epsilon}$. Let $f(A, B)$ and $F(A, B)$ are the binary forms defined by

$$f(A, B) := (3A^g - B^g), \qquad F(A, B) := f(A, B)f(B, A).$$

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

$$M < m = q_1 q_2 q_3 \leq 8M,$$

where q_1, q_2 and q_3 are primes subject the condition

$$P^{2/3-(1/2)\epsilon} < q_1 < q_2 < q_3 \leq 2P^{2/3-(1/2)\epsilon}$$

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

By $r(m)$ we denote the number of pairs (A, B) with $\Omega P < A, B \leq 2^{\frac{1}{g}}\Omega P$, for which $F(A, B)$ is divisible by some m, and for which the condition in Lemma 3 is satisfied. We write

$$S_1(P) := \sum_{M<m\leq 8M} r(m)$$

and

$$S_2(P) := \sum_{M<m\leq 8M} r^2(m).$$

Lemma 4(Yu [12])

(i) $S_1(P) \gg P^2(\log P)^{-3}$,
(ii) $S_2(P) \ll P^{2+2\epsilon}$

Proof: See the proofs of Lemma 5 and Lemma 6 in [12]. □

Proof of Theorem: From Lemma 4, we have

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

We note that a number d in Lemma 3 can be divisible by at most $\binom{3g+1}{3}$ different m, because d can have at most $3g+1$ prime factors q which satisfies $P^{2/3-(1/2)\epsilon} < q \leq 2P^{2/3-(1/2)\epsilon}$. Thus the left-hand side of (1) gives a lower bound for the cardinality of a set $D(P)$ which satisfies:

(1) $D(P) \subset [-\frac{3}{4} \cdot 25\Omega^{2g}P^{2g}, -\frac{3}{4}\Omega^{2g}P^{2g}]$;
(2) every $d \in D(P)$ is divisible by some m and is given by the form $-\frac{3}{4}F(A, B)$ for some A, B satisfying the condition in Lemma 3;
(3) if d_1, d_2, $\in D(P)$ are distinct, then g.c.d.(d_1, d_2) is not divisible by any m.

For every $d \in D(p)$, we write $d = d_0 f^2$ such that d_0 is square-free. Suppose $D'(P)$ is the subset of $D(P)$ consisting of the elements d with d_0 divisible by some m. Then we have

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

Setting

$$P = \frac{1}{\Omega}(\frac{4}{3} \cdot \frac{1}{25}X)^{1/2g},$$

we have proved the theorem. □

Acknowledgement This paper was written when the author stayed in Madison. The author greatly thank Ken Ono for his warm hospitality and generous support. The author also thank the referee for some helpful suggestions.

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, in Number Theory Noordijkerhout 1983 Proceedings, Vol. 1068, Springer, Berlin.

[3] M. Craig, A construction for irregular discriminants, Osaka J. Math, **14**, 365 – 402.

[4] H. Davenport and H. Heilbronn, On the density of discrimnants of cubic fields II, Proc. Roy, Soc. A **322** (1971), 4055 – 420.

[5] J. F. Mestre, Courbes elliptiques et groups de classes d'idéaux de certains corps quadratiques, Seminar on Number Theory, 1979-1980, Exp. No. 15, 18pp., Univ. Bordeaux I, Talence, 1980.

[6] J. F. Mestre, Groupes de classes d'idéaux non cyclique de corps de nombre, Seminar on Number Theory, Paris 1981-1982(Paris, 1981/1982), 189-200, Progr. Math., 38, Birkhäuser Boston, Boston, MA, 1983.

[7] M. R. Murty, Exponents of class groups of quadratic fields, in Topics in Number Theory,(University Park, PA, 1997), 229 – 239, Mathematical Applications, Vol 467, Kluwer Acad. Publ., Dordrecht, 1999.

[8] T. Nagell, Über die Klassenzahl imaginar quadratischer Zahkörper, Abh. Math. Seminar Univ. Hambrug **1** (1922), 140 – 150.

[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 Thoery, **5** (1973), 237 – 241.

[11] Y. Yamamoto, On ramified Galoia extensions of quadratic number fields, Osaka J. Math. **7** (1970), 57–76.

[12] G. Yu, A note on the divisibility of class numbers of real quadratic fields, J. Number Theory, **97** (2002), 35 –44.