Real quadratic fields with class number divisible by 3

Dongho Byeon
School of Mathematical Sciences, Seoul National University, Seoul 151-747, Korea
E-mail: dhbyeon@math.snu.ac.kr

and

Eunhee Koh
Department of Mathematics, Pohang University of Science and Technology
Pohang 790-784, Korea
E-mail: ehkoh@postech.ac.kr

Abstract. We shall show that the number of real quadratic fields whose absolute discriminant is $\leq x$ and whose class number is divisible by 3 is $>> x^{\frac{7}{8}}$ improving the existing best known bound $>> x^{\frac{5}{6}}$ of K. Chakraborty and R. Murty.

1 Introduction

Recently K. Chakraborty and R. Murty [1] showed that the number of real quadratic fields whose absolute discriminant is $\leq x$ and whose class number is divisible by 3 is $>> x^{\frac{5}{6}}$ improving Murty's previous bound $>> x^{\frac{1}{6}}$ in [4]. On

[0] *Mathematics Subject Classification(2000):* 11R11, 11R29

[0] This work was supported by Korea Research Foundation Grant KRF-2002-003-C00001.

the other hand Soundararajan [5] has shown that the number of imaginary quadratic fields whose absolute discriminant is $\leq x$ and whose class number is divisible by 3 is $>> x^{\frac{7}{8}}$, which also improved Murty's previous bound $>> x^{\frac{5}{6}}$ in [4]. Heuristics of Cohen and Lenstra [2] predict that the probability of such an event is positive.
In this note, applying Soundararajan's results in [5] to the case of real quadratic fields, we shall show the following:

Theorem 1.1 *The number of real quadratic fields whose absolute discriminant is $\leq x$ and whose class number is divisible by 3 is $>> x^{\frac{7}{8}}$.*

To apply Soundararajan's results we need the following theorem, which can be obtained from Kishi and Miyake's classification of quadratic fields with class number divisible by 3 in [3].

Theorem 1.2 *Let m and n be two positive integers satisfying $m \equiv 1$ (mod 18), $n \equiv 1$ (mod 54) and $(m,n) = 1$. If the polynomial $f(X) := X^3 - 3mX - 2n$ is irreducible over $\mathbb{Q}$, then the class number of the quadratic field $\mathbb{Q}(\sqrt{3(m^3 - n^2)})$ is divisible by 3.*

2 Preliminary

In [3], Kishi and Miyake classified all quadratic fields whose class number is divisible by 3 as follows. Let $g(Z)$ be an irreducible polynomials over $\mathbb{Q}$ of the form

$$g(Z) = Z^3 - uwZ - u^2, \quad u, w \in \mathbb{Z},$$

where u and w are relatively prime, $d := 4uw^3 - 27u^2$ is not a square in $\mathbb{Z}$, and one of the following conditions holds:

(1) $3 \nmid w$;
(2) $3 \mid w$, $uw \not\equiv 3 \pmod 9$, and $u \equiv w \pm 1 \pmod 9$;
(3) $3 \mid w$, $uw \equiv 3 \pmod 9$, and $u \equiv w \pm 1 \pmod{27}$.

Then the roots of $g(Z) = 0$ generate an unramified cyclic cubic extension of the quadratic field $\mathbb{Q}(\sqrt{d})$. Conversely, every quadratic field whose class number is divisible by 3 and every unramified cyclic cubic extension of it are given in this way by a suitable pair of integers u and w.

3 Proof of results

First we shall prove Theorem 1.2.

Proof of Theorem 1.2: Let m and n be two positive integers satisfying $m \equiv 1 \pmod{18}$, $n \equiv 1 \pmod{54}$ and $(m,n) = 1$. Put $u := (2n)^2$ and $w := 3m$. Then u,w are relatively prime and satisfy (3), that is,

$$3 \mid w, \ \ uw \equiv 3 \pmod 9, \text{ and } u \equiv w + 1 \pmod{27}.$$

Thus by the above preliminary, the class number of the quadratic field

$$\mathbb{Q}(\sqrt{4uw^3 - 27u^2}) = \mathbb{Q}(\sqrt{4(2n)^2(3m)^3 - 27(2n)^4}) = \mathbb{Q}(\sqrt{3(m^3 - n^2)})$$

is divisible by 3, if the polynomial

$$g(Z) = Z^3 - uwZ - u^2 = Z^3 - (2n)^2(3m)Z - (2n)^4$$

is irreducible over $\mathbb{Q}$. Divide $g(Z)$ by $(2n)^3$, and put $X := Z/(2n)$ then we get

$$f(X) = X^3 - 3mX - 2n$$

and Theorem 1.2 follows. □

Let x be a positive real number and $T := x^{\frac{1}{16}}$. Put $M := T^{\frac{2}{3}}x^{\frac{1}{3}}/2$ and $N := Tx^{\frac{1}{2}}/2^4$. Let $N(x,T)$ be the number of positive square-free integers $d \le x$ with at least one solution to

$$m^3 - n^2 = 27 \cdot t^2 d, \tag{1}$$

where $T < t \le 2T$, $M < m \le 2M$, $N < n \le 2N$, $(m,t) = (m,n) = (t,6) = 1$, $m \equiv 19 \pmod{18 \cdot 6}$, and $n \equiv 55 \pmod{54 \cdot 6}$. Then by a slight modification of the results of Soundararajan in [5], we can obtain

$$N(x,T) >> x^{\frac{7}{8}}. \tag{2}$$

.

Proof of Theorem 1.1: From Theorem 1.2, we know that for a positive square-free integer d satisfying the equation (1), the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is divisible by 3 when the polynomial $f(X) = X^3 - 3mX - 2n$ is irreducible over $\mathbb{Q}$. Thus the number of real quadratic fields whose absolute discriminant is $\leq x$ and whose class number is divisible by 3 is

$$\geq N(x,T) - \sharp\{M < m \leq 2M, N < n \leq 2N \mid f(X) \text{ is reducible}\}. \quad (3)$$

Now we estimate $\sharp\{M < m \leq 2M, N < n \leq 2N \mid f(X) \text{ is reducible}\}$ by the same method in [1]. Let us fix $2n$. If $f(X)$ is reducible, then we can write $f(X) = (X+c)(X^2 - cX + d)$, where $-2n = cd$ and $-3m = d - c^2$. Thus $-3m$ is uniquely determined by the number of divisors of $-2n$. Let $d(-2n)$ represents the number of positive divisors of $-2n$. Then it is well known that $\sum_{N<n\leq 2N} d(-2n) << N \log N$. Thus

$$\sharp\{M < m \leq 2M, N < n \leq 2N \mid f(X) \text{ is reducible}\} << N \log N. \quad (4)$$

Finally applying (4) and (2) to (3), we complete the proof of Theorem 1.1. □

Acknowledgement The authors thank Ken Ono for introducing [5] to them.

References

[1] K. Chakraborty and R. Murty, On the number of real quadratic fields with class number divisible by 3, Proc. American Math. soc., **131** (2002), 41–44.

[2] H. Cohen and H .W Lenstra, Heuristics on class groups of number fields, in: Number Theory (Noordwijkerhout 1983), Lecture Notes in Math. 1068, Springer-Verlag, New York, 33–62.

[3] Y. Kishi and K. Miyake, Parametrization of the quadratic fields whose class numbers are divisible by three, J. Number Theory, **80** (2000), 209–217.

[4] M. Ram Murty, Exponents of class groups of quadratic fields, in: Topics in number theory (University Park, PA, 1997), Math. Appl., 467, Kluwer Acad. Publ., Dordrecht, 1999, 229–239.

[5] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, J. London Math. Soc., **61** (2000), 681–690.