PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 131, Number 1, Pages 41–44
S 0002-9939(02)06603-0
Article electronically published on May 15, 2002

ON THE NUMBER OF REAL QUADRATIC FIELDS WITH CLASS NUMBER DIVISIBLE BY 3

K. CHAKRABORTY AND M. RAM MURTY

(Communicated by Dennis A. Hejhal)

Abstract. We find a lower bound for the number of real quadratic fields whose class groups have an element of order 3. More precisely, we establish that the number of real quadratic fields whose absolute discriminant is $\leq x$ and whose class group has an element of order 3 is $\gg x^{\frac{5}{6}}$ improving the existing best known bound $\gg x^{\frac{1}{6}}$ of R. Murty.

1. Introduction

R. Murty [7] showed that if $g \geq 3$ is an integer, then the number of imaginary quadratic fields whose absolute discriminant is $\leq x$ and whose class group has an element of order g is $\gg x^{\frac{1}{2}+\frac{1}{g}}$. Recently, K. Soundararajan [8] has improved this to $\gg x^{\frac{1}{2}+\frac{2}{g}}$. R. Murty also showed in [7] that the number of real quadratic fields whose discriminant is $\leq x$ and whose class group has an element of order g is $\gg x^{\frac{1}{2g}}$.

The problem of divisibility of class numbers of quadratic fields has a long history. Gauss studied the case $g = 2$. The case $g = 3$ was studied by Davenport and Heilbronn [4]. If $r_3(D)$ is the 3 rank of the class group of a real quadratic field, then one can get the following upper bound from their work [4]:

$$\#\{D \leq x : r_3(D) \geq 1\} \leq \frac{4}{9}x.$$

We do not get any lower bound on the number of real quadratic fields whose class number is divisible by 3.

For any given g the infinitude of such fields was established by Nagell [9], Honda [6], Ankeny and Chowla [1], Hartung [5], Yamamoto [11] and Weinberger [10]. Recently R. Murty and Cardon [2] have extended the quantitative result stated in the beginning, to the case of quadratic function fields.

Conjectures of Cohen and Lenstra [3] predict a positive probability for such an event.

We now state the result of this paper.

Theorem 1. *The number of real quadratic fields whose absolute discriminant is $\leq x$ and whose class group has an element of order 3 is $\gg x^{\frac{5}{6}}$.*

Received by the editors August 15, 2001.
2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R11.
Key words and phrases. Class group, real quadratic fields.

2. Proof of Theorem 1

We will consider polynomials of the type

$$f(x) = x^3 + ax + b$$

and denote its discriminant as $D(f)$ which is equal to $[-(4a^3 + 27b^2)]$. We also denote by K the splitting field of $f(x)$. We need a couple of lemmas before we go to the actual proof of Theorem 1. The following is a basic result and we include a proof to make the paper self contained.

Lemma 2.1. *Let $f(x) = x^3 + ax + b \in \mathbb{Z}[x]$ be irreducible and suppose its discriminant is not a perfect square. Then the Galois group of K over $\mathbb{Q}$ is S_3.*

Proof. Let us denote the Galois group in question by G. As $f(x)$ is irreducible over $\mathbb{Q}$, we must have that 3 divides $|G|$. Now $\mathbb{Q}(\sqrt{D(f)}) \subseteq K$. As $D(f)$ is not a perfect square we must have that 2 also divides $|G|$. This implies that $G = S_3$. □

The following lemma counts the number of $a \leq A$ and $b \leq B$ such that $f(x)$ has the above mentioned (Lemma 2.1) two properties.

Lemma 2.2.

$$\begin{aligned} \# \quad & \{|a| \leq A, |b| \ \leq B : f(x) \textit{ is irreducible and } D(f) \neq \square\} \\ \gg \quad & AB. \end{aligned}$$

Proof. We denote the set in the lemma by S. Clearly,

$$\begin{aligned} \# \quad & S \geq AB - \\ \# \quad & \{|a| \leq A, |b| \ \leq B : f(x) \text{ is reducible}\} - \#\{|a| \leq A, |b| \ \leq B : D(f) = \square\}. \end{aligned}$$

At first we estimate $\#\{|a| \leq A, |b| \ \leq B : f(x) \ \text{ is reducible}\}$. Let us fix b. Now if $f(x)$ is reducible, by the rational root theorem it must have a linear factor $x + c$, where $c \ |b$. We write $b = cd$, then $f(x) = (x + c)(x^2 - cx + d)$. This implies $a = d - c^2$. Thus a is uniquely determined by the number of divisors of b. It is well known that $\sum_{|b| \leq B} d(b) \leq 2B \log B$. Here $d(b)$ represents the number of positive divisors of b. Thus the cardinality of this set is $\leq 2B \log B$.

The next step is to get an upper bound of $\#\{|a| \leq A, |b| \ \leq B : D(f) = \square\}$. We have

$$-4a^3 - 27b^2 = c^2. \tag{2.1}$$

Hence,

$$-4a^3 = (c + 3\sqrt{-3}\ b)((c - 3\sqrt{-3}\ b).$$

Thus $(4a^3) = \alpha_1\alpha_2$, where α_1, α_2 are two ideals in $\mathbb{Q}(\sqrt{-3})$. We fix a. Now the number of solutions of (2.1) is $O(A^\epsilon)$, as the number of ideals dividing $(4a^3)$ is at most $O(A^\epsilon)$ for any $\epsilon > 0$. Moreover, the ring of integers of $\mathbb{Q}(\sqrt{-3})$ is a PID and so for each pair of ideal divisors α_1, α_2 such that $(4a^3) = \alpha_1\alpha_2$, the number of choices of c, b in (2.1) is bounded by 6. Thus $\#\{D(f) = \square\} \ll A^{1+\epsilon}$. This completes the proof of the lemma. □

Now we prove Theorem 1.

Proof. A proposition of Yamamoto ([11], Proposition 1) states that if $2a$ and $3b$ are relatively prime and the Galois group of K over $\mathbb{Q}$ is equal to S_3, then the extension K over $\mathbb{Q}(\sqrt{D(f)})$ is unramified. Throughout the proof we always choose a and b such that $2a$ and $3b$ are coprime to each other. Now we assume the Galois group of K over $\mathbb{Q}$ to be equal to S_3, thus by the above proposition K over $\mathbb{Q}(\sqrt{D(f)})$ is unramified in our situation. The Galois group of K over $\mathbb{Q}(\sqrt{D(f)})$ is equal to C_3, the cyclic group of order 3. Thus by class field theory, K is contained in Hilbert class field of $\mathbb{Q}(\sqrt{D(f)})$. Thus 3 divides the class number of $\mathbb{Q}(\sqrt{D(f)})$.

We consider a large and negative and b positive such that $D(f)$ becomes positive. Precisely speaking, we consider $-c_1x^{\frac{1}{3}} < a \leq -c_2x^{\frac{1}{3}}$ and $c_3x^{\frac{1}{2}} < b \leq c_4x^{\frac{1}{2}}$, where $c_i, i = 1, 2, 3, 4$, are suitable constants. Thus we are considering all real quadratic fields as above whose absolute discriminant is $\leq x$. Our aim is to get a lower bound on the number of such fields.

We have $x^{\frac{1}{3}}$ choices of a and $x^{\frac{1}{2}}$ choices of b, thus we have at least $x^{\frac{1}{3}}.x^{\frac{1}{2}} = x^{\frac{5}{6}}$ many choices of such real quadratic fields by using the previous two lemmas.

Now the only thing we have to check is that there are a negligible number of duplications among these fields. Let S be the set of $D(f)$'s counted above which give rise to same fields more than once. For such a $D(f)$ in S,

$$4a_1^3 + 27b_1^2 = c^2(4a_2^3 + 27b_2^2),$$
$$4(a_1^3 - c^2a_2^3) = 27(b_2c + b_1)(b_2c - b_1).$$

Because $|4a_1^3 + 27b_1^2| \asymp x$ and $|4a_2^3 + 27b_2^2| \asymp x$, we have that c is bounded.

We fix a_1 and a_2. Then we have a fixed number on the left-hand side of the above identity. The choices of b_1 and b_2 are derived from the divisors of this number. It is an elementary fact of number theory that the number of divisors of a number n is $O(n^\epsilon)$. The number of possible values of a_1 and a_2 is $O(x^{\frac{2}{3}})$ and therefore the total number of elements in S cannot exceed $O(x^{\frac{2}{3}+\epsilon})$. The final enumeration gives

$$\gg x^{\frac{5}{6}} - O(x^{\frac{2}{3}+\epsilon})$$

distinct real quadratic fields $\mathbb{Q}(\sqrt{D(f)})$ whose class group has an element of order 3. This completes the proof of the theorem. □

References

[1] N. Ankeny and S. Chowla: On the divisibility of the class numbers of quadratic fields, *Pacific Journal of Math.*, **5**(1995), 321–324. MR **19:**18f

[2] David A. Cardon and M. Ram Murty: Exponents of class groups of quadratic function fields over finite fields, *Canadian Math. Bulletin*, **44** (2001), 398–407.

[3] H. Cohen and H. W. Lenstra Jr.: Heuristics on class groups of number fields, *Springer Lecture Notes*, **1068** in Number Theory Noordwijkerhout 1983 Proceedings. MR **85j:**11144

[4] H. Davenport and H. Heilbronn: On the density of discriminants of cubic fields II, *Proc. Royal Soc.*, A **322** (1971), 405–420. MR **58:**10816

[5] 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. MR **50:**4528

[6] T. Honda: A few remarks on class numbers of imaginary quadratic fields, *Osaka J. Math.*, **12** (1975), 19–21. MR **52:**8083

[7] M. Ram Murty: Exponents of class groups of quadratic fields, *Topics in Number Theory (University Park, PA, 1997), Math. Appl.* ***467****, Kluwer Acad. Publ., Dordrecht*, (1999), 229–239. MR **2000b:**11123

[8] K. Soundararajan: Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc.*, **61** (2000), no. 2, 681–690. MR **2001i:**11128

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

[10] P. Weinberger: Real quadratic fields with class numbers divisible by n, *J. Number Theory*, **5** (1973), 237–241. MR **49:**252

[11] Y. Yamamoto: On unramified Galois extensions of quadratic number fields, *Osaka J. Math.*, **7** (1970), 57–76. MR **42:**1800

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6

E-mail address: `kalyan@mast.queensu.ca`

Current address: Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211 019, U. P., India

E-mail address: `kalyan@mri.ernet.in`

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6

E-mail address: `murty@mast.queensu.ca`