A SHORT NOTE ON THE DIVISIBILITY OF CLASS NUMBERS OF REAL QUADRATIC FIELDS

JAITRA CHATTOPADHYAY

ABSTRACT. For any integer \( l \geq 1 \), let \( p_1, p_2, \ldots, p_{l+2} \) be distinct prime numbers \( \geq 5 \). For all real numbers \( X > 1 \), we let \( N_{3,l}(X) \) denote the number of real quadratic fields \( K \) whose absolute discriminant \( d_K \leq X \) and \( d_K \) is divisible by \( (p_1 \ldots p_{l+2}) \) together with the class number \( h_K \) of \( K \) divisible by \( 2^l \cdot 3 \). Then, in this short note, by following the method in [3], we prove that \( N_{3,l}(X) \gg X^{\frac{7}{8}} \) for all large enough \( X \)’s.

1. Introduction

The problem of the divisibility of class numbers of number fields has been of immense interest to number theorists for quite a long time. Many mathematicians have studied the divisibility problem of class number for quadratic fields.

Nagell [9] showed that there exist infinitely many imaginary quadratic fields whose class numbers are divisible by a given positive integer \( g \). Later, Ankeny and Chowla [1] also proved the same result. The analogous result for real quadratic fields had been proved by Weinberger [12], Yamamoto [13] and many others.

Apart from the qualitative results, a great deal of work has also been done towards the quantitative versions. For a positive integer \( g \), we let \( N_{g}^{+}(X) \) (respectively, \( N_{g}^{-}(X) \)) denote the number of real (respectively, imaginary) quadratic fields \( K \) whose absolute value of the discriminant is \( d_K \leq X \) and the class number \( h_K \) is divisible by \( g \). Then the general problem is to find lower bounds for the magnitude of \( N_{g}^{+}(X) \) (respectively, \( N_{g}^{-}(X) \)) as \( X \to \infty \). M. Ram Murty [10] proved that, for any integer \( g \geq 3 \), the inequalities \( N_{g}^{-}(X) \gg X^{\frac{1}{2} + \frac{1}{g}} \) and \( N_{g}^{+}(X) \gg X^{\frac{1}{2g}} \) hold. The behavior of \( N_{g}^{+}(X) \) and \( N_{g}^{-}(X) \) have also been studied in [8], [11] and [14].

The case \( g = 3 \) has been studied in [3], [4], [5], [6], [7] and in many other papers. Byeon [2] studied the case \( g = 5 \) and \( g = 7 \) and in both the cases, he showed that \( N_{g}^{+}(X) \gg X^{\frac{1}{2}} \), which is an improvement over the main result of [10].

In this short note, we shall study the following related problem. For a given natural number \( l \geq 1 \), we fix \( l + 2 \) distinct prime numbers \( \geq 5 \), say, \( p_1, \ldots, p_{l+2} \) and let \( g \geq 3 \), \( g \neq p_i \) for all \( i \), be a given odd integer. We let \( N_{g,l}(X) \) denote the number of real quadratic fields \( K \) whose absolute discriminant \( d_K \leq X \), \( h_K \) is divisible by \( g \) and \( d_K \) is divisible by \( (p_1 \ldots p_{l+2}) \). This, in turn, implies that \( 2^l \cdot 3 \) divides \( h_K \). Then the general problem is to find the magnitude of \( N_{g,l}(X) \).

In this short note, by adopting the method of [3], we prove the following theorem.

Theorem 1. We have, \( N_{3,l}(X) \gg X^{\frac{7}{8}} \) for all large enough real numbers \( X \).
2. Preliminaries

In [7], Kishi and Miyake gave a complete classification of quadratic fields \( K \) whose class number \( h_K \) is divisible by 3 as follows:

**Lemma 1.** Let \( g(T) = T^3 - uwT - u^2 \in \mathbb{Z}[T] \) be a polynomial with integer coefficients \( u \) and \( w \) such that \( \text{gcd}(u, w) = 1 \), \( d = 4uw^3 - 27u^2 \) is not a perfect 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 \( u \equiv w + 1 \pmod{9} \)

(3) \( 3 \mid w, uw \equiv 3 \pmod{9}, \) and \( u \equiv w + 1 \pmod{27} \)

If \( g(T) \) is irreducible over \( \mathbb{Q} \), then the roots of the polynomial \( g(T) \) generate an unramified cyclic cubic extension \( L \) over \( K := \mathbb{Q}(\sqrt{d}) \) (which in turn implies, by Class Field Theory, that 3 divides \( h_K \)). Conversely, suppose \( K \) is a quadratic field over \( \mathbb{Q} \) with 3 dividing the class number \( h_K \). If \( L \) is an unramified cyclic cubic extension over \( K \), then \( L \) is obtained by adjoining the roots of \( g(T) \) in \( K \) for some suitable choices of \( u \) and \( w \).

Using Lemma 1, Byeon and Koh [3] proved the following result.

**Lemma 2.** Let \( m \) and \( n \) be two relatively prime positive integers satisfying \( m \equiv 1 \pmod{18} \) and \( n \equiv 1 \pmod{54} \). If the polynomial \( f(T) = T^3 - 3mT - 2n \) 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.

In [11], Soundararajan proved the following result (see also [3]).

**Lemma 3.** Let \( X \) be a large positive real number and \( T = X^{1/4} \). Also, let \( M = \frac{T^{2/3}X^{1/2}}{2} \) and \( N = \frac{T^{1/3}X^{1/2}}{2} \). If \( N(X) \) denotes the number of positive square-free integers \( d \leq X \) with at least one integer solution \((m, n, t)\) to the equation

\[
m^3 - n^2 = 27t^2d
\]

satisfying \( T < t \leq 2T, M < m \leq 2M, N < n \leq 2N, \text{gcd}(m, t) = \text{gcd}(m, n) = \text{gcd}(t, 6) = 1, m \equiv 19 \pmod{18 \cdot 6} \) and \( n \equiv 55 \pmod{54 \cdot 6} \), then, we have,

\[N(X) \asymp \frac{MN}{T} + o(MT^{2/3}X^{1/2}) \gg X^{7/8}.
\]

The following result was proved in [4] which provides a lower bound of the number of irreducible cubic polynomials with bounded coefficients.

**Lemma 4.** Let \( M \) and \( N \) be two positive real numbers. Let

\[S = \{ f(T) = T^3 + mT + n \in \mathbb{Z}[T] : |m| \leq M, |n| \leq N, f(T) \text{ is irreducible over } \mathbb{Q}, \text{ and } D(f) = -(4m^3 + 27n^2) \text{ is not a perfect square} \}\]

be a subset of \( \mathbb{Z}[T] \). Then \(|S| \gg MN\).
3. Proof of Theorem \[1\]

Let \( l \geq 1 \) be an integer and let \( g = 2^l \cdot 3 \). Let \( K \) be a real quadratic field over \( \mathbb{Q} \) and its class number is \( h_K \). Note that \( h_K \equiv 0 \pmod{2^l} \) if and only if \( h_K \equiv 0 \pmod{2^l} \) and \( h_K \equiv 0 \pmod{3} \).

**Claim 1.** The number of quadratic field \( \mathbb{Q}(\sqrt{d}) \) satisfying \( d \leq X \), \( d \) is divisible by \( p_1 p_2 \ldots p_{l+2} \) and \( 3 \) divides \( h_K \) is \( \gg X^{\frac{7}{8}} \).

For each \( i = 1, 2, \ldots, l+2 \), let \( a_i \) and \( b_i \) be integers such that
\[
(2) \quad 3a_i - 2b_i \not\equiv 0 \pmod{p_i}.
\]
Then, consider the simultaneous congruences
\[
X \equiv 19 \pmod{18 \cdot 6}
\]
\[
X \equiv 1 + a_i p_i \pmod{p_i^2},
\]
for all \( i = 1, 2, \ldots, l+2 \). Then, by the Chinese Reminder Theorem, there is a unique integer solution \( m \) modulo \( 18 \cdot 6 \prod_{i=1}^{l+2} p_i^2 \). Thus, the number of such integers \( m \leq X \) is
\[
((1 + o(1)) X / \left( 18 \cdot 6 \prod_{i=1}^{l+2} p_i^2 \right) \text{ as } X \to \infty.
\]
Let \( N_1(X) \) be the set of all such integers \( m \leq X \).

Similarly, we consider the simultaneous congruences
\[
X \equiv 55 \pmod{54 \cdot 6}
\]
\[
X \equiv 1 + b_i p_i \pmod{p_i^2},
\]
for all \( i = 1, 2, \ldots, l+2 \). Then, by the Chinese Reminder Theorem, there is a unique integer solution \( n \) modulo \( 54 \cdot 6 \prod_{i=1}^{l+2} p_i^2 \). Thus, the number of such integers \( n \leq X \) is
\[
((1 + o(1)) X / \left( 54 \cdot 6 \prod_{i=1}^{l+2} p_i^2 \right) \text{ as } X \to \infty.
\]
Let \( N_2(X) \) be the set of all such integers \( n \leq X \).

Let \( X \) be a large positive real number and \( T = X^{\frac{1}{36}} \). Also, let
\[
M = T^\frac{5}{2} X^\frac{1}{2}, \quad N = T X^\frac{1}{24}.
\]
Now, we shall count the number of tuples \((m, n, t)\) satisfying \((1)\) with \( T < t \leq 2T \), \( M < m \leq 2M \), \( N < n \leq 2N \), \( \gcd(m, t) = \gcd(m, n) = \gcd(t, 6) = 1 \), \( m \in N_1(X) \), \( n \in N_2(X) \) with square-free integer \( d \). Then, by Lemma \[3\] we see that
\[
N(X) \gg X^{7/8}.
\]
Now note that for any integers \( m \in N_1(X) \) and \( n \in N_2(X) \), we see that
\[
m^3 - n^2 = (a_i p_i + 1)\cdot 3 - (b_i p_i + 1)\cdot 2 \equiv 3a_i p_i + 1 - 2b_i p_i - 1 \equiv p_i(3a_i - 2b_i) \pmod{p_i^2},
\]
for all \( i = 1, 2, \ldots, l+2 \). By \((2)\), since \( 3a_i - 2b_i \not\equiv 0 \pmod{p_i} \) for all \( i \), we see that \( m^3 - n^2 \not\equiv 0 \pmod{p_i^2} \) and hence \( p_i \) divides the square-free part of \( m^3 - n^2 \) which is \( d \). Thus, \( p_1 p_2 \ldots p_{l+2} \) divides \( d \) for all such \( d \)’s.
In order finish the proof of Claim 1, by Lemma 2, it is enough to count the number of tuples \((m, n, t)\) satisfying (1) for which \(f(X) = T^3 - 3mT - 2n\) is irreducible over \(\mathbb{Q}\). By Lemma [4], the number of such irreducible polynomial \(f(T)\) is at least \(\gg MN \gg X^{7/8}\), which proves Claim 1.

Now, to finish the proof of the theorem, we see that at least \(\gg X^{7/8}\) number of real quadratic fields \(K = \mathbb{Q}(\sqrt{d})\) satisfying \(h_K \equiv 0 \pmod{3}\) and \(\omega(d) \geq l + 2\), where \(\omega(n)\) denotes the number of distinct prime factors of \(n\). Therefore, by Gauss’ theory of genera, we conclude that the class number \(h_K\) of corresponding real quadratic field is divisible by \(2^l\) also. Combining this fact with Claim 1, we get the theorem.

Acknowledgements. I would like to sincerely thank Prof. Florian Luca for his insightful remarks and having fruitful discussions with him. I acknowledge Prof. R. Thangadurai for going through the article and suggesting valuable points to improve the presentation of the paper. I am thankful to the referee for his/her valuable suggestions to improve the presentation of the paper. I am grateful to Dept. of Atomic Energy, Govt. of India and Harish-Chandra Research Institute for providing financial support to carry out this research.

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] D. Byeon, Real quadratic fields with class number divisible by 5 or 7, *Manu. Math.*, 120 (2006) (2) 211-215.
[3] D. Byeon and E. Koh, Real quadratic fields with class number divisible by 3, *Manu. Math.*, 111 (2003), 261-263.
[4] K. Chakraborty and M. Ram Murty, On the number of real quadratic fields with class number divisible by 3, *Proc. Amer. Math. Soc.*, 131 (2002), 41-44.
[5] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields, *Proc. Royal Soc. A.*, 322 (1971), 405-420.
[6] T. Honda, On real quadratic fields whose class numbers are multiples of 3, *J.Reine Angew. Math.*, 223 (1968), 101-102.
[7] Y. Kishi and K. Miyake, Parametrization of the quadratic fields whose class numbers are divisible by three, *J. Number Theory*, 80 (2000), 209-217.
[8] F. Luca, A note on the divisibility of class numbers of real quadratic fields, *C. R. Math. Acad. Sci. Soc. R. Can.*, 25 (2003) (3), 71-75.
[9] T. Nagell, Uber die Klassenzahl imaginair quadratischer Zahlkorper, *Abh. Math. Seminar Univ. Hamburg*, 1 (1922) (1), 140-150.
[10] 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.
[11] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc.*, 61 (2000) (2), 681-690.
[12] P. Weinberger, Real quadratic fields with class numbers divisible by \(n\), *J. Number Theory*, 5 (1973), 237-241.
[13] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.*, 7 (1970), 57-76.
[14] G. Yu, A note on the divisibility of class numbers of real quadratic fields, *J. Number Theory*, 97 (2002), 35-44.

Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhunsi, Allahabad - 211019, India

E-mail address, Jaitra Chattopadhyay: jaitrachattopadhyay@hri.res.in