Trends in Mathematics
Information Center for Mathematical Sciences
Volume 4, Number 1, June 2001, Pages 26–30

DIVISIBILITY PROPERTIES OF CLASS NUMBERS

DONGHO BYEON

Abstract. Divisibility properties of class numbers is very important to know the structure of ideal class groups of number fields. However, very little is known. In this paper, we will survey the recent works on this subject, specially, related to quadratic fields.

1. Introduction

Let K be a number field and $\mathbb{Z}_K$ be the ring of integers of K. We say that two fractional ideal I and J of K are equivalent if there exists $\alpha \in K^*$ such that $J = \alpha I$. The set of equivalence classes is called the class group of K and is denoted $Cl(K)$. Then the following theorem is well known.

Theorem 1.1. *For any number field K, the class group $Cl(K)$ is a finite Abelian group.*

The cardinality of class group $Cl(K)$ is called the class number of K and is denoted $h(K)$. Note that $h(K) = 1$ if and only if $\mathbb{Z}_K$ is a PID which in turn is if and only if $\mathbb{Z}_K$ is a UFD. Hence the class group is the obstruction to $\mathbb{Z}_K$ being a UFD.

From Theorem 1.1, we know that divisiblity properties of class numbers $h(K)$ is very important to know the structure of class groups $Cl(K)$. However, very little is known. In this paper, we will survey the recent works on this subject, specially, related to quadratic number fields.

2. Imaginary quadratic fields

The following theorem on divisibility of class numbers of imaginary quadratic fields is well known.

Theorem 2.1. *(Ankeny and Chowla* [1]*, Humbert* [10]*, and Nagell* [17]*) For a given positive integer $g \geq 3$, there are infinitely many imaginary quadratic fields whose class number is divisible by g.*

Remark. A similar theorem for the case $g = 2$ is a classical work of Gauss and for the case $g = 3$ was proved by Davenport and Heilbronn [7].

To prove this theorem, Ankeny and Chowla [1] used the following two lemmas.

2000 *Mathematics Subject Classification.* 11R11, 11R29.
Key words and phrases. number field, ideal class group, class number.
Received August 30, 2000.

©2001 Information Center for Mathematical Sciences

Lemma 2.2. *([1]) Let g be a positive even integer and $d = 3^g - x^2$ a square-free positive integer such that $2|x$ and $0 < x < (2 \cdot 3^{g-1})^{\frac{1}{2}}$. Then the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ is divisible by g.*

Lemma 2.3. *([1]) Let g be a sufficiently large positive even integer. Then*

$$\sharp\{d = 3^g - x^2 \textit{in Lemma 2.2}\} \geq \frac{1}{25} 3^{\frac{g}{2}}.$$

Recently, M. R. Murty [16] extended Theorem 2.1 and by using the seive of Eratosthenes, obtained following the first nontrivial estimate for the number of such imaginary quadratic fields.

Theorem 2.4. *(M. R. Murty [16]) Let $g \geq 3$. The number of imaginary quadratic fields whose absolute discriminant is $\leq x$ $(x > 0)$ and whose class number is divisible by g is $>> x^{\frac{1}{2}+\frac{1}{g}}$.*

For the complementary question, Chowla conjectured and Hartung [8] proved that the following theorem.

Theorem 2.5. *(Hartung [8]) For a given prime $p \geq 3$, there are infinitely many imaginary quadratic fields whose class number is not divisible by p.*

To prove this theorem, Hartung [8] used Kronecker relation;

$$\sum_s H(4n - s^2) = 2 \sum_{d|n, d > \sqrt{n}} d,$$

where $H(N)$ $(N \equiv 0, 3 \pmod 4)$ is the Hurwitz-Kronecker class number, i,e, the class number of quadratic forms of discriminant $-N$.

After works by Bruinier [2], Byeon [3], Horie and Onishi [11] [12] [13], Jochonowitz [14] and Ono and Skinner [19] address various refinements and genralizations. Recently, Kohnen and Ono [15] applied Sturm's work [20] on the congruence of modular forms to an half integral weight modular form and obtained following the first nontrivial estimate for the number of such imaginary quadratic fields.

Theorem 2.6. *(Kohnen and Ono [15]) Let $p > 3$ be a prime. The number of imaginary quadratic fields whose absolute discriminant is $\leq x$ $(x > 0)$ and whose class number is not divisible by p is $>>_p \frac{\sqrt{x}}{log x}$.*

3. Real quadratic fields

The following theorem is Theorem 2.1's analogue for real quadratic fields.

Theorem 3.1. *(Weinberger [21], Yamamoto [22]) For a given positive integer $g \geq 3$, there are infinitely many real quadratic fields whose class number is divisible by g.*

To prove this theorem, Yamamoto [22] used class field theory and Weinberger [21] used similar method in Ankeny and Chowla's proof [1]. But his proof is more difficult because of the existence of fundamental units in real quadratic fields.

Recently, for the complementary question, by refining Ono's idea [18], we obtained the following theorem.

Theorem 3.2. *(Byeon [4]) Let $p > 3$ be a prime. The number of real quadratic fields whose absolute discriminant is $\leq x$ $(x > 0)$ and whose class number is not divisible by p is $>>_p \frac{\sqrt{x}}{log x}$.*

To prove this theorem, we proved the following two propositions.

Proposition 3.3. *([4]) Let $D > 0$ be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{D})$. Let $R_p(D)$ denote the p-adic regulator of $\mathbb{Q}(\sqrt{D})$ and $|\cdot|_p$ denote the usual multiplicative p-adic valuation normalized so that $|p|_p = \frac{1}{p}$. Let $p > 3$ be prime and $\delta = -1$ or 1. If there is a fundamental discriminant D_0 coprime to p of a real quadratic field $\mathbb{Q}(\sqrt{D_0})$ such that*

$$\begin{aligned} &(i) \quad (\frac{D_0}{p}) = \delta \\ &(ii) \quad h(D_0) \not\equiv 0 \ mod\ p, \\ &(iii) \quad |R_p(D_0)|_p = \frac{1}{p}, \end{aligned}$$

then for each δ,

$$\sharp\{0 < D < X \mid h(D) \not\equiv 0 \ (mod\ p),\ (\frac{D}{p}) = \delta,\ and\ |R_p(D)|_p = \frac{1}{p}\} >>_p \frac{\sqrt{X}}{logX}.$$

Proposition 3.4. *([4]) Let $p > 3$ be prime and $\delta = -1$ or 1. If $\delta = -1$, then for any $p \equiv 3$ (mod 4), let D be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{p^2-1})$ and if $\delta = 1$, then for any p, let D be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{p^2+4})$. Then for each δ, D satisfies the condition in Theorem 1.3, i.e.,*

$$\begin{aligned} &(i) \quad (\frac{D}{p}) = \delta \\ &(ii) \quad h(D) \not\equiv 0 \ mod\ p, \\ &(iii) \quad |R_p(D)|_p = \frac{1}{p}. \end{aligned}$$

To prove Proposition 3.3, we applied Sturm's work [20] on the congruence of modular forms to Cohen modular forms [5] whose Fourier coefficients are essentially special values of Dirichlet L-series $L(s, \chi_D)$ with the usual Kronecker character χ_D. To prove Proposition 3.4, we used well known units in $\mathbb{Q}(\sqrt{p^2-1})$ or $\mathbb{Q}(\sqrt{p^2+4})$ and Hua's upper bound for $L(1, \chi_D)$ [9].

4. Concluding Remarks

For imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ $(D < 0)$, Cohen and Lenstra [6] predict that the "probability" $p \not| \, h(\mathbb{Q}(\sqrt{D})$ is

$$\prod_{i=1}^{\infty}(1 - \frac{1}{p^i})$$

and the "probability" $p| \ h(\mathbb{Q}(\sqrt{D})$ is

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

For real quadratic fields $\mathbb{Q}(\sqrt{D})$ $(D > 0)$, they [6] conjectured that the "probability" $p \not| \, h(\mathbb{Q}(\sqrt{D})$ is

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

and the "probability" $p|\ h(\mathbb{Q}(\sqrt{D})$ is

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

Although extensive numerical evidence lends credence to these heuristics, apart from the works of Davenport and Heilbronn [7] when $p = 3$, little has been proved.

Finally, we give a natural formulation of the concerned above problems for arbitrary number fields.

Divisibility (or indivisibility) problem of class numbers

Let S be an interesting infinite set of number fields K and p a prime.

Problem 1. *Are there infinitely many number fields K in S, whose class number $h(K)$ is divisible by p (or is not divisible by p)?*

Problem 2. *If the answer of Problem 1 is yes, then how often such K appears in S?*

References

[1] N. Ankeny and S. Chowla, *On the divisibility of the class numbers of quadratic fields,* Pacific Journal of Math. **5** (1955), 321–324.

[2] J. H. Brunier, *Nonvanishing modulo l of Fourier coefficients of half-integral weight modular forms,* Duke Math. Journal **98** (1999), 595–611.

[3] D. Byeon, *A note on the basic Iwasawa λ-invariants of imaginary quadratic fields and congruence of modular forms,* Acta Arith. **89** (1999), 295–299.

[4] D. Byeon, *Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields,* Compositio Math., to appear.

[5] H. Cohen, *Sums involving the values at negative integers of L-functions of qudaratic characters,* Math. Ann. **217** (1975), 271–285.

[6] H. Cohen and H. W. Lenstra, *Heuristics on class groups of number fields,* Number Theory, Noordwijkerhout 1983, Springer Lect. Notes **1068** (1984), 33–62

[7] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. Lond. A **322** (1971), 405–420.

[8] 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.

[9] L. -K. Hua, *On the least solution of Pell's equation,* Bull. Amer. Math. Soc., **48** (1942), 731–735.

[10] P. Humbert, *Sur les nombres de classes de certains corps quadratiques,* Comment. Math. Helv. **12** (1939/40) 235-245; also **13** (1940/41) 67.

[11] K. Horie, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields,* Invent. Math. **88** (1987), 31–38.

[12] K. Horie, *Trace formula and imaginary quadratic fields,* Math. Ann. **288** (1990), 605-612.

[13] K. Horie and Y. Onishi, *The existence of certain infinite families of imaginary quadratic fields,* J. Reine und ange. Math. **390** (1988), 97–113.

[14] N. Jochonowitz, *Congruence between modular forms of half integral weights and implications for class numbers and elliptic curves,* preprint.

[15] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate-Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. **135** (1999), 387–398.

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

[17] T. Nagell, *Uber die klassenzahl imaginar-quadratischer Zahlkorper,* Abh. Math. Sem. Univ. Hamburg **1** (1922), 140–150.

[18] K. Ono, *Indivisibility of class numbers of real quadratic fields*, Compositio Math., **119** (1999), 1–11.

[19] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo l,* Ann. Math. **147** (1998), 451–468.

[20] J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes **1240** (1984), 275–280.

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

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

School of Mathematics, Korea Institute for Advanced Study, Seoul, Korea
E-mail address: `dhbyeon@ kias.re.kr`