Hindawi Publishing Corporation
Abstract and Applied Analysis
Volume 2012, Article ID 570154, 4 pages
doi:10.1155/2012/570154

Research Article

Divisibility Criteria for Class Numbers of Imaginary Quadratic Fields Whose Discriminant Has Only Two Prime Factors

A. Pekin

Department of Mathematics, Faculty of Science, Istanbul University, 34134 Istanbul, Turkey

Correspondence should be addressed to A. Pekin, aypekin@istanbul.edu.tr

Received 17 October 2012; Accepted 4 November 2012

Academic Editor: Haydar Akca

We will prove a theorem providing sufficient condition for the divisibility of class numbers of certain imaginary quadratic fields by $2g$, where $g > 1$ is an integer and the discriminant of such fields has only two prime divisors.

1. Introduction

Let $K = Q(\sqrt{D})$ be the quadratic fields with discriminant D and $h = h(D)$ its class number. In the narrow sense, the class number of K is denoted by $h^+(D)$, where, if $D > 0$, then $h^+(D) = 2h(D)$ and the fundamental unit ε_D has norm 1, otherwise $h^+(D) = h(D)$. If the discriminant of $|D|$ has two distinct prime divisors, then by the genus theory of Gauss the 2-class group of K is cyclic. The problem of the divisibility of class numbers for number fields has been studied by many authors. There are Hartung [1], Honda [2], Murty [3], Nagel [4], Soundararajan [5], Weinberger [6], Yamamoto [7], among them. Ankeny and Chowla [8] proved that there exists infinitely many imaginary quadratic fields each with class numbers divisible by g where g is any given rational integer. Later, Belabas and Fouvry [9] proved that there are infinitely many primes p such that the class number of the real quadratic field $K = Q(\sqrt{p})$ is not divisible by 3. Furthermore, many authors [7, 10–13] have studied the conditions for $h^+(D)$ to be divisible by 2^n when the 2-class group of K is cyclic. However the criterion for $h^+(D)$ to be divisible by 2^n is known for only $n \leq 4$ and the existence of quadratic fields with arbitrarily large cyclic 2-class groups is not known yet. Recently, Byeon and Lee [14] proved that there are infinitely many imaginary quadratic fields whose ideal class group has an element of order $2g$ and whose discriminant has only two prime divisors. In this paper, we will prove a theorem that the order of the ideal class group of certain imaginary quadratic field is divisible by

$2g$. Moreover, we notice that the discriminant of these fields has only different two prime divisors. Finally, we will give a table as an application to our main theorem.

2. Main Theorem

Our main theorem is the following.

Theorem 2.1. *Let $D = pq$ be square-free integer with primes $p \equiv q \equiv 1 (\mathrm{mod}\, 4)$. If there is a prime $r \equiv 1 (\mathrm{mod}\, 8)$ satisfying $(D/r) = 1$, then $t \mid h(D)$ for at least positive integer t where $t \geq 2$.*

In order to prove this theorem we need the following fundamental lemma and some theorems.

Lemma 2.2. *If D is of the form $p \cdot q$ where p and q are primes $p \equiv q \equiv 1 (\mathrm{mod}\, 4)$, then there is a prime $r \equiv 1 (\mathrm{mod}\, 8)$ such that $(D/r) = 1$.*

Proof. Let a and b be quadratic nonresidues for p and q are primes such that $(a/p) = -1$, $(b/q) = -1$, where $(\ )$ denotes Legendre symbol and $\mathrm{g} \cdot \mathrm{c} \cdot \mathrm{d}(p, q) = 1$. Therefore, by Chinese Remainder Theorem, we can write $w \equiv a (\mathrm{mod}\, p)$, $w \equiv b (\mathrm{mod}\, q)$ for a positive integer w. Now, we consider the numbers of the form $pqk + w$ such that $pqk_0 + w \equiv 1 (\mathrm{mod}\, 8)$ for some $1 \leq k_0 \leq 8$. Since $pqk_0 + w$ are distinct residues mod(8) for some $1 \leq k_0 \leq 8$, then we get $pq(8n + k_0) + w = 8pqn + pqk_0 + w$, $n \geq 0$. We assert that $\mathrm{g} \cdot \mathrm{c} \cdot \mathrm{d}(8pq, pqk_0 + w) = 1$. Really, we suppose that $\mathrm{g} \cdot \mathrm{c} \cdot \mathrm{d}(8pq, pqk_0 + w) = m > 1$, then there is a prime s such that $s \mid m$, and so we have $s \mid 8pq$, $s \mid pqk_0 + w$. Thereby this follows that $s = 2$, p or q. But since $pqk_0 + w \equiv 1 (\mathrm{mod}\, 8)$, then $s \neq 2$ and $s \mid m$; this is in contradiction with $w \equiv a (\mathrm{mod}\, p)$, $w \equiv b (\mathrm{mod}\, q)$. Therefore, $\mathrm{g} \cdot \mathrm{c} \cdot \mathrm{d}(8pq, pqk_0 + w) = 1$ holds. Thus, by the Dirichlet theorem on primes, there is a prime r satisfying $r = pq(8n + k_0) + w = 8pqn + pqk_0 + w$. Hence, it is seen that $r \equiv 1 (\mathrm{mod}\, 8)$. □

The following theorem is generalized by Cowles [15].

Theorem 2.3. *Let r, m, t be positive integers with $m > 1$ and $t > 1$, and let $n = r^2 - 4m^t$ be square-free and negative. If m^c is not the norm of a primitive element of O_K whenever c properly divides t, then $t \mid h(n)$.*

Cowles proved this theorem by using the decomposition of the prime divisors in O_K. But Mollin has emphasized in [16] that it contains some misprints and then he has provided the following theorem which is more useful in practise than Theorem 2.4.

Theorem 2.4. *Let n be a square-free integer of the form $n = r^2 - 4m^t$ where r, m, and t are positive integers such that $m > 1$ and $t > 1$. If $r^2 \leq 4m^{t-1}(m - 1)$, then $t \mid h(n)$.*

Theorem 2.5. *Let n be a square-free integer, and let $m > 1$, $t > 1$ be integers such that*

(i) *$\mp m^t$ is the norm of a primitive element from $K = Q(\sqrt{n})$,*

(ii) *$\mp m^c$ is not the norm of a primitive element from K for all c properly dividing t,*

(iii) *if $t = |m|_2$, then $n \equiv 1 (\mathrm{mod}\, 8)$.*

Then t divides the exponent of ψ_K, where ψ_K is the class group of K.

3. Proof of Main Theorem

Now we will provide a proof for the fundamental theorem which is more practical than all of the works above mentioned.

Table 1

D	p	q	r	$h(D)$
65	5	13	17	8
1165	5	233	41	20
3341	13	257	41	72
10685	5	2137	73	116
30769	29	1061	41	112
45349	101	449	17	168
95509	149	641	17	176
97309	73	1333	89	216
102689	29	3541	73	496
125009	41	3049	17	504
18497	53	349	41	168
20453	113	181	17	116
223721	137	1633	97	496
378905	5	75781	41	592
567137	17	333613	89	640
650117	13	50009	17	848
735929	373	1973	41	1664
847085	5	169417	73	936
874589	241	3629	17	1160
875705	5	175141	41	1328
876461	53	16537	73	1584
971081	109	8909	17	1464
971413	29	33497	73	336
978809	13	75293	89	1728
987169	97	10177	17	624
999997	757	1321	17	380

Proof. From the assumption of Lemma 2.2, it follows that there is suitable prime r with $r \equiv 1(\bmod 8)$ such that $(D/r) = 1$. However, from the properties of the Legendre symbol, we can write $(Dy^2/r^2) = 1$ for any integer y. Since $(2, r) = 1$, then we have $(Dy^2/r^t) = 1$. Therefore, there are integers $x = a/2, y = b/2$ such that the equation $x^2 - Dy^2 = \mp r^t$ has a solution in integers. Hence, we can write $a^2 - Db^2 = \mp 4r^t$, where $a \equiv b(\bmod 2)$. From this equation, it is seen that r^t is the norm of a primitive element of O_K, and, then by Theorem 2.5, t divides $h(n)$. □

We have the following results.

Corollary 3.1. *Let D be a square-free and negative integer in the form of $D = n^2 - 4r^{2g} = p \cdot q$ with $n > 1$, $g > 1$ are positive integers and p, q, r are primes such that $p \equiv q \equiv 1(\bmod 4)$, $r \equiv 1(\bmod 8)$. If r^{2g} is the norm of a primitive element of O_K, then the order of the ideal class group of $K = Q(\sqrt{D})$ is $2g$.*

Corollary 3.2. *Let D be a square-free and negative integer in the form of $D = p \cdot q$, then there exists exactly 34433 imaginary quadratic fields satisfying assertion of the main theorem.*

4. Table

The above-mentioned imaginary quadratic fields $K = Q(\sqrt{D})$ correspond to some values of $D\,(5 \leq D \leq 10^6)$ which are given in Table 1. We have provided a table of the examples to illustrate the results above, using C programming language. Moreover, it is easily seen that the class numbers of imaginary quadratic fields of $K = (Q\sqrt{D})$ are divisible by $2g$ from Table 1.

Acknowledgment

This work was partially supported by the scientific research project with the number IU-YADOP 12368.

References

[1] P. Hartung, "Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by n," *Journal of Number Theory*, vol. 6, pp. 276–278, 1974.

[2] T. Honda, "A few remarks on class numbers of imaginary quadratic number fields," *Osaka Journal of Mathematics*, vol. 12, pp. 19–21, 1975.

[3] M. R. Murty, "The ABC conjecture and exponents of class groups of quadratic fields," in *Number Theory*, vol. 210 of *Contemporary Mathematics*, pp. 85–95, American Mathematical Society, Providence, RI, USA, 1998.

[4] T. Nagel, "Über die Klassenzahl imaginär quadratischer Zahlkörper," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 1, pp. 140–150, 1992.

[5] K. Soundararajan, "Divisibility of class numbers of imaginary quadratic fields," *Journal of the London Mathematical Society. Second Series*, vol. 61, no. 3, pp. 681–690, 2000.

[6] P. J. Weinberger, "Real quadratic fields with class numbers divisible by n," *Journal of Number Theory*, vol. 5, pp. 237–241, 1973.

[7] Y. Yamamoto, "Divisibility by 16 of class number of quadratic fields whose 2-class groups are cyclic," *Osaka Journal of Mathematics*, vol. 21, no. 1, pp. 1–22, 1984.

[8] N. C. Ankeny and S. Chowla, "On the divisibility of the class number of quadratic fields," *Pacific Journal of Mathematics*, vol. 5, pp. 321–324, 1955.

[9] K. Belabas and E. Fouvry, "Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier," *Duke Mathematical Journal*, vol. 98, no. 2, pp. 217–268, 1999.

[10] P. Barrucand and H. Cohn, "Note on primes of type $x^2 + 32y^2$, class number, and residuacity," *Journal für die Reine und Angewandte Mathematik*, vol. 238, pp. 67–70, 1969.

[11] H. Bauer, "Zur berechnung der 2-klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen diskriminantenprimteilern," *Journal für die Reine und Angewandte Mathematik*, vol. 248, pp. 42–46, 1971.

[12] H. Hasse, "Über die teilbarkeit durch 2^3 der Klassenzahl imaginärquadratischer Zahlkörper mit genau zwei verschiedenen diskriminantenprimteilern," *Journal für die Reine und Angewandte Mathematik*, vol. 241, pp. 1–6, 1970.

[13] P. Kaplan, K. S. Williams, and K. Hardy, "Divisibilité par 16 du nombre des classes au sens strict des corps quadratiques réels dont le deux-groupe des classes est cyclique," *Osaka Journal of Mathematics*, vol. 23, no. 2, pp. 479–489, 1986.

[14] D. Byeon and S. Lee, "Divisibility of class numbers of imaginary quadratic fields whose discriminant has only two prime factors," *Japan Academy. Proceedings. Series A. Mathematical Sciences*, vol. 84, no. 1, pp. 8–10, 2008.

[15] M. J. Cowles, "On the divisibility of the class number of imaginary quadratic fields," *Journal of Number Theory*, vol. 12, no. 1, pp. 113–115, 1980.

[16] R. A. Mollin, "Diophantine equations and class numbers," *Journal of Number Theory*, vol. 24, no. 1, pp. 7–19, 1986.