RIMS Kôkyûroku Bessatsu
B34 (2012), 117–125

On the divisibility of class numbers of imaginary quadratic fields whose discriminant has only two odd prime factors

By

Akiko Ito*

Abstract

For a given positive integer n, there exist infinitely many imaginary quadratic fields whose class number is divisible by n. In this paper, we show that there exist infinitely many imaginary quadratic fields whose class number is divisible by $2n$ and whose discriminant has only two odd prime divisors. This is an analogue of the result of D. Byeon and S. Lee [3].

§ 1. Introduction

For a given positive integer n, there are infinitely many imaginary quadratic fields whose class number is divisible by n. Such results are obtained by T. Nagell [8], N. C. Ankeny and S. Chowla [1], R. A. Mollin [7], etc. Similarly, for a given positive integer n, there exist infinitely many real quadratic fields whose class number is divisible by n. Y. Yamamoto [11], P. J. Weinberger [10], etc. obtained such results. Their proofs were given by constructing such quadratic fields explicitly. We begin with a result of Ankeny and Chowla.

Theorem 1.1 (Ankeny and Chowla, [1]). *Let n be a positive even integer and d be a square-free integer of the form $3^n - x^2$, where x is an even integer such that $0 < x < (2 \cdot 3^{n-1})^{1/2}$. Then*

$$n \mid h(-d),$$

where $h(-d)$ denotes the class number of the quadratic field $\mathbb{Q}(\sqrt{-d})$.

Received June 1, 2011. Revised April 23, 2012. Revised June 7, 2012. Accepted June 18, 2012.
2000 Mathematics Subject Classification(s): 11R11, 11R29.
Key Words: *imaginary quadratic fields, class numbers, discriminants.*
Supported by Grant-in-Aid for JSPS Fellows (22-222) from Japan Society for the Promotion of Science.

*Graduate School of Mathematics, Nagoya University, Aichi 464-8602, Japan.
e-mail: m07004a@math.nagoya-u.ac.jp

Using this theorem, they proved that there are infinitely many imaginary quadratic fields whose class number is divisible by a given positive integer. Mollin [7] gave a generalization of Theorem 1.1. He studied the divisibility of the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{x^2 - m^n})$ and $\mathbb{Q}(\sqrt{x^2 - 4m^n})$, where m and n are integers greater than 1 and x is a positive integer. As a refinement of his result, K. Soundararajan proved the following:

Theorem 1.2 (Soundararajan, [9]). *Let n be an integer greater than 2. Suppose that $d \geq 63$ is a square-free integer such that $t^2 d = m^n - x^2$, where t, m and x are positive integers with $\gcd(m, 2x) = 1$ and with $m^n < (d+1)^2$. Then,*

$$n \mid h(-d).$$

Using Theorem 1.2, he obtained the quantitative estimate of the number of imaginary quadratic fields whose class number is divisible by n. Many other results on the divisibility of class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{x^2 - m^n})$ and $\mathbb{Q}(\sqrt{x^2 - 4m^n})$ are also known (cf. [4], [5], [6], [11], etc.). In this paper, we consider whether there are infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{x^2 - m^n})$ and $\mathbb{Q}(\sqrt{x^2 - 4m^n})$ whose class number is divisible by n and whose discriminant has only two odd prime divisors. D. Byeon and S. Lee proved the following:

Theorem 1.3 (Byeon and Lee, [3]). *Let n be an integer greater than 1. Then, there are infinitely many imaginary quadratic fields whose class number is divisible by $2n$ and whose discriminant has only two odd prime divisors.*

This theorem was proved by showing the following proposition.

Proposition 1.4. *Let n be an integer greater than 1. Then,*

$$\sharp\left\{ (p,q) \;\middle|\; p, q : \textit{odd prime such that } p \not\equiv q \bmod 4 \textit{ and } 2n \mid h(-pq). \right\} = \infty.$$

More precisely, in the proof of Theorem 1.3, they construct an infinite family of imaginary quadratic fields satisfying the conditions from the fields $\mathbb{Q}(\sqrt{x^2 - 4m^{2n}})$, where x is a positive odd integer and m is an integer greater than 1 such that $\gcd(m, x) = 1$ and $4m^{2n} > x^2$. In this case, we have $4m^{2n} - x^2 = pq \equiv 3 \bmod 4$. Then, p and q are odd prime numbers such that $p \not\equiv q \bmod 4$. The case where $p \equiv q \bmod 4$ is not treated. Therefore, we consider this case and obtain the following:

Theorem 1.5. *Let n be an integer greater than 1. Then,*

$$\sharp\left\{ (p,q) \;\middle|\; p, q : \textit{odd prime such that } p \equiv q \bmod 4 \textit{ and } 2n \mid h(-pq). \right\} = \infty.$$

In fact, in Theorem 1.5, we prove that there exist infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{x^2 - m^{2n}})$ satisfying the conditions, where x is a positive even integer and m is an odd integer greater than 1 such that $\gcd(m, x) = 1$ and $m^{2n} > x^2$. In this case, we have $m^{2n} - x^2 = pq \equiv 1 \bmod 4$. Then, p and q are odd prime numbers such that $p \equiv q \bmod 4$.

This paper is organized as follows. In Section 2, we state the proof of Theorem 1.5. Concerning Proposition 1.4 and Theorem 1.5, we also show that if $\gcd(n, 3) = 1$, there exist infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{x^2 - m^{2n}})$ whose class number is divisible by $2n$ and whose discriminant has only two odd prime divisors p and q such that $p \not\equiv q \bmod 4$, where x is a positive odd integer and m is a positive even integer such that $\gcd(m, x) = 1$ and $m^{2n} > x^2$. We state this result (Theorem 3.1) in Section 3.1 and prove this in Section 3.2. The method of the proofs of Theorems 1.5 and 3.1 are based on the one in [3]. We use the result of J. Brüdern, K. Kawada and T. D. Wooley [2] on the number of integer values of the polynomial $2\Phi(x)$ which are the sum of two primes, where $\Phi(x) \in \mathbb{Z}[x]$. We also state an application of Theorem 3.1 related to large cyclic 2-class groups in Section 3.3.

§ 2. Proof of Theorem 1.5

In this section, we state the proof of Theorem 1.5.

§ 2.1. Preliminary

To show Theorem 1.5, we use the result of Brüdern, Kawada and Wooley that almost all integer values of the polynomial $2\Phi(x) \in \mathbb{Z}[x]$ are the sum of two primes.

Theorem 2.1 (Brüdern, Kawada and Wooley, [2]). *Let $\Phi(x) \in \mathbb{Z}[x]$ be a polynomial of degree k with positive leading coefficient and let $S_k(N, \Phi)$ be the number of positive integers n with $1 \le n \le N$, for which the equation $2\Phi(n) = p+q$ has no solution in primes p and q. Then, there exists an absolute constant $c > 0$ such that*

$$S_k(N, \Phi) \ll_\Phi N^{1-c/k}.$$

Remark. In Theorem 2.1, $S_k(N, \Phi) \ll_\Phi N^{1-c/k}$ means that there is a constant C which depends on Φ and satisfies $S_k(N, \Phi) < CN^{1-c/k}$ for sufficiently large N.

§ 2.2. Proof of Theorem 1.5

First, we consider the prime divisors of the discriminants of imaginary quadratic fields. We use Theorem 2.1. Let n be an integer greater than 1. Define

$$\Phi(x) := (4x + 1)^n \in \mathbb{Z}[x].$$

From Theorem 2.1, there are infinitely many positive integers m', for which the equation

$$2\Phi(m') = 2(4m'+1)^n = p+q \tag{2.1}$$

has a solution in odd primes p and q. Since $2\Phi(m') = 2(4m'+1)^n \equiv 2 \bmod 4$, the prime numbers p and q satisfy one of the following conditions: (i) $p \equiv q \equiv 1 \bmod 4$, (ii) $p \equiv q \equiv 3 \bmod 4$. We can assume $p > q$ without loss of generality. For m', p and q satisfying the equation (2.1), we put $m := 4m'+1$ and $x := \dfrac{p-q}{2}$. From

$$m^{2n} - x^2 = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 = pq, \tag{2.2}$$

we see that there are infinitely many distinct positive square-free integers of the form $m^{2n} - x^2$ that has only two odd prime divisors, where m is an odd integer greater than 1 and x is a positive even integer.

Secondly, we show $2n \mid h(-pq)$. We can write

$$(m^{2n}) = (x^2 + pq) = (x + \sqrt{-pq})(x - \sqrt{-pq})$$

in $\mathbb{Q}(\sqrt{-pq})$. We easily see that ideals $(x + \sqrt{-pq})$ and $(x - \sqrt{-pq})$ are coprime. Then,

$$(x + \sqrt{-pq}) = \mathcal{I}^{2n} \tag{2.3}$$

for some ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{Q}(\sqrt{-pq})}$. Assume that the ideal class containing $\mathcal{I}$ has order r less than $2n$. From $r \mid 2n$, we have $r \leq n$. Since $-pq \equiv 3 \bmod 4$, we find $\mathcal{O}_{\mathbb{Q}(\sqrt{-pq})} = \mathbb{Z}[\sqrt{-pq}]$. Then, we can write

$$\mathcal{I}^r = (u + v\sqrt{-pq})$$

for some integers u and v. Note that u and v are not zero. In fact, we see

$$(x + \sqrt{-pq}) = \mathcal{I}^{2n} = (\mathcal{I}^r)^{\frac{2n}{r}} = (u + v\sqrt{-pq})^{\frac{2n}{r}}.$$

If $u = 0$ or $v = 0$, the above equation does not hold. Since

$$\mathbb{Q}(\sqrt{-pq}) \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}),$$

we have $\mathcal{O}^{\times}_{\mathbb{Q}(\sqrt{-pq})} = \{\pm 1\}$. Then,

$$x + \sqrt{-pq} = \pm(u + v\sqrt{-pq})^{\frac{2n}{r}}.$$

Taking the norm of both sides of the equation (2.3), we have

$$m^{2n} = x^2 + pq = N(\mathcal{I}^r)^{\frac{2n}{r}} = (u^2 + v^2pq)^{\frac{2n}{r}}.$$

Since $u^2 \geq 1$, $v^2 \geq 1$ and $n/r \geq 1$ hold, we see

$$m^{2n} = (u^2 + v^2 pq)^{\frac{2n}{r}} \geq (1 + pq)^2.$$

Then,

$$m^n - 1 \geq pq. \tag{2.4}$$

From the equation (2.2), we have

$$(m^n + x)(m^n - x) = pq.$$

Since

$$m^n + x = \frac{p+q}{2} + \frac{p-q}{2} = p,$$

we find $m^n + x = p$ and $m^n - x = q$. On the other hand, from the equation (2.4),

$$m^n + x > m^n - 1 \geq pq.$$

This is a contradiction. Then,

$$r = 2n.$$

The proof of Theorem 1.5 is completed.

§ 3. Another proof of Proposition 1.4

In this section, we state another proof of Proposition 1.4. We construct another infinite family of imaginary quadratic fields satisfying the condition. First, we state this construction (Theorem 3.1) in Section 3.1. Secondly, we prove Theorem 3.1 in Section 3.2. Finally, we state an application of this theorem in Section 3.3.

§ 3.1. Result

Concerning Theorem 1.5, we obtain the following:

Theorem 3.1. *Let n be an integer greater than 1 such that $\gcd(n, 3) = 1$. Then, there exist infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{x^2 - m^{2n}})$ whose class number is divisible by $2n$ and whose discriminant has only two odd prime divisors p and q such that $p \not\equiv q \bmod 4$, where x is a positive odd integer and m is a positive even integer such that $\gcd(m, x) = 1$ and $m^{2n} > x^2$.*

This is another proof of Proposition 1.4 for the case where $\gcd(n, 3) = 1$.

§ 3.2. Proof of Theorem 3.1

In this section, we prove Theorem 3.1. Although the method of the proof is based on the one in Proposition 1.4 and Theorem 1.5, we need several changes.

Let n be an integer greater than 1 such that $\gcd(n,3)=1$. Define

$$\Phi(x) := (4x+2)^n \in \mathbb{Z}[x].$$

From Theorem 2.1, there are infinitely many positive integers m', for which the equation

$$2\Phi(m') = 2(4m'+2)^n = p+q \tag{3.1}$$

has a solution in odd primes p and q. Since $2\Phi(m') = 2(4m'+2)^n \equiv 0 \bmod 4$, the prime numbers p and q satisfy one of the following conditions: (i) $p \equiv 1 \bmod 4$, $q \equiv 3 \bmod 4$, (ii) $p \equiv 3 \bmod 4$, $q \equiv 1 \bmod 4$. We can assume $p > q$ without loss of generality. For m', p and q satisfying the equation (3.1), we put $m := 4m'+2$ and $x := \dfrac{p-q}{2}$. From

$$m^{2n} - x^2 = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 = pq, \tag{3.2}$$

we see that there are infinitely many distinct positive square-free integers of the form $m^{2n} - x^2$ that has only two odd prime divisors, where m is a positive even integer and x is a positive odd integer. Next, we show $2n \mid h(-pq)$. We can write

$$(m^{2n}) = (x^2 + pq) = (x+\sqrt{-pq})(x-\sqrt{-pq})$$

in $\mathbb{Q}(\sqrt{-pq})$. We easily see that ideals $(x+\sqrt{-pq})$ and $(x-\sqrt{-pq})$ are coprime. Then,

$$(x+\sqrt{-pq}) = \mathcal{I}^{2n} \tag{3.3}$$

for some ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbb{Q}(\sqrt{-pq})}$. Assume that the ideal class containing $\mathcal{I}$ has order r less than $2n$. From $r \mid 2n$, we have $r \leq n$. Since $-pq \equiv 1 \bmod 4$, we find $\mathcal{O}_{\mathbb{Q}(\sqrt{-pq})} = \mathbb{Z}\left[\dfrac{1+\sqrt{-pq}}{2}\right]$. Then, we can write

$$\mathcal{I}^r = \left(\frac{u+v\sqrt{-pq}}{2}\right)$$

for some non-zero integers u and v with $u \equiv v \bmod 2$. Since

$$\mathbb{Q}(\sqrt{-pq}) \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3}),$$

we have $\mathcal{O}^{\times}_{\mathbb{Q}(\sqrt{-pq})} = \{\pm 1\}$. Then,

$$x+\sqrt{-pq} = \pm\left(\frac{u+v\sqrt{-pq}}{2}\right)^{\frac{2n}{r}}.$$

To check the parity of u and v, we need the following lemma:

Lemma 3.2 (Kishi, [6, p. 190] and Ito, [4, pp. 384-385])**.** (1) *Let d be a positive square-free integer such that $d \equiv 3 \bmod 8$. For any positive integer s,*

$$\left(\frac{u_1 + v_1\sqrt{-d}}{2}\right)^s \in \mathbb{Z}[\sqrt{-d}]$$

if and only if

$$3 \mid s,$$

where u_1 and v_1 are odd integers.
(2) *Let d be a positive square-free integer such that $d \equiv 7 \bmod 8$. For any positive integer s,*

$$\left(\frac{u_1 + v_1\sqrt{-d}}{2}\right)^s \notin \mathbb{Z}[\sqrt{-d}],$$

where u_1 and v_1 are odd integers.

By Lemma 3.2 and the assumption of Theorem 3.1, we have $u \equiv v \equiv 0 \bmod 2$. We write $u = 2u'$ and $v = 2v'$ for some integers u' and v'. Taking the norm of both sides of the equation (3.3), we have

$$m^{2n} = x^2 + pq = N(\mathcal{I}^r)^{\frac{2n}{r}} = (u'^2 + v'^2pq)^{\frac{2n}{r}}.$$

Since $u'^2 \geq 1$, $v'^2 \geq 1$ and $n/r \geq 1$ hold, we see

$$m^{2n} = (u'^2 + v'^2pq)^{\frac{2n}{r}} \geq (1 + pq)^2.$$

Then,

$$m^n - 1 \geq pq. \tag{3.4}$$

From the equation (3.2), we have

$$(m^n + x)(m^n - x) = pq.$$

Since

$$m^n + x = \frac{p+q}{2} + \frac{p-q}{2} = p,$$

we find $m^n + x = p$ and $m^n - x = q$. On the other hand, from the equation (3.4),

$$m^n + x > m^n - 1 \geq pq.$$

This is a contradiction. Then,

$$r = 2n.$$

The proof of Theorem 3.1 is completed.

§ 3.3. Application of Theorem 3.1

In this section, we state an application of Theorem 3.1. As a classical problem, the question whether there exist quadratic fields with arbitrarily large cyclic 2-class group is known. Combining Proposition 1.4 or Theorem 3.1 and genus theory of Gauss, we have the following:

Corollary 3.3. *Let t be a positive integer. Then, there are infinitely many imaginary quadratic fields whose* 2*-class group is a cyclic group of order divisible by* 2^t*.*

We obtain this corollary by applying Proposition 1.4 or Theorem 3.1 to the case where $n = 2^t$. In [3], an infinite family of imaginary quadratic fields satisfying the above condition is constructed from the fields $\mathbb{Q}(\sqrt{x^2 - 4m^{2n}})$. On the other hand, we construct such an infinite family from the fields $\mathbb{Q}(\sqrt{x^2 - m^{2n}})$. These facts imply that for any given positive integer t there are infinitely many imaginary quadratic fields of both forms $\mathbb{Q}(\sqrt{x^2 - 4m^{2n}})$ and $\mathbb{Q}(\sqrt{x^2 - m^{2n}})$ whose 2-class group is a cyclic group of order divisible by 2^t.

Acknowledgement. The author would like to thank the organizers. She wishes to express her gratitude to the referee for careful reading and useful comments. And she thanks Professor Manabu Ozaki and Doctor Satoshi Fujii for helpful discussions and valuable advice. She also thanks Professor Kohji Matsumoto and Professor Hiroshi Suzuki for continuous encouragement.

References

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

[2] Brüdern, J., Kawada, K. and Wooley, T. D., Additive representation in thin sequences, II: The binary Goldbach problem, *Mathematica,* **47** (2000), no. 1-2, 117–125.

[3] Byeon, D. and Lee, S., Divisibility of class numbers of imaginary quadratic fields whose discriminant has only two prime factors, *Proc. Japan Acad. Ser. A Math. Sci.,* **84** (2008), no. 1, 8–10.

[4] Ito, A., Remarks on the divisibility of the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - q^n})$, *Glasgow Math. J.,* **53** (2011), 379–389.

[5] Ito, A., A note on the divisibility of class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{a^2 - k^n})$, *Proc. Japan Acad. Ser. Math. Sci.,* **87** (2011), no. 9, 151–155.

[6] Kishi, Y., Note on the divisibility of the class number of certain imaginary quadratic fields, *Glasg. Math. J.,* **51** (2009), no. 1, 187–191; Corrigendum, *Glasg. Math. J.,* **52** (2010), no. 1, 207–208.

[7] Mollin, R. A., Solutions of Diophantine equations and divisibility of class numbers of complex quadratic fields, *Glasgow Math. J.,* **38** (1996), 195–197.

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

[9] Soundararajan, K., Divisibility of class numbers of imaginary quadratic fields, *J. London Math. Soc. (2),* **61** (2000), no. 3, 681–690.

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

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