IDEAL CLASS GROUPS OF IMAGINARY QUADRATIC FIELDS

DONGHO BYEON

Abstract. Let d be a square-free positive integer and $\mathrm{CL}(-d)$ the ideal class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. In this paper, we show that given any odd integer $g \geq 3$ and any integers $r \geq 1$, s with $0 \leq s \leq r$, there are infinitely many d such that $\mathrm{CL}(-d)$ contains an element of order g and $\mathrm{CL}(-d)/\mathrm{CL}(-d)^4 \cong (\mathbb{Z}/2\mathbb{Z})^{r-s} \times (\mathbb{Z}/4\mathbb{Z})^s$.

1. Introduction

Let d be a square-free positive integer and $\mathrm{CL}(-d)$ the ideal class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. Ankeny and Chowla [AC] proved that given any positive integer g, there are infinitely many d such that $\mathrm{CL}(-d)$ contains an element of order g. For real quadratic fields, Weinberger [We] obtained a similar result.

Let e_{2^n} be the 2^n-rank of $\mathrm{CL}(-d)$, which is the maximal integer $t \geq 0$ such that there is an injection from $(\mathbb{Z}/2^n\mathbb{Z})^t$ to $\mathrm{CL}(-d)$. Gauss' genus theory shows that $e_2 + 1$ is the number of prime factors of d (resp. 4d) if $d \equiv 3 \pmod 4$ (resp. otherwise). Morton [Mo] showed that if d satisfies some conditions, e_4 can be calculated from the Legendre symbols of the prime factors of d and e_8 can be determined from a conjugacy class in the Galois group of a suitable normal extension of $\mathbb{Q}$ and proved that there are infinitely many d such that e_2, e_4 and e_8 have arbitrarily assigned values. For real quadratic fields, Rédei [Ré] obtained a similar result.

In this paper, we prove that given any odd integer $g \geq 3$, there are infinitely many d such that $\mathrm{CL}(-d)$ has an element of order g and $e_2 \geq 1$, e_4 have arbitrarily assigned values.

The author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2020R1F1A1A01053449).

Theorem 1.1. *Let d be a square-free positive integer and $\mathrm{CL}(-d)$ the ideal class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. For given any odd integer $g \geq 3$ and any integers $r \geq 1$, s with $0 \leq s \leq r$, there are infinitely many d such that $\mathrm{CL}(-d)$ contains an element of order g and*

$$\mathrm{CL}(-d)/\mathrm{CL}(-d)^4 \cong (\mathbb{Z}/2\mathbb{Z})^{r-s} \times (\mathbb{Z}/4\mathbb{Z})^s.$$

We remark that Theorem 1.1 does not include the case where both exponents are 0, that is, the class number of $\mathbb{Q}(\sqrt{-d})$ is odd.

Our proof of Theorem 1.1 depends on the calculation of the Legendre symbols. So we can not obtain a similar result for general e_8. But we can prove the following theorem for special e_8 which can be calculated from the quartic residue symbol.

Theorem 1.2. *Let d be a square-free positive integer and $\mathrm{CL}(-d)$ the ideal class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. For given any odd integer $g \geq 3$ and any integers $r \geq 1$, $\rho = \{0, 1\}$, there are infinitely many d such that $\mathrm{CL}(-d)$ contains an element of order g and*

$$\mathrm{CL}(-d)/\mathrm{CL}(-d)^8 \cong (\mathbb{Z}/2\mathbb{Z})^{r-1} \times (\mathbb{Z}/4\mathbb{Z})^{\rho} \times (\mathbb{Z}/8\mathbb{Z})^{1-\rho}.$$

It seems to difficult to prove that for a fixed integer $g \geq 3$, there are infinitely many d such that $\mathrm{CL}(-d)$ has an element of order g and $e_2 = 0$, that is, there are infinitely many primes $p \equiv 3 \pmod 4$ such that $\mathrm{CL}(-p)$ has an element of order g. Using the idea of Balog and Ono [BO], Byeon and Lee [BL] (resp. Lapkova [La]) proved that there are infinitely many imaginary quadratic fields whose discriminant has only two (resp. three) prime factors and whose ideal class group has an element of arbitrary order g. For real quadratic fields, Chattopadhyay [Ch] proved that given any positive integer l, there are infinitely many real quadratic fields whose discriminant has l or more prime factors and whose ideal class group has an element of order 3.

2. Preliminaries

To prove Theorem 1.1 and Theorem 1.2, we need the following lemmas.

Lemma 2.1. *Let $g \geq 2$ be an integer. Suppose that $d = 4m^{2g} - n^2$ is square-free, where m and n are positive integers with $(n, 2) = 1$ and $2m^g - n > 1$. Then $\mathrm{CL}(-d)$ contains an element of order $2g$.*

Proof. See [BL, Proof of Theorem 1.2]. □

Lemma 2.2. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial which has a positive leading coefficient with degree ≥ 1. Let A, B be relatively prime odd integers and u, v, C positive integers with $0 < u, v < C$ and $(u, C) = (v, C) = 1$. Suppose there is at least one integer m' such that*

$$2f(m') \equiv Au + Bv \pmod{C} \text{ and } (AB, f(m')) = 1.$$

Then there are infinitely many integers m such that

$$2f(m) = Ap + Bq$$

for some primes $p \equiv u$ and $q \equiv v \pmod{C}$.

Proof. Proof of Lemma 2.2 is exactly same to [BJ, Proof of Lemma 2.2] if 9 is changed by C. □

3. Proof of Theorem 1.1

To prove Theorem 1.1, we need the following lemma.

Lemma 3.1. *Let $d = Dq$ be a positive integer such that $D = p_1 \cdots p_r$ is a product of r primes with*

$$p_i \equiv 1 \pmod{4} \text{ and } \left(\frac{p_i}{p_j}\right) = 1 \text{ for } i \neq j,$$

and q is a prime with

$$q \equiv 3 \pmod{4}, \ \left(\frac{q}{p_i}\right) = 1 \text{ for } 1 \leq i \leq s \text{ and } \left(\frac{q}{p_i}\right) = -1 \text{ for } s+1 \leq i \leq r.$$

Then

$$\mathrm{CL}(-d)/\mathrm{CL}(-d)^4 \cong (\mathbb{Z}/2\mathbb{Z})^{r-s} \times (\mathbb{Z}/4\mathbb{Z})^s.$$

Proof. See [Mo, p. 160]. □

Now we can prove Theorem 1.1.

Proof of Theorem 1.1. First we consider the case $s \geq 1$. Let p_i $(1 \leq i \leq r-1)$ be fixed primes such that

$$\begin{aligned} &p_i \equiv 1 \pmod 4 \text{ for } 1 \leq i \leq r-1, \\ &\left(\frac{p_i}{p_j}\right) = 1 \text{ for } i \neq j, \\ &\left(\frac{3}{p_i}\right) = 1 \text{ for } 1 \leq i \leq s-1, \\ &\left(\frac{3}{p_i}\right) = -1 \text{ for } s \leq i \leq r-1. \end{aligned}$$

If $r \geq 2$, Let $A = 1$, $B = p_1 \cdots p_{r-1}$, $C = 4p_1 \cdots p_{r-1}$, $u = 4 - 3p_1 \cdots p_{r-1}$, $v = 3$ and if $r = 1$, let $A = 1$, $B = 1$, $C = 4$, $u = 1$, $v = 3$. Let $f(x) = 2x^{2g}$. By Lemma 2.2, there are infinitely many integers m such that

$$4m^{2g} = Ap + Bq$$

for some primes $p \equiv u$ and $q \equiv v \pmod C$. We note that

$$p \equiv 1 \pmod 4, \ \left(\frac{p}{p_i}\right) = \left(\frac{p_i}{p}\right) = 1 \text{ for } 1 \leq i \leq r-1$$

and

$$q \equiv 3 \pmod 4, \ \left(\frac{q}{p_i}\right) = \left(\frac{q}{p}\right) = 1 \text{ for } 1 \leq i \leq s-1, \ \left(\frac{q}{p_i}\right) = -1 \text{ for } s \leq i \leq r-1.$$

Let $n = 2m^{2g} - \min\{Ap, Bq\} > 0$. Then we have

$$d := 4m^{4g} - n^2 = \left(\frac{Ap+Bq}{2}\right)^2 - \left(\pm\frac{Ap-Bq}{2}\right)^2 = ABpq.$$

By Lemma 2.1 and Lemma 3.1, $\mathrm{CL}(-d)$ contains an element of order $4g$ and

$$\mathrm{CL}(-d)/\mathrm{CL}(-d)^4 \cong (\mathbb{Z}/2\mathbb{Z})^{r-s} \times (\mathbb{Z}/4\mathbb{Z})^s.$$

Now we consider the case $s = 0$. Assume that g is odd. Let p_i $(1 \leq i \leq r-1)$ be fixed primes such that

$$\begin{aligned} &p_i \equiv 1 \pmod 4 \text{ for } 1 \leq i \leq r-1, \\ &\left(\frac{p_i}{p_j}\right) = 1 \text{ for } i \neq j, \\ &\left(\frac{3}{p_i}\right) = -1 \text{ for } 1 \leq i \leq r-1, \\ &\left(\frac{5}{p_i}\right) = 1 \text{ for } 1 \leq i \leq r-1. \end{aligned}$$

If $r \geq 2$, let $A = p_1 \cdots p_{r-1}$, $B = 1$, $C = 12p_1 \cdots p_{r-1}$, $u = 5$, $v = 4 \cdot 3^g - 5p_1 \cdots p_{r-1}$ and if $r = 1$, let let $A = 1$, $B = 1$, $C = 12$, $u = 5$, $v = 4 \cdot 3^g - 5$. Let $f(x) = 2(3x^2)^g$. By Lemma 2.2, there are infinitely many integers m such that

$$4(3m^2)^g = Ap + Bq$$

for some primes $p \equiv u$ and $q \equiv v \pmod C$. We note that

$$p \equiv 1 \pmod 4, \ \left(\frac{p}{p_i}\right) = \left(\frac{p_i}{p}\right) = 1 \text{ for } 1 \leq i \leq r-1$$

and

$$q \equiv 3 \pmod 4, \ \left(\frac{q}{p_i}\right) = \left(\frac{q}{p}\right) = -1 \text{ for } 1 \leq i \leq r-1.$$

Let $n = 2(3m^2)^g - \min\{Ap, Bq\} > 0$. Then we have

$$d := 4(3m^2)^{2g} - n^2 = ABpq.$$

By Lemma 2.1 and Lemma 3.1, $\mathrm{CL}(-d)$ contains an element of order $2g$ and

$$\mathrm{CL}(-d)/\mathrm{CL}(-d)^4 \cong (\mathbb{Z}/2\mathbb{Z})^r.$$

□

Remark. The condition that g is odd in Theorem 1.1 is only required for the case $s = 0$.

4. Proof of Theorem 1.2

Before we prove Theorem 1.2, we briefly explain how to compute e_8. For details, see [Mo]. Let d be the square-free positive integer in Lemma 3.1 and $\mathfrak{p}_i$ the prime ideals of $\mathbb{Q}(\sqrt{-d})$ lying above p_i. Then there are ideals $\mathfrak{z}_j$ of $\mathbb{Q}(\sqrt{-d})$ such that

$$\mathfrak{z}_j^2 \sim \mathfrak{p}_i \text{ for } 1 \le i \le s.$$

Let ξ be the group homomorphism

$$\xi : \{\pm 1\} \to \mathbb{F}_2 \text{ defined by } \xi(1) = 0, \ \xi(-1) = 1$$

and

$$\chi_i(\mathfrak{z}_j) = \Big(\frac{N\mathfrak{z}_j, -d}{p_i}\Big) \text{ for } (1 \le i, j \le s),$$

where N is the norm from $\mathbb{Q}(\sqrt{-d})$ to $\mathbb{Q}$ and $\left(\frac{a,b}{p}\right)$ is the Hilbert symbol. Then we have the following Lemma.

Lemma 4.1. *Let d be the square-free positive integer in Lemma 3.1 and let ρ be the rank over $\mathbb{F}_2$ of the $s \times s$ matrix*

$$M' = (\xi\chi_i(\mathfrak{z}_j)) \ (1 \le i, j \le s).$$

Then

$$\mathrm{CL}(-d)/\mathrm{CL}(-d)^8 \cong (\mathbb{Z}/2\mathbb{Z})^{r-s} \times (\mathbb{Z}/4\mathbb{Z})^{\rho} \times (\mathbb{Z}/8\mathbb{Z})^{s-\rho}.$$

Proof. See [Mo, p. 161]. □

The values $\chi_i(\mathfrak{z}_j)$ can be determined from the Frobenius symbol $\left(\frac{\Sigma_D/\mathbb{Q}}{q}\right)$ for some normal extension Σ_D of $\mathbb{Q}$ and the quartic residue symbols $\left(\frac{p_i}{p_j}\right)_4$, where the quartic residue symbol $\left(\frac{a}{p}\right)_4$ is defined for primes $p \equiv 1 \pmod 4$ and quadratic residues a of p by the formula

$$\pm 1 = \Big(\frac{a}{p}\Big)_4 \equiv a^{\frac{p-1}{4}} \pmod p.$$

But the diagonal terms $\chi_i(\mathfrak{z}_i)$ can be calculated using only the quartic residue symbols.

Lemma 4.2. [Mo, Lemma 7] *For $1 \le i \le s$, we have*

$$\chi_i(\mathfrak{z}_i) = \Big(\frac{D/p_i}{p_i}\Big)_4 \Big(\frac{-q}{p_i}\Big)_4.$$

Now we can prove Theorem 1.2.

Proof of Theorem 1.2. First we consider the case $\rho = 0$. Let p_i $(1 \le i \le r-1)$ be fixed primes such that

$$\begin{aligned} &p_i \equiv 1 \pmod 4 \text{ for } 1 \le i \le r-1, \\ &\Big(\frac{p_i}{p_j}\Big) = 1 \text{ for } i \ne j, \\ &\Big(\frac{3}{p_i}\Big) = -1 \text{ for } 1 \le i \le r-1. \end{aligned}$$

If $r \ge 2$, let $A = 1$, $B = p_1 \cdots p_{r-1}$, $C = 4p_1 \cdots p_{r-1}$, $u = 4 - 3p_1 \cdots p_{r-1}$, $v = 3$ and if $r = 1$, let $A = 1$, $B = 1$, $C = 4$, $u = 1$, $v = 3$. Let $f(x) = 2x^{4g}$. By Lemma 2.2, there are infinitely many integers m such that

$$4m^{4g} = Ap + Bq$$

for some primes $p \equiv u$ and $q \equiv v \pmod C$. We note that

$$p \equiv 1 \pmod 4, \ \Big(\frac{p}{p_i}\Big) = \Big(\frac{p_i}{p}\Big) = 1 \text{ for } 1 \le i \le r-1$$

and

$$q \equiv 3 \pmod 4, \ \Big(\frac{q}{p}\Big) = 1, \ \Big(\frac{q}{p_i}\Big) = -1 \text{ for } 1 \le i \le r-1.$$

Let $n = 2m^{4g} - \min\{Ap, Bq\} > 0$. Then we have

$$d := 4m^{8g} - n^2 = ABpq.$$

By Lemma 4.2, we have

$$\chi_1(\mathfrak{z}_1) = \Big(\frac{ABp/p}{p}\Big)_4 \Big(\frac{-q}{p}\Big)_4 = \Big(\frac{-p_1 \cdots p_{r-1} q}{p}\Big)_4 = \Big(\frac{-4}{p}\Big)_4 = 1,$$

so

$$\rho = 0.$$

By Lemma 2.1 and Lemma 4.1, $\mathrm{CL}(-d)$ contains an element of order $8g$ and

$$\mathrm{CL}(-d)/\mathrm{CL}(-d)^8 \cong (\mathbb{Z}/2\mathbb{Z})^{r-1} \times (\mathbb{Z}/8\mathbb{Z}).$$

Now we consider the case $\rho = 1$. Assume that g is odd. Let p_i $(1 \le i \le r-1)$ be fixed primes such that

$$\begin{aligned} &p_i \equiv 1 \pmod 4 \text{ for } 1 \le i \le r-1, \\ &\Big(\frac{p_i}{p_j}\Big) = 1 \text{ for } i \ne j, \\ &\Big(\frac{3}{p_i}\Big) = -1 \text{ for } 1 \le i \le r-1, \\ &p_i \equiv 1 \pmod 5 \text{ for } 1 \le i \le r-1. \end{aligned}$$

If $r \ge 2$, let $A = 1$, $B = p_1 \cdots p_{r-1}$, $C = 20p_1 \cdots p_{r-1}$, $u = 4 \cdot 5^{2g} - 3p_1 \cdots p_{r-1}$, $v = 3$ and if $r = 1$, let $A = 1$, $B = 1$, $C = 20$, $u = 4 \cdot 5^{2g} - 3$, $v = 3$. Let $f(x) = 2(5x^2)^{2g}$. By Lemma 2.2, there are infinitely many integers m such that

$$4(5m^2)^{2g} = Ap + Bq$$

for some primes $p \equiv u$ and $q \equiv v \pmod C$. We note that

$$p \equiv 1 \pmod 4, \ \Big(\frac{p}{p_i}\Big) = \Big(\frac{p_i}{p}\Big) = 1 \text{ for } 1 \le i \le r-1$$

and

$$q \equiv 3 \pmod 4, \ \Big(\frac{q}{p}\Big) = 1, \ \Big(\frac{q}{p_i}\Big) = -1 \text{ for } 1 \le i \le r-1.$$

Let $n = 2(5m^2)^{2g} - \min\{Ap, Bq\} > 0$. Then we have

$$d := 4(5m^2)^{4g} - n^2 = ABpq.$$

By Lemma 4.2, we have

$$\chi_1(\mathfrak{z}_1) = \Big(\frac{ABp/p}{p}\Big)_4 \Big(\frac{-q}{p}\Big)_4 = \Big(\frac{-p_1 \cdots p_{r-1}q}{p}\Big)_4 = \Big(\frac{-4 \cdot 5^2}{p}\Big)_4 = -1,$$

so

$$\rho = 1.$$

By Lemma 2.1 and Lemma 4.1, $\mathrm{CL}(-d)$ contains an element of order $4g$ and

$$\mathrm{CL}(-d)/\mathrm{CL}(-d)^8 \cong (\mathbb{Z}/2\mathbb{Z})^{r-1} \times (\mathbb{Z}/4\mathbb{Z}).$$

□

Remark. The condition that g is odd in Theorem 1.2 is only required for the case $\rho = 1$.

Acknowledgment. The authors thank the referees for their careful readings and many valuable suggestions.

References

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

[BJ] D. Byeon and K. Jeong, *Sums of two rational cubes with many prime factors*, J. Number Theory **179** (2017), 240–255.

[BL] D. Byeon and S. Lee, *Divisibilty of class numbers of imaginary quadratic fields whose discriminant has only two prime factors*, Proc. Japan Acad. Ser. A **84** (2008), 8–10.

[BO] A. Balog and K. Ono, *Elements of class groups and Shafarevich-Tate groups of elliptic curves*, Duke Math. J. **120** (2003), 35–63.

[Ch] J. Chattopadhyay, *A short note on the divisibility of class number of real quadratic fields*, J. Ramanujan Math. Soc. **34** (2019), 389–392.

[La] K. Lapkova, *Divisibilty of class numbers of imaginary quadratic fields whose discriminant has only three prime factors*, Acta Math. Hungar. **137** (2012), 36–63.

[Mo] P. Morton, *Density results for the 2-classgroups of imaginary quadratic fields*, J. Reine Angew. Math. **332** (1982), 156–187.

[Ré] L. Rédei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I*, J. Reine Angew. Math. **180** (1938), 1–43.

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

Department of Mathematical Sciences,
Seoul National University
Seoul, Korea,
E-mail: dhbyeon@snu.ac.kr