Functiones et Approximatio
49.1 (2013), 111–135
doi: 10.7169/facm/2013.49.1.8

EXISTENCE OF AN INFINITE FAMILY OF PAIRS OF QUADRATIC FIELDS $\mathbb{Q}(\sqrt{m_1 D})$ AND $\mathbb{Q}(\sqrt{m_2 D})$ WHOSE CLASS NUMBERS ARE BOTH DIVISIBLE BY 3 OR BOTH INDIVISIBLE BY 3

Akiko Ito

Abstract: Let m_1, m_2, and m_3 be distinct square-free integers (including 1). First, we show that there exist infinitely many square-free integers d with $\gcd(m_1m_2, d) = 1$ such that the class numbers of $\mathbb{Q}(\sqrt{m_1 d})$ and $\mathbb{Q}(\sqrt{m_2 d})$ are both divisible by 3. This is a generalization of a result of T. Komatsu [15]. Secondly, we show that there exist infinitely many positive fundamental discriminants D with $\gcd(m_1m_2m_3, D) = 1$ such that the class numbers of real quadratic fields $\mathbb{Q}(\sqrt{m_1 D})$, $\mathbb{Q}(\sqrt{m_2 D})$, and $\mathbb{Q}(\sqrt{m_3 D})$ are all indivisible by 3 when m_1, m_2, and m_3 are positive. This is a generalization of a result of D. Byeon [4]. We add an application of this result to the Iwasawa invariants related to Greenberg's conjecture.

Keywords: quadratic fields, class numbers, Iwasawa invariants.

1. Introduction

For a given positive integer n, there are infinitely many imaginary quadratic fields whose class numbers are divisible by n. Such results are obtained by T. Nagell [18], N. C. Ankeny and S. Chowla [1], R. A. Mollin [17], etc. Similarly, for a given positive integer n, there are infinitely many real quadratic fields whose class numbers are divisible by n. Y. Yamamoto [25], P. J. Weinberger [24], etc. obtained such results. All the proofs of them were given by constructing such quadratic fields explicitly. Many results on the divisibility of the class number of quadratic fields are known for the case $n = 3$ particularly. We begin with a result of T. Komatsu.

Theorem 1.1 (Komatsu, [15]). *Fix a non-zero integer t. Then, there exist infinitely many both positive and negative square-free integers d such that the class numbers of quadratic fields $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{td})$ are both divisible by* 3.

Supported by Grant-in-Aid for JSPS Fellows (22-222) from Japan Society for the Promotion of Science.

2010 Mathematics Subject Classification: primary: 11R11; secondary: 11R29

The result for the case $t = -1$ is already known by [14]. For the case where $t = -3$ and $d > 1$, Theorem 1.1 follows from the Scholz inequality (Theorem 1.2 below), as there are infinitely many real quadratic fields whose class numbers are divisible by 3.

Theorem 1.2 (Scholz, [21], cf. [23, Theorem 10.10]). *Let $d > 1$ be square-free. Let r_0 be the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{d})$ and s_0 the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3d})$. Then,*

$$r_0 \leqslant s_0 \leqslant r_0 + 1.$$

One of the purpose of this paper is the following result which is regarded as a generalization of Theorem 1.1.

Theorem 1.3. *Let m_1 and m_2 be distinct square-free integers (including 1). Then, there exist infinitely many both positive and negative square-free integers d with $\gcd(m_1 m_2, d) = 1$ such that the class numbers of quadratic fields $\mathbb{Q}(\sqrt{m_1 d})$ and $\mathbb{Q}(\sqrt{m_2 d})$ are both divisible by 3.*

In detail, we see that Theorem 1.3 holds true for pairs of two real quadratic fields, for pairs of two imaginary quadratic fields, or for pairs of real and imaginary quadratic fields respectively. On the other hand, D. Byeon proved the following theorem.

Theorem 1.4 (Byeon, [4]). *Let t be a square-free integer. Then, there exist infinitely many positive fundamental discriminants D with a positive inferior limit density such that the class numbers of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{tD})$ are both indivisible by 3.*

For $t = -3$, Theorem 1.4 follows from Theorem 1.2. We denote by $h(d)$ the class number of a quadratic field $\mathbb{Q}(\sqrt{d})$. By Theorem 1.2, for a square-free integer $d > 1$, if $3 \nmid h(-3d)$, then $3 \nmid h(d)$. It is known that there exist infinitely many positive fundamental discriminants D with a positive inferior limit density such that $3 \nmid h(-3D)$ by [19]. Therefore, there exist infinitely many positive fundamental discriminants D with a positive inferior limit density such that the class numbers of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-3D})$ are both indivisible by 3. Another goal of this paper is a generalization of Theorem 1.4.

Theorem 1.5. *Let m_1, m_2, and m_3 be square-free positive integers (including 1).*

(1) *There exist infinitely many positive fundamental discriminants D with a positive inferior limit density such that $\gcd(m_1 m_2 m_3, D) = 1$ and the class numbers of real quadratic fields $\mathbb{Q}(\sqrt{m_1 D})$, $\mathbb{Q}(\sqrt{m_2 D})$, and $\mathbb{Q}(\sqrt{m_3 D})$ are all indivisible by 3.*

(2) *There exist infinitely many positive fundamental discriminants D with a positive inferior limit density such that $\gcd(m_1 m_2, D) = 1$ and the class numbers of quadratic fields $\mathbb{Q}(\sqrt{m_1 D})$ and $\mathbb{Q}(\sqrt{-m_2 D})$ are both indivisible by 3.*

This paper is organized as follows. In Section 2, we give a proof of Theorem 1.3 by constructing an explicit cubic polynomial which gives an unramified cyclic cubic extension of a quadratic field. In Section 2.1, we state the method of this construction. We treat two cases where $4 \nmid m_1 m_2$ and $4 \mid m_1 m_2$ respectively (Theorems 2.1 and 2.2). Theorem 1.3 follows from these theorems. We prove Theorem 2.1 in Section 2.2 and prove Theorem 2.2 in Section 2.3. To check the divisibility of the class numbers of the quadratic fields, we use a result of P. Llorente and E. Nart [16]. In Section 3, we give a proof of Theorem 1.5. To show this theorem, we essentially use a result of J. Nakagawa and K. Horie [19]. In Section 3.1, we state their result. In Section 3.2, we prove Theorem 1.5. In Section 3.3, we add an application of Theorem 1.5 to the Iwasawa invariants related to Greenberg's conjecture.

2. Proof of Theorem 1.3

In this section, we give a proof of Theorem 1.3, modifying the method in [15].

2.1. Construction

Let m_1 and m_2 be distinct square-free integers (including 1). First, we treat the case where $4 \nmid m_1 m_2$ and $2 \nmid m_2$. Let $\mathcal{L}$ be the set of all prime numbers l which are inert in the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ and satisfy the condition

$$\left(\frac{m_1}{l}\right) = \left(\frac{m_2}{l}\right) = 1,$$

where $(\cdot/\cdot)$ denotes the Legendre symbol. We can show that $\mathcal{L}$ is an infinite set not containing 2 and 3, using the Chebotarev density theorem as in [15, Lemma 1.1]. We fix $l \in \mathcal{L}$. Let s be a prime number such that $s \neq 2,\ 3,\ l$ and $s \nmid m_1 m_2$. We take integers n_1 and n_2 satisfying the following conditions: for each $i = 1,\ 2$,

$$n_i \equiv \begin{cases} 0 \bmod 9 & \text{if } m_i \not\equiv 0 \bmod 3, \\ 0 \bmod 3 & \text{if } m_i \equiv 0 \bmod 3, \end{cases}$$

$$m_i n_i^2 \equiv 1 \bmod l,$$

$$n_i \equiv 0 \bmod s^2,$$

and

$$\begin{cases} n_1 \equiv 0 \bmod 2, \\ n_2 \equiv 1 \bmod 2. \end{cases}$$

Note that there exist such integers n_i by the Chinese remainder theorem. Now put $r_1 := m_1 n_1^2$, $r_2 := m_2 n_2^2$, and $r := r_1 r_2$. It follows from the assumption on n_i that r_1 is even and r_2 is odd. Let P be the set of prime numbers defined by

$$P := \{p : \text{prime} \mid p \neq 3, s \text{ and } p | r(r-1)(r_1 - r_2)\}.$$

It is easy to see that 2 and l are contained in P. Let Q be the subset of P defined by

$$Q := \{q : \text{prime} \mid q \neq 3 \text{ and } q|m_1m_2\}.$$

When $m_1m_2 = -1$, ± 3, -9, the set Q is empty. We treat the set Q including the case where Q is empty. Note that $s \notin Q$. We denote by T the set of integers t satisfying the following conditions:

$$\begin{cases} t \equiv \pm 3s \bmod 27s^3, & \\ t \equiv -1 \bmod l, & \\ t \not\equiv r,\ r_1 \bmod p & \text{for any } p \in P, \\ 2t \not\equiv 3(r_1+r_2) \bmod q & \text{for any } q \in Q. \end{cases}$$

We can use the Chinese remainder theorem to make sure the set T is infinite. Define three subsets of T as follows. For the case where $r_1 > 0$ and $r_2 > 0$, let

$$T_1 := \left\{t \in T \mid t \geqslant \frac{3}{2}\mathrm{Max}\{r_1, r_2\}\right\}$$

and

$$T_2 := \{t \in T \mid t \leqslant \mathrm{Max}\{r_1, r_2\}\}.$$

For $r < 0$, let

$$T_3 := \{t \in T \mid t > t_0\},$$

where t_0 is a real number such that $t_0 > \mathrm{Max}\{r_1, r_2\}$ and $2t_0^3 - 3(r_1+r_2)t_0^2 + 6rt_0 - r(r_1+r_2) = 0$. Note that the real number t_0 is uniquely determined (see the proof of Lemma 2.11). Define

$$D_{r_1,r_2}(X) := \frac{1}{27}(3X^2+r)\{2X^3 - 3(r_1+r_2)X^2 + 6rX - r(r_1+r_2)\}.$$

For any $t \in T$, we can check the integrality of $D_{r_1,r_2}(t)$. Let $\mathcal{F}(S)$ denote the family $\{\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)}) \mid t \in S\}$ for a subset S of T. For a prime number p and an integer a, we denote by $v_p(a)$ the greatest exponent n such that $p^n \mid a$. Then, we have the following theorem.

Theorem 2.1. *Let m_1 and m_2 be distinct square-free integers (including 1) with $4 \nmid m_1m_2$. For every $t \in T$, the class numbers of quadratic fields $\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)})$ and $\mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)})$ are both divisible by 3 and $\gcd(m_1m_2/3^{v_3(m_1m_2)}, D_{r_1,r_2}(t)) = 1$. Moreover, the families $\mathcal{F}(T_1)$, $\mathcal{F}(T_2)$, and $\mathcal{F}(T_3)$ each include infinitely many quadratic fields. In particular, if m_1 and m_2 are positive and $t \in T_1$ (resp. $t \in T_2$), then the quadratic fields $\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)})$ and $\mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)})$ are both real (resp. both imaginary). Furthermore, if $m_2 < 0 < m_1$ and $t \in T_3$, then $D_{r_1,r_2}(t)$ is positive. In this case, the quadratic field $\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)})$ is real and the quadratic field $\mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)})$ is imaginary.*

This theorem is essential for the proof of the case $4 \nmid m_1 m_2$ of Theorem 1.3. In fact, the case $12 \nmid m_1 m_2$ of Theorem 1.3 follows from Theorem 2.1 immediately. For the case $3 \mid m_1 m_2$, we can show Theorem 1.3 by using Theorem 2.1 as follows. By the congruence relation r_1, r_2, and t, we find $v_3(D_{r_1,r_2}(t)) = 3$. Then,

$$\mathbb{Q}\left(\sqrt{m_i D_{r_1,r_2}(t)}\right) = \mathbb{Q}\left(\sqrt{\frac{m_i}{3}\frac{D_{r_1,r_2}(t)}{3^3}}\right)$$

when $3 \mid m_i$ and

$$\mathbb{Q}\left(\sqrt{m_i D_{r_1,r_2}(t)}\right) = \mathbb{Q}\left(\sqrt{3m_i\frac{D_{r_1,r_2}(t)}{3^3}}\right)$$

when $3 \nmid m_i$. Putting $m_i' := m_i/3$ (resp. $m_i' := 3m_i$) when $3 \mid m_i$ (resp. $3 \nmid m_i$), we have $\gcd(m_1' m_2', D_{r_1,r_2}(t)/3^3) = 1$. Moreover, the class numbers of $\mathbb{Q}(\sqrt{m_1' D_{r_1,r_2}(t)/3^3})$ and $\mathbb{Q}(\sqrt{m_2' D_{r_1,r_2}(t)/3^3})$ are both divisible by 3.

Next, we treat the case $4 \mid m_1 m_2$. Although the method of the construction is based on the above, we need several changes. The definition of the set $\mathcal{L}$ is the same as above. We fix $l \in \mathcal{L}$. Let s be a prime number such that $s \neq 2$, 3, l and $s \nmid m_1 m_2$. We take integers n_1 and n_2 satisfying the following conditions: for each $i = 1$, 2,

$$n_i \equiv \begin{cases} 0 \bmod 9 & \text{if } m_i \not\equiv 0 \bmod 3, \\ 0 \bmod 3 & \text{if } m_i \equiv 0 \bmod 3, \end{cases}$$

$$m_i n_i^2 \equiv 1 \bmod l,$$

$$n_i \equiv 0 \bmod s^2,$$

and

$$n_i \equiv 2 \bmod 4.$$

Note that there exist such integers n_i by the Chinese remainder theorem. Put $r_1 := m_1 n_1^2$, $r_2 := m_2 n_2^2$, and $r := r_1 r_2$ similarly. It follows from the assumption on n_i that r_i is even. Let P be the set of prime numbers defined by

$$P := \{p : \text{prime} \mid p \neq 2, 3, s \text{ and } p | r(r-1)(r_1 - r_2)\}.$$

It is easy to see $l \in P$. Let Q be the subset of P defined by

$$Q := \{q : \text{prime} \mid q \neq 2, 3 \text{ and } q | m_1 m_2\}.$$

When $m_1 m_2 = -4$, ± 12, -36, the set Q is empty. We treat the set Q including the case where Q is empty. Note that $s \notin Q$. We denote by T the set of integers t satisfying the following conditions:

$$\begin{cases} t \equiv \pm 6s \bmod 8 \cdot 27 s^3, \\ t \equiv -1 \bmod l, \\ t \not\equiv r_1,\ r_2 \bmod p & \text{for any } p \in P, \\ 2t \not\equiv 3(r_1 + r_2) \bmod q & \text{for any } q \in Q. \end{cases}$$

We see from the Chinese remainder theorem that the set T is infinite. The definitions of T_i $(i = 1, 2, 3)$, $D_{r_1,r_2}(t)$, and $\mathcal{F}(S)$ are the same as above. It follows from the congruence relation of r_1, r_2, and t that $D_{r_1,r_2}(t)$ is an integer. Then, we obtain the following theorem.

Theorem 2.2. *Let m_1 and m_2 be distinct square-free integers (including 1) with $4 \mid m_1m_2$. For every $t \in T$, the class numbers of quadratic fields $\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)})$ and $\mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)})$ are both divisible by 3 and $\gcd(m_1m_2/(4 \cdot 3^{v_3(m_1m_2)}), D_{r_1,r_2}(t)) = 1$. Moreover, the families $\mathcal{F}(T_1)$, $\mathcal{F}(T_2)$, and $\mathcal{F}(T_3)$ each include infinitely many quadratic fields. In particular, if m_1 and m_2 are positive and $t \in T_1$ (resp. $t \in T_2$), then the quadratic fields $\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)})$ and $\mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)})$ are both real (resp. both imaginary). Furthermore, if $m_2 < 0 < m_1$ and $t \in T_3$, then $D_{r_1,r_2}(t)$ is positive. In this case, the quadratic field $\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)})$ is real and the quadratic field $\mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)})$ is imaginary.*

This theorem is essential for the proof of the case $4 \mid m_1m_2$ of Theorem 1.3. We can show Theorem 1.3 by using Theorem 2.2 as follows. First, we treat the case $3 \nmid m_1m_2$. It follows from the congruence relation r_1, r_2, and t that $v_2(D_{r_1,r_2}(t)) = 6$. Then,

$$\mathbb{Q}\left(\sqrt{m_iD_{r_1,r_2}(t)}\right) = \mathbb{Q}\left(\sqrt{m_i\frac{D_{r_1,r_2}(t)}{2^6}}\right).$$

We see $\gcd(m_1m_2, D_{r_1,r_2}(t)/2^6) = 1$. Moreover, the class numbers of the quadratic fields $\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)/2^6})$ and $\mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)/2^6})$ are both divisible by 3. Secondly, we treat the case $3 \mid m_1m_2$. It follows from the congruence relation r_1, r_2, and t that $v_2(D_{r_1,r_2}(t)) = 6$ and $v_3(D_{r_1,r_2}(t)) = 3$. Then,

$$\mathbb{Q}\left(\sqrt{m_iD_{r_1,r_2}(t)}\right) = \mathbb{Q}\left(\sqrt{\frac{m_i}{3}\frac{D_{r_1,r_2}(t)}{2^63^3}}\right)$$

when $3 \mid m_i$ and

$$\mathbb{Q}\left(\sqrt{m_iD_{r_1,r_2}(t)}\right) = \mathbb{Q}\left(\sqrt{3m_i\frac{D_{r_1,r_2}(t)}{2^63^3}}\right)$$

when $3 \nmid m_i$. Putting $m_i' := m_i/3$ (resp. $m_i' := 3m_i$) when $3 \mid m_i$ (resp. $3 \nmid m_i$), we have $\gcd(m_1'm_2', D_{r_1,r_2}(t)/(2^63^3)) = 1$. Moreover, the class numbers of $\mathbb{Q}(\sqrt{m_1'D_{r_1,r_2}(t)/(2^63^3)})$ and $\mathbb{Q}(\sqrt{m_2'D_{r_1,r_2}(t)/(2^63^3)})$ are both divisible by 3.

2.2. Proof of Theorem 2.1

In this section, we give a proof of Theorem 2.1. We can show Theorem 2.2 similarly. The proof consists of three parts: the divisibility of the class numbers of the quadratic fields (Proposition 2.10), the determination of the sign of $D_{r_1,r_2}(t)$ (Proposition 2.12), and the infiniteness of $\mathcal{F}(T)$ (Proposition 2.13). Before these proofs, we show the following lemma.

Lemma 2.3. *We have*

$$\gcd(m_1 m_2/3^{v_3(m_1 m_2)}, D_{r_1,r_2}(t)) = 1.$$

Proof. When $m_1 m_2 = -1, \pm 3, -9$, we easily see that the statement holds true. Then, we treat the case $m_1 m_2 \neq -1, \pm 3, -9$, that is, the case where Q is not empty. Assume $\gcd(m_1 m_2/3^{v_3(m_1 m_2)}, D_{r_1,r_2}(t)) \neq 1$. For every prime number ρ_1 with $\rho_1 \mid \gcd(m_1 m_2/3^{v_3(m_1 m_2)}, D_{r_1,r_2}(t))$, we have $27 D_{r_1,r_2}(t) \equiv 0 \bmod \rho_1$. Then,

$$\begin{aligned} 27 D_{r_1,r_2}(t) &= (3t^2 + r)\{2t^3 - 3(r_1 + r_2)t^2 + 6rt - r(r_1 + r_2)\} \\ &\equiv 3t^4(2t - 3(r_1 + r_2)) \equiv 0 \bmod \rho_1. \end{aligned}$$

It follows from $\rho_1 \neq 3$ that $\rho_1 \in Q$. By definition of the set T, we see $2t \not\equiv 3(r_1 + r_2) \bmod \rho_1$. Then, $t \equiv 0 \bmod \rho_1$. On the other hand, it follows from $m_1 m_2/3^{v_3(m_1 m_2)} \equiv 0 \bmod \rho_1$ that ρ_1 divides r. Then, $t \equiv r \equiv 0 \bmod \rho_1$. Note that $\rho_1 \in P$. This is a contradiction by definition of the set T. ■

First, we show the divisibility of the class numbers of the quadratic fields. To prove $3 \mid h(m_i D_{r_1,r_2}(t))$ $(i = 1, 2)$, we use a result of P. Llorente and E. Nart [16]. Let $f(Z)$ be an irreducible cubic polynomial of the form $f(Z) = Z^3 - \alpha Z - \beta$ for $\alpha, \beta \in \mathbb{Z}$. We denote by K_f the minimal splitting field of $f(Z)$ over $\mathbb{Q}$. Then, $k_f := \mathbb{Q}(\sqrt{4\alpha^3 - 27\beta^2})$ is contained in K_f. Assume that $4\alpha^3 - 27\beta^2$ is not a square and $\gcd(\alpha, \beta) = 2^e 3^{e'} s^{e''}$ for some integers e, e', and e''. Let δ, δ', and δ'' be the maximal integers such that $\alpha/(2^{2\delta} 3^{2\delta'} s^{2\delta''})$ and $\beta/(2^{3\delta} 3^{3\delta'} s^{3\delta''})$ are integers. Put $\alpha_0 := \alpha/(2^{2\delta} 3^{2\delta'} s^{2\delta''})$ and $\beta_0 := \beta/(2^{3\delta} 3^{3\delta'} s^{3\delta''})$. Llorente and Nart proved the following proposition.

Proposition 2.4 (Llorente and Nart, [16]). *Assume $v_p(\alpha_0) < 2$ or $v_p(\beta_0) < 3$ for each prime number p.*

(1) *If $p \neq 3$, then the prime ideals of k_f over p are unramified in the extension K_f/k_f if and only if the condition $1 \leqslant v_p(\beta_0) \leqslant v_p(\alpha_0)$ is not satisfied.*
(2) *If $p = 3$, $\alpha_0 \equiv 3 \bmod 9$, and $\beta_0^2 \equiv \alpha_0 + 1 \bmod 27$, then the prime ideals of k_f over 3 are unramified in the extension K_f/k_f.*

Remark 2.5. In [16], more general situations are treated. However, Proposition 2.4 is enough for us.

We shall show $3 \mid h(m_1 D_{r_1,r_2}(t))$ and $3 \mid h(m_2 D_{r_1,r_2}(t))$ for each $t \in T$. For a fixed $t \in T$, we put $u := t^3 + 3rt$, $w := 3t^2 + r$, $a := u - r_1 w$, $b := u - r_2 w$, and $c := t^2 - r$. Then, u, w, a, b, and c are integers such that

$$(t + \sqrt{r})^3 = u + w\sqrt{r}$$

and

$$r_2 a^2 - r_1 b^2 = (r_2 - r_1)c^3.$$

We note that $r_1 \neq r_2$. This follows from the uniqueness of factorization into prime factors and the assumption that m_1 and m_2 are square-free. Define $f_1(Z) := Z^3 - 3cZ - 2a$ and $f_2(Z) := Z^3 - 3cZ - 2b$.

Lemma 2.6. *The polynomials $f_1(Z)$ and $f_2(Z)$ are both irreducible over $\mathbb{F}_l$. In particular, they are both irreducible over $\mathbb{Q}$.*

Proof. We can show this lemma in a way similar to [15, Lemma 2.2]. We see from $r_i = m_i n_i^2 \equiv 1 \bmod l$ $(i = 1, 2)$ and $t \equiv -1 \bmod l$ that $a \equiv b \equiv -8 \bmod l$ and $c \equiv 0 \bmod l$. Then, $f_i(Z) \equiv Z^3 + 16 \bmod l$ for each $i = 1, 2$. Since l is inert in the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, the polynomial $Z^3 - 2$ is irreducible over $\mathbb{F}_l$ and so is $Z^3 + 16$. Therefore, $f_i(Z)$ are both irreducible over $\mathbb{F}_l$ and hence also over $\mathbb{Q}$, where $i = 1, 2$. ■

Lemma 2.7. *The cyclic cubic extensions K_{f_i}/k_{f_i} are both everywhere unramified at finite places, where $i = 1, 2$.*

By the definitions of the integers a, b, and c, we have

$$4(3c)^3 - 27(2a)^2 = 54^2 r_1 D_{r_1,r_2}(t) = 54^2 m_1 n_1^2 D_{r_1,r_2}(t) = (54n_1)^2 m_1 D_{r_1,r_2}(t)$$

and

$$4(3c)^3 - 27(2b)^2 = 54^2 r_2 D_{r_1,r_2}(t) = 54^2 m_2 n_2^2 D_{r_1,r_2}(t) = (54n_2)^2 m_2 D_{r_1,r_2}(t).$$

Then, $k_{f_1} = \mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(t)})$ and $k_{f_2} = \mathbb{Q}(\sqrt{m_2 D_{r_1,r_2}(t)})$. To prove Lemma 2.7, we need the following two lemmas.

Lemma 2.8.

(1) *c is odd.*
(2) *We have* $\gcd(ab, c) = 3^e s^{e'}$ *for some integers e, e'.*

Proof. (1) We see from $2 \in P$ that $t \not\equiv r \bmod 2$. Then, $c = t^2 - r \equiv 1 \bmod 2$, that is, c is odd.

(2) Let ρ_2 be a prime divisor of $\gcd(ab, c)$. Note that ρ_2 is odd. Since ρ_2 divides $c = t^2 - r$, we see $t^2 \equiv r \bmod \rho_2$. It follows from $\rho_2 \mid ab$ that

$$0 \equiv ab \equiv (u - r_1 w)(u - r_2 w) \equiv 16t^4(t - r_1)(t - r_2) \bmod \rho_2.$$

Then, (i) $\rho_2 \mid t$ or (ii) $t \equiv r_1 \bmod \rho_2$ or (iii) $t \equiv r_2 \bmod \rho_2$. First, we treat Case(i). Since ρ_2 divides t, we see $r \equiv t^2 \equiv t \equiv 0 \bmod \rho_2$. Then, $\rho_2 \mid r$, that is, $\rho_2 \in P \cup \{3, s\}$. If $\rho_2 \in P$, we have $t \not\equiv r \bmod \rho_2$. This is a contradiction. Therefore, $\rho_2 = 3$, s. Secondly, we treat Case(ii). Since $t \equiv r_1 \bmod \rho_2$ holds, we see

$$r_1^2 \equiv t^2 \equiv r = r_1 r_2 \bmod \rho_2.$$

If ρ_2 divides r_1, we have $r \equiv 0 \bmod \rho_2$. Then, $\rho_2 \in P \cup \{3, s\}$. Since $t \not\equiv r \bmod p$ holds for every $p \in P$, it must be $\rho_2 = 3$, s. If ρ_2 does not divide r_1, we see $r_1 \equiv r_2 \bmod \rho_2$, that is, $\rho_2 \mid r_1 - r_2$. Then, $\rho_2 \in P \cup \{3, s\}$. If $\rho_2 \in P$, we have $t \not\equiv r_1 \bmod \rho_2$. This is a contradiction. Therefore, $\rho_2 = 3$, s. Finally, we treat Case(iii). Since $t \equiv r_2 \bmod \rho_2$ holds, we see

$$r_2^2 \equiv t^2 \equiv r = r_1 r_2 \bmod \rho_2.$$

If ρ_2 divides r_2, then $r \equiv 0 \bmod \rho_2$, that is, $\rho_2 \in P \cup \{3, s\}$. Since $t \not\equiv r \bmod p$ holds for every $p \in P$, it must be $\rho_2 = 3,\ s$. If ρ_2 does not divide r_2, we have $r_2 \equiv r_1 \bmod \rho_2$. Then, $t \equiv r_1 \equiv r_2 \bmod \rho_2$, that is, $t \equiv r_1 \bmod \rho_2$. This case can result in Case(ii) and then $\rho_2 = 3,\ s$. ■

Lemma 2.9. *We have* $r_i \equiv 0 \bmod 27$, *where* $i = 1,\ 2$.

Proof. When $m_i \not\equiv 0 \bmod 3$, we have $n_i \equiv 0 \bmod 9$. Then, $r_i = m_i n_i^2 \equiv 0 \bmod 27$. When $m_i \equiv 0 \bmod 3$, we have $n_i \equiv 0 \bmod 3$. Then, $r_i = m_i n_i^2 \equiv 0 \bmod 27$. ■

Proof of Lemma 2.7. Since $v_s(D_{r_1,r_2}(t)) = 5$ and $s \nmid m_1 m_2$ hold, we have $k_{f_i} \neq \mathbb{Q}$, where $i = 1,\ 2$. Then, we can use Proposition 2.4. In this case, we take $\alpha = 3c$, $\beta = 2a$ or $2b$. By Lemma 2.8 (2), we have $\gcd(ab, c) = 3^e s^{e'}$ for some integers $e,\ e'$. Then, the assumption $v_p(\alpha_0) < 2$ or $v_p(\beta_0) < 3$ is satisfied for each prime number p, where α_0 and β_0 are as in Proposition 2.4. Moreover, the condition $1 \leqslant v_p(\beta_0) \leqslant v_p(\alpha_0)$ is not satisfied when $p \neq 3,\ s$. By Proposition 2.4 (1), the prime ideals of k_{f_i} over p are unramified in the extension K_{f_i}/k_{f_i} when $p \neq 3,\ s$. Now, we treat the case $p = s$. Since

$$\frac{a}{s^3} \equiv \frac{b}{s^3} \equiv \frac{t^3}{s^3} \not\equiv 0 \bmod s$$

and

$$\frac{c}{s^2} \equiv \frac{t^2}{s^2} \not\equiv 0 \bmod s$$

hold, we have $\delta'' = 1$, where δ'' is as in Proposition 2.4. Then, we find $\alpha_0 = 3c/(2^{2\delta} 3^{2\delta'} s^2)$ and $v_s(\alpha_0) = 0$. Therefore, the condition $1 \leqslant v_s(\beta_0) \leqslant v_s(\alpha_0)$ is not satisfied, that is, the prime ideals of k_{f_i} over s are unramified in K_{f_i}/k_{f_i}. Next, we treat the case $p = 3$. Put $t_1 := \frac{t}{3s}$. We see $t_1 \equiv \pm 1 \bmod 9$. By Lemma 2.9, we obtain

$$\frac{a}{3^3 s^3} = \frac{t^3 + 3rt - 3r_1 t^2 - r_1 r}{3^3 s^3} \equiv t_1^3 \equiv \pm 1 \bmod 27,$$
$$\frac{b}{3^3 s^3} = \frac{t^3 + 3rt - 3r_2 t^2 - r_2 r}{3^3 s^3} \equiv t_1^3 \equiv \pm 1 \bmod 27,$$

and

$$\frac{c}{3^2 s^2} = \frac{t^2 - r}{3^2 s^2} \equiv t_1^2 \equiv 1 \bmod 9.$$

Then, $\delta' = 1$, where δ' is as in Proposition 2.4. By Lemma 2.8 (1), the integer c is odd. Then, $\delta = 0$, where δ is as in Proposition 2.4. Hence, $(\alpha_0, \beta_0) = \left(\frac{3c}{3^2 s^2}, \frac{2a}{3^3 s^3}\right)$ if $\beta = 2a$ and $(\alpha_0, \beta_0) = \left(\frac{3c}{3^2 s^2}, \frac{2b}{3^3 s^3}\right)$ otherwise. Since $\alpha_0 \equiv 3 \bmod 27$ and $\beta_0 \equiv \pm 2 \bmod 27$ hold, we see

$$\beta_0^2 \equiv \alpha_0 + 1 \bmod 27.$$

By Proposition 2.4 (2), the prime ideals of k_{f_i} over 3 are unramified in the extension K_{f_i}/k_{f_i}. The proof of Lemma 2.7 is completed. ■

Lemma 2.7 shows that 3 divides the orders of the narrow class groups of $\mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(t)})$ and $\mathbb{Q}(\sqrt{m_2 D_{r_1,r_2}(t)})$. Since the difference between these orders and the class numbers of $\mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(t)})$ and $\mathbb{Q}(\sqrt{m_2 D_{r_1,r_2}(t)})$ is only a power of 2, the following proposition holds.

Proposition 2.10. *For any $t \in T$, we have*

$$3 \mid h(m_1 D_{r_1,r_2}(t)) \qquad \text{and} \qquad 3 \mid h(m_2 D_{r_1,r_2}(t)).$$

Secondly, we consider whether $D_{r_1,r_2}(t)$ is positive or not. Define

$$g_{r_1,r_2}(X) := 2X^3 - 3(r_1 + r_2)X^2 + 6rX - r(r_1 + r_2).$$

Then,

$$D_{r_1,r_2}(X) = \frac{1}{27}(3X^2 + r)g_{r_1,r_2}(X).$$

Concerning the sign of $D_{r_1,r_2}(t)$, we obtain the following lemma.

Lemma 2.11.

(1) *Assume r_1 and r_2 are positive integers. Then, $D_{r_1,r_2}(t)$ is positive if $t \geqslant \frac{3}{2}\mathrm{Max}\{r_1, r_2\}$ and $D_{r_1,r_2}(t)$ is negative if $t \leqslant \mathrm{Max}\{r_1, r_2\}$.*

(2) *Assume $r_1 r_2$ is a negative integer. If $t > t_0$, then $D_{r_1,r_2}(t)$ is positive, where t_0 is a real number such that $t_0 \geqslant \mathrm{Max}\{r_1, r_2\}$ and $g_{r_1,r_2}(t_0) = 0$.*

Proof. (1) Since $\frac{1}{27}(3t^2 + r)$ is positive, the sign of $D_{r_1,r_2}(t)$ coincides with that of $g_{r_1,r_2}(t)$. The derivative of $g_{r_1,r_2}(X)$ is

$$g'_{r_1,r_2}(X) = 6(X - r_1)(X - r_2).$$

We see

$$g_{r_1,r_2}(r_1) = -r_1(r_1 - r_2)^2 < 0$$

and

$$g_{r_1,r_2}(r_2) = -r_2(r_2 - r_1)^2 < 0.$$

Then, $g_{r_1,r_2}(X) = 0$ has only one real root. This root is larger than $\mathrm{Max}\{r_1, r_2\}$. Therefore, if $t \leqslant \mathrm{Max}\{r_1, r_2\}$, then $g_{r_1,r_2}(t)$ is negative, that is, $D_{r_1,r_2}(t)$ is negative. Assume $r_1 > r_2 > 0$. We see

$$g_{r_1,r_2}(3r_1/2) = \frac{1}{4}r_1 r_2(5r_1 - 4r_2) > 0.$$

Since $g_{r_1,r_2}(3r_1/2)$ is positive and $g_{r_1,r_2}(X)$ is monotonically increasing for $X > \mathrm{Max}\{r_1, r_2\}$, we obtain $g_{r_1,r_2}(t) > 0$ when $t \geqslant 3r_1/2$. Then, $D_{r_1,r_2}(t)$ is positive when $t \geqslant 3r_1/2$.

(2) We may assume $r_1 > 0 > r_2$, that is, $m_1 > 0 > m_2$. We see

$$g'_{r_1,r_2}(X) = 6(X - r_1)(X - r_2).$$

Since $g_{r_1,r_2}(r_1) = -r_1(r_1 - r_2)^2$ is negative and $g_{r_1,r_2}(r_2) = -r_2(r_2 - r_1)^2$ is positive, there exists only one real number t_0 such that $t_0 > r_1 = \mathrm{Max}\{r_1, r_2\}$ and $g_{r_1,r_2}(t_0) = 0$. Then, $g_{r_1,r_2}(t)$ is positive when $t > t_0$. If $t > \sqrt{-r/3}$, then $3t^2 + r > 0$. Therefore, $D_{r_1,r_2}(t)$ is positive when $t > \mathrm{Max}\{t_0, \sqrt{-r/3}\}$. Here, $\mathrm{Max}\{t_0, \sqrt{-r/3}\} = t_0$. In fact, we see from

$$g_{r_1,r_2}\left(\sqrt{\frac{-r}{3}}\right) = \frac{16r}{3}\sqrt{\frac{-r}{3}} < 0$$

that $t_0 > \sqrt{-r/3}$. ■

By Lemma 2.11, we obtain the following proposition.

Proposition 2.12.

(1) *Assume m_1 and m_2 are positive integers. If $t \in T_1$, then the quadratic fields $\mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(t)})$ and $\mathbb{Q}(\sqrt{m_2 D_{r_1,r_2}(t)})$ are both real. If $t \in T_2$, then the quadratic fields $\mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(t)})$ and $\mathbb{Q}(\sqrt{m_2 D_{r_1,r_2}(t)})$ are both imaginary.*

(2) *Assume $m_1 > 0 > m_2$. If $t \in T_3$, then the quadratic field $\mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(t)})$ is real and the quadratic field $\mathbb{Q}(\sqrt{m_2 D_{r_1,r_2}(t)})$ is imaginary.*

Finally, we consider whether $\mathcal{F}(T)$ and $\mathcal{F}_i(T)$ $(i = 1, 2, 3)$ include infinitely many quadratic fields. We obtain the following proposition.

Proposition 2.13. *We have $\sharp\, \mathcal{F}(T) = \infty$. In particular, $\sharp\, \mathcal{F}(T_1) = \infty$, $\sharp\, \mathcal{F}(T_2) = \infty$, and $\sharp\, \mathcal{F}(T_3) = \infty$.*

Proof. We can show this proposition in a way similar to [15, Proposition 2.7]. We will prove $\sharp\, \mathcal{F}(T) = \infty$. We can show $\sharp\, \mathcal{F}(T_1) = \infty$, $\sharp\, \mathcal{F}(T_2) = \infty$, and $\sharp\, \mathcal{F}(T_3) = \infty$ in the same way. Assume S is a non-empty subset of T such that $\mathcal{F}(S)$ is finite. We will show that we can choose a_0 from T so that $\mathcal{F}(S) \subsetneq \mathcal{F}(S \cup \{a_0\})$. The choice of a_0 is as follows. Let M_S be the composite field of all quadratic fields which belong to $\mathcal{F}(S)$ and let P_S be the set of prime numbers ramifying in $M_S/\mathbb{Q}$. Since $M_S/\mathbb{Q}$ is of finite degree, the set P_S is finite. Note that $s \in P_S$. There exists at least one prime number $q_1 \notin P \cup P_S \cup \{3\}$ such that $\left(\frac{(-r/3)}{q_1}\right) = 1$. We fix such a prime number q_1. Then, there exists at least one integer x such that $3x^2 + r \equiv 0 \bmod q_1$. We fix such an integer x. Define

$$x_0 := \begin{cases} x & \text{if } 3x^2 + r \not\equiv 0 \bmod q_1^2 \\ x + q_1 & \text{if } 3x^2 + r \equiv 0 \bmod q_1^2. \end{cases}$$

If $x_0 = x + q_1$, then $3x_0^2 + r \equiv 6q_1 x \bmod q_1^2$. Assume $3x_0^2 + r \equiv 0 \bmod q_1^2$. By $q_1 \neq 2, 3$, we find $q_1 \mid x$, that is, $q_1 \mid r$. This is a contradiction with $q_1 \notin P \cup \{3, s\}$. Then, we always have $3x_0^2 + r \equiv 0 \bmod q_1$ and $3x_0^2 + r \not\equiv 0 \bmod q_1^2$. Since

$$3g_{r_1,r_2}(X) = (2X - 3(r_1 + r_2))(3X^2 + r_1 r_2) + 16 r_1 r_2 X$$

holds,

$$3g_{r_1,r_2}(x_0) = (2x_0 - 3(r_1 + r_2))(3x_0^2 + r_1r_2) + 16r_1r_2x_0 \equiv 16r_1r_2x_0 \equiv 0 \bmod q_1$$

if $g_{r_1,r_2}(x_0) \equiv 0 \bmod q_1$. It follows from $2 \in P$ and $q_1 \notin P \cup \{3, s\}$ that $q_1 \mid x_0$. Then, $q_1 \mid r$, that is, $q_1 \in P \cup \{3, s\}$. This is a contradiction. Therefore, $g_{r_1,r_2}(x_0) \not\equiv 0 \bmod q_1$. Since $q_1 \neq 3$ and $v_{q_1}(3x_0^2 + r) = 1$ hold,

$$D_{r_1,r_2}(x_0) = \frac{3x_0^2 + r}{27} g_{r_1,r_2}(x_0) \equiv 0 \bmod q_1$$

and

$$D_{r_1,r_2}(x_0) \not\equiv 0 \bmod q_1^2.$$

On the other hand, it follows from $q_1 \notin P \cup \{3, s\}$ and the Chinese remainder theorem that there exists $a_0 \in T$ such that $a_0 \equiv x_0 \bmod q_1^2$. Then,

$$D_{r_1,r_2}(a_0) \equiv D_{r_1,r_2}(x_0) \equiv 0 \bmod q_1$$

and

$$D_{r_1,r_2}(a_0) \equiv D_{r_1,r_2}(x_0) \not\equiv 0 \bmod q_1^2.$$

This implies that q_1 ramifies in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(a_0)})/\mathbb{Q}$. Since $\gcd(m_1, D_{r_1,r_2}(a_0)) = 3^e$ for some integer e and $q_1 \neq 3$ holds, the prime number q_1 also ramifies in $\mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(a_0)})/\mathbb{Q}$. Then, q_1 also ramifies in $M_S(\sqrt{m_1 D_{r_1,r_2}(a_0)})/\mathbb{Q}$. By the assumption $q_1 \notin P_S$, this implies

$$M_S \subsetneq M_S\left(\sqrt{m_1 D_{r_1,r_2}(a_0)}\right),$$

that is,

$$\mathcal{F}(S) \subsetneq \mathcal{F}(S \cup \{a_0\}).$$

The family $\mathcal{F}(S \cup \{a_0\})$ is also finite. Repeating this, we can construct an infinite increasing sequence of subsets S_i of T such that

$$\mathcal{F}(S) \subsetneq \mathcal{F}(S_1) \subsetneq \mathcal{F}(S_2) \subsetneq \cdots,$$

where $i \in \mathbb{N}$ and $S \subsetneq S_1 \subsetneq S_2 \subsetneq \cdots$. This implies $\sharp\, \mathcal{F}(T) = \infty$. ■

Theorem 2.1 follows from Lemma 2.3, Propositions 2.10, 2.12, and 2.13.

2.3. Proof of Theorem 2.2

In this section, we show Theorem 2.2 (the case $4 \mid m_1m_2$), modifying the method of the proof of Theorem 2.1. First, we show the following lemma.

Lemma 2.14. *We have*

$$\gcd(m_1m_2/(4 \cdot 3^{v_3(m_1m_2)}), D_{r_1,r_2}(t)) = 1.$$

Proof. When $m_1m_2 = -4, \pm 12, -36$, we easily see that the statement holds true. Then, we treat the case $m_1m_2 \neq -4, \pm 12, -36$, that is, the case where Q is not empty. Assume $\gcd(m_1m_2/(4\cdot 3^{v_3(m_1m_2)}), D_{r_1,r_2}(t)) \neq 1$. For every prime number ρ_3 with $\rho_3 \mid \gcd(m_1m_2/(4\cdot 3^{v_3(m_1m_2)}), D_{r_1,r_2}(t))$, we have $27D_{r_1,r_2}(t) \equiv 0 \bmod \rho_3$. Then,

$$\begin{aligned} 27D_{r_1,r_2}(t) &= (3t^2+r)\{2t^3 - 3(r_1+r_2)t^2 + 6rt - r(r_1+r_2)\} \\ &\equiv 3t^4\{2t - 3(r_1+r_2)\} \equiv 0 \bmod \rho_3. \end{aligned}$$

It follows from $\rho_3 \neq 2, 3$ that $\rho_3 \in Q$. By definition of the set T, we see $2t \not\equiv 3(r_1+r_2) \bmod \rho_3$. Then, $t \equiv 0 \bmod \rho_3$. On the other hand, $\rho_3 \mid m_1$ or $\rho_3 \mid m_2$. Then, $t \equiv r_1 \equiv 0 \bmod \rho_3$ or $t \equiv r_2 \equiv 0 \bmod \rho_3$. This is a contradiction by definition of the set T. ■

Secondly, we show the divisibility of the class numbers of the quadratic fields. The definitions of the integers u, w, a, b, and c are the same as in Section 2.2. To prove $3 \mid h(m_iD_{r_1,r_2}(t))$ $(i = 1, 2)$, we use Proposition 2.4. Define $f_1(Z) := Z^3 - 3cZ - 2a$ and $f_2(Z) := Z^3 - 3cZ - 2b$ as in Section 2.2. We can show that $f_1(Z)$ and $f_2(Z)$ are both irreducible over $\mathbb{Q}$ in a way similar to Lemma 2.6. Using Proposition 2.4, we obtain the following lemma.

Lemma 2.15. *The cyclic cubic extensions K_{f_i}/k_{f_i} are both everywhere unramified at finite places, where $i = 1, 2$.*

It follows from the definitions of a, b, and c that $k_{f_1} = \mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)})$ and $k_{f_2} = \mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)})$. To prove Lemma 2.15, we need the following two lemmas.

Lemma 2.16.

(1) *c is even.*

(2) *We have $\gcd(ab, c) = 2^e 3^{e'} s^{e''}$ for some integers e, e', and e''.*

Proof. (1) Since t and r are even, $c = t^2 - r$ is also even.

(2) By (1), c is even. The integer ab is also even. Then, $2 \mid \gcd(ab, c)$. Let ρ_4 be an odd prime divisor of $\gcd(ab, c)$. Since ρ_4 divides $c = t^2 - r$, we have $t^2 \equiv r \bmod \rho_4$. It follows from $\rho_4 \mid ab$ that

$$0 \equiv ab \equiv (u - r_1w)(u - r_2w) \equiv 16t^4(t - r_1)(t - r_2) \bmod \rho_4.$$

Then, (i) $\rho_4 \mid t$ or (ii) $t \equiv r_1 \bmod \rho_4$ or (iii) $t \equiv r_2 \bmod \rho_4$. First, we treat Case(i). Since ρ_4 divides t, we see $r \equiv t^2 \equiv t \equiv 0 \bmod \rho_4$. Then, $\rho_4 \mid r$, that is, $\rho_4 \in P \cup \{3, s\}$. It follows from $\rho_4 \mid r$ that $\rho_4 \mid r_1$ or $\rho_4 \mid r_2$. If $\rho_4 \in P$, we have $t \not\equiv r_1, r_2 \bmod \rho_4$. This is a contradiction. Therefore, $\rho_4 = 3$, s. Secondly, we treat Case(ii). Since $t \equiv r_1 \bmod \rho_4$ holds, we see

$$r_1^2 \equiv t^2 \equiv r = r_1r_2 \bmod \rho_4.$$

If ρ_4 divides r_1, we have $r \equiv 0 \bmod \rho_4$. Then, $\rho_4 \in P \cup \{3, s\}$. Since $t \not\equiv r_1, r_2 \bmod p$ holds for every $p \in P$, it must be $\rho_4 = 3$, s. If ρ_4 does not divide r_1, we see $r_1 \equiv r_2 \bmod \rho_4$, that is, $\rho_4 \mid r_1 - r_2$. Then, $\rho_4 \in P \cup \{3, s\}$. If $\rho_4 \in P$, we have $t \not\equiv r_1 \bmod \rho_4$. This is a contradiction. Therefore, $\rho_4 = 3$, s. Finally, we treat Case(iii). Since $t \equiv r_2 \bmod \rho_4$ holds, we see

$$r_2^2 \equiv t^2 \equiv r = r_1 r_2 \bmod \rho_4.$$

If ρ_4 divides r_2, then $r \equiv 0 \bmod \rho_4$, that is, $\rho_4 \in P \cup \{3, s\}$. Since $t \not\equiv r_1, r_2 \bmod p$ holds for every $p \in P$, it must be $\rho_4 = 3$, s. If ρ_4 does not divide r_2, we have $r_2 \equiv r_1 \bmod \rho_4$. Then, $t \equiv r_1 \equiv r_2 \bmod \rho_4$, that is, $t \equiv r_1 \bmod \rho_4$. This case can result in Case(ii) and then $\rho_4 = 3$, s. ■

Lemma 2.17. *We have* $r_i \equiv 0 \bmod 27$, *where* $i = 1$, 2.

Proof. We can show this lemma in a way similar to Lemma 2.9. ■

Proof of Lemma 2.15. Since $v_s(D_{r_1,r_2}(t)) = 5$ and $s \nmid m_1 m_2$ hold, we have $k_{f_i} \neq \mathbb{Q}$, where $i = 1$, 2. Then, we can use Proposition 2.4. In this case, we take $\alpha = 3c$, $\beta = 2a$ or $2b$. By Lemma 2.16 (2), we have $\gcd(ab, c) = 2^e 3^{e'} s^{e''}$ for some integers e, e', and e''. Then, the assumption $v_p(\alpha_0) < 2$ or $v_p(\beta_0) < 3$ is satisfied for each prime number p, where α_0 and β_0 are as in Proposition 2.4. Moreover, the condition $1 \leqslant v_p(\beta_0) \leqslant v_p(\alpha_0)$ is not satisfied when $p \neq 2$, 3, s. Then, the prime ideals of k_{f_i} over p are unramified in the extension K_{f_i}/k_{f_i} when $p \neq 2$, 3, s. Now, we treat the case $p = 2$, s. Since

$$\frac{a}{2^3} = \frac{t^3 + 3rt - 3r_1 t^2 - r_1 r}{2^3} \equiv \frac{t^3}{2^3} \equiv 1 \bmod 2,$$

$$\frac{b}{2^3} = \frac{t^3 + 3rt - 3r_2 t^2 - r_2 r}{2^3} \equiv \frac{t^3}{2^3} \equiv 1 \bmod 2,$$

and

$$\frac{c}{2^2} = \frac{t^2 - r}{2^2} \equiv \frac{t^2}{2^2} \equiv 1 \bmod 2$$

hold, we see $\delta = 1$, where δ is as in Proposition 2.4. Then, $\alpha_0 = 3c/(2^2 3^{2\delta'} s^{2\delta''})$ is odd, that is, $v_2(\alpha_0) = 0$. Therefore, the condition $1 \leqslant v_2(\beta_0) \leqslant v_2(\alpha_0)$ is not satisfied. Since

$$\frac{a}{s^3} \equiv \frac{b}{s^3} \equiv \frac{t^3}{s^3} \not\equiv 0 \bmod s$$

and

$$\frac{c}{s^2} \equiv \frac{t^2}{s^2} \not\equiv 0 \bmod s$$

hold, we have $\delta'' = 1$, where δ'' is as in Proposition 2.4. Then, we find $\alpha_0 = 3c/(2^2 3^{2\delta'} s^2)$ and $v_s(\alpha_0) = 0$. Therefore, the condition $1 \leqslant v_s(\beta_0) \leqslant v_s(\alpha_0)$ is not satisfied. By Proposition 2.4 (1), the prime ideals of k_f over 2, s are unramified in the extension K_f/k_f. Next, we treat the case $p = 3$. It follows from Lemma 2.17 that

$$\frac{a}{3^3} = \frac{t^3 + 3rt - 3r_1 t^2 - r_1 r}{3^3} \equiv \frac{t^3}{3^3} \not\equiv 0 \bmod 3,$$

$$\frac{b}{3^3} = \frac{t^3+3rt-3r_2t^2-r_2r}{3^3} \equiv \frac{t^3}{3^3} \not\equiv 0 \bmod 3,$$

and

$$\frac{c}{3^2} = \frac{t^2-r}{3^2} \equiv \frac{t^2}{3^2} \not\equiv 0 \bmod 3.$$

Then, $\delta' = 1$, where δ' is as in Proposition 2.4. Hence, $(\alpha_0, \beta_0) = \left(\frac{3c}{6^2s^2}, \frac{2a}{6^3s^3}\right)$ if $\beta = 2a$ and $(\alpha_0, \beta_0) = \left(\frac{3c}{6^2s^2}, \frac{2b}{6^3s^3}\right)$ otherwise. Since

$$\frac{t}{6s} \equiv \pm 1 \bmod 9,$$

$$\frac{a}{6^3s^3} = \frac{t^3+3rt-3r_1t^2-r_1r}{6^3s^3} \equiv \frac{t^3}{6^3s^3} \equiv \pm 1 \bmod 27,$$

$$\frac{b}{6^3s^3} = \frac{t^3+3rt-3r_2t^2-r_2r}{6^3s^3} \equiv \frac{t^3}{6^3s^3} \equiv \pm 1 \bmod 27,$$

and

$$\frac{c}{6^2s^2} = \frac{t^2-r}{6^2s^2} \equiv \frac{t^2}{6^2s^2} \equiv 1 \bmod 9$$

hold, we see $\alpha_0 \equiv 3 \bmod 27$ and $\beta_0 \equiv \pm 2 \bmod 27$. Then, $\beta_0^2 \equiv \alpha_0 + 1 \bmod 27$. By Proposition 2.4 (2), the prime ideals of k_f over 3 are unramified in the extension K_f/k_f. The proof of Lemma 2.15 is completed. ■

By Lemma 2.15, we obtain the following proposition.

Proposition 2.18. *We have* $3 \mid h(m_1D_{r_1,r_2}(t))$ *and* $3 \mid h(m_2D_{r_1,r_2}(t))$ *for any* $t \in T$.

Thirdly, we consider whether $D_{r_1,r_2}(t)$ is positive or not. We have the following lemma.

Lemma 2.19.

(1) *Assume* r_1 *and* r_2 *are positive integers. Then,* $D_{r_1,r_2}(t)$ *is positive if* $t \geqslant \frac{3}{2}\mathrm{Max}\{r_1, r_2\}$ *and* $D_{r_1,r_2}(t)$ *is negative if* $t \leqslant \mathrm{Max}\{r_1, r_2\}$.
(2) *Assume* r_1r_2 *is a negative integer. If* $t > t_0$*, then* $D_{r_1,r_2}(t)$ *is positive, where* t_0 *is a real number such that* $t_0 \geqslant \mathrm{Max}\{r_1, r_2\}$ *and* $g_{r_1,r_2}(t_0) = 0$.

Proof. We can show this lemma in a way similar to Lemma 2.11. ■

By Lemma 2.19, we obtain the following proposition.

Proposition 2.20.

(1) *Assume* m_1 *and* m_2 *are positive integers. If* $t \in T_1$*, then the quadratic fields* $\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)})$ *and* $\mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)})$ *are both real. If* $t \in T_2$*, then the quadratic fields* $\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)})$ *and* $\mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)})$ *are both imaginary.*

(2) *Assume* $m_1 > 0 > m_2$. *If* $t \in T_3$, *then the quadratic field* $\mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(t)})$ *is real and the quadratic field* $\mathbb{Q}(\sqrt{m_2 D_{r_1,r_2}(t)})$ *is imaginary.*

Finally, we consider whether $\mathcal{F}(T)$ and $\mathcal{F}_i(T)$ ($i = 1, 2, 3$) include infinitely many quadratic fields. We obtain the following proposition.

Proposition 2.21. *We have* $\sharp\, \mathcal{F}(T) = \infty$. *In particular,* $\sharp\, \mathcal{F}(T_1) = \infty$, $\sharp\, \mathcal{F}(T_2) = \infty$, *and* $\sharp\, \mathcal{F}(T_3) = \infty$.

Proof. We can show this proposition in a way similar to Proposition 2.13. We will prove $\sharp\, \mathcal{F}(T) = \infty$. We can show $\sharp\, \mathcal{F}(T_1) = \infty$, $\sharp\, \mathcal{F}(T_2) = \infty$, and $\sharp\, \mathcal{F}(T_3) = \infty$ in the same way. Assume S is a non-empty subset of T such that $\mathcal{F}(S)$ is finite. We will show that we can choose a_0 from T so that $\mathcal{F}(S) \subsetneq \mathcal{F}(S \cup \{a_0\})$. The choice of a_0 is as follows. Let M_S be the composite field of all quadratic fields which belong to $\mathcal{F}(S)$ and let P_S be the set of prime numbers ramifying in $M_S/\mathbb{Q}$. Since $M_S/\mathbb{Q}$ is of finite degree, the set P_S is finite. Note that $s \in P_S$. There exists at least one prime number $q_1 \notin P \cup P_S \cup \{2, 3\}$ such that $\left(\frac{(-r/3)}{q_1}\right) = 1$. We fix such a prime number q_1. Then, there exists at least one integer x such that $3x^2 + r \equiv 0 \bmod q_1$. We fix such an integer x. Define

$$x_0 := \begin{cases} x & \text{if } 3x^2 + r \not\equiv 0 \bmod q_1^2 \\ x + q_1 & \text{if } 3x^2 + r \equiv 0 \bmod q_1^2. \end{cases}$$

If $x_0 = x + q_1$, then $3x_0^2 + r \equiv 6q_1 x \bmod q_1^2$. Assume $3x_0^2 + r \equiv 0 \bmod q_1^2$. By $q_1 \neq 2, 3$, we find $q_1 \mid x$, that is, $q_1 \mid r$. This is a contradiction with $q_1 \notin P \cup \{2, 3, s\}$. Then, we always have $3x_0^2 + r \equiv 0 \bmod q_1$ and $3x_0^2 + r \not\equiv 0 \bmod q_1^2$. Since

$$3g_{r_1,r_2}(X) = (2X - 3(r_1 + r_2))(3X^2 + r_1 r_2) + 16 r_1 r_2 X$$

holds,

$$3g_{r_1,r_2}(x_0) = (2x_0 - 3(r_1 + r_2))(3x_0^2 + r_1 r_2) + 16 r_1 r_2 x_0 \equiv 16 r_1 r_2 x_0 \equiv 0 \bmod q_1$$

if $g_{r_1,r_2}(x_0) \equiv 0 \bmod q_1$. It follows from $q_1 \notin P \cup \{2, 3, s\}$ that $q_1 \mid x_0$. Then, $q_1 \mid r$, that is, $q_1 \in P \cup \{2, 3, s\}$. This is a contradiction. Therefore, $g_{r_1,r_2}(x_0) \not\equiv 0 \bmod q_1$. Since $q_1 \neq 3$ and $v_{q_1}(3x_0^2 + r) = 1$ hold,

$$D_{r_1,r_2}(x_0) = \frac{3x_0^2 + r}{27} g_{r_1,r_2}(x_0) \equiv 0 \bmod q_1$$

and

$$D_{r_1,r_2}(x_0) \not\equiv 0 \bmod q_1^2.$$

On the other hand, it follows from $q_1 \notin P \cup \{2, 3, s\}$ and the Chinese remainder theorem that there exists $a_0 \in T$ such that $a_0 \equiv x_0 \bmod q_1^2$. Then,

$$D_{r_1,r_2}(a_0) \equiv D_{r_1,r_2}(x_0) \equiv 0 \bmod q_1$$

and

$$D_{r_1,r_2}(a_0) \equiv D_{r_1,r_2}(x_0) \not\equiv 0 \bmod q_1^2.$$

This implies that q_1 ramifies in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(a_0)})/\mathbb{Q}$. Since $\gcd(m_1, D_{r_1,r_2}(a_0)) = 2\cdot 3^e$ for some integer e and $q_1 \neq 2, 3$ holds, the prime number q_1 also ramifies in $\mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(a_0)})/\mathbb{Q}$. Then, q_1 also ramifies in $M_S(\sqrt{m_1 D_{r_1,r_2}(a_0)})/\mathbb{Q}$. By the assumption $q_1 \notin P_S$, this implies

$$M_S \subsetneq M_S\left(\sqrt{m_1 D_{r_1,r_2}(a_0)}\right),$$

that is,

$$\mathcal{F}(S) \subsetneq \mathcal{F}(S \cup \{a_0\}).$$

Here, the family $\mathcal{F}(S \cup \{a_0\})$ is also finite. Repeating this, we can construct an infinite increasing sequence of subsets S_i of T such that

$$\mathcal{F}(S) \subsetneq \mathcal{F}(S_1) \subsetneq \mathcal{F}(S_2) \subsetneq \cdots,$$

where $i \in \mathbb{N}$ and $S \subsetneq S_1 \subsetneq S_2 \subsetneq \cdots$. This implies $\sharp\, \mathcal{F}(T) = \infty$. ■

Theorem 2.2 follows from Lemma 2.14, Propositions 2.18, 2.20, and 2.21.

3. Proof of Theorem 1.5

In this section, we show Theorem 1.5, modifying the method in [4]. To prove this, we use a result of Nakagawa and Horie [19]. In Section 3.1, we state their result. In Section 3.2, we prove Theorem 1.5. In Section 3.3, we give an application of Theorem 1.5.

3.1. Result of Nakagawa and Horie

For a given prime number p, there are infinitely many imaginary quadratic fields whose class numbers are indivisible by p. Such results are obtained by P. Hartung [8], K. Horie [10, 11], K. Horie and Y. Ônishi [9], W. Kohnen and K. Ono [13], etc. Similarly, for a given prime number p, there are infinitely many real quadratic fields whose class numbers are indivisible by p. K. Ono [20], D. Byeon [2, 3], etc. obtained such results. For $p = 3$, results of H. Davenport and H. Heilbronn [5] and J. Nakagawa and K. Horie [19] are known. We begin with their results.

Suppose $0 < X \in \mathbb{R}$. We denote by $S_+(X)$ the set of positive fundamental discriminants $0 < D < X$ of quadratic fields. Similarly, we denote by $S_-(X)$ the set of negative fundamental discriminants $-X < D < 0$ of quadratic fields. The following theorem is known as a corollary that is obtained from a result of [5].

Theorem 3.1 (Davenport and Heilbronn, [5]).

(1)
$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X) \mid 3 \nmid h(D)\}}{\sharp\{D \in S_+(X)\}} \geqslant \frac{5}{6}.$$

(2)
$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_-(X) \mid 3 \nmid h(D)\}}{\sharp\{D \in S_-(X)\}} \geqslant \frac{1}{2}.$$

Nakagawa and Horie [19] improved Theorem 3.1. We state their result. Let m and N be positive integers satisfying the following conditions:

(I) If p is an odd prime divisor of $\gcd(m, N)$, then $p^2 \mid N$ and $p^2 \nmid m$.
(II) If N is even, then condition (i) or (ii) is satisfied.
- (i) $4 \mid N$ and $m \equiv 1 \bmod 4$.
- (ii) $16 \mid N$ and $m \equiv 8, 12 \bmod 16$.

We construct two sets depending upon these integers m, N.

$$S_+(X, m, N) := \{D \in S_+(X) \mid D \equiv m \bmod N\}$$

$$S_-(X, m, N) := \{D \in S_-(X) \mid D \equiv m \bmod N\}$$

As a refinement of Theorem 3.1, Nakagawa and Horie proved the following theorem.

Theorem 3.2 (Nakagawa and Horie, [19]).

(1)
$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X, m, N) \mid 3 \nmid h(D)\}}{\sharp S_+(X, m, N)} \geqslant \frac{5}{6}.$$

(2)
$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_-(X, m, N) \mid 3 \nmid h(D)\}}{\sharp S_-(X, m, N)} \geqslant \frac{1}{2}.$$

(3)
$$\sharp S_+(X, m, N) \sim \sharp S_-(X, m, N) \sim \frac{3X}{\pi^2 \varphi(N)} \prod_{p \mid N:prime} \frac{q}{p+1},$$

where $\varphi(N)$ is the Euler function, $q := 4$ if $p = 2$, and $q := p$ otherwise.

Next, we state a result of Byeon [4]. Theorem 1.4 is obtained from the following proposition.

Proposition 3.3 (Byeon, [4, Proof of Proposition 3.1]). *Let $t > 1$ be a square-free integer. Then, for any two positive integers m and N satisfying conditions (I) and (II), we have the following:*

(1)
$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X, m, tN) \mid 3 \nmid h(D) \text{ and } 3 \nmid h(tD)\}}{\sharp S_+(X, m, tN)} \geqslant \frac{2}{3}.$$

(2)
$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X,m,tN) \mid 3 \nmid h(D) \text{ and } 3 \nmid h(-tD)\}}{\sharp S_+(X,m,tN)} \geqslant \frac{1}{3}.$$

Using the method of the proof of Proposition 3.3, we obtain the following theorem.

Theorem 3.4. *Let m_1, m_2, and m_3 be square-free positive integers (including 1). Assume that positive integers m and N satisfy conditions (I), $16 \mid N$, $m \equiv 1 \bmod 4$, and $\gcd(mN, m_1m_2m_3) \mid 2^3$. Put $M_1 := m_1m_2m_3N$ and $M_2 := m_1m_2N$. Then, we have the following:*

(1)
$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X,m,M_1) \mid 3 \nmid h(m_iD),\ \text{where } i = 1,2,3\}}{\sharp S_+(X,m,M_1)} \geqslant \frac{1}{3}.$$

(2)
$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X,m,M_2) \mid 3 \nmid h(m_1D) \text{ and } 3 \nmid h(-m_2D)\}}{\sharp S_+(X,m,M_2)} \geqslant \frac{1}{3}.$$

For any $D \in S_+(X,m,M_1)$, we have $\gcd(m_1m_2m_3, D) = 1$ (see Lemma 3.7 in Section 3.2). Similarly, for any $D \in S_+(X,m,M_2)$, we find $\gcd(m_1m_2, D) = 1$ (see Section 3.2). Therefore, Theorem 1.5 follows from this theorem.

Remark 3.5. For given positive integers m_1, m_2, and m_3 (resp. m_1 and m_2), we can take integers m and N satisfying the conditions in Theorem 3.4. Integers m and M_1 (resp. m and M_2) satisfy conditions (I) and (II).

By Theorems 3.2 (3) and 3.4, we obtain the following corollary.

Corollary 3.6. *Let m_1, m_2, and m_3 be square-free positive integers (including 1). Assume that positive integers m and N satisfy conditions (I), $16 \mid N$, $m \equiv 1 \bmod 4$, and $\gcd(mN, m_1m_2m_3) \mid 2^3$. Put $M_1 := m_1m_2m_3N$ and $M_2 := m_1m_2N$. Then, we have the following:*

(1)
$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X,m,M_1) \mid 3 \nmid h(m_iD),\ \text{where } i = 1,2,3\}}{\sharp S_+(X)} \geqslant \frac{1}{3\varphi(M_1)} \prod_{p \mid M_1 : prime} \frac{q}{p+1}.$$

(2)
$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X,m,M_2) \mid 3 \nmid h(m_1D) \text{ and } 3 \nmid h(-m_2D)\}}{\sharp S_+(X)} \geqslant \frac{1}{3\varphi(M_2)} \prod_{p \mid M_2 : prime} \frac{q}{p+1},$$

where $\varphi(N)$ denotes the Euler function, $q := 4$ if $p = 2$, and $q := p$ otherwise.

3.2. Proof of Theorem 3.4

In this section, we show Theorem 3.4. First, we prove Theorem 3.4 (1). Define

$$S_+(X, m, M_1, m_i) := \{\widetilde{m_i}D \mid D \in S_+(X, m, M_1)\},$$

where $\widetilde{m_i}$ denotes m_i if $m_i \equiv 1 \bmod 4$ and $4m_i$ otherwise. Note that

$$\sharp S_+(X, m, M_1) = \sharp S_+(X, m, M_1, m_i),$$

where $i = 1, 2, 3$.

Lemma 3.7. *For any $D \in S_+(X, m, M_1)$, we have* $\gcd(m_1m_2m_3, D) = 1$.

Proof. Since $16 \mid N$ and $m \equiv 1 \bmod 4$ hold, $D \equiv 1 \bmod 4$ for any $D \in S_+(X, m, M_1)$. Then, $\gcd(m_1m_2m_3, D)$ is odd. Let ρ be an odd prime divisor of $\gcd(m_1m_2m_3, D)$. It follows from $D \equiv m \bmod M_1$ that ρ divides m. This implies that ρ divides $\gcd(m_1m_2m_3, m)$. By the assumption of Theorem 3.4, $\gcd(mN, m_1m_2m_3) \mid 2^3$. Then, $\rho \mid 2^3$. This is a contradiction. ■

It follows from Lemma 3.7 and $D \equiv 1 \bmod 4$ that $\widetilde{m_i}D$ is the fundamental discriminant of a quadratic field. Then,

$$S_+(X, m, M_1, m_i) = S_+(\widetilde{m_i}X, \widetilde{m_i}m, \widetilde{m_i}M_1),$$

where $i = 1, 2, 3$. Integers $\widetilde{m_i}m$ and $\widetilde{m_i}M_1$ satisfy conditions (I) and (II). Using Theorem 3.2 (1), we find

$$\begin{aligned}
\liminf_{X\to\infty} & \frac{\sharp\{D \in S_+(X, m, M_1) \mid 3 \nmid h(m_iD)\}}{\sharp S_+(X, m, M_1)} \\
&= \liminf_{X\to\infty} \frac{\sharp\{\widetilde{m_i}D \in S_+(X, m, M_1, m_i) \mid 3 \nmid h(\widetilde{m_i}D)\}}{\sharp S_+(X, m, M_1, m_i)} \\
&= \liminf_{X\to\infty} \frac{\sharp\{\widetilde{m_i}D \in S_+(X, \widetilde{m_i}m, \widetilde{m_i}M_1) \mid 3 \nmid h(\widetilde{m_i}D)\}}{\sharp S_+(X, \widetilde{m_i}m, \widetilde{m_i}M_1)} \geqslant \frac{5}{6}.
\end{aligned}$$

We can show

$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X, m, M_1) \mid 3 \nmid h(m_iD) \text{ and } 3 \nmid h(m_jD)\}}{\sharp S_+(X, m, M_1)} \geqslant \frac{2}{3}$$

as follows, where i, $j \in \{1, 2, 3\}$ are distinct integers. The equation

$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X, m, M_1) \mid 3 \nmid h(m_iD)\}}{\sharp S_+(X, m, M_1)} \geqslant \frac{5}{6}$$

implies that if $\varepsilon > 0$, then for sufficiently large $X \in \mathbb{R}$,

$$\frac{\sharp\{D \in S_+(X, m, M_1) \mid 3 \nmid h(m_iD)\}}{\sharp S_+(X, m, M_1)} \geqslant \frac{5}{6} - \varepsilon.$$

It follows that

$$\begin{aligned}
&\sharp S_+(X,m,M_1)\\
&\quad \geqslant \sharp\{D\in S_+(X,m,M_1)\mid 3\nmid h(m_iD)\text{ or }3\nmid h(m_jD)\}\\
&\quad = \sharp\{D\in S_+(X,m,M_1)\mid 3\nmid h(m_iD)\}+\sharp\{D\in S_+(X,m,M_1)\mid 3\nmid h(m_jD)\}\\
&\qquad -\sharp\{D\in S_+(X,m,M_1)\mid 3\nmid h(m_iD)\text{ and }3\nmid h(m_jD)\} =: A(X).
\end{aligned}$$

If $\varepsilon>0$, then for sufficiently large $X\in\mathbb{R}$ we have

$$\begin{aligned}
A(X) &\geqslant \left(\frac{5}{6}-\varepsilon\right)\sharp S_+(X,m,M_1)+\left(\frac{5}{6}-\varepsilon\right)\sharp S_+(X,m,M_1)\\
&\quad -\sharp\{D\in S_+(X,m,M_1)\mid 3\nmid h(m_iD)\text{ and }3\nmid h(m_jD)\}\\
&= \left(\frac{5}{3}-2\varepsilon\right)\sharp S_+(X,m,M_1)\\
&\quad -\sharp\{D\in S_+(X,m,M_1)\mid 3\nmid h(m_iD)\text{ and }3\nmid h(m_jD)\}.
\end{aligned}$$

Then, for sufficiently large $X\in\mathbb{R}$ we have

$$\begin{aligned}
&\sharp\{D\in S_+(X,m,M_1)\mid 3\nmid h(m_iD)\text{ and }3\nmid h(m_jD)\}\\
&\qquad\qquad \geqslant \left(\frac{2}{3}-2\varepsilon\right)\sharp S_+(X,m,M_1),
\end{aligned}$$

that is,

$$\frac{\sharp\{D\in S_+(X,m,M_1)\mid 3\nmid h(m_iD)\text{ and }3\nmid h(m_jD)\}}{\sharp S_+(X,m,M_1)}\geqslant \frac{2}{3}-2\varepsilon.$$

Therefore,

$$\liminf_{X\to\infty}\frac{\sharp\{D\in S_+(X,m,M_1)\mid 3\nmid h(m_iD)\text{ and }3\nmid h(m_jD)\}}{\sharp S_+(X,m,M_1)}\geqslant \frac{2}{3}.$$

Similarly, we obtain

$$\liminf_{X\to\infty}\frac{\sharp\{D\in S_+(X,m,M_1)\mid 3\nmid h(m_iD),\ \text{where } i=1,2,3\}}{\sharp S_+(X,m,M_1)}\geqslant \frac{1}{3}.$$

The proof of Theorem 3.4 (1) is completed. Next, we show Theorem 3.4 (2), modifying the method in the above. In this case, we define

$$S_+(X,m,M_2,-m_2) := \{-\widetilde{m_2}D \mid D\in S_+(X,m,M_2)\},$$

where $\widetilde{m_2}$ denotes m_2 if $-m_2\equiv 1 \bmod 4$ and $4m_2$ otherwise. Note that

$$\sharp S_+(X,m,M_2)=\sharp S_+(X,m,M_2,m_1)=\sharp S_+(X,m,M_2,-m_2).$$

For any $D\in S_+(X,m,M_2)$, we see $\gcd(m_1m_2,D)=1$. Then,

$$S_+(X,m,M_2,m_1)=S_+(\widetilde{m_1}X,\widetilde{m_1}m,\widetilde{m_1}M_2)$$

and

$$S_+(X, m, M_2, -m_2) = S_-(\widetilde{m_2}X, \widetilde{m_2}m', \widetilde{m_2}M_2),$$

where m' is a positive integer satisfying $-\widetilde{m_2}m \equiv \widetilde{m_2}m' \bmod \widetilde{m_2}M_2$. Integers $\widetilde{m_1}m$ and $\widetilde{m_1}M_2$ (resp. $\widetilde{m_2}m'$ and $\widetilde{m_2}M_2$) satisfy conditions (I) and (II). Using Theorem 3.2 (1) and (2), we find

$$\begin{aligned}
&\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X, m, M_2) \mid 3 \nmid h(m_1 D)\}}{\sharp S_+(X, m, M_2)} \\
&\qquad = \liminf_{X\to\infty} \frac{\sharp\{\widetilde{m_1}D \in S_+(X, m, M_2, m_1) \mid 3 \nmid h(\widetilde{m_1}D)\}}{\sharp S_+(X, m, M_2, m_1)} \\
&\qquad = \liminf_{X\to\infty} \frac{\sharp\{\widetilde{m_1}D \in S_+(X, \widetilde{m_1}m, \widetilde{m_1}M_2) \mid 3 \nmid h(\widetilde{m_1}D)\}}{\sharp S_+(X, \widetilde{m_1}m, \widetilde{m_1}M_2)} \geqslant \frac{5}{6}
\end{aligned}$$

and

$$\begin{aligned}
&\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X, m, M_2) \mid 3 \nmid h(-m_2 D)\}}{\sharp S_+(X, m, M_2)} \\
&\qquad = \liminf_{X\to\infty} \frac{\sharp\{-\widetilde{m_2}D \in S_+(X, m, M_2, -m_2) \mid 3 \nmid h(-\widetilde{m_2}D)\}}{\sharp S_+(X, m, M_2, -m_2)} \\
&\qquad = \liminf_{X\to\infty} \frac{\sharp\{-\widetilde{m_2}D \in S_-(X, \widetilde{m_2}m', \widetilde{m_2}M_2) \mid 3 \nmid h(-\widetilde{m_2}D)\}}{\sharp S_-(X, \widetilde{m_2}m', \widetilde{m_2}M_2)} \geqslant \frac{1}{2}.
\end{aligned}$$

Combining the above inequalities, we can likewise obtain

$$\liminf_{X\to\infty} \frac{\sharp\{D \in S_+(X, m, M_2) \mid 3 \nmid h(m_1 D) \text{ and } 3 \nmid h(-m_2 D)\}}{\sharp S_+(X, m, M_2)} \geqslant \frac{1}{3}.$$

The proof of Theorem 3.4 (2) is completed.

3.3. Application

In this section, we give an application of Theorem 1.5 to the Iwasawa invariants of the cyclotomic $\mathbb{Z}_3$-extension of a quadratic field. We begin with a result of K. Iwasawa.

Theorem 3.8 (Iwasawa, [12]). *Let p be a prime number, k an algebraic number field of finite degree, and K/k an arbitrary $\mathbb{Z}_p$-extension. If p does not split in k and the class number of k is indivisible by p, then $\lambda_p(K/k) = \mu_p(K/k) = \nu_p(K/k) = 0$, where $\lambda_p(K/k)$, $\mu_p(K/k)$, and $\nu_p(K/k)$ are the Iwasawa invariants of K/k.*

If k is an abelian field, the Iwasawa μ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of k is equal to 0 [6]. For a prime number p, we denote by $\lambda_p(d)$, $\mu_p(d)$, and $\nu_p(d)$ the Iwasawa λ-, μ-, and ν-invariant of the cyclotomic $\mathbb{Z}_p$-extension of a quadratic field $\mathbb{Q}(\sqrt{d})$. By Theorems 3.4 and 3.8, we obtain the following two corollaries.

Corollary 3.9. *Let m_1 and m_2 be square-free positive integers (including 1).*

(1) *There exist infinitely many positive fundamental discriminants D with a positive inferior limit density such that $\gcd(m_1m_2, D) = 1$ and $\lambda_3(m_iD) = \mu_3(m_iD) = \nu_3(m_iD) = 0$, where $i = 1, 2$.*

(2) *There exist infinitely many positive fundamental discriminants D with a positive inferior limit density such that $\gcd(m_1m_2, D) = 1$, $\lambda_3(m_1D) = \mu_3(m_1D) = \nu_3(m_1D) = 0$, and $\lambda_3(-m_2D) = \mu_3(-m_2D) = \nu_3(-m_2D) = 0$.*

Corollary 3.10. *Let m_1, m_2, and m_3 be distinct square-free positive integers (including 1) with $3 \mid (m_1 - m_2)(m_2 - m_3)(m_3 - m_1)$. Then, there exist infinitely many positive fundamental discriminants D with a positive inferior limit density such that $\gcd(m_1m_2m_3, D) = 1$ and $\lambda_3(m_iD) = \mu_3(m_iD) = \nu_3(m_iD) = 0$, where $i = 1, 2, 3$.*

The idea of this application is based on the one in [19] and [22]. If k is a totally real field, for any prime number p, it is conjectured that the Iwasawa λ_p- and μ_p-invariants of the cyclotomic $\mathbb{Z}_p$-extension of k are equal to 0 (Greenberg's Conjecture, [7]). We can say that Corollaries 3.9 (1) and 3.10 are related to this conjecture. These corollaries are proved by taking N and m, where N and m are integers in Theorem 3.4. For example, we can take N and m as follows.

$\mathbb{Q}(\sqrt{m_1D})$, $\mathbb{Q}(\sqrt{m_2D})$			
m_1	m_2	m	N
$\bar{0}$	$\bar{0}$	1	16
$\bar{0}$	$\bar{1}$	p_1	$16p_1^2$
$\bar{0}$	$\bar{2}$	1	16
$\bar{1}$	$\bar{1}$	$3p_2$	144
$\bar{1}$	$\bar{2}$	$3p_2$	144
$\bar{2}$	$\bar{2}$	$3p_2$	144

$\mathbb{Q}(\sqrt{m_1D})$, $\mathbb{Q}(\sqrt{-m_2D})$			
m_1	$-m_2$	m	N
$\bar{0}$	$\bar{0}$	1	16
$\bar{0}$	$\bar{1}$	p_1	$16p_1^2$
$\bar{0}$	$\bar{2}$	1	16
$\bar{1}$	$\bar{1}$	$3p_2$	144
$\bar{1}$	$\bar{2}$	$3p_2$	144
$\bar{2}$	$\bar{2}$	$3p_2$	144

$\mathbb{Q}(\sqrt{m_1D})$, $\mathbb{Q}(\sqrt{m_2D})$, $\mathbb{Q}(\sqrt{m_3D})$				
m_1	m_2	m_3	m	N
$\bar{0}$	$\bar{0}$	$\bar{0}$	1	16
$\bar{0}$	$\bar{0}$	$\bar{1}$	p'_1	$16p'^2_1$
$\bar{0}$	$\bar{1}$	$\bar{1}$	p'_1	$16p'^2_1$
$\bar{0}$	$\bar{0}$	$\bar{2}$	1	16
$\bar{0}$	$\bar{2}$	$\bar{2}$	1	16
$\bar{1}$	$\bar{1}$	$\bar{1}$	$3p'_2$	144
$\bar{1}$	$\bar{1}$	$\bar{2}$	$3p'_2$	144
$\bar{1}$	$\bar{2}$	$\bar{2}$	$3p'_2$	144
$\bar{2}$	$\bar{2}$	$\bar{2}$	$3p'_2$	144
$\bar{0}$	$\bar{1}$	$\bar{2}$	–	–

Remark 3.11. We define $\bar{0}$, $\bar{1}$, and $\bar{2}$ as $\bar{0} \equiv 0 \bmod 3$, $\bar{1} \equiv 1 \bmod 3$, and $\bar{2} \equiv 2 \bmod 3$. Integers p_1, p_2, p_1', and p_2' are defined as prime numbers such that $p_1 \equiv 5 \bmod 12$ and $p_1 \nmid m_1m_2$, such that $p_2 \equiv 3 \bmod 4$ and $p_2 \nmid 3m_1m_2$, such that $p_1' \equiv 5 \bmod 12$ and $p_1' \nmid m_1m_2m_3$, and such that $p_2' \equiv 3 \bmod 4$ and $p_2' \nmid 3m_1m_2m_3$ respectively. The existence of these prime numbers follows from the theorem on arithmetic progressions.

Acknowledgements. The author wishes to express her gratitude to Professor Toru Komatsu, Professor Shin Nakano, Doctor Satoshi Fujii, Doctor Takayuki Morisawa, Doctor Filippo Alberto Edoardo Nuccio Mortarino Majno di Capriglio, and Yoshichika Iizuka for helpful discussions. She also thanks Professor Kohji Matsumoto and Professor Hiroshi Suzuki for continuous encouragement.

References

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

[2] D. Byeon, *Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields*, Compositio Math. **126** (2001), no. 3, 249–256.

[3] D. Byeon, *Existence of certain fundamental discriminants and class numbers of real quadratic fields*, J. Number Theory **98** (2003), no. 2, 432–437.

[4] D. Byeon, *Class numbers of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{tD})$*, Proc. Amer. Math. Soc. **132** (2004), no. 11, 3137–3140.

[5] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.

[6] B. Ferrero and L.C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), no. 2, 377–395.

[7] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), no. 1, 263–284.

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

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

[11] K. Horie, *Trace formulae and imaginary quadratic fields*, Math. Ann. **288** (1990), 605–612.

[12] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.

[13] 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.

[14] T. Komatsu, *A family of infinite pairs of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-D})$ whose class numbers are both divisible by* 3, Acta Arith. **96** (2001), 213–221.

[15] T. Komatsu, *An infinite family of pairs of quadratic fields* $\mathbb{Q}(\sqrt{D})$ *and* $\mathbb{Q}(\sqrt{mD})$ *whose class numbers are both divisible by* 3, Acta Arith. **104** (2002), 129–136.

[16] P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. **87** (1983), 579–585.

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

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

[19] J. Nakagawa and K. Horie, *Elliptic curves with no rational points*, Proc. Amer. Math. Soc. **104** (1988), 20–24.

[20] K. Ono, *Indivisibility of class numbers of real quadratic fields*, Compositio Math. **119** (1999), no. 1, 1–11.

[21] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math. **166** (1932), 201–203.

[22] H. Taya, *Iwasawa invariants and class numbers of quadratic fields for the prime* 3, Proc. Amer. Math. Soc. **128** (2000), no. 5, 1285–1292.

[23] L.C. Washington, *Introduction to Cyclotomic fields*, second edition, GTM **83**, Springer.

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

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

Address: Akiko Ito: Shibaura Institute of Technology, 307 Fukasaku, Minuma-ku, Saitama-shi, Saitama 337-8570, Japan.

E-mail: i035895@shibaura-it.ac.jp

Received: 26 May 2012