Functiones et Approximatio
60.1 (2019), 61–76
doi: 10.7169/facm/1688

ON THE 3-DIVISIBILITY OF CLASS NUMBERS OF PAIRS OF QUADRATIC FIELDS WITH SPLITTING CONDITIONS

Akiko Ito

Abstract: Let m_1 and m_2 be distinct square-free integers. We show that there exist infinitely many 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 under the splitting conditions of prime numbers. This improves results of T. Komatsu and the author.

Keywords: quadratic fields, class numbers.

1. Introduction

For a fixed positive integer n, there exist infinitely many both imaginary and real quadratic fields with class numbers divisible by n. Such results were obtained by T. Nagell [21], N. C. Ankeny and S. Chowla [1], Y. Yamamoto [26], P. J. Weinberger [24], R. A. Mollin [18], H. Ichimura [8], etc.

Recently, T. Komatsu [14], [15] gave infinite families of pairs of quadratic fields whose class numbers are both divisible by 3.

Theorem 1.1 (T. Komatsu, [14], [15]). *Fix a non-zero integer m. 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 $\mathbb{Q}(\sqrt{md})$ are both divisible by* 3.

For the case where $m = -3$ and $d > 1$, Theorem 1.1 also follows from the Scholz inequality [22]. As other results on explicit construction of infinite families of pairs of quadratic fields whose class numbers are both divisible by a given positive integer, Y. Iizuka, Y. Konomi, and S. Nakano [9], T. Komatsu [16], M. Aoki and Y. Kishi [2] are known. We note that D. Byeon [3] and A. I. [10] showed the existence of infinite families of pairs of quadratic fields whose class numbers are both indivisible by 3.

In 2013, the author proved the following theorem which is regarded as a generalization of Theorem 1.1.

Supported by Research Grant in Kanagawa University (2016).
2010 Mathematics Subject Classification: primary: 11R11; secondary: 11R29

Theorem 1.2 (A. I., [10]). *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 which satisfy the following conditions:*

(1) $\gcd(m_1 m_2, d) = 1$,
(2) $3 \mid h(\mathbb{Q}(\sqrt{m_1 d}))$ *and* $3 \mid h(\mathbb{Q}(\sqrt{m_2 d}))$,

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

In the present paper, by improving the methods of the proofs of Theorem 1.1 and Theorem 1.2, we will show that this theorem holds true under the splitting conditions of prime numbers.

Theorem 1.3. *Let m_1 and m_2 be distinct square-free integers (including 1) and let S_+, S_-, and S_0 be mutually disjoint finite sets of prime numbers not containing prime factors of $6m_1m_2$. Then, there exist infinitely many both positive and negative square-free integers d which satisfy the following conditions:*

(1) $\gcd(m_1 m_2, d) = 1$,
(2-1) *every prime number $\eta \in S_+$ splits in $\mathbb{Q}(\sqrt{d})$,*
(2-2) *every prime number $\eta \in S_-$ is inert in $\mathbb{Q}(\sqrt{d})$,*
(2-3) *every prime number $\eta \in S_0$ is ramified in $\mathbb{Q}(\sqrt{d})$,*
(3) $3 \mid h(\mathbb{Q}(\sqrt{m_1 d}))$ *and* $3 \mid h(\mathbb{Q}(\sqrt{m_2 d}))$.

Theorem 1.2 is embodied in Theorem 1.3. Results of Y. Yamamoto [26], K. James and K. Ono [12], I. Kimura [13], A. Wiles [25], A. I. [11], etc. gave a hint on this study.

Many quadratic fields with the class number divisible by 3 exist. In fact, lower bounds on the number of such quadratic fields with bounded discriminant are addressed by N. C. Ankeny and S. Chowla [1], M. R. Murty [19], [20], K. Soundararajan [23], Y. Gang [6], K. Chakraborty and M. R. Murty [5], D. Byeon and E. Koh [4], D. R. Heath-Brown [7], etc. and it is known that

$$\sharp\left\{0 < d \leqslant X \mid d : \text{square-free, } 3 \mid h(\mathbb{Q}(\sqrt{-d}))\right\} \gg X^{9/10}$$

for any sufficiently large X, for example.

Theorem 1.3 implies we can find various infinite families of quadratic fields with the class number divisible by 3 under strict restrictions. We give an example.

Example 1.4. Assume $m_1 = 7$, $m_2 = 11$, $S_+ = \{5\}$, and $S_0 = \{503\}$. It follows from Theorem 1.3 that

$$\begin{aligned} &\sharp\left\{ d : \text{square-free} \;\middle|\; \begin{array}{c} 3 \mid h(\mathbb{Q}(\sqrt{7d})),\ 3 \mid h(\mathbb{Q}(\sqrt{11d})), \\ \gcd(77, d) = 1, \\ \left(\dfrac{d}{5}\right) = 1,\ \left(\dfrac{d}{503}\right) = 0 \end{array} \right\} \\ &\qquad = \sharp\left\{ d : \text{square-free} \;\middle|\; \begin{array}{c} 3 \mid h(\mathbb{Q}(\sqrt{7d})),\ 3 \mid h(\mathbb{Q}(\sqrt{11d})), \\ \gcd(77, d) = 1, \\ d \equiv 1006, 1509 \bmod 2515 \end{array} \right\} = \infty, \end{aligned}$$

where $(\cdot/\cdot)$ denotes the Legendre symbol. On the other hand, assume $m_1 = 7$, $m_2 = 11$, $S_- = \{5\}$, and $S_0 = \{503\}$. It also follows from Theorem 1.3 that

$$\sharp \left\{ d : \text{square-free} \;\middle|\; \begin{array}{c} 3 \mid h(\mathbb{Q}(\sqrt{7d})),\ 3 \mid h(\mathbb{Q}(\sqrt{11d})), \\ \gcd(77, d) = 1, \\ \left(\dfrac{d}{5}\right) = -1,\ \left(\dfrac{d}{503}\right) = 0 \end{array} \right\} = \infty.$$

These two infinite set are mutually disjoint. By taking various sets S_+, S_-, and S_0, we can find many infinite families for given integers m_1, m_2.

This paper is organized as follows. In Section 2, we construct pairs of such quadratic fields explicitly and explain a key theorem (Theorem 2.1). Theorem 1.3 follows from this. In Section 3, we give a proof of Theorem 2.1. In Section 4, we discuss one further question.

2. Construction

We obtain Theorem 1.3 by constructing infinite families explicitly. The details are as follows.

Let m_1 and m_2 be distinct square-free integers (including 1) and let S_+, S_-, and S_0 be mutually disjoint finite sets of prime numbers not containing prime factors of $6m_1m_2$. We denote by $\mathcal{L}$ the set of all prime numbers l which are inert in the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ and satisfy the condition

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

We can show that $\mathcal{L}$ is an infinite set not containing 2 and 3 by using the Chebotarev density theorem (cf. [15, Lemma 1.1]). Fix $l \in \mathcal{L} \setminus (S_+ \cup S_- \cup S_0)$. We take integers n_1 and n_2 satisfying the following conditions: for each $i = 1, 2$,

$$n_i \equiv \begin{cases} 0 \bmod 9 & \text{if } m_i \not\equiv 0 \bmod 3, \\ 0 \bmod 3 & \text{if } m_i \equiv 0 \bmod 3, \end{cases}$$
$$m_i n_i^2 \equiv 1 \bmod l,$$
$$n_i \equiv 0 \bmod \eta^2 \quad \text{for all } \eta \in S_+ \cup S_- \cup S_0,$$
$$n_i \equiv 4 \bmod 8.$$

There exist such integers n_i by the Chinese remainder theorem. Put $r_i := m_i n_i^2$ and $r := r_1 r_2$, where $i = 1, 2$. Note that $r_1 \neq r_2$. Since $n_i \equiv 4 \bmod 8$ holds, r_i and r are even. Let P be the set of prime numbers defined by

$$P := \{p : \text{prime} \mid p \notin \{2, 3\} \cup S_+ \cup S_- \cup S_0 \text{ and } p \,|\, r(r-1)(r_1 - r_2)\}.$$

The set P is not empty. In fact, l is contained in P because of $l \mid (r - 1)$ and $l \notin \{2, 3\} \cup S_+ \cup S_- \cup S_0$. Let Q be the subset of P defined by

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

We treat the set Q including the case where Q is empty. We denote by T the set of integers t satisfying the following conditions:

(i) $t \equiv -1 \bmod l$,
(ii) $t \equiv \pm 6 \prod_{\eta \in S_0} \eta \bmod 8 \cdot 27 \prod_{\eta \in S_0} \eta^3$,
(iii) For $\eta \in S_+$,

$$\begin{cases} \left(\dfrac{2t}{\eta}\right) = 1 & \text{if } 3 \nmid m_1 m_2, \\ \left(\dfrac{2t'}{\eta}\right) = 1 & \text{if } 3 \mid m_1 m_2, \end{cases}$$

(iv) For $\eta \in S_-$,

$$\begin{cases} \left(\dfrac{2t}{\eta}\right) = -1 & \text{if } 3 \nmid m_1 m_2, \\ \left(\dfrac{2t'}{\eta}\right) = -1 & \text{if } 3 \mid m_1 m_2, \end{cases}$$

(v) $t \not\equiv r_1, r_2 \bmod p \quad for\ all\ p \in P$,
(vi) $2t \not\equiv 3(r_1 + r_2) \bmod q \quad for\ all\ q \in Q$,

where t' is an integer with $t = 3t'$. The set T is infinite by the Chinese remainder theorem. Define three subsets of T as follows. For the case where $r_1 > 0$ and $r_2 > 0$, let

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

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 Theorem 2.1 (5)) and T_1, T_2, T_3 are also infinite. Define

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

Since $3 \mid t$ and $r_i = m_i n_i^2 \equiv 0 \bmod 27$ hold, we have $3t^2 + r \equiv 0 \bmod 27$. Then, $D_{r_1,r_2}(t)$ is an integer for any $t \in T$. Let $\mathcal{F}(S)$ denote the family $\{\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)}) \mid t \in S\}$ 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 $p^n \mid a$. Concerning $D_{r_1,r_2}(t)$, the following theorem holds.

Theorem 2.1. *Let m_1 and m_2 be distinct square-free integers (including 1) and let S_+, S_-, and S_0 be mutually disjoint finite sets of prime numbers not containing prime factors of $6m_1m_2$. Then, we have the following:*

(1) $\gcd(m_1m_2/2^{v_2(m_1m_2)}3^{v_3(m_1m_2)}, D_{r_1,r_2}(t)) = 1$.

(2-1) *When* $\gcd(m_1m_2, 6) = 1$, *every prime number* $\eta \in S_+$ *splits in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)})$, *every prime number* $\eta \in S_-$ *is inert in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)})$, *and every prime number* $\eta \in S_0$ *is ramified in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)})$.

(2-2) *When* $3 \mid m_1m_2$ *and* $2 \nmid m_1m_2$, *every prime number* $\eta \in S_+$ *splits in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$, *every prime number* $\eta \in S_-$ *is inert in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$, *and every prime number* $\eta \in S_0$ *is ramified in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$.

(2-3) *When* $3 \nmid m_1m_2$ *and* $2 \mid m_1m_2$, *every prime number* $\eta \in S_+$ *splits in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$, *every prime number* $\eta \in S_-$ *is inert in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$, *and every prime number* $\eta \in S_0$ *is ramified in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$.

(2-4) *When* $6 \mid m_1m_2$, *every prime number* $\eta \in S_+$ *splits in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$, *every prime number* $\eta \in S_-$ *is inert in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$, *and every prime number* $\eta \in S_0$ *is ramified in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$.

(3) $3 \mid h(\mathbb{Q}(\sqrt{m_1D_{r_1,r_2}(t)}))$ *and* $3 \mid h(\mathbb{Q}(\sqrt{m_2D_{r_1,r_2}(t)}))$ *for any* $t \in T$.

(4) *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*).

(5) *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.*

(6) *The families* $\mathcal{F}(T_1)$, $\mathcal{F}(T_2)$, *and* $\mathcal{F}(T_3)$ *each include infinitely many quadratic fields.*

Theorem 1.3 follows from this. The details are as follows.

When $\gcd(m_1m_2, 6) = 1$, we see from Theorem 2.1 (1) that

$$\gcd(m_1m_2, D_{r_1,r_2}(t)) = 1.$$

By Theorem 2.1 (2-1), (3), (4), (5), (6), we can take d as the square-free part of $D_{r_1,r_2}(t)$.

When $3 \mid m_1m_2$ and $2 \nmid m_1m_2$, it follows from the congruence relations on r_1, r_2 and t that $v_3(D_{r_1,r_2}(t)) = 3$. Then,

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

when $3 \mid m_i$ and

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

when $3 \nmid m_i$. Put $m_i' := m_i/3$ (resp. $m_i' := 3m_i$) when $3 \mid m_i$ (resp. $3 \nmid m_i$). By Theorem 2.1 (1), we have

$$\gcd(m_1'm_2', D_{r_1,r_2}(t)/3^3) = \gcd(m_1m_2/3^{v_3(m_1m_2)}, D_{r_1,r_2}(t)) = 1.$$

Since $\mathbb{Q}\big(\sqrt{m_i' D_{r_1,r_2}(t)/3^3}\big) = \mathbb{Q}\big(\sqrt{m_i D_{r_1,r_2}(t)}\big)$ holds, it follows from Theorem 2.1 (3) that the class number of the quadratic field $\mathbb{Q}\big(\sqrt{m_i' D_{r_1,r_2}(t)/3^3}\big)$ is divisible by 3. By Theorem 2.1 (2-2), every prime number $\eta \in S_+$ splits in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$, every prime number $\eta \in S_-$ is inert in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$, and every prime number $\eta \in S_0$ is ramified in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$. Then, we can take d as the square-free part of $D_{r_1,r_2}(t)/3^3$ for given integers m_i' because of Theorem 2.1 (4), (5), (6).

When $3 \nmid m_1 m_2$ and $2 \mid m_1 m_2$, it follows from the congruence relations on r_1, r_2 and t that $v_2(D_{r_1,r_2}(t)) = 6$. Then,

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

By Theorem 2.1 (1), we see

$$\gcd(m_1 m_2, D_{r_1,r_2}(t)/2^6) = \gcd(m_1 m_2/2^{v_2(m_1 m_2)}, D_{r_1,r_2}(t)) = 1.$$

Since $\mathbb{Q}\big(\sqrt{m_i D_{r_1,r_2}(t)}\big) = \mathbb{Q}\big(\sqrt{m_i D_{r_1,r_2}(t)/2^6}\big)$ holds, it follows from Theorem 2.1 (3) that the class number of the quadratic field $\mathbb{Q}\big(\sqrt{m_i D_{r_1,r_2}(t)/2^6}\big)$ is divisible by 3. By Theorem 2.1 (2-3), every prime number $\eta \in S_+$ splits in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$, every prime number $\eta \in S_-$ is inert in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$, and every prime number $\eta \in S_0$ is ramified in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$. Then, we can take d as the square-free part of $D_{r_1,r_2}(t)/2^6$ because of Theorem 2.1 (4), (5), (6).

When $6 \mid m_1 m_2$, it follows from the congruence relations on r_1 , r_2 and t that

$$\mathbb{Q}\big(\sqrt{m_i D_{r_1,r_2}(t)}\big) = \mathbb{Q}\left(\sqrt{\frac{m_i}{3} \frac{D_{r_1,r_2}(t)}{2^6 3^3}}\right)$$

when $3 \mid m_i$ and

$$\mathbb{Q}\big(\sqrt{m_i D_{r_1,r_2}(t)}\big) = \mathbb{Q}\left(\sqrt{3 m_i \frac{D_{r_1,r_2}(t)}{2^6 3^3}}\right)$$

when $3 \nmid m_i$. Put $m_i' := m_i/3$ (resp. $m_i' := 3m_i$) when $3 \mid m_i$ (resp. $3 \nmid m_i$). By Theorem 2.1 (1), we see

$$\gcd(m_1' m_2', D_{r_1,r_2}(t)/2^6 3^3) = \gcd(m_1 m_2/2^{v_2(m_1 m_2)} 3^{v_3(m_1 m_2)}, D_{r_1,r_2}(t)) = 1.$$

Since $\mathbb{Q}\big(\sqrt{m_i' D_{r_1,r_2}(t)/2^6 3^3}\big) = \mathbb{Q}\big(\sqrt{m_i D_{r_1,r_2}(t)}\big)$ holds, it follows from Theorem 2.1 (3) that the class number of the quadratic field $\mathbb{Q}\big(\sqrt{m_i' D_{r_1,r_2}(t)/2^6 3^3}\big)$ is divisible by 3. By Theorem 2.1 (2-4), every prime number $\eta \in S_+$ splits in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$, every prime number $\eta \in S_-$ is inert in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$, and every prime number $\eta \in S_0$ is ramified in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$. Then, we can take d as the square-free part of $D_{r_1,r_2}(t)/2^6 3^3$ for given integers m_i' because of Theorem 2.1 (4), (5), (6).

We will give a proof of Theorem 2.1 in the next section.

3. Proof of Theorem 2.1

3.1. Proof of Theorem 2.1 (1)

We write the statement of Theorem 2.1 (1) again here.

Theorem 3.1 (Theorem 2.1 (1)). *We have*

$$\gcd(m_1m_2/2^{v_2(m_1m_2)}3^{v_3(m_1m_2)}, D_{r_1,r_2}(t)) = 1.$$

Proof. When $m_1m_2/2^{v_2(m_1m_2)}3^{v_3(m_1m_2)} = \pm 1$, the statement holds true. Then, we treat the case $m_1m_2/2^{v_2(m_1m_2)}3^{v_3(m_1m_2)} \neq \pm 1$. Assume

$$\gcd(m_1m_2/2^{v_2(m_1m_2)}3^{v_3(m_1m_2)}, D_{r_1,r_2}(t)) \neq 1.$$

For every prime number ρ with $\rho \mid \gcd(m_1m_2/2^{v_2(m_1m_2)}3^{v_3(m_1m_2)}, D_{r_1,r_2}(t))$, we have $27D_{r_1,r_2}(t) \equiv 0 \bmod \rho$ and $r \equiv 0 \bmod \rho$. Then,

$$27D_{r_1,r_2}(t) \equiv 3t^4(2t - 3(r_1 + r_2)) \equiv 0 \bmod \rho.$$

We see from $\rho \neq 2, 3$ that $\rho \in Q \subset P$. By the definition of t, we have $2t \not\equiv 3(r_1 + r_2) \bmod \rho$. Therefore, $27D_{r_1,r_2}(t) \equiv 0 \bmod \rho$ implies $\rho \mid t$. On the other hand, it follows from $m_1m_2/2^{v_2(m_1m_2)}3^{v_3(m_1m_2)} \equiv 0 \bmod \rho$ that $\rho \mid m_1$ or $\rho \mid m_2$. Then,

$$t \equiv m_1 \equiv 0 \bmod \rho \qquad \text{or} \qquad t \equiv m_2 \equiv 0 \bmod \rho,$$

that is,

$$t \equiv r_1 \equiv 0 \bmod \rho \qquad \text{or} \qquad t \equiv r_2 \equiv 0 \bmod \rho.$$

This is a contradiction by the definition of t. ■

3.2. Proof of Theorem 2.1 (2)

We write the statement of Theorem 2.1 (2) again here.

Theorem 3.2 (Theorem 2.1 (2)).

(2-1) *When* $\gcd(m_1m_2, 6) = 1$, *every prime number* $\eta \in S_+$ *splits in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)})$, *every prime number* $\eta \in S_-$ *is inert in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)})$, *and every prime number* $\eta \in S_0$ *is ramified in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)})$.

(2-2) *When* $3 \mid m_1m_2$ *and* $2 \nmid m_1m_2$, *every prime number* $\eta \in S_+$ *splits in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$, *every prime number* $\eta \in S_-$ *is inert in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$, *and every prime number* $\eta \in S_0$ *is ramified in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$.

(2-3) *When* $3 \nmid m_1m_2$ *and* $2 \mid m_1m_2$, *every prime number* $\eta \in S_+$ *splits in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$, *every prime number* $\eta \in S_-$ *is inert in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$, *and every prime number* $\eta \in S_0$ *is ramified in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$.

(2-4) *When* $6 \mid m_1m_2$, *every prime number* $\eta \in S_+$ *splits in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$, *every prime number* $\eta \in S_-$ *is inert in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$, *and every prime number* $\eta \in S_0$ *is ramified in* $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$.

Proof. When $\eta \in S_0$, we see that $v_\eta(D_{r_1,r_2}(t)) = 5$. Then, η is ramified in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)})$. It follows from $\eta \neq 2, 3$ that η is also ramified in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$, $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$, and $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$.

When $\eta \in S_+ \cup S_-$, we have

$$D_{r_1,r_2}(t) \equiv 2t'^2 t^3 \bmod \eta.$$

We see

$$\left(\frac{D_{r_1,r_2}(t)}{\eta}\right) = \left(\frac{2t}{\eta}\right) = 1 \text{ (resp. } -1) \qquad \text{if } \eta \in S_+ \text{ (resp. } \eta \in S_-)$$

for the case where $\gcd(m_1 m_2, 6) = 1$,

$$\left(\frac{D_{r_1,r_2}(t)/3^3}{\eta}\right) = \left(\frac{2t'}{\eta}\right) = 1 \text{ (resp. } -1) \qquad \text{if } \eta \in S_+ \text{ (resp. } \eta \in S_-)$$

for the case where $3 \mid m_1 m_2$ and $2 \nmid m_1 m_2$,

$$\left(\frac{D_{r_1,r_2}(t)/2^6}{\eta}\right) = \left(\frac{2t}{\eta}\right) = 1 \text{ (resp. } -1) \qquad \text{if } \eta \in S_+ \text{ (resp. } \eta \in S_-)$$

for the case where $3 \nmid m_1 m_2$ and $2 \mid m_1 m_2$,

$$\left(\frac{D_{r_1,r_2}(t)/2^6 3^3}{\eta}\right) = \left(\frac{2t'}{\eta}\right) = 1 \text{ (resp. } -1) \qquad \text{if } \eta \in S_+ \text{ (resp. } \eta \in S_-)$$

for the case where $6 \mid m_1 m_2$. This implies that every prime number $\eta \in S_+$ splits in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)})$, $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$, $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$, $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$, and every prime $\eta \in S_-$ is inert in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)})$, $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/3^3})$, $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6})$, $\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)/2^6 3^3})$. ■

3.3. Proof of Theorem 2.1 (3)

We write the statement of Theorem 2.1 (3) again here.

Theorem 3.3 (Theorem 2.1 (3)). *We have* $3 \mid h(\mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(t)}))$ *and* $3 \mid h(\mathbb{Q}(\sqrt{m_2 D_{r_1,r_2}(t)}))$ *for any* $t \in T$.

We prove this theorem by constructing an explicit cubic polynomial which gives an unramified cyclic cubic extension of a quadratic field. We use a result of P. Llorente and E. Nart [17]. In Section 3.3.1, we explain their result [17] and show how to apply this to our case. In Section 3.3.2, we give such cubic polynomials and a proof of Theorem 2.1 (3).

3.3.1. Preparation

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. Let θ be a root of $f(Z)$. If we have $v_p(\alpha) \geqslant 2$ and $v_p(\beta) \geqslant 3$ for a prime number p, then θ/p is a root of $h(Z) := Z^3 - (\alpha/p^2)Z - (\beta/p^3)$. The polynomial $h(Z)$ is also irreducible over $\mathbb{Q}$, and we see $K_f = K_h$, $k_f = k_h$. Then, we can assume $v_p(\alpha) < 2$ or $v_p(\beta) < 3$ for each prime number p. Put $K := \mathbb{Q}(\theta)$, a cubic field. We denote by $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$ the prime ideals of K over p. On the decomposition of prime numbers in a cubic field, P. Llorente and E. Nart [17] showed the following.

Proposition 3.4 (Llorente and Nart, [17, Theorem 1]). *The primes of* $\mathbb{Q}$ *decompose in* K *as follows:*

(1) *If* $p \neq 3$, *then* $(p) = \mathfrak{p}$, $\mathfrak{pq}$, $\mathfrak{pqr}$, $\mathfrak{pq}^2$ *if and only if the condition* $1 \leqslant v_p(\beta) \leqslant v_p(\alpha)$ *is not satisfied. Otherwise,* $(p) = \mathfrak{p}^3$.
(2) *If* $p = 3$, $\alpha \equiv 3 \bmod 9$, *and* $\beta^2 \equiv \alpha + 1 \bmod 27$, *then* $(p) = \mathfrak{p}$, $\mathfrak{pq}$, $\mathfrak{pqr}$, $\mathfrak{pq}^2$.

Assume that $4\alpha^3 - 27\beta^2$ is not a square, that is, $k_f \neq \mathbb{Q}$. Then, $(p) \neq \mathfrak{p}^3$ in K if and only if the prime ideals of k_f over p are unramified in the extension K_f/k_f. Because of this, we can rewrite Proposition 3.4 as follows.

Proposition 3.5.

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

We use this proposition in the next section.

3.3.2. Proof of Theorem 2.1 (3)

Now, we treat our case. For a fixed $t \in T$, 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

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

and

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

We take $\alpha = 3c$, $\beta = 2a$, $2b$ and define

$$f_1(Z) := Z^3 - 3cZ - 2a, \qquad f_2(Z) := Z^3 - 3cZ - 2b.$$

It follows from $r_i \equiv 1 \bmod l$ ($i = 1, 2$) 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 $i \in \{1, 2\}$. 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, $f_1(Z)$, $f_2(Z)$ are irreducible over $\mathbb{F}_l$, and hence also over $\mathbb{Q}$. We need the following lemma.

Lemma 3.6. *We have*

$$\gcd(ab, c) = 2^e \cdot 3^{e'} \prod_{\eta \in S_+ \cup S_- \cup S_0} \eta^{e_\eta}$$

for some integers e, e', *and* e_η.

Proof. Since t and r are even, the integer $c = t^2 - r$ is also even. It follows from $2 \mid u$ and $2 \mid w$ that the integer ab is also even. Then, $2 \mid \gcd(ab, c)$. Let ρ be an odd prime divisor of $\gcd(ab, c)$. Since ρ divides $c = t^2 - r$, we have $t^2 \equiv r \bmod \rho$. We see from $\rho \mid ab$ that

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

Then, (i) $\rho \mid t$ or (ii) $t \equiv r_1 \bmod \rho$ or (iii) $t \equiv r_2 \bmod \rho$. First, we treat Case(i). Since $t \equiv t^2 \equiv r \equiv 0 \bmod \rho$ holds, we have $\rho \mid r$. Then, $\rho \mid r_1$ or $\rho \mid r_2$, that is, $t \equiv r_1 \bmod \rho$ or $t \equiv r_2 \bmod \rho$. This implies $\rho \notin P$, that is, $\rho \in \{3\} \cup S_+ \cup S_- \cup S_0$. Secondly, we treat Case(ii). We see from

$$r_1^2 \equiv t^2 \equiv r = r_1 r_2 \mod \rho$$

that $\rho \mid r_1(r_1 - r_2)$, that is, $\rho \mid r_1$ or $\rho \mid r_1 - r_2$. If $\rho \mid r_1$, then $\rho \mid r$. Since $t \equiv r_1 \bmod \rho$ holds, we have $\rho \notin P$. Then, $\rho \in \{3\} \cup S_+ \cup S_- \cup S_0$. If $\rho \mid r_1 - r_2$, then $\rho \in P \cup \{3\} \cup S_+ \cup S_- \cup S_0$. Since $t \equiv r_1 \bmod \rho$, we see $\rho \notin P$. Then, $\rho \in \{3\} \cup S_+ \cup S_- \cup S_0$. Finally, we treat Case(iii). By

$$r_2^2 \equiv t^2 \equiv r = r_1 r_2 \mod \rho,$$

we have $\rho \mid r_2(r_2 - r_1)$, that is, $\rho \mid r_2$ or $\rho \mid r_2 - r_1$. If $\rho \mid r_2$, then $\rho \mid r$. We see from $t \equiv r_2 \bmod \rho$ that $\rho \notin P$, that is, $\rho \in \{3\} \cup S_+ \cup S_- \cup S_0$. If $\rho \mid r_2 - r_1$, then $t \equiv r_2 \equiv r_1 \bmod \rho$, that is, $t \equiv r_1 \bmod \rho$. This case can result in Case(ii), and then $\rho \in \{3\} \cup S_+ \cup S_- \cup S_0$. ■

We see from this lemma that

$$\gcd(\alpha, \beta) = 2^{\overline{e}} \cdot 3^{\overline{e'}} \prod_{\eta \in S_+ \cup S_- \cup S_0} \eta^{e_\eta}$$

for some integers $\overline{e}$ and $\overline{e'}$. Let δ, δ', and δ_η be the maximal integers such that

$$\frac{\alpha}{2^{2\delta} 3^{2\delta'} \prod_{\eta \in S_+ \cup S_- \cup S_0} \eta^{2\delta_\eta}}, \ \frac{\beta}{2^{3\delta} 3^{3\delta'} \prod_{\eta \in S_+ \cup S_- \cup S_0} \eta^{3\delta_\eta}} \in \mathbb{Z}.$$

Put

$$\alpha_0 := \frac{\alpha}{2^{2\delta} 3^{2\delta'} \prod_{\eta \in S_+ \cup S_- \cup S_0} \eta^{2\delta_\eta}} = \frac{3c}{2^{2\delta} 3^{2\delta'} \prod_{\eta \in S_+ \cup S_- \cup S_0} \eta^{2\delta_\eta}}$$

and

$$\beta_0 := \frac{\beta}{2^{3\delta} 3^{3\delta'} \prod_{\eta \in S_+ \cup S_- \cup S_0} \eta^{3\delta_\eta}} = \frac{2a \quad (\text{resp. } 2b)}{2^{3\delta} 3^{3\delta'} \prod_{\eta \in S_+ \cup S_- \cup S_0} \eta^{3\delta_\eta}}.$$

Define $h_i(Z) := Z^3 - \alpha_0 Z - \beta_0$, where $i = 1, 2$. Then, $v_p(\alpha_0) < 2$ or $v_p(\beta_0) < 3$ for each prime number p, the polynomials $h_i(Z)$ are also irreducible over $\mathbb{Q}$, $K_{f_i} = K_{h_i}$, and $k_{f_i} = k_{h_i}$. Note that

$$4(3c)^3 - 27(2a)^2, \qquad 4(3c)^3 - 27(2b)^2 = 54^2 r_i D_{r_1,r_2}(t) = (54n_i)^2 m_i D_{r_1,r_2}(t).$$

Then, $k_{f_i} = k_{h_i} = \mathbb{Q}(\sqrt{m_i D_{r_1,r_2}(t)})$. It follows from Theorem 2.1 (2-1), (2-2), (2-3), (2-4) that every prime number $\eta \in S_0$ is ramified in $k_{f_i} = k_{h_i}$. Then, $k_{h_i} \neq \mathbb{Q}$. Our situation satisfies the assumption of Proposition 3.5. By using this proposition, we show the following lemma.

Lemma 3.7. *The cyclic cubic extensions K_{h_i}/k_{h_i} are both everywhere unramified at finite places, where $i = 1, 2$.*

Proof. When $\eta \notin \{2, 3\} \cup S_+ \cup S_- \cup S_0$, the condition $1 \leqslant v_\eta(\beta_0) \leqslant v_\eta(\alpha_0)$ is not satisfied. By Proposition 3.5 (1), the prime ideals of k_{h_i} over η are unramified in the extension K_{h_i}/k_{h_i}.

When $\eta = 2$, we have $v_2(2a) = v_2(2b) = 4$ and $v_2(3c) = 2$. Then, $\delta = 1$ and the condition $1 \leqslant v_2(\beta_0) \leqslant v_2(\alpha_0)$ is not satisfied. By Proposition 3.5 (1), the prime ideals of k_{h_i} over 2 are unramified in the extension K_{h_i}/k_{h_i}.

When $\eta \in S_+ \cup S_-$, we have $3c \equiv 3t^2 \not\equiv 0 \bmod \eta$. Then, $\delta_\eta = 0$ and $v_\eta(\alpha_0) = 0$. This implies that the condition $1 \leqslant v_\eta(\beta_0) \leqslant v_\eta(\alpha_0)$ is not satisfied. By Proposition 3.5 (1), the prime ideals of k_{h_i} over η are unramified in the extension K_{h_i}/k_{h_i}.

When $\eta \in S_0$, we have $v_\eta(2a) = v_\eta(2b) = 3$ and $v_\eta(3c) = 2$. Then, $\delta_\eta = 1$ and the condition $1 \leqslant v_\eta(\beta_0) \leqslant v_\eta(\alpha_0)$ is not satisfied. By Proposition 3.5 (1), the prime ideals of k_{h_i} over η are unramified in the extension K_{h_i}/k_{h_i}.

When $\eta = 3$, we see $v_3(3c) = 3$. By the definition of a and b, we have $v_3(2a) = v_3(2b) = 3$. Then, $\delta' = 1$. Put $t_1 := \dfrac{t}{6\prod_{\eta \in S_0} \eta}$. By the definition of t, we see $t_1 \equiv \pm 1 \bmod 9$ and $t_1^3 \equiv \pm 1 \bmod 27$. Since

$$\alpha_0 = \frac{3c}{6^2 \prod_{\eta \in S_0} \eta^2} \equiv \frac{3t^2}{6^2 \prod_{\eta \in S_0} \eta^2} \equiv 3t_1^2 \equiv 3 \mod 27$$

and

$$\beta_0 = \frac{2a \text{ (resp. } 2b)}{6^3 \prod_{\eta \in S_0} \eta^3} \equiv \frac{2t^3}{6^3 \prod_{\eta \in S_0} \eta^3} \equiv 2t_1^3 \equiv \pm 2 \mod 27$$

hold, we have $\beta_0^2 \equiv \alpha_0 + 1 \bmod 27$. By Proposition 3.5 (2), the prime ideals of k_{h_i} over 3 are unramified in the extension K_{h_i}/k_{h_i}. ∎

Lemma 3.7 implies that $3 \mid h(k_{h_i})$. The proof of Theorem 2.1 (3) is completed.

3.4. Proof of Theorem 2.1 (4), (5)

We write the statement of Theorem 2.1 (4), (5) again here.

Theorem 3.8 (Theorem 2.1 (4), (5)).

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

(2) *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 $\mathbb{Q}(\sqrt{m_1 D_{r_1,r_2}(t)})$ is real and the quadratic field $\mathbb{Q}(\sqrt{m_2 D_{r_1,r_2}(t)})$ is imaginary.*

Proof. Define

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

We can show this theorem in a way similar to [10, Lemma 2.11]. For the convenience of the reader, we write this here.

(1) We may assume $m_1 > m_2$. Since $\dfrac{1}{27}(3t^2+r)$ 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

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

Then, $g_{r_1,r_2}(X) = 0$ has only one real root. This root is larger than $r_1 = \max\{r_1, r_2\}$. Because of this, if $t \in T_2$, then $g_{r_1,r_2}(t)$ is negative, that is, $D_{r_1,r_2}(t)$ is negative. We have

$$g_{r_1,r_2}(3r_1/2) = \frac{1}{4}r_1r_2(5r_1 - 4r_2) > 0.$$

Since $g_{r_1,r_2}(X)$ is monotonically increasing for $X > r_1 = \max\{r_1, r_2\}$, we obtain $g_{r_1,r_2}(t) > 0$ when $t \geqslant 3r_1/2 = 3\max\{r_1, r_2\}/2$. Then, $D_{r_1,r_2}(t)$ is positive if $t \in T_1$.

(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 $t_0 \geqslant r_1 = \max\{r_1, r_2\}$ and $g_{r_1,r_2}(t_0) = 0$. If $t > \sqrt{-r/3}$, then $3t^2 + r > 0$. Therefore, $D_{r_1,r_2}(t)$ is positive when $t > \max\{t_0, \sqrt{-r/3}\}$. Here, $\max\{t_0, \sqrt{-r/3}\} = t_0$. 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 $t_0 > \sqrt{-r/3}$. Then, $D_{r_1,r_2}(t)$ is positive if $t \in T_3$. ∎

3.5. Proof of Theorem 2.1 (6)

We write the statement of Theorem 2.1 (6) again here.

Theorem 3.9 (Theorem 2.1 (6)). *The families $\mathcal{F}(T_1)$, $\mathcal{F}(T_2)$, and $\mathcal{F}(T_3)$ each include infinitely many quadratic fields.*

Proof. Assume S is a non-empty subset of T_i such that $\mathcal{F}(S)$ is finite, where $i = 1$, 2, 3. We will show that we can choose a_0 from T_i such 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 $M_S/\mathbb{Q}$. Note that $S_0 \subset P_S$ and the set P_S is finite. Define $\mathcal{P} := P \cup P_S \cup S_+ \cup S_- \cup \{2, 3\}$. There exists at least one prime number $q_1 \notin \mathcal{P}$ such that $\left(\dfrac{(-r/3)}{q_1}\right) = 1$. We fix such a prime number q_1. Then, there exists at least one integer x such that $3x^2 + r \equiv 0 \mod q_1$. We fix such an integer x. Define

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

When $x_0 = x$, we have

$$3x_0^2 + r = 3x^2 + r \begin{cases} \equiv 0 \mod q_1 \\ \not\equiv 0 \mod q_1^2. \end{cases}$$

When $x_0 = x + q_1$, we see

$$3x_0^2 + r = (3x^2 + r) + (6q_1x + 3q_1^2) \begin{cases} \equiv 3x^2 + r \equiv 0 \mod q_1 \\ \equiv (3x^2 + r) + 6q_1x \equiv 6q_1x \mod q_1^2. \end{cases}$$

If $q_1^2 \mid 3x_0^2 + r$, we have $q_1 \mid 6x$. Since $q_1 \notin \{2, 3\}$ holds, we see $q_1 \mid x$. Then, $q_1 \mid r$ by $3x^2 + r \equiv 0 \bmod q_1^2$. This is a contradiction. Therefore, $v_{q_1}(3x_0^2 + r) = 1$. Since

$$(2x - 3(r_1 + r_2))(3x^2 + r_1r_2) + 16r_1r_2x = 3g_{r_1,r_2}(x)$$

holds, we have

$$3g_{r_1,r_2}(x_0) \equiv 16r_1r_2x_0 \mod q_1.$$

Assume $g_{r_1,r_2}(x_0) \equiv 0 \bmod q_1$. We have $q_1 \mid 16r_1r_2x_0$. It follows from $q_1 \notin \mathcal{P}$ that $q_1 \mid x_0$. Since $3x_0^2 + r \equiv 0 \bmod q_1$ holds, we have $q_1 \mid r$, a contradiction. Then, $g_{r_1,r_2}(x_0) \not\equiv 0 \bmod q_1$. We see from $v_{q_1}(1/27) = 0$, $v_{q_1}(3x_0^2 + r) = 1$, and $v_{q_1}(g_{r_1,r_2}(x_0)) = 0$ that $v_{q_1}(D_{r_1,r_2}(x_0)) = 1$. It follows from

$$q_1 \notin P \cup \{2, 3\} \cup S_+ \cup S_- \cup S_0 \subset \mathcal{P}$$

and the Chinese remainder theorem that there exists $a_0 \in T_i$ such that $a_0 \equiv x_0 \bmod q_1^2$. Then,

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

and

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

This implies q_1 ramifies in $\mathbb{Q}(\sqrt{D_{r_1,r_2}(a_0)})/\mathbb{Q}$ and so in $M_S(\sqrt{D_{r_1,r_2}(a_0)})/\mathbb{Q}$. By the assumption $q_1 \notin P_S$, this implies

$$M_S \subsetneq M_S\big(\sqrt{D_{r_1,r_2}(a_0)}\big),$$

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_j of T_i such that

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

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

4. Further discussion

As seen in Section 1, lower bounds of the number of quadratic fields with class number divisible by 3 are investigated. We can raise the following question naturally.

Question 4.1. *Let m_1 and m_2 be distinct square-free integers* (*including* 1) *and let S_+, S_-, and S_0 be mutually disjoint finite sets of prime numbers not containing prime factors of* $6m_1m_2$. *Estimate the number of quadratic fields $\mathbb{Q}(\sqrt{d})$ with bounded discriminant which satisfy the following conditions:*

(1) $\gcd(m_1m_2, d) = 1$,
(2-1) *every prime number $\eta \in S_+$ splits in $\mathbb{Q}(\sqrt{d})$,*
(2-2) *every prime number $\eta \in S_-$ is inert in $\mathbb{Q}(\sqrt{d})$,*
(2-3) *every prime number $\eta \in S_0$ is ramified in $\mathbb{Q}(\sqrt{d})$,*
(3) $3 \mid h(\mathbb{Q}(\sqrt{m_1 d}))$ *and* $3 \mid h(\mathbb{Q}(\sqrt{m_2 d}))$.

We end by making an observation about this. Let $N(X)$ be the number of such square-free integers d with $|d| \leqslant X$, where X is a real number. For given integers m_1, m_2 and sets S_+, S_-, S_0, we fix l, n_1, n_2, that is, r_1, r_2. It follows from Theorem 1.3, the definition of t, and the Chinese remainder theorem that

$$\begin{aligned} N(X) &\gg \sharp\{\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)}) \mid t \in T,\ |D_{r_1,r_2}(t)| \leqslant X\} \\ &\gg \sharp\{\mathbb{Q}(\sqrt{D_{r_1,r_2}(t)}) \mid t \equiv A \bmod B,\ |D_{r_1,r_2}(t)| \leqslant X\} \end{aligned}$$

for any sufficiently large X, where A and B are some integers. We note that at least

$$\sharp\{t \in \mathbb{Z} \mid t \equiv A \bmod B,\ |D_{r_1,r_2}(t)| \leqslant X\} \gg X^{1/5}$$

for any sufficiently large X since the degree of $D_{r_1,r_2}(t)$ is 5. If the number of integers t such that $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{D_{r_1,r_2}(t)})$, $t \equiv A \bmod B$, and $|D_{r_1,r_2}(t)| \leqslant X$ is relatively small for any fixed square-free integer d, we can obtain a lower bound of $N(X)$ by using the above equation. We do not know whether this assumption holds true or not.

We hope that Question 4.1 will be solved because it also might lead to estimating of the number of quadratic fields with the class number divisible by 3 under other conditions.

Acknowledgements. The author wishes to express her gratitude to Professor Toru Komatsu, Professor Filippo Alberto Edoardo Nuccio Mortarino Majno di Capriglio, Professor Yasushi Mizusawa, and Professor Hisao Taya for helpful discussions. Further, she thanks the referee for careful reading and useful comments.

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] M. Aoki and Y. Kishi, *An infinite family of pairs of imaginary quadratic fields with both class numbers divisible by five*, J. Number Theory **176** (2017), 333–343.

[3] 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.

[4] D. Byeon and E. Koh, *Real quadratic fields with class number divisible by* 3, Manuscripta Math. **111** (2003), 261–263.

[5] K. Chakraborty and M. R. Murty, *On the number of real quadratic fields with class number divisible by* 3, Proc. Amer. Math. Soc. **131** (2003), 41–44.

[6] Y. Gang, *A note on the divisibility of class numbers of real quadratic fields*, J. Number Theory **97** (2002), no. 1, 35–44.

[7] D. R. Heath-Brown, *Quadratic class numbers divisible by* 3, Funct. Approx. Comment. Math. **37** (2007), 203–211; Corrigendum, Funct. Approx. Comment. Math. **43** (2010), 227.

[8] H. Ichimura, *Note on the class numbers of certain real quadratic fields*, Abh. Math. Sem. Univ. Hamburg **73** (2003), 281–288.

[9] Y. Iizuka, Y. Konomi, and S. Nakano, *On the class number divisibility of pairs of quadratic fields obtained from points on elliptic curves*, J. Math. Soc. Japan **68** (2016), 899–915.

[10] A. Ito, *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, Funct. Approx. Comment. Math. **49** (2013), 111–135.

[11] A. Ito, *On certain infinite families of imaginary quadratic fields whose Iwasawa* λ*-invariant is equal to* 1, Acta Arith. **168** (2015), 301–339.

[12] K. James and K. Ono, *Selmer groups of quadratic twists of elliptic curves*, Math. Ann. **314** (1999), 1–17.

[13] I. Kimura, *A note on the existence of certain infinite families of imaginary quadratic fields*, Acta Arith. **110** (2003), no. 1, 37–43; Corrigendum, Acta Arith. **114** (2004), no. 4, 397.

[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] T. Komatsu, *An infinite family of pairs of imaginary quadratic fields with ideal classes of a given order*, Int. J. Number Theory, **13** (2017), no.2, 253–260.

[17] 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.

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

[19] M. R. Murty, *The abc conjecture and exponents of class groups of quadratic fields*, Number theory (Tiruchirapalli, 1996), 85–95, Contemp. Math. **210**, Amer. Math. Soc., Providence, RI, 1998.

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

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

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

[23] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc.(2) **61** (2000), 681–690.

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

[25] A. Wiles, *On class groups of imaginary quadratic fields*, J. London Math. Soc. **92** (2015), 411–426.

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

Address: Akiko Ito: Tokyo University of Information Sciences, 4-1, Onaridai, Wakaba-ku, Chiba, 265-8501, Japan.

E-mail: ai206314@rsch.tuis.ac.jp

Received: 29 June 2017; **revised:** 7 April 2018