Chin. Ann. Math. Ser. B
43(2), 2022, 307–318
DOI: 10.1007/s11401-022-0319-4

Chinese Annals of Mathematics, Series B

A Note on 3-Divisibility of Class Number of Quadratic Field*

Jianfeng XIE[1] Kuok Fai CHAO[2]

Abstract In this paper, the authors show that there exists infinitely many family of pairs of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{D+n})$ with $D, n \in \mathbb{Z}$ whose class numbers are both divisible by 3.

Keywords Quadratic field, Class number, Hilbert class field
2000 MR Subject Classification 11R29, 11R11

1 Introduction

The class number of algebraic number field is a classical topic being studied in a long history in number theory. Gauss proposed the following profound conjectures

Conjecture 1.1 There are infinitely many real quadratic fields with class number one.

Conjecture 1.2 There are only 9 imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ with class number one, here $D = -1, -2, -3, -7, -11, -19, -43, -67$ and -163.

Conjecture 1.2 has been verified by Baker and Stark respectively in 1967. But Conjecture 1.1 is still an open problem so far. It seems that the case of real quadratic field is quite different to that of imaginary quadratic field. Due to this reason partly, some scholars think about the divisibility of class numbers of quadratic fields. Komatsu [5] gives an infinite family of pairs of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{mD})$ with $m, D \in \mathbb{Z}$ whose class numbers are multiple of 3. In [2], Iizuka, Konomi and Nakano construct an infinite family of pairs of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{mD+n})$ with $D \in \mathbb{Q}, m, n \in \mathbb{Z}$ whose class numbers are both divisible by 3 or 5 or 7. Recently Iizuka [1] proposes the following conjecture and proves that this conjecture holds for imaginary quadratic fields when $p = 3, n = 1$.

Conjecture 1.3 (see [1]) For any prime number p and any positive integer n, there is an infinite family of $n+1$ successive real (or imaginary) quadratic fields

$$\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{D+1}), \cdots, \mathbb{Q}(\sqrt{D+n})$$

Manuscript received May 8, 2019. Revised July 8, 2021.
[1]Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, China. E-mail: xjfnt@mail.ustc.edu.cn
[2]Lui Che Woo College, University of Macau, Macau, China. E-mail: kchao@um.edu.mo
*This work was supported by Anhui Initiative in Quantum Information Technologies (No. AHY150200).

with $D \in \mathbb{Z}$ whose class numbers are divisible by p.

Inspired by these results, one can consider such problem: For a given positive integer n, does there exist an infinite family of pairs of real (imaginary) quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{D+n})$ with $D \in \mathbb{Z}$ whose class numbers are both divisible by 3?

From now on we call the real (resp. imaginary) case for the case of pairs of real (resp. imaginary) quadratic fields for short. In this paper, we give the positive answer for the problem above, More concretely, we have

Theorem 1.1 *For arbitrary positive integer n, there exist infinity many pairs of quadratic fields $\mathbb{Q}(\sqrt{D})$, $\mathbb{Q}(\sqrt{D+n})$ with some $D \in \mathbb{Z}$ such that their class numbers can be divided by* 3 *for the real case and imaginary case, respectively.*

We note that our main result is for any positive number. In particular, taking $n = 1$ in the imaginary case, it is the case studied by Iizuka.

Notation Throughout this paper, $\mathbb{Z}, \mathbb{Q}, \mathbb{F}_p$ denote the ring of rational integers, the field of rational numbers and the finite field of order p, respectively. For a prime number p and an integer a, $v_p(a)$ denotes the greatest exponent m such that $p^m \mid a$, i.e., p-adic valuation. For a algebraic number field K, $K_{\mathbf{p}}$ denotes its completion with respect to its nonzero prime ideal $\mathbf{p}$. We denote the class group of K and the class number of K by Cl_K and $h(K)$, respectively.

2 The Local-Global Principle for $x^m - d$

In this section, we would like discuss the reducibility of polynomial $x^m - d$ which will play a key role in our paper. At first, we recall a fact in algebraic number theory.

Theorem 2.1 (see [3]) *Let L/K be a finite extension of number fields and O_L, O_K denote their rings of integers respectively. Suppose that* p *is a nonzero prime ideal of O_K and $\boldsymbol{q}_1, \cdots, \boldsymbol{q}_g$ are all the distinct prime ideals of O_L that lie above* p. *Take $\alpha \in L$ such that $L = K(\alpha)$, and let $f(T)$ be an irreducible polynomial over K with $f(\alpha) = 0$. Factor $f(x)$ into the product $f = \prod_{i=1}^{h} f_i$ of irreducible polynomials with coefficients in K_{p}. Then, we have $g = h$. By changing the order of $f_1, \cdots, f_g$, we obtain isomorphisms of fields over K_{p},*

$$K_{\mathrm{p}}[T]/((f_i(T))) \cong L_{\boldsymbol{q}_i}, \quad T \to \alpha, \ 1 \le i \le g.$$

Next theorem is an immediate consequence of Chebotarev's density theorem. Since we cannot find the proof in any literature, we give one for the sake of completeness.

Theorem 2.2 *Let L/K be a cyclic extension of number fields, then there are infinitely many places of K which do not split in L.*

Proof Denote $G = Gal(L/K)$ and $n = [L : K]$. Let $\mathbf{q}$ be a nonzero prime of O_L and $\mathbf{p} = O_K \cap \mathbf{q}$. Indeed, there are only finitely many ramified nonzero prime ideals. Since we only focus on the existence of infinitely many places of K which do not split in L, we get rid of these

finitely many prime ideals. From now on, we can assume that $\mathbf{p}$ is unramified in L. Denote $\mathfrak{P} = \{\text{nonzero prime ideals of } O_K \text{ which is unramified in } L\}$. Then we have a fact that $\mathbf{p}$ does not split in L if and only if $G_{\mathbf{q}} = G$, where $G_{\mathbf{q}}$ is the decomposition group of $\mathbf{q}$. Since G is cyclic, we choose a generator σ of G. Let $S = \left\{\mathbf{p} \in \mathfrak{P} \mid \left(\frac{L/K}{\mathbf{p}}\right) = \sigma\right\}$, where $\left(\frac{L/K}{\cdot}\right)$ is the Artin symbol. Thus for each $\mathbf{p} \in S$, $\mathbf{p}$ does not split in L. By density theorem, $\delta(S) = \frac{1}{n}$, where $\delta(S)$ is the Dirichlet density of S. This means S consists of infinitely many elements.

Then we can investigate the irreducibility of the polynomials in the form of $x^m - d$ with $m \in \mathbb{Z}^+, d \in \mathbb{Q}$. At first we deal with a general case.

Theorem 2.3 *Suppose that the polynomial $f(x) = x^m - d \in \mathbb{Q}[x]$ is irreducible over the cyclotomic field $\mathbb{Q}(\zeta_m), d \in \mathbb{Q}^\times$. There are infinitely many prime places q of $\mathbb{Q}$ such that $f(x)$ is irreducible over $\mathbb{Q}_q$ and over $\mathbb{F}_q$.*

Proof Let L be the splitting field of $f(x)$ in $\mathbb{C}$. Consider the finite extension $L/\mathbb{Q}(\zeta_m)$. Since $f(x)$ is irreducible over $\mathbb{Q}(\zeta_m)$, this is a cyclic extension of degree m. By Theorem 2.2, there exists infinitely many prime places of $\mathbb{Q}(\zeta_m)$ which do not split in L. We denote M the set of all such prime places. For any $\mathbf{q} \in M$, we factor $f(x)$ into the product of irreducible polynomials with coefficients in $\mathbb{Q}(\zeta_m)_{\mathbf{q}}$, i.e., $f = \prod_{i=1}^{h} f_i$. According to Theorem 2.1 and the fact that $\mathbf{q}$ does not split in L, we know that $h = 1$, which means that $f(x)$ is irreducible over $\mathbb{Q}(\zeta_m)_{\mathbf{q}}$.

Let q be the prime place of $\mathbb{Q}$ which lies under $\mathbf{q}$. It is immediate to know that $\mathbb{Q}_q$ is a subfield of $\mathbb{Q}(\zeta_m)_{\mathbf{q}}$. Since $f(x)$ is irreducible over $\mathbb{Q}(\zeta_m)_{\mathbf{q}}$, then is also irreducible over $\mathbb{Q}_q$.

Set $d = \frac{b}{c}, (b, c) = 1, b, c \in \mathbb{Z}, c \neq 0$. We choose $\mathbf{q} \in M$ such that $\mathbf{q} \cap \mathbb{Q} = (q)$ and $(q, b, c) = 1$. We note that there are infinitely many non-zero prime ideals $\mathbf{q}$ satisfying this choice due to the prime factorizations of b and c. If $f(x)$ is reducible over $\mathbb{F}_q$, so is $cf(x)$. Then by Hensel's Lemma, $cf(x)$ is also reducible over $\mathbb{Z}_q[x]$ and then over $\mathbb{Q}_q[x]$. This means $f(x)$ is reducible over $\mathbb{Q}_q$, which leads a contradiction.

It may not be easy to determine whether a polynomial in the form of $x^m - d$ is irreducible over $\mathbb{Q}(\zeta_m)$ or not. However, when m is odd, we can just consider this problem over $\mathbb{Q}$. Let us recall a result in [7] which is needed in the proof of Lemma 2.2.

Lemma 2.1 (see [7]) *If m is odd and the polynomial $x^m - d, d \in \mathbb{Q}^\times$ has no root in $\mathbb{Q}$, then it has no root in $\mathbb{Q}(\zeta_m)$.*

Lemma 2.2 *If m is odd and the polynomial $x^m - d, d \in \mathbb{Q}^\times$ is irreducible over $\mathbb{Q}$, then it is also irreducible over $\mathbb{Q}(\zeta_m)$.*

Proof Let $\alpha = \sqrt[m]{d} \in \mathbb{R}$. Firstly we show that if $1 \leq i < m$, then $\alpha^i \notin \mathbb{Q}(\zeta_m)$. Since $x^m - d$ is irreducible over $\mathbb{Q}$, then $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ is a basis of the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$, and hence they are linearly independent over $\mathbb{Q}$. Thus $\alpha^i \notin \mathbb{Q}$. For the polynomial $x^m - d^i$, since its unique real root $\sqrt[n]{d^i} = \alpha^i$ is not in $\mathbb{Q}$, $\alpha^i \notin \mathbb{Q}(\zeta_m)$ by Lemma 2.1.

It is clear that the splitting field of $x^m - d$ is $\mathbb{Q}(\zeta_m)(\alpha)$. Assume that $x^m - d$ is reducible over $\mathbb{Q}(\zeta_m)$, then the degree of the minimal polynomial $f(x)$ of α over $\mathbb{Q}(\zeta_m)$ is less than m, namely, $\deg f(x) = h$. So $f(x)$ can be written in the form of $f(x) = (x-\alpha)(x-\zeta_m^{i_1}\alpha)\cdots(x-\zeta_m^{i_{h-1}}\alpha)$, $1 \le i_j < m$, $1 \le j \le h-1$. Hence the constant term of $f(x)$ is $\alpha^h\zeta_m^{i_1}\cdots\zeta_m^{i_{h-1}} \in \mathbb{Q}(\zeta_m)$. This means $\alpha^h \in \mathbb{Q}(\zeta_m)$, which leads a contradiction. Therefore $x^m - d$ is irreducible over $\mathbb{Q}(\zeta_m)$.

Combining Lemma 2.2 and Theorem 2.3, we get the following result.

Theorem 2.4 *If m is odd and the polynomial $f(x) = x^m - d, d \in \mathbb{Q}^\times$ is irreducible over $\mathbb{Q}$, then there are infinitely many places q of $\mathbb{Q}$ such that $f(x)$ is irreducible over $\mathbb{Q}_q$ and then over $\mathbb{F}_q$.*

Now we can get an equivalent statement, which can be seen as a kind of local-global principle.

Theorem 2.5 *Assume that m is odd and $f(x) = x^m - d,\ d \in \mathbb{Q}^\times$. Then $f(x)$ is reducible over $\mathbb{Q}$ if and only if $f(x)$ is reducible over $\mathbb{F}_q$ except finitely many places q of $\mathbb{Q}$.*

Remark 2.1 There do exist polynomials $f(x) = x^m - d$ with m being even such that $f(x)$ is irreducible over $\mathbb{Q}$ but is reducible over every $\mathbb{F}_q$, where q runs through all prime places of $\mathbb{Q}$. For example, $x^4 + 1$ and $x^{10} - 5$ are the cases.

3 A Construction of Quadratic Fields $(\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{D+n}))$

In this section, we discuss how we can construct a pair of fields $(\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{D+n}))$ whose class numbers can be divided by 3. Recall that Hilbert class field H of a number field K is the maximal unramified abelian extension of K, and there is a canonical isomorphic $Gal(H/K) \cong Cl_K$. It is clear that the class number of K can be divided by 3 if and only if there exists a cyclic unramified cubic extension of K. It is a hint for a construction. Kishi and Miyake [4] give the following characterization of all quadratic fields which admits a cyclic unramified cubic extension.

Theorem 3.1 (see [4]) *Choose $(u, w) \in \mathbb{Z} \times \mathbb{Z}$, and let $g(Z) = Z^3 - uwZ - u^2$. If*

(1) *$d = 4uw^3 - 27u^2$ is not a square in $\mathbb{Z}$;*

(2) *u and w are relatively prime;*

(3) *$g(Z)$ is irreducible over $\mathbb{Q}$;*

(4) *one of the following conditions holds:* (3.1)

(I) $3 \nmid w$;

(II) $3 \mid w,\ uw \not\equiv 3 (\mathrm{mod}\ 9),\ u \equiv w \pm 1 (\mathrm{mod}\ 9)$;

(III) $3 \mid w,\ uw \equiv 3 (\mathrm{mod}\ 9),\ u \equiv w \pm 1 (\mathrm{mod}\ 27)$;

then the normal closure of $\mathbb{Q}(\theta)$, where θ is a root of $g(Z)$, is a cyclic, cubic, unramified extension of $\mathbb{Q}(\sqrt{d})$; in particular, then $K = \mathbb{Q}(\sqrt{d})$ has class number divisible by 3. Conversely, every quadratic number field K with class number divisible by 3 and every unramified, cyclic, cubic extension of K is given by a suitable choice of integers u and w.

Remark 3.1 The condition (1) in (3.1) is critical. The reason why we develop the story of irreducibility of $x^m - d$ in Section 2 is to serve for the condition (3) in (3.1).

To achieve our goals, a natural idea is to find integer pairs (u_1, w_1) and (u_2, w_2) such that both of them satisfy all the conditions in (3.1), and

$$u_2 w_2^3 - 27u_2^2 = a^2(4u_1 w_1^3 - 27u_1^2 + nb^2) \quad \text{for some } a, b \in \mathbb{Q} \setminus \{0\}. \tag{3.2}$$

If so, let $D = \frac{1}{b^2}(4u_1 w_1^3 - 27u_1^2)$, then $D + n = \frac{1}{a^2}(4u_2 w_2^3 - 27u_2^2)$. Thus by Theorem 3.1, the class numbers of $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{D+n})$ are divisible by 3.

In order to find such integer pairs (u_1, w_1) and (u_2, w_2), we consider the integer pairs (x_1, y_1) and (x_2, y_2) such that

$$4y_2^3 - 27x_2^2 = c^2(4y_1^3 - 27x_1^2 + n) \quad \text{for some } c \in \mathbb{Z} \setminus \{0\}. \tag{3.3}$$

If so, let $u_1 = x_1^2, w_1 = y_1$ and $u_2 = \frac{x_2^2}{k^3}, w_2 = \frac{y_2}{k}$ for some $k \in \mathbb{Z} \setminus \{0\}$. Then we have

$$\begin{cases} 4u_1 w_1^3 - 27u_1^2 = x_1^2(4y_1^3 - 27x_2^2), \\ 4u_2 w_2^3 - 27u_2^2 = \dfrac{x_2^2}{k^6}(4y_2^3 - 27x_2^2). \end{cases} \tag{3.4}$$

From (3.3)–(3.4), we get

$$4u_2 w_2^3 - 27u_2^2 = \Big(\frac{x_2 c k^3}{x_1}\Big)^2 (4u_1 w_1^3 - 27u_1^2 + nx_1^2).$$

Thus we are back to the situation (3.2). Clearly we only need to find integer pairs (x_1, y_1) and (x_2, y_2) satisfying equation (3.3). Furthermore, we mention that

$$\begin{aligned} \mathbb{Q}(\sqrt{D}) &= \mathbb{Q}(\sqrt{4u_1 w_1^3 - 27u_1^2}) = \mathbb{Q}(\sqrt{4y_1^3 - 27x_1^2}), \\ \mathbb{Q}(\sqrt{D+n}) &= \mathbb{Q}(\sqrt{4u_2 w_2^3 - 27u_2^2}) = \mathbb{Q}(\sqrt{4y_2^3 - 27x_2^2}). \end{aligned}$$

3.1 First step

Now we start to construct some solutions for equation (3.3). Assume that there exist integer pairs (x_1, y_1) and (x_2, y_2) satisfying equation (3.3) and let

$$y_1 = t^2, \ y_2 = ky_1, \quad \text{where } t, k \in \mathbb{Z}. \tag{3.5}$$

It follows that

$$27(x_2 + cx_1)(x_2 - cx_1) = 4(k^3 - c^2)t^6 - nc^2. \tag{3.6}$$

Put

$$k = n + 4, \quad c = 2k. \tag{3.7}$$

One can check that $4(k^3 - c^2) = nc^2$. Then we can simplify the right-hand side of (3.6)

$$\begin{aligned} 27(x_2 + cx_1)(x_2 - cx_1) &= 4(k^3 - c^2)t^6 - nc^2 \\ &= nc^2(t^6 - 1) \\ &= nc^2(t^3 + 1)(t^3 - 1). \end{aligned}$$

In order to ensure this equality holds, we can put

$$\begin{aligned} \frac{nck(p-1)}{lp}(t^3 + 1) &= 3(x_2 + cx_1), \\ \frac{clp}{k(p-1)}(t^3 - 1) &= 9(x_2 - cx_1), \end{aligned}$$

here p is a prime number and l is a positive integer. We will explain why these two integers are introduced. Solving this equation by regarding x_1 and x_2 as variables, we get

$$\begin{aligned} x_1 &= \frac{1}{18lkp(p-1)}[3nk^2(p-1)^2(t^3 + 1) - l^2p^2(t^3 - 1)], \\ x_2 &= \frac{c}{18lkp(p-1)}[3nk^2(p-1)^2(t^3 + 1) + l^2p^2(t^3 - 1)]. \end{aligned} \tag{3.8}$$

It is clear that (3.3) holds if we set (x_1, y_1) and (x_2, y_2) as in (3.5) and (3.8). We note that we can ensure x_1, x_2 are integers by choosing proper integer t. This will be discussed in Theorem 3.2.

Now regarding $4y_1^3 - 27x_1^2$ as a polynomial in t, i.e., let

$$f(t) = 4y_1^3 - 27x_1^2 = [(2 + 3\sqrt{3}\alpha)t^3 + 3\sqrt{3}\beta][(2 - 3\sqrt{3}\alpha)t^3 - 3\sqrt{3}\beta],$$

where

$$\begin{aligned} \alpha &= \frac{3nk^2(p-1)^2 - l^2p^2}{18lk(p-1)p}, \\ \beta &= \frac{3nk^2(p-1)^2 + l^2p^2}{18lk(p-1)p}. \end{aligned}$$

It is clear that the leading coefficient of $f(t)$ is $4 - 27\alpha^2$. Since $\alpha \in \mathbb{Q}$, $4 - 27\alpha^2 \neq 0$. It is clear that there exist infinitely many integers t_0 such that $f(t_0) > 0$ (resp. $f(t_0) < 0$) when $4 - 27\alpha^2 > 0$ (resp. $4 - 27\alpha^2 < 0$). Based on this fact, we always can choose proper t to ensure that both quadratic fields $\mathbb{Q}(\sqrt{f(t)})$ and $\mathbb{Q}(\sqrt{f(t) + n})$ are real or imaginary. For the imaginary case, we should require $4 - 27\alpha^2 < 0$. It is easy to be achieved by choosing $l > (4\sqrt{3} + 3n)k$. Now we consider the real case. We realize that $4 - 27\alpha^2 > 0$ if and only if $|\alpha| < \frac{2}{3\sqrt{3}}$. It is equivalent to $\frac{|3nk^2(p-1)^2 - l^2p^2|}{lk(p-1)p} < 4\sqrt{3}$ (recall that $18\alpha = \frac{3nk^2(p-1)^2 - l^2p^2}{lk(p-1)p}$). The following lemma asserts that the condition $4 - 27\alpha^2 > 0$ can be achieved as well. This is the reason why we introduce the integer l above.

Lemma 3.1 *Let n, k, p be positive integers such that $p > 3[\sqrt{3n}k]$. Then there exists integer l such that $\frac{|3nk^2(p-1)^2 - l^2p^2|}{lk(p-1)p} < 4\sqrt{3}$.*

Proof Let $l = [\sqrt{3n}k]$, and $d = \sqrt{3n}k - [\sqrt{3n}k]$. Note that $0 \le d < 1$. We have

$$\begin{aligned}
\frac{|\ 3nk^2(p-1)^2 - l^2p^2\ |}{lk(p-1)p} &= \frac{|\ (l+d)^2(p-1)^2 - l^2p^2\ |}{lk(p-1)p} \\
&= \frac{|\ (2l+d)d(p-1)^2 - (2p-1)l^2\ |}{lk(p-1)p} \\
&< \frac{(2l+d)d}{lk}\frac{p-1}{p} + \frac{(2p-1)l}{k(p-1)p} \\
&< \frac{(2l+1)}{lk}\frac{p-1}{p} + \frac{2p-1}{p-1}\frac{l}{pk} \\
&< \frac{3}{k} + 3\frac{l}{3lk} \text{ (by } 0 < \frac{2p-1}{p-1} < 3 \text{ and } p > 3l) \\
&< \frac{4}{k} \\
&< 4\sqrt{3}.
\end{aligned}$$

3.2 Second step

Set (x_1, y_1) and (x_2, y_2) as in (3.5) and (3.8). Let $u_1 = x_1^2, w_1 = y_1, u_2 = \frac{x_2^2}{k^3}$ and $w_2 = \frac{y_2}{k}$. Here we mention that $w_1 = w_2 = t^2$. Consider the polynomials

$$F_1(Z) = Z^3 - u_1wZ - u_1^2, \quad F_2(Z) = Z^3 - u_2wZ - u_2^2,$$

respectively. We will show that (u_1, w) and (u_2, w) satisfy all the conditions in Theorem 3.1 under a suitable choice of t. If so, let

$$D = 4y_1^3 - 27x_1^2 = \frac{1}{x_1^2}(4u_1w_1^3 - 27u_1^2),$$

then

$$D + n = \frac{4y_2^3 - 27x_2^2}{c^2} = \frac{k^6}{x_2^2c^2}(4u_2w_2^3 - 27u_2^2).$$

Thus we get two quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{D+n})$ whose class numbers are divisible by 3.

Now the aim is to ensure the polynomials $F(Z)$ and $G(Z)$ are irreducible by choosing suitable t. Recall

$$\begin{aligned}
\alpha &= \frac{3nk^2(p-1)^2 - l^2p^2}{18lk(p-1)p}, \\
\beta &= \frac{3nk^2(p-1)^2 + l^2p^2}{18lk(p-1)p},
\end{aligned}$$

and let

$$\begin{aligned}
f_1(Z) &= Z^3 - \beta^4, \\
f_2(Z) &= Z^3 - \frac{16}{k^2}\alpha^4.
\end{aligned}$$

We require that p is a prime number and is coprime to $6nkl$. Then it is easy to check that $v_p(\beta^4) = v_p\big(\frac{16}{k^2}\alpha^4\big) = -4$. So $\beta^4 \notin \mathbb{Q}^3$, $\frac{16}{k^2}\alpha^4 \notin \mathbb{Q}^3$, which means $f_1(Z)$ and $f_2(Z)$ are irreducible

over $\mathbb{Q}$. By Theorem 2.4, there exist two primes q_1 and q_2 (not necessary to be different) such that $f_1(Z)$ is irreducible over $\mathbb{F}_{q_1}$ and $f_2(Z)$ is irreducible over $\mathbb{F}_{q_2}$, respectively. Thus we get the following lemma.

Lemma 3.2 *If $t \equiv 0(\mathrm{mod}\ q_1q_2)$, then $F_1(Z)$ and $F_2(Z)$ are both irreducible over $\mathbb{Q}$.*

Proof Since $w = t^2$ in the setting above and $t \equiv 0(\mathrm{mod}\ q_1q_2)$, it is clear that $w \equiv 0(\mathrm{mod}\ q_1)$. From (3.8), we can see that $u_1 \equiv \frac{3nk^2(p-1)^2+l^2p^2}{18lk(p-1)p}(\mathrm{mod}\ q_1)$, then $F_1(Z) \equiv f_1(Z)(\mathrm{mod}\ q_1)$, which means $F_1(Z)$ is irreducible over $\mathbb{F}_{q_1}$. Hence we know that $F_1(Z)$ is irreducible over $\mathbb{Q}$. The irreducibility of $F_2(Z)$ follows in a similar way.

Remark 3.2 In the proof of Lemma 3.2 above, we abuse the notation of congruence and hence consider the congruence of a rational number $\frac{m}{n}$ modulus prime p. Indeed if we restrict n not having any p factor, $\frac{1}{n}$ can be viewed as the reciprocal (or inverse) of n modulus p and it still makes sense under this restriction.

For convenience, recall that

$$\begin{aligned}
&k = n + 4, \quad y_1 = t^2, \quad y_2 = ky_1,\\
&x_1 = \frac{1}{18lkp(p-1)}[3nk^2(p-1)^2(t^3+1) - l^2p^2(t^3-1)],\\
&x_2 = \frac{c}{18lkp(p-1)}[3nk^2(p-1)^2(t^3+1) + l^2p^2(t^3-1)],\\
&u_1 = x_1^2, \quad u_2 = \frac{x_2^2}{k^3},\\
&w_1 = w_2 = t^2,\\
&D = 4y_1^3 - 27x_1^2 = \frac{1}{x_1^2}(4u_1w_1^3 - 27u_1^2),\\
&D + n = \frac{4y_2^3 - 27x_2^2}{c^2} = \frac{k^6}{x_2^2c^2}(4u_2w_2^3 - 27u_2^2)
\end{aligned}$$

and denote $g = 18k^2(p-1)(3nk^2(p-1)^2 + l^2p^2)|(3nk^2(p-1)^2 - l^2p^2)|$. By Theorem 2.3, there exist infinitely many primes q such that -3 is quadratic non-residue in $\mathbb{F}_q$. Choose such a prime number q_0. Applying Theorem 3.1, we have

Theorem 3.2 *Choose a prime number p such that $p \equiv 1(\mathrm{mod}\ 18nlk)$ and let*

$$\begin{aligned}
&t \equiv 1(\mathrm{mod}\ g),\\
&t \equiv -1(\mathrm{mod}\ p),\\
&t \equiv 0(\mathrm{mod}\ q_0q_1q_2),
\end{aligned} \tag{3.9}$$

here q_0 is prime to integers g, p, q_2, q_2. Then pairs (u_1, w_1) and (u_2, w_2) satisfy the conditions of Theorem 3.1*, so*

$$\begin{aligned}
&\mathbb{Q}(\sqrt{4u_1w_1^3 - 27u_1^2}) = \mathbb{Q}(\sqrt{D}),\\
&\mathbb{Q}(\sqrt{4u_2w_2^3 - 27u_2^2}) = \mathbb{Q}(\sqrt{D+n})
\end{aligned}$$

both admit an unramified cyclic cubic extension. In particular, their class numbers are both divisible by 3.

Remark 3.3 We should ensure g, p, q_0, q_1, q_2 are all coprime mutually. We claim that this can be done. Firstly, once n is given, so $k = n + 4$ and then we can get l as in Lemma 3.1. According to Dirichlet's Prime Number theorem, we can choose a prime number p such that

- $p \equiv 1 (\mathrm{mod}\ 18lnk)$ and
- $p > 3[\sqrt{3n}k]$.

Then one can check that $p \nmid g$. Finally, since there exist infinitely many q_i satisfying corresponding property, $i = 0, 1, 2$, we can choose q_0, q_1, q_2 in turn such that g, p, q_0, q_1, q_2 are coprime mutually. If so, by Chinese Remainder theorem, there exist infinitely many integers t satisfying the congruence conditions (3.9).

Proof According to the congruence conditions (3.9), one can check that x_1, x_2 are integers, and $k^2 \mid x_2$. At first we show x_1, x_2 are integers. Indeed, since $p \nmid 18lk(p-1)$, it suffices to show that

$$\begin{aligned} &p \mid 3nk^2(p-1)^2(t^3+1) \pm l^2p^2(t^3-1), \\ &18lk(p-1) \mid 3nk^2(p-1)^2(t^3+1) \pm l^2p^2(t^3-1). \end{aligned}$$

Due to $t \equiv -1 (\mathrm{mod}\ p)$, we have $p \mid t^3 + 1$, then

$$\begin{aligned} &p \mid 3nk^2(p-1)^2(t^3+1), \\ &p \mid 3nk^2(p-1)^2(t^3+1) \pm l^2p^2(t^3-1). \end{aligned}$$

Since $18l \mid (p-1)$, we have $18lk(p-1) \mid 3nk^2(p-1)^2(t^3+1)$. Because $t \equiv 1 (\mathrm{mod}\ 18k(p-1))$, we have $18k(p-1) \mid t^3 - 1$ and then $18lk(p-1) \mid l^2p^2(t^3-1)$. Now it is clear that

$$18lk(p-1) \mid 3nk^2(p-1)^2(t^3+1) \pm l^2p^2(t^3-1).$$

Now we turn to check that $k^2 \mid x_2$. Since $a = 2k$, it suffices to show that $9lp(p-1)k^2 \mid 3nk^2(p-1)^2(t^3+1)$ and $9lp(p-1)k^2 \mid l^2p^2(t^3-1)$. We realize that $p \mid 3nk^2(p-1)^2(t^3+1)$ and $p \mid l^2p^2(t^3-1)$ have been proved already. Since $9l \mid (p-1)$, we get $9l(p-1)k^2 \mid 3nk^2(p-1)^2(t^3+1)$. Because $t \equiv 1 (\mathrm{mod}\ 9l(p-1)k^2)$, we have $9l(p-1)k^2 \mid l^2p^2(t^3-1)$.

Moreover, we have

$$\begin{aligned} &(t, 3nk^2(p-1)^2 + l^2p^2) = 1, \\ &(t, 3nk^2(p-1)^2 - l^2p^2) = 1. \end{aligned}$$

We clarify that the conditions (3.1) in Theorem 3.1 are satisfied in the settings of u_1, u_2, w_1 and w_2 above. We note that $(t, a) = 1$. Then we have $(w_1, u_1) = 1$ and $(w_2, u_2) = 1$ immediately. By the assumption $t \equiv 0 (\mathrm{mod}\ q_0q_1q_2)$, it implies that $t \equiv 0 (\mathrm{mod}\ q_1q_2)$. By Lemma 3.2, we know that $F_1(Z)$ and $F_2(Z)$ are both irreducible. It is clear that conditions (2) and (3) in (3.1)

are fulfilled. Then we check that the condition (I) in (3.1) is satisfied. We recall $t \equiv 1 (\mathrm{mod}\ g)$, and it implies $(3, t) = 1$. Then $3 \nmid w_1$ and $3 \nmid w_2$ follow by $w_1 = w_2 = t^2$.

It remains to show that condition (1) in Theorem 3.1 is satisfied as well, namely, $4u_1w^3 - 27u_1^2$ and $4u_2w^3 - 27u_2^2$ are not squares in $\mathbb{Z}$. By the choice of q_0, $4u_1w^3 - 27u_1^2 \equiv -27u_1^2 \not\equiv m^2 (\mathrm{mod}\ q_0)$, here m can be any integer. This means $4u_1w^3 - 27u_1^2$ is not a square. Similarly we can show that $4u_2w^3 - 27u_2^2$ is not a square as well. By Theorem 3.1, $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{D+n})$ admit an unramified cyclic cubic extension, respectively.

4 The Proof of Theorem 1.1

To show that our construction can generate infinitely many pairs $(\mathbb{Q}(\sqrt{D}),\ \mathbb{Q}(\sqrt{D+n}))$ with their class numbers being divisible by 3, we recall a celebrated result on integral points by Siegel [6]. Let $M_{\mathbb{Q}}$ be the set of all standard absolute values on $\mathbb{Q}$.

Theorem 4.1 (see [6]) *Let S be a finite set such that $\{\infty\} \subset S \subset M_{\mathbb{Q}}$ and $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree $d \geq 3$ with distinct roots in $\mathbb{C}$. Then*

$$\sharp\{(x, y) \in R_S \times R_S \mid y^2 = f(x)\} < \infty,$$

where R_S is the ring of S-integers of $\mathbb{Q}$, i.e., $R_S = \{x \in \mathbb{Q} \mid v_p(x) \geq 0$ for all $p \in M_{\mathbb{Q}} \backslash S\}$.

Lemma 4.1 *Suppose that $f(x) \in \mathbb{Q}[x]$ is a polynomial of degree $d \geq 3$ with distinct roots in $\mathbb{C}$, and $T \subset \mathbb{Z}$ consists of infinitely many integers and put $E = \{\mathbb{Q}(\sqrt{f(t)}) \mid t \in T\}$, then E contains infinitely quadratic fields.*

Proof We assume that $f(x) \in \mathbb{Z}[x]$. Otherwise we choose an integer d such that $d^2 f(x) \in \mathbb{Z}[x]$ and consider the polynomial $d^2 f(x)$ instead since $\mathbb{Q}(\sqrt{f(t)}) = \mathbb{Q}(\sqrt{d^2 f(t)})$. Because T is a countable set, we can denote this ordered set by $T = \{t_i \mid i \in I\}$ with a countable set I. Assume E is a finite set, then there exist finitely many primes $p_1, p_2, \cdots, p_N$ $(N \in \mathbb{Z}^+)$ such that for any $i \in I$, we have

$$f(t_i) = \Big(\prod_{j=1}^{N} p_j^{h_{ij}} \Big) a_i^2, \quad h_{ij} \in \{0, 1\},\ a_i \in \mathbb{Z}.$$

Furthermore, there exists a integer $d = \prod\limits_{j=1}^{N} p_j^{h_{ij}}$ for a specific i such that there are infinitely many $i' \in I$,

$$f(t_{i'}) = d a_{i'}^2, \quad a_{i'} \in \mathbb{Z}.$$

Let $S = \{\infty\}$. Then $R_S = \mathbb{Z}$. Consider the set

$$A = \Big\{ (x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y^2 = \frac{f(x)}{d} \Big\}.$$

It follows that there exist infinitely many pairs of $(t_{i'}, a_{i'})$ in A. But by Siegel's theorem 4.1, A is a finite set, which leads to a contradiction. Hence E is a set with infinite many elements.

Proof of Theorem 1.1 For the real case, we choose a proper l in Lemma 3.1. Set

$$B = \Big(\frac{3nk^2(p-1)^2 + l^2p^2}{4\sqrt{3}lkp(p-1) - 3nk^2(p-1)^2 + l^2p^2}\Big)^{\frac{1}{3}},$$

one can check that $4w_1^3 - 27u_1^2 > 0$ when $t > B$. This guarantees that

$$\mathbb{Q}(\sqrt{4y_1^3 - 27x_1^2}) = \mathbb{Q}(\sqrt{D}),$$
$$\mathbb{Q}(\sqrt{4y_2^3 - 27x_2^2}) = \mathbb{Q}(\sqrt{D+n})$$

are real quadratic fields.

For the imaginary case, choose an integer $l > (4\sqrt{3}+3n)k$. When $t > 0$, we have $4y_2^3 - 27x_2^2 < 0$. This means the quadratic fields

$$\mathbb{Q}(\sqrt{4y_1^3 - 27x_1^2}) = \mathbb{Q}(\sqrt{D}),$$
$$\mathbb{Q}(\sqrt{4y_2^3 - 27x_2^2}) = \mathbb{Q}(\sqrt{D+n})$$

are imaginary.

Let

$$T_1 = \{t \in \mathbb{Z} \mid t \text{ satisfies the condition (3.9) in Theorem 3.2 and } t > B\},$$
$$T_2 = \{t \in \mathbb{Z} \mid t \text{ satisfies the condition (3.9) in Theorem 3.2 and } t > 0\},$$
$$T = \begin{cases} T_1 & \text{for the real case,} \\ T_2 & \text{for the imaginary case.} \end{cases}$$

Chinese Remainder theorem implies that the set T consists of infinite elements. Let $f(t) = 4y_1^3 - 27x_1^2$ and $E = \{\mathbb{Q}(\sqrt{f(t)}) \mid t \in T\}$.

Since $f(t)$ has no repeated roots which is in the form of $[(2+3\sqrt{3}b)t^3 + 3\sqrt{3}c][(2-3\sqrt{3}b)t^3 - 3\sqrt{3}c]$ with $\alpha, \beta \in \mathbb{Q}^\times$, Lemma 4.1 implies that E contains infinitely many quadratic fields. Moreover, let $D_t = f(t)$, $t \in T$, Theorem 3.2 implies that $3 \mid h(\mathbb{Q}(\sqrt{D_t}))$, $3 \mid h(\mathbb{Q}(\sqrt{D_t + n}))$. Then we complete our proof.

Acknowledgement We thank the anonymous referees for the valuable comments on our manuscript.

References

[1] Iizuka, Y., On the class number divisibility of pairs of imaginary quadratic fields, *J. Number Theory*, **184**, 2018, 122–127.

[2] Iizuka, Y., Konomi, Y. and Nakano, S., An application of the arithmetic of elliptic curves to the class number problem for quadratic fields, *Tokyo J. Math.*, **1**, 2021, 1–15.

[3] Kato, K., Kurokawa, N. and Saito, T., Number Theory 2: Introduction to Class Field Theory, American Mathematical Society, Providence, 2011.

[4] Kishi, Y. and Miyake, K., Parametrization of the quadratic fields whose class numbers are divisible by three, *J. Number Theory*, **80**, 2000, 209–217.

[5] Komatsu, T., 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.

[6] Silverman, J., The Arithmetic of Elliptic Curves, 2nd edition, Graduate Texts in Mathematics, Springer-Verlag, New York, 2009.

[7] Xie, J. F. and Chao, K. F., On the divisibility of class numbers of imaginary quadratic fields $(\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt{D+m}))$, *Ramanujan J.*, **53**, 2020, 517–528.