



Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



An infinite family of pairs of imaginary quadratic fields with both class numbers divisible by five



Miho Aoki^a, Yasuhiro Kishi^{b,*}

^a Department of Mathematics, Interdisciplinary Faculty of Science and Engineering, Shimane University, Matsue, Shimane, 690-8504, Japan

^b Department of Mathematics, Faculty of Education, Aichi University of Education, Kariya, Aichi, 448-8542, Japan

ARTICLE INFO

Article history:

Received 21 October 2016
Received in revised form 30 November 2016
Accepted 13 December 2016
Available online xxxx
Communicated by D. Goss

MSC:

primary 11R11
secondary 11R16, 11R29

Keywords:

Quadratic fields
Quartic fields
Class numbers

ABSTRACT

We construct a new infinite family of pairs of imaginary quadratic fields with both class numbers divisible by five. Let n be a positive integer that satisfy $n \equiv \pm 3 \pmod{500}$ and $n \not\equiv 0 \pmod{3}$. We prove that 5 divides the class numbers of both $\mathbb{Q}(\sqrt{2 - F_n})$ and $\mathbb{Q}(\sqrt{5(2 - F_n)})$, where F_n is the n th Fibonacci number.

© 2017 Elsevier Inc. All rights reserved.

1. Introduction

Some infinite families of quadratic fields with class numbers divisible by a fixed integer N were given by Nagell [15], Ankeny and Chowla [1], Yamamoto [19], Weinberger [18], Gross and Rohrich [5], Ichimura [6] and Louboutin [13]. In the case $N = 5$, some results

* Corresponding author.

E-mail addresses: aoki@riko.shimane-u.ac.jp (M. Aoki), ykishi@aecc.aichi-edu.ac.jp (Y. Kishi).

are known due to Parry [16], Mestre [14], Sase [17] and Byeon [3]. One of the authors [10], by using the Fibonacci numbers F_n , gave an infinite family of imaginary quadratic fields with class numbers divisible by five: the $\mathbb{Q}(\sqrt{-F_n})$ with $n \equiv 25 \pmod{50}$.

Recently, Komatsu [11,12] and Ito [9] (resp. Iizuka, Konomi and Nakano [7]) gave infinite families of pairs of quadratic fields with both class numbers divisible by 3 (resp. 3, 5 or 7). In the present article, by using the Fibonacci numbers F_n , we will give an infinite family of pairs of imaginary quadratic fields with both class numbers divisible by 5.

Theorem. *For $n \in \mathcal{N} := \{n \in \mathbb{N} \mid n \equiv \pm 3 \pmod{500}, n \not\equiv 0 \pmod{3}\}$, the class numbers of both $\mathbb{Q}(\sqrt{2-F_n})$ and $\mathbb{Q}(\sqrt{5(2-F_n)})$ are divisible by 5. Moreover, the set of pairs $\{(\mathbb{Q}(\sqrt{2-F_n}), \mathbb{Q}(\sqrt{5(2-F_n)})) \mid n \in \mathcal{N}\}$ is infinite.*

For an algebraic extension K/k , denote the norm map and the trace map of K/k by $N_{K/k}$ and $\text{Tr}_{K/k}$, respectively. For simplicity, we denote N_K and Tr_K if the base field is $k = \mathbb{Q}$. For a prime number p and an integer m , we denote the greatest exponent μ of p such that $p^\mu \mid m$ by $v_p(m)$.

2. Certain parametric quartic polynomial

Let $k = \mathbb{Q}(\sqrt{5})$. For an algebraic integer $\alpha \in k$, we consider the polynomial

$$f(X) = f_\alpha(X) := X^4 - TX^3 + (N+2)X^2 - TX + 1 \in \mathbb{Z}[X], \quad (2.1)$$

where $T := \text{Tr}_k(\alpha)$ and $N := N_k(\alpha)$. The discriminant of $f(X)$ is $\text{disc}(f) = d_1^2 d_2$ with $d_1 := T^2 - 4N$ and $d_2 := (N+4)^2 - 4T^2$. Let L be the minimal splitting field of $f(X)$ over \mathbb{Q} . All four complex roots of $f(X)$ are units of L and can be denoted by $\varepsilon, \varepsilon^{-1}, \eta, \eta^{-1}$, $|\varepsilon| \geq |\varepsilon^{-1}|$, $|\eta| \geq |\eta^{-1}|$, $\alpha = \varepsilon + \varepsilon^{-1}$, $\bar{\alpha} = \eta + \eta^{-1}$, where $\bar{\alpha}$ denotes the Galois conjugate of α (see [2, Lemmas 2.2 and 2.3]). We assume $\alpha \notin \mathbb{Z}$, $\alpha^2 - 4 \notin \mathbb{Z}^2$, $d_2 \in 5\mathbb{Q}^2$ and $\alpha^2 - 4 > 0$. The assumptions $\alpha \notin \mathbb{Z}$ and $\alpha^2 - 4 \notin \mathbb{Z}^2$ imply that the polynomial $f(X)$ is \mathbb{Q} -irreducible, and we have $\text{Gal}(L/\mathbb{Q}) \simeq C_4$ from $d_2 \in 5\mathbb{Q}^2$ (see [2, Proposition 2.1]). Furthermore, we have $\varepsilon, \eta \in \mathbb{R}$ by the assumption $\alpha^2 - 4 > 0$, $d_2 > 0$ and the factorization

$$f(X) = (X^2 - \alpha X + 1)(X^2 - \bar{\alpha} X + 1) = (X - \varepsilon)(X - \varepsilon^{-1})(X - \eta)(X - \eta^{-1}) \quad (2.2)$$

(see [2, Lemma 2.7]). Set $\tilde{L} = L(\zeta_5)$ where ζ_5 is a primitive fifth root of unity. Since $\text{Gal}(\tilde{L}/\mathbb{Q}) \supset \text{Gal}(\tilde{L}/k) \simeq C_2 \times C_2$ and $\text{Gal}(\tilde{L}/\mathbb{Q})/\text{Gal}(\tilde{L}/\mathbb{Q}(\zeta_5)) \simeq \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq C_4$, we have $\text{Gal}(\tilde{L}/\mathbb{Q}) \simeq C_2 \times C_4$. Therefore, $\text{Gal}(\tilde{L}/\mathbb{Q})$ has three subgroups of order 4. One of them is isomorphic to $C_2 \times C_2$ that corresponds to the subfield k , the others are isomorphic to C_4 . Let us denote them by $\langle \tau \rangle$ ($\simeq C_4$) and $\langle \tau' \rangle$ ($\simeq C_4$) for some automorphisms $\tau, \tau' \in \text{Gal}(\tilde{L}/\mathbb{Q})$ of order 4. Note that $\zeta_5^\tau \neq \zeta_5, \zeta_5^4$, because τ acts trivial

on $k = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$ if $\zeta_5^\tau = \zeta_5$ or ζ_5^4 . Likewise, we have $\zeta_5^{\tau'} \neq \zeta_5, \zeta_5^4$. We may assume that $\zeta_5^\tau = \zeta_5^2$ and $\zeta_5^{\tau'} = \zeta_5^2$.

Lemma 1. *The actions of τ and τ' on the roots $\varepsilon, \varepsilon^{-1}, \eta$ and η^{-1} of $f(X)$ are as follows:*

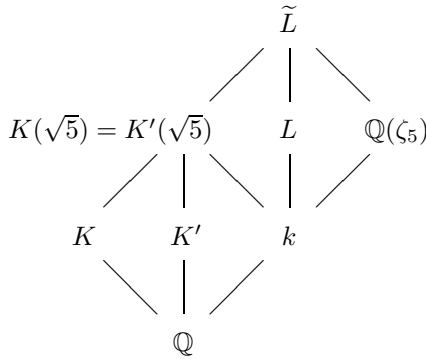
$$\begin{aligned} \tau &: \varepsilon \mapsto \eta \mapsto \varepsilon^{-1} \mapsto \eta^{-1} \mapsto \varepsilon \\ \tau' &: \varepsilon \mapsto \eta^{-1} \mapsto \varepsilon^{-1} \mapsto \eta \mapsto \varepsilon \end{aligned}$$

Proof. If $\varepsilon^\tau = \varepsilon^{-1}$, then we have $\alpha^\tau = (\varepsilon + \varepsilon^{-1})^\tau = \alpha$. This is a contradiction since the restriction of τ to L is a generator of $\text{Gal}(L/\mathbb{Q}) (\simeq C_4)$. Therefore, we have $\varepsilon^\tau \neq \varepsilon^{-1}$, and hence $\varepsilon^\tau = \eta$ or η^{-1} . Similarly we have $\varepsilon^{\tau'} = \eta$ or η^{-1} . Without loss of generality, we can assume that $\varepsilon^\tau = \eta$ and $\varepsilon^{\tau'} = \eta^{-1}$. Next, we will prove $\eta^\tau = \varepsilon^{-1}$. We get $\eta^\tau \neq \eta^{-1}$ by the same argument as the proof of $\varepsilon^\tau \neq \varepsilon^{-1}$. If $\eta^\tau = \varepsilon$, then we have $(\varepsilon + \eta)^\tau = \varepsilon + \eta$, $(\varepsilon\eta)^\tau = \varepsilon\eta$, $(\varepsilon^{-1} + \eta^{-1})^\tau = \varepsilon^{-1} + \eta^{-1}$, $(\varepsilon^{-1}\eta^{-1})^\tau = \varepsilon^{-1}\eta^{-1}$, and hence $\varepsilon + \eta, \varepsilon\eta, \varepsilon^{-1} + \eta^{-1}, \varepsilon^{-1}\eta^{-1} \in \mathbb{Q}$. Noting (2.2), therefore, $f(X)$ is factored in $\mathbb{Q}[X]$ as

$$f(X) = (X^2 - (\varepsilon + \eta)X + \varepsilon\eta)(X^2 - (\varepsilon^{-1} + \eta^{-1})X + \varepsilon^{-1}\eta^{-1}).$$

However, this contradicts the assumption that $f(X)$ is irreducible over \mathbb{Q} . We conclude $\eta^\tau \neq \varepsilon$ and hence $\eta^\tau = \varepsilon^{-1}$. Similarly we can get $(\eta^{-1})^{\tau'} = \varepsilon^{-1}$. The proof is complete. \square

Let K and K' denote the subfields of \tilde{L} correspond to $\langle \tau \rangle$ and $\langle \tau' \rangle$, respectively.



Lemma 2. *We have*

$$\begin{aligned} (\varepsilon - \varepsilon^{-1})(\eta - \eta^{-1}) &= \begin{cases} \sqrt{d_2} & \text{if } N > 0, \\ -\sqrt{d_2} & \text{if } N < 0, \end{cases} \\ \varepsilon\eta + \varepsilon^{-1}\eta^{-1} &= \begin{cases} \frac{N + \sqrt{d_2}}{2} & \text{if } N > 0, \\ \frac{N - \sqrt{d_2}}{2} & \text{if } N < 0 \end{cases} \quad \text{and} \quad \varepsilon\eta^{-1} + \varepsilon^{-1}\eta = \begin{cases} \frac{N - \sqrt{d_2}}{2} & \text{if } N > 0, \\ \frac{N + \sqrt{d_2}}{2} & \text{if } N < 0. \end{cases} \end{aligned}$$

Proof. Put $\lambda := (\varepsilon - \varepsilon^{-1})(\eta - \eta^{-1})$. By using $N = \alpha\bar{\alpha} = (\varepsilon + \varepsilon^{-1})(\eta + \eta^{-1})$, we have $\varepsilon\eta + \varepsilon^{-1}\eta^{-1} = (N + \lambda)/2$ and $\varepsilon\eta^{-1} + \varepsilon^{-1}\eta = (N - \lambda)/2$. By direct calculation, we get $\lambda^2 = d_2$. Recall that $\varepsilon, \eta \in \mathbb{R}$. Since $\alpha = \varepsilon + \varepsilon^{-1}$ (resp. $\bar{\alpha} = \eta + \eta^{-1}$) is positive if and only if ε (resp. η) is positive, and $|\varepsilon| \geq |\varepsilon^{-1}|$ and $|\eta| \geq |\eta^{-1}|$, we have

$$N = \alpha\bar{\alpha} > 0 \iff \varepsilon\eta > 0 \iff \lambda = (\varepsilon - \varepsilon^{-1})(\eta - \eta^{-1}) > 0.$$

The proof is complete. \square

Lemma 3. *Let i, j be integers which are not divisible by 5. If $\varepsilon^i\eta^j \in L^5$, then we have $\varepsilon, \eta \in L^5$.*

Proof. We put $\text{Gal}(\tilde{L}/k) \simeq \langle \sigma \rangle \times \langle \sigma' \rangle \simeq C_2 \times C_2$, where $\varepsilon^\sigma = \varepsilon^{-1}$, $\eta^\sigma = \eta$, $\varepsilon^{\sigma'} = \varepsilon$ and $\eta^{\sigma'} = \eta^{-1}$. If $\varepsilon^i\eta^j \in L^5$, then so are $(\varepsilon^i\eta^j)^\sigma = \varepsilon^{-i}\eta^j$, their ratio ε^{2i} and their product η^{2j} . Since $\gcd(2i, 5) = \gcd(2j, 5) = 1$, we conclude that both ε and η are fifth powers in L . \square

3. Fibonacci and Lucas sequences

Let (F_n) and (L_n) be the Fibonacci and Lucas sequences, respectively, defined by $F_1 = 1, F_2 = 1, F_{n+2} = F_{n+1} + F_n$ ($n \in \mathbb{Z}$) and $L_1 = 1, L_2 = 3, L_{n+2} = L_{n+1} + L_n$ ($n \in \mathbb{Z}$). Assertions (1) and (2) in the following lemma follow from the explicit formulae for

$$F_n = \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}} \quad \text{and} \quad L_n = \omega^n + \bar{\omega}^n,$$

where $\omega = (1 + \sqrt{5})/2$ and $\bar{\omega} = (1 - \sqrt{5})/2$. We can prove (3) by direct calculation.

Lemma 4. *For any $n \in \mathbb{Z}$, we have the following.*

- (1) $L_n^2 = 5F_n^2 + (-1)^n 4$.
- (2) $5F_{2n-1} + L_{2n-1} + (-1)^n 4 = 2L_n^2$ and $5F_{2n-1} + L_{2n-1} - (-1)^n 4 = 10F_n^2$.
- (3) $(F_n) \bmod 5^3$ is 500-periodic and $F_n \equiv 2 \pmod{5^3}$ if $n \equiv \pm 3 \pmod{500}$.

From now on, we assume that n (> 3) is an odd integer and consider the polynomial (2.1) for $\alpha = (L_n + (F_n - 2)\sqrt{5})/2$. By (2.1) and Lemma 4 (1), we get

$$f(X) = f_\alpha(X) = X^4 - L_n X^3 + (5F_n - 4)X^2 - L_n X + 1,$$

and all four roots of $f(X)$ are given by $\varepsilon, \varepsilon^{-1}, \eta, \eta^{-1}$ which satisfy $\alpha = \varepsilon + \varepsilon^{-1}$, $\bar{\alpha} = \eta + \eta^{-1}$. Moreover, we see from $d_1 = T^2 - 4N = 5(F_n - 2)^2$ and $d_2 = (N + 4)^2 - 4T^2 = 5(F_n - 2)^2$ that the discriminant of $f(X)$ is $\text{disc}(f) = d_1^2 d_2 = 5^3 (F_n - 2)^6$. Furthermore, since $\alpha \notin \mathbb{Z}$, $\alpha^2 - 4 \notin \mathbb{Z}^2$, $d_2 \in 5\mathbb{Q}^2$ and $\alpha^2 - 4 > 0$, the polynomial $f(X)$ is

\mathbb{Q} -irreducible, all the roots $\varepsilon, \varepsilon^{-1}, \eta, \eta^{-1}$ are real, and $\text{Gal}(L/\mathbb{Q}) \simeq C_4$ (see §2). Next, we will prove that the three quadratic fields contained in \tilde{L} are $\mathbb{Q}(\sqrt{2-F_n})$, $\mathbb{Q}(\sqrt{5(2-F_n)})$ and $k = \mathbb{Q}(\sqrt{5})$.

Lemma 5. Put $\alpha = (L_n + (F_n - 2)\sqrt{5})/2$ for an odd integer $n > 3$ and $\zeta = \zeta_5$. For the roots ε, η of $f_\alpha(X)$, we have the following.

- (1) $\xi_1 := (\varepsilon + \varepsilon^{-1})(\zeta + \zeta^{-1}) + (\eta + \eta^{-1})(\zeta^2 + \zeta^{-2}) = \{-L_n + 5(F_n - 2)\}/2$.
- (2) $\xi_2 := (\varepsilon - \varepsilon^{-1})^2(\zeta - \zeta^{-1})^2 + (\eta - \eta^{-1})^2(\zeta^2 - \zeta^{-2})^2 = -5(F_n - 2)(5F_n + L_n)/2$.
- (3) $\xi_3 := (\varepsilon - \varepsilon^{-1})(\eta - \eta^{-1})(\zeta - \zeta^{-1})(\zeta^2 - \zeta^{-2}) = -5(F_n - 2)$.

Proof. Set $c = \zeta + \zeta^{-1} = (-1 + \sqrt{5})/2$. Noting that $\alpha = \varepsilon + \varepsilon^{-1}$ and $\bar{\alpha} = \eta + \eta^{-1}$, we have $\xi_1 = \alpha c + \bar{\alpha}(c^2 - 2)$ and $\xi_2 = (\alpha^2 - 4)(c^2 - 4) + (\bar{\alpha}^2 - 4)(c - 2)$. The assertions (1) and (2) follow by using Lemma 4 (1). From Lemma 2 and $N > 0$, we have $(\varepsilon - \varepsilon^{-1})(\eta - \eta^{-1}) = \sqrt{d_2} = (F_n - 2)\sqrt{5}$. On the other hand, we have $(\zeta - \zeta^{-1})(\zeta^2 - \zeta^{-2}) = c^3 - 4c = -\sqrt{5}$. Hence we get the assertion (3). \square

Lemma 6. Under the same situation as in Lemma 5, we have the following.

- (1) $\text{Tr}_{\tilde{L}/K}(\varepsilon\zeta) = \{-L_n + 5(F_n - 2) + 2\xi\}/4$, where $\xi := (\varepsilon - \varepsilon^{-1})(\zeta - \zeta^{-1}) + (\eta - \eta^{-1})(\zeta^2 - \zeta^{-2})$ is such that

$$\xi^2 = \begin{cases} -5^2(F_n - 2)F_{\frac{n+1}{2}}^2 & \text{if } n \equiv 1 \pmod{4}, \\ -5(F_n - 2)L_{\frac{n+1}{2}}^2 & \text{if } n \equiv 3 \pmod{4}. \end{cases}$$

- (2) $\text{Tr}_{\tilde{L}/K'}(\varepsilon\zeta) = \{-L_n + 5(F_n - 2) + 2\xi'\}/4$, where $\xi' := (\varepsilon - \varepsilon^{-1})(\zeta - \zeta^{-1}) - (\eta - \eta^{-1})(\zeta^2 - \zeta^{-2})$ is such that

$$\xi'^2 = \begin{cases} -5(F_n - 2)L_{\frac{n+1}{2}}^2 & \text{if } n \equiv 1 \pmod{4}, \\ -5^2(F_n - 2)F_{\frac{n+1}{2}}^2 & \text{if } n \equiv 3 \pmod{4}. \end{cases}$$

Proof. We prove only the assertion (1). By Lemma 1, we have

$$\gamma := \text{Tr}_{\tilde{L}/K}(\varepsilon\zeta) = \varepsilon\zeta + \eta\zeta^2 + \varepsilon^{-1}\zeta^{-1} + \eta^{-1}\zeta^{-2}$$

and

$$\gamma^{\tau'} = \eta^{-1}\zeta^2 + \varepsilon\zeta^{-1} + \eta\zeta^{-2} + \varepsilon^{-1}\zeta.$$

Now $\gamma = \{(\gamma + \gamma^{\tau'}) + (\gamma - \gamma^{\tau'})\}/2$ with

$$\gamma + \gamma^{\tau'} = \xi_1 = \frac{-L_n + 5(F_n - 2)}{2}$$

and

$$\begin{aligned} (\gamma - \gamma^{\tau'})^2 &= \{(\varepsilon - \varepsilon^{-1})(\zeta - \zeta^{-1}) + (\eta - \eta^{-1})(\zeta^2 - \zeta^{-2})\}^2 \\ &= \xi_2 + 2\xi_3 = -\frac{5(F_n - 2)(5F_n + L_n + 4)}{2} \end{aligned}$$

by Lemma 5. Therefore, we get the desired result, by Lemma 4 (2). \square

By Lemma 6, we get the following proposition immediately.

Proposition 1. *We have*

$$(K, K') = \begin{cases} (\mathbb{Q}(\sqrt{2 - F_n}), \mathbb{Q}(\sqrt{5(2 - F_n)})) & \text{if } n \equiv 1 \pmod{4}, \\ (\mathbb{Q}(\sqrt{5(2 - F_n)}), \mathbb{Q}(\sqrt{2 - F_n})) & \text{if } n \equiv 3 \pmod{4}. \end{cases}$$

4. Certain parametric quintic polynomial

For an element $\gamma \in L$, we define

$$\begin{aligned} g_{\gamma, \tau}(X) &:= X^5 - 10N_L(\gamma)X^3 - 5N_L(\gamma)N_k\mathrm{Tr}_{L/k}(\gamma)X^2 \\ &\quad + 5N_L(\gamma)\{N_L(\gamma) - N_k\mathrm{Tr}_{L/k}(\gamma^{1+\tau})\}X - N_L(\gamma)N_k\mathrm{Tr}_{L/k}(\gamma^{2+\tau}) \in \mathbb{Q}[X], \\ g_{\gamma, \tau'}(X) &:= X^5 - 10N_L(\gamma)X^3 - 5N_L(\gamma)N_k\mathrm{Tr}_{L/k}(\gamma)X^2 \\ &\quad + 5N_L(\gamma)\{N_L(\gamma) - N_k\mathrm{Tr}_{L/k}(\gamma^{1+\tau'})\}X - N_L(\gamma)N_k\mathrm{Tr}_{L/k}(\gamma^{2+\tau'}) \in \mathbb{Q}[X]. \end{aligned}$$

Define subsets \mathcal{M}_τ and $\mathcal{M}_{\tau'}$ of $\tilde{L} = L(\zeta_5)$ by

$$\begin{aligned} \mathcal{M}_\tau &:= \{\gamma \in \tilde{L}^\times \mid \gamma^{3+4\tau+2\tau^2+\tau^3} \notin \tilde{L}^5\}, \\ \mathcal{M}_{\tau'} &:= \{\gamma \in \tilde{L}^\times \mid \gamma^{3+4\tau'+2\tau'^2+\tau'^3} \notin \tilde{L}^5\}. \end{aligned}$$

Proposition 2 ([8, Example 3.3], [4, Chapter 5, Examples (2), p. 253]). *Let the notation be as above. Assume $\gamma \in \mathcal{M}_\tau \cap L$ (resp. $\gamma \in \mathcal{M}_{\tau'} \cap L$). Then the minimal splitting field of $g_{\gamma, \tau}$ (resp. $g_{\gamma, \tau'}$) over \mathbb{Q} is a D_5 -extension containing K (resp. K').*

Recall $d_2 \in 5\mathbb{Q}^2$. Let t be the positive integer so that $d_2 = 5t^2$, and denote $\alpha = (T + b\sqrt{5})/2$ ($b \in \mathbb{Z}$). Now we calculate the coefficients of $g_{\gamma, \tau}(X)$ and $g_{\gamma, \tau'}(X)$ in the case $\gamma = \varepsilon, \eta$.

Lemma 7. For $\gamma = \varepsilon, \eta$, we have the following.

- (1) $N_L(\gamma) = 1$.
- (2) $N_k \text{Tr}_{L/k}(\gamma) = N$.
- (3) $N_k \text{Tr}_{L/k}(\gamma^{1+\tau}) = N_k \text{Tr}_{L/k}(\gamma^{1+\tau'}) = T^2 - 2N - 4$.
- (4) $N_k \text{Tr}_{L/k}(\gamma^{2+\tau}) = \begin{cases} \{N(T^2 - 2N) - 5btT\}/2 - 3N & \text{if } N > 0, \\ \{N(T^2 - 2N) + 5btT\}/2 - 3N & \text{if } N < 0, \end{cases}$
 $N_k \text{Tr}_{L/k}(\gamma^{2+\tau'}) = \begin{cases} \{N(T^2 - 2N) + 5btT\}/2 - 3N & \text{if } N > 0, \\ \{N(T^2 - 2N) - 5btT\}/2 - 3N & \text{if } N < 0. \end{cases}$

Proof. Let $\bar{\tau} = \tau|_L$ be the restriction of τ to L . Then $\bar{\tau}$ is a generator of the cyclic quartic Galois group $\text{Gal}(L/\mathbb{Q})$, and $\bar{\tau}^2$ is the generator of $\text{Gal}(L/k)$. We can show the assertions (1), (2) and (3) by these facts and $\alpha = \varepsilon + \varepsilon^{-1}$ and $\bar{\alpha} = \eta + \eta^{-1}$ are roots of $X^2 - TX + N$. Therefore, we will give a proof of the assertion (4) only for $N_k \text{Tr}_{L/k}(\varepsilon^{2+\tau})$ in the case $N > 0$ (we can prove the other assertions similarly). In this case, we see from Lemmas 1 and 2 that

$$\begin{aligned} N_k \text{Tr}_{L/k}(\varepsilon^{2+\tau}) &= N_k \text{Tr}_{L/k}(\varepsilon^2 \eta) = N_k(\varepsilon^2 \eta + \varepsilon^{-2} \eta^{-1}) \\ &= (\varepsilon^2 \eta + \varepsilon^{-2} \eta^{-1})(\eta^2 \varepsilon^{-1} + \eta^{-2} \varepsilon) \\ &= \bar{\alpha}^2(\varepsilon \eta + \varepsilon^{-1} \eta^{-1}) + \alpha^2(\varepsilon \eta^{-1} + \varepsilon^{-1} \eta) - 3N \\ &= \frac{N + \sqrt{d_2}}{2} \bar{\alpha}^2 + \frac{N - \sqrt{d_2}}{2} \alpha^2 - 3N \\ &= \frac{N}{2}(\alpha^2 + \bar{\alpha}^2) - \frac{t\sqrt{5}}{2}(\alpha^2 - \bar{\alpha}^2) - 3N. \end{aligned}$$

Since $\alpha - \bar{\alpha} = b\sqrt{5}$, we have $\alpha^2 + \bar{\alpha}^2 = T^2 - 2N$, $\alpha^2 - \bar{\alpha}^2 = bT\sqrt{5}$. Thus we get the assertion. \square

Lemma 8. Put $\alpha = (L_n + (F_n - 2)\sqrt{5})/2$ for an odd integer $n > 3$. For the roots $\gamma = \varepsilon, \eta$ of $f_\alpha(X)$, we have the following.

- (1) $N_L(\gamma) = 1$.
- (2) $N_k \text{Tr}_{L/k}(\gamma) = 5F_n - 6$.
- (3) $N_k \text{Tr}_{L/k}(\gamma^{1+\tau}) = N_k \text{Tr}_{L/k}(\gamma^{1+\tau'}) = 5F_n^2 - 10F_n + 4$.
- (4) $N_k \text{Tr}_{L/k}(\gamma^{2+\tau}) = 5(F_n - 2)\{(F_n - 2)(5F_n - L_n + 4) + 10\}/2 + 4$,
 $N_k \text{Tr}_{L/k}(\gamma^{2+\tau'}) = 5(F_n - 2)\{(F_n - 2)(5F_n + L_n + 4) + 10\}/2 + 4$.

Proof. The assertions (1), (2) and (3) follow from Lemma 7 and Lemma 4 (1). We will prove the assertion (4). Since $N = 5F_n - 6 > 0$, we have from Lemma 7 (4) and Lemma 4 (1) that

$$\begin{aligned} N_k \operatorname{Tr}_{L/k}(\gamma^{2+\tau}) &= \frac{1}{2} \{ (5F_n - 6)(L_n^2 - 10F_n + 12) - 5L_n(F_n - 2)^2 \} - 15F_n + 18 \\ &= \frac{1}{2} \{ (5F_n - 6)(5F_n^2 - 10F_n + 8) - 5L_n(F_n - 2)^2 - 30F_n + 28 \} + 4 \\ &= \frac{5(F_n - 2)}{2} \{ (F_n - 2)(5F_n - L_n + 4) + 10 \} + 4. \end{aligned}$$

We can prove the equality for $N_k \operatorname{Tr}_{L/k}(\gamma^{2+\tau'})$ similarly. \square

Lemma 9. Put $\alpha = (L_n + (F_n - 2)\sqrt{5})/2$ for an odd integer $n > 3$. If $n \not\equiv 0 \pmod{3}$, then for the roots $\gamma = \varepsilon, \eta$ of $f_\alpha(X)$ and for any integers i, j which are not divisible by 5, we have $\varepsilon^i \eta^j \notin L^5$.

Proof. For any $x \in L^5$, since $L \subset \mathbb{R}$, there exists only one $y \in L$ satisfying $x = y^5$, we denote it by $\sqrt[5]{x}$. Suppose to the contrary that $\varepsilon^i \eta^j \in L^5$. Then we have $\varepsilon, \eta \in L^5$ by Lemma 3. Recall that $\bar{\tau}^2$ is the generator of $\operatorname{Gal}(L/k)$, where $\bar{\tau} = \tau|_L$. For $y = \sqrt[5]{\varepsilon} \in L$, we have

$$(y^{\bar{\tau}^2})^5 = (y^5)^{\bar{\tau}^2} = \varepsilon^{\bar{\tau}^2} = \varepsilon^{-1}.$$

This equality yields $(\sqrt[5]{\varepsilon})^{\bar{\tau}^2} = \sqrt[5]{\varepsilon^{-1}}$. Therefore, we have

$$\beta := \operatorname{Tr}_{L/k}(\sqrt[5]{\varepsilon}) = \sqrt[5]{\varepsilon} + (\sqrt[5]{\varepsilon})^{\bar{\tau}^2} = \sqrt[5]{\varepsilon} + \sqrt[5]{\varepsilon^{-1}} \in k.$$

By direct calculation, we get $\beta^5 - 5\beta^3 + 5\beta = \varepsilon + \varepsilon^{-1} = \alpha = (L_n + (F_n - 2)\sqrt{5})/2$, and $h(\beta) = 0$, where

$$\begin{aligned} h(X) &:= \left(X^5 - 5X^3 + 5X - \frac{L_n}{2} \right)^2 - \frac{5(F_n - 2)^2}{4} \\ &= X^{10} - 10X^8 + 35X^6 - L_n X^5 - 50X^4 + 5L_n X^3 + 25X^2 - 5L_n X + 5F_n - 6. \end{aligned}$$

On the one hand, $h(X)$ is reducible over \mathbb{Q} because it has a root $\beta \in k = \mathbb{Q}(\sqrt{5})$. On the other hand, since

$$F_n \equiv L_n \equiv 1 \pmod{2} \quad \text{if } n \equiv 1, 2 \pmod{3}, \quad (4.1)$$

we have that

$$h(X) \equiv X^{10} + X^6 + X^5 + X^3 + X^2 + X + 1 \pmod{2}$$

is irreducible over \mathbb{F}_2 . Hence $h(X)$ is \mathbb{Q} -irreducible. Since we obtain a contradiction, the proof is complete. \square

5. Proof of our theorem

In this section, we will prove our main theorem in §1. The keys of the proof are Proposition 2 and the following proposition.

Proposition 3 ([17, Proposition 2]). *Let $p (\neq 2)$ and q be prime numbers. Suppose that the polynomial*

$$\varphi(X) = X^p + \sum_{j=0}^{p-2} a_j X^j, \quad a_j \in \mathbb{Z}$$

is irreducible over \mathbb{Q} and satisfies the condition

$$v_q(a_j) < p - j \quad \text{for some } j, 0 \leq j \leq p - 2. \quad (5.1)$$

Let θ be a root of $\varphi(X)$.

(1) *If q is different from p , then q is totally ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$ if and only if*

$$0 < \frac{v_q(a_0)}{p} \leq \frac{v_q(a_j)}{p - j} \quad \text{for every } j, 1 \leq j \leq p - 2.$$

(2) *If neither*

$$0 < \frac{v_p(a_0)}{p} \leq \frac{v_p(a_j)}{p - j} \quad \text{for every } j, 1 \leq j \leq p - 2 \quad (5.2)$$

nor

$$v_p(\varphi^{(j)}(-a_0)) < p - j \quad \text{for some } j, 0 \leq j \leq p - 1 \quad (5.3)$$

holds, then p is not totally ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$, where $\varphi^{(j)}(X)$ is the j -th differential of $\varphi(X)$.

Proof of Theorem. Let n be in \mathcal{N} . First, we will show $\varepsilon \in \mathcal{M}_\tau \cap L$ and $\varepsilon \in \mathcal{M}_{\tau'} \cap L$, where \mathcal{M}_τ and $\mathcal{M}_{\tau'}$ are defined in §4. By Lemma 1, we have

$$\varepsilon^{3+4\tau+2\tau^2+\tau^3} = \varepsilon^3 \eta^4 \varepsilon^{-2} \eta^{-1} = \varepsilon \eta^3. \quad (5.4)$$

If $\varepsilon \eta^3 \in \tilde{L}^5$, then we have $\varepsilon^2 \eta^6 = N_{\tilde{L}/L}(\varepsilon \eta^3) \in L^5$, which contradicts Lemma 9. Hence we have $\varepsilon \eta^3 \notin \tilde{L}^5$. From (5.4), therefore, we get $\varepsilon \in \mathcal{M}_\tau \cap L$. Similarly, we can see that

$$\varepsilon^{3+4\tau'+2\tau'^2+\tau'^3} = \varepsilon^3 \eta^{-4} \varepsilon^{-2} \eta = \varepsilon \eta^{-3} \notin \tilde{L}^5,$$

and so $\varepsilon \in \mathcal{M}_{\tau'} \cap L$. Let $g_{\varepsilon,\tau}(X)$ and $g_{\varepsilon,\tau'}(X)$ be the polynomials defined in §4. From Lemma 8, we have

$$\begin{aligned} g_{\varepsilon,\tau}(X) &= X^5 - 10X^3 - 5(5F_n - 6)X^2 - 5(5F_n^2 - 10F_n + 3)X \\ &\quad - \frac{5(F_n - 2)}{2} \{(F_n - 2)(5F_n - L_n + 4) + 10\} - 4, \\ g_{\varepsilon,\tau'}(X) &= X^5 - 10X^3 - 5(5F_n - 6)X^2 - 5(5F_n^2 - 10F_n + 3)X \\ &\quad - \frac{5(F_n - 2)}{2} \{(F_n - 2)(5F_n + L_n + 4) + 10\} - 4. \end{aligned}$$

By Proposition 2, the minimal splitting fields $\text{Spl}_{\mathbb{Q}}(g_{\varepsilon,\tau})$ of $g_{\varepsilon,\tau}(X)$ and $\text{Spl}_{\mathbb{Q}}(g_{\varepsilon,\tau'})$ of $g_{\varepsilon,\tau'}(X)$ are D_5 -extensions containing K and K' , respectively, and the quadratic fields K and K' are given by Proposition 1. Therefore, it is enough to prove that both C_5 -extensions $\text{Spl}_{\mathbb{Q}}(g_{\varepsilon,\tau})/K$ and $\text{Spl}_{\mathbb{Q}}(g_{\varepsilon,\tau'})/K'$ are unramified. We will prove only for $\text{Spl}_{\mathbb{Q}}(g_{\varepsilon,\tau})/K$ (we can prove similarly for $\text{Spl}_{\mathbb{Q}}(g_{\varepsilon,\tau'})/K'$).

Let θ be a root of $g_{\varepsilon,\tau}(X)$ and consider the quintic extension $\mathbb{Q}(\theta)/\mathbb{Q}$. For a prime number q , a prime ideal of K above q is ramified in $\text{Spl}_{\mathbb{Q}}(g_{\varepsilon,\tau})/K$ if and only if q is totally ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$ because $[\text{Spl}_{\mathbb{Q}}(g_{\varepsilon,\tau}) : K] = 5$ and $[K : \mathbb{Q}] = 2$. Hence we prove that no prime number q is totally ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$ by using Proposition 3. We denote the coefficient of X^j of $g_{\varepsilon,\tau}(X)$ by a_j . First, $g_{\varepsilon,\tau}(X)$ satisfies the condition (5.1) because $v_q(a_3) < 5 - 3 = 2$ for any prime number q . From Proposition 3 (1), we see that no prime $q \neq 5$ is totally ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$ since $v_q(a_3) = 0$ if $q \neq 2$ and $v_2(a_2) = 0$ by (4.1). We will show, therefore, that 5 is not totally ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$. Since $a_0 \equiv -4 \pmod{5}$ is not divisible by 5, (5.2) does not hold. Furthermore, by the assumption $n \equiv \pm 3 \pmod{500}$ and Lemma 4 (3), we have $F_n - 2 \equiv 0 \pmod{5^3}$, $-a_0 \equiv 4 \pmod{5^5}$, $5F_n - 6 = 5(F_n - 2) + 4 \equiv 4 \pmod{5^4}$, $5F_n^2 - 10F_n + 3 = 5F_n(F_n - 2) + 3 \equiv 3 \pmod{5^4}$, and hence

$$\begin{aligned} g_{\varepsilon,\tau}(-a_0) &\equiv 4^5 - 10 \cdot 4^3 - 5 \cdot 4 \cdot 4^2 - 5 \cdot 3 \cdot 4 - 4 \equiv 0 \pmod{5^5}, \\ g_{\varepsilon,\tau}^{(1)}(-a_0) &\equiv 5 \cdot 4^4 - 30 \cdot 4^2 - 10 \cdot 4 \cdot 4 - 5 \cdot 3 = 625 \equiv 0 \pmod{5^4}, \\ g_{\varepsilon,\tau}^{(2)}(-a_0) &\equiv 20 \cdot 4^3 - 60 \cdot 4 - 10 \cdot 4 = 1000 \equiv 0 \pmod{5^3}, \\ g_{\varepsilon,\tau}^{(3)}(-a_0) &\equiv 60 \cdot 4^2 - 60 = 900 \equiv 0 \pmod{5^2}, \\ g_{\varepsilon,\tau}^{(4)}(-a_0) &\equiv 120 \cdot 4 \equiv 0 \pmod{5}. \end{aligned}$$

Then (5.3) does not hold. Hence 5 is not totally ramified in $\mathbb{Q}(\theta)/\mathbb{Q}$.

Finally, we prove that the set $\{(\mathbb{Q}(\sqrt{2-F_n}), \mathbb{Q}(\sqrt{5(2-F_n)})) \mid n \in \mathcal{N}\}$ is infinite. For an integer m , let $s(m)$ denote the square free integer satisfying $m = s(m)A^2$ for some $A \in \mathbb{N}$, and assume that $\{(\mathbb{Q}(\sqrt{2-F_n}), \mathbb{Q}(\sqrt{5(2-F_n)})) \mid n \in \mathcal{N}\}$ is finite. Then the set $\{s(F_n - 2) \mid n \in \mathcal{N}\}$ is finite. Since \mathcal{N} is infinite, there exists $k \geq 1$ such that

$\mathcal{N}_k := \{n \in \mathcal{N} \mid s(F_n - 2) = k\}$ is infinite. For any integer $n \in \mathcal{N}_k$, let $F_n - 2 = kA_n^2$. Then by Lemma 4 (1), we have

$$L_n^2 = 5F_n^2 - 4 = 5(kA_n^2 + 2)^2 - 4 = 5k^2A_n^4 + 20kA_n^2 + 16.$$

This implies that infinitely many pairs (A_n, L_n) are integer solutions of the equation

$$Y^2 = 5k^2X^4 + 20kX^2 + 16.$$

However, the equation has only finitely many integer solutions by Siegel's theorem. This is a contradiction. Hence the proof is complete. \square

References

- [1] N.C. Ankeny, S. Chowla, On the divisibility of the class number of quadratic fields, *Pacific J. Math.* 5 (1955) 321–324.
- [2] M. Aoki, Y. Kishi, On systems of fundamental units of certain quadratic fields, *Int. J. Number Theory* 11 (2015) 2019–2035.
- [3] D. Byeon, Real quadratic fields with class number divisible by 5 or 7, *Manuscripta Math.* 120 (2006) 211–215.
- [4] H. Cohen, *Advanced Topics in Computational Number Theory*, GTM, vol. 193, Springer-Verlag, New York, 2000.
- [5] B.H. Gross, D.E. Rohrlich, Some results on the Mordell–Weil group of the Jacobian of the Fermat curve, *Invent. Math.* 44 (1978) 201–224.
- [6] H. Ichimura, Note on the class numbers of certain real quadratic fields, *Abh. Math. Semin. Univ. Hambg.* 73 (2003) 281–288.
- [7] Y. Iizuka, Y. Konomi, 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.
- [8] M. Imaoka, Y. Kishi, On dihedral extensions and Frobenius extensions, in: *Galois Theory and Modular Forms*, in: *Dev. Math.*, vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 195–220.
- [9] A. Ito, Existence of an infinite family of pairs of quadratic fields $\mathbb{Q}(\sqrt{m_1D})$ and $\mathbb{Q}(\sqrt{m_2D})$ whose class numbers are both divisible by 3 or both indivisible by 3, *Funct. Approx. Comment. Math.* 49 (2013) 111–135.
- [10] Y. Kishi, A new family of imaginary quadratic fields whose class number is divisible by five, *J. Number Theory* 128 (2008) 2450–2458.
- [11] 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.
- [12] 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.
- [13] S.R. Louboutin, On the divisibility of the class number of imaginary quadratic number fields, *Proc. Amer. Math. Soc.* 137 (2009) 4025–4028.
- [14] J.-F. Mestre, Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, *J. Reine Angew. Math.* 343 (1983) 23–35.
- [15] T. Nagell, Über die Klassenzahl imaginär-quadratischer Zahlkörper, *Abh. Math. Semin. Univ. Hambg.* 1 (1922) 140–150.
- [16] C.J. Parry, On the class number of relative quadratic fields, *Math. Comp.* 32 (1978) 1261–1270.
- [17] M. Sase, On a family of quadratic fields whose class numbers are divisible by five, *Proc. Japan Acad. Ser. A Math. Sci.* 74 (1998) 120–123.
- [18] P.J. Weinberger, Real quadratic fields with class numbers divisible by n , *J. Number Theory* 5 (1973) 237–241.
- [19] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, *Osaka J. Math.* 7 (1970) 57–76.