A family of pairs of imaginary cyclic fields of degree \((p - 1)/2\) with both class numbers divisible by \(p\)

Miho Aoki · Yasuhiro Kishi

Received: date / Accepted: date

Abstract Let \(p\) be a prime number with \(p \equiv 5 \pmod{8}\). We construct a new infinite family of pairs of imaginary cyclic fields of degree \((p - 1)/2\) with both class numbers divisible by \(p\). Let \(k_0\) be the unique subfield of \(\mathbb{Q}(\zeta_p)\) of degree \((p - 1)/4\) and \(u_p = (t + b\sqrt{p})/2 > 1\) be the fundamental unit of \(k := \mathbb{Q}(\sqrt{p})\). We put \(D_{m,n} := \mathcal{L}_m(2F_m - F_n \mathcal{L}_m)\) for integers \(m\) and \(n\), where \(\{F_n\}\) and \(\{L_n\}\) are linear recurrence sequences of degree two associated to the characteristic polynomial \(P(X) = X^2 - tX - 1\). We assume that there exists a pair \((m_0, n_0)\) of integers satisfying certain congruence relations. Then we show that there exists a positive integer \(N_q\) which satisfies the both class numbers of \(k_0(\sqrt{D_{m,n}})\) and \(\mathbb{Q}(\sqrt{pD_{m,n}})\) are divisible by \(p\) for any pairs \((m, n)\) with \(m \equiv m_0 \pmod{N_q}\), \(n \equiv n_0 \pmod{N_q}\) and \(n > 3\). Furthermore, we show that if we assume that ERH holds, then there exists the pair \((m_0, n_0)\).

Keywords Class numbers · Abelian number fields · Fundamental units · Gauss sums · Jacobi sums · Linear recurrence sequences

Mathematics Subject Classification (2010) MSC 11R11 · 11R16 · 11R29

1 Introduction

Let \(N\) be a natural number. Some infinite families of pairs of quadratic fields like \(\mathbb{Q}(\sqrt{D})\) and \(\mathbb{Q}(\sqrt{mD})\) with class numbers divisible by \(N\) were given by Scholz [11] \((N = 3)\), Komatsu [7,8] \((N = 3, \text{arbitrary } N)\), and Iizuka, Konomi and Nakano [5] \((N = 3, 5, 7)\). In the previous paper [3], the authors constructed such an infinite family in the case \(N = 5\) explicitly by using the Fibonacci numbers \(F_n\).

**Theorem 1** ([3]) 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.

The purpose of this paper is to give this type of an explicit infinite family of pairs of imaginary cyclic fields of degree \((p - 1)/2\) with both class numbers divisible by \(p\) for any prime numbers \(p\) such that \(p \equiv 5 \pmod{8}\).

This work was supported by JSPS KAKENHI Grant Numbers JP26400015 and JP15K04779.

Miho Aoki
Department of Mathematics, Interdisciplinary Faculty of Science and Engineering, Shimane University, Matsue, Shimane, 690-8504, Japan
E-mail: aoki@riko.shimane-u.ac.jp

Yasuhiro Kishi
Department of Mathematics, Faculty of Education, Aichi University of Education, Kariya, Aichi, 448-8542, Japan
E-mail: ykishi@auecc.aichi-edu.ac.jp
Let \( p \) be a prime number with \( p \equiv 5 \pmod{8} \) and let \( \zeta := \zeta_p \) be a primitive \( p \)-th root of unity. Let \( \delta \) be a generator of \( \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \) and put \( \delta_0 := \delta^{(p-1)/4} \). Moreover, we put \( \omega_0 := \zeta + \zeta^{p_0} + \zeta^{3p_0} + \zeta^{5p_0} \). Then \( k_0 := \mathbb{Q}(\omega_0) \) is the unique subfield of \( \mathbb{Q}(\zeta) \) of degree \( (p-1)/4 \). Let \( u_p > 1 \) be the fundamental unit of \( k = \mathbb{Q}(\sqrt{p}) \) and denote

\[
    u_p = \frac{t + b \sqrt{p}}{2} \quad (t, b \in \mathbb{Z}, \ t, b > 0).
\]

We use the following general linear recurrence sequences instead of Fibonacci numbers. By using the trace \( t \) of \( u_p \), define two sequences \( \{F_n\}, \{L_n\} \) by

\[
    \begin{align*}
    F_0 &:= 0, \quad F_1 := 1, \quad F_{n+2} := tF_{n+1} + F_n \quad (n \in \mathbb{Z}), \\
    L_0 &:= 2, \quad L_1 := t, \quad L_{n+2} := tL_{n+1} + L_n \quad (n \in \mathbb{Z}).
    \end{align*}
\]

For integers \( m \) and \( n \) and a prime number \( q \) \((\neq p)\), we put

\[
    D_{m,n} := L_m(2F_m - F_nL_m)b,
\]

\[
    N_q := \begin{cases}
    \text{lcm}(p^2(p-1),q-1) & \text{if } \left(\frac{p}{q}\right) = 1, \\
    \text{lcm}(p^2(p-1),2(q+1)) & \text{if } \left(\frac{p}{q}\right) = -1.
    \end{cases}
\]

When \( m \) and \( n \) are odd and \( n > 3 \), \( D_{m,n} \) is negative since \( F_{-m} = (-1)^{m+1}F_m \) and \( L_{-m} = (-1)^mL_m \).

In this paper, we first prove that if there exists a pair \((m_0, n_0)\) of integers and a prime number \( q \) satisfying certain congruence relations (Main Theorem (i), (ii)), then the class numbers of both cyclotomic fields \( k \) of degree \( (p-1)/2 \) are divisible by \( p \). Moreover, there are some examples in which the class numbers of both \( k_0(\sqrt{D_{m,n}}) \) and \( k_0(\sqrt{pD_{m,n}}) \) are both imaginary and their maximal real subfields are both \( k_0 = \mathbb{Q}(\omega_0) \). It is expected that the class number of \( k_0 \) is divisible by \( p \) (Vander's conjecture). Moreover, there are some examples in which the class numbers of both \( k_0(\sqrt{D_{m,n}}) \) and \( k_0(\sqrt{pD_{m,n}}) \) are both divisible by \( p \), but that of neither \( \mathbb{Q}(\sqrt{D_{m,n}}) \) nor \( \mathbb{Q}(\sqrt{pD_{m,n}}) \) is divisible by \( p \) (see Remark (i) in (2)).

2 Main Theorems

Let \( p \) be a prime number with \( p \equiv 5 \pmod{8} \) and \( \{F_n\}, \{L_n\} \) be the recurrence sequences defined in (1). For integers \( m, n \) and a prime number \( q \) \((\neq p)\), we put

\[
    \alpha = \alpha(m,n) := \frac{L_nL_m + (L_mF_n - 2F_m)b\sqrt{p}}{2},
\]

\[
    f_\alpha(X) := X^4 - TX^3 + (N + 2)X^2 - TX + 1,
\]

\[
    f_{\alpha,q}(X) := f_\alpha \mod q \in \mathbb{F}_q[X],
\]

where \( N := N_{k/\mathbb{Q}}(\alpha), \ T := \text{Tr}_{k/\mathbb{Q}}(\alpha) \).

**Main Theorem 1** We assume that there exist integers \( m_0, n_0 \) with \( m_0 \equiv n_0 \equiv 1 \pmod{2} \) and a prime number \( q \) such that

(i) \( (L_{m_0}F_{n_0} - 2F_{m_0})b \equiv 0 \pmod{p^2} \),

(ii) \( q \nmid 2bp \) and \( f_{\alpha,q}(a) = 0 \) for some \( i \in \{1, 2, 4\} \) and \( a \in \mathbb{F}_q \setminus \mathbb{F}^p_q \), where \( \alpha := \alpha(m_0, n_0) \).
Then for any pairs
\[(m,n) \in \mathcal{N} := \{(m,n) \in \mathbb{Z}^2 \mid m \equiv m_0 \pmod{N_q}, \ n \equiv n_0 \pmod{N_q}, \ n > 3\},\]
the class numbers of both imaginary cyclic fields \(k_0(\sqrt{D_{m,n}})\) and \(k_0(\sqrt{pD_{m,n}})\) of degree \((p-1)/2\) are divisible by \(p\). Moreover, the set of pairs
\[\{(k_0(\sqrt{D_{m,n}}), k_0(\sqrt{pD_{m,n}})) \mid (m,n) \in \mathcal{N}\}\]
is infinite.

Remark 1 (1) Let \(p = 13\). Then \(t = 3\), \(b = 1\), and \((q,m_0,n_0) = (53,15,55)\) satisfies the conditions (i), (ii) of Main Theorem 1, and hence the class numbers of both \(k_0(\sqrt{D_{m_0,n_0}})\) and \(k_0(\sqrt{pD_{m_0,n_0}})\) are divisible by \(p\). In this case, the class numbers of \(\mathbb{Q}(\sqrt{D_{m_0,n_0}})\) and \(\mathbb{Q}(\sqrt{pD_{m_0,n_0}})\) are

\[7102491402551842304 = 2^9 \cdot 7 \cdot 1981721931515581\]
and

\[59331908185385308160 = 2^{12} \cdot 5 \cdot 2897065829364517,\]
respectively, and neither of them is divisible by \(p = 13\), where
\[D_{m_0,n_0} = -3529794987028264311196913270006746882588864\]
\[= -2^6 \cdot 3^2 \cdot 13^2 \cdot 61 \cdot 109 \cdot 131 \cdot 211 \cdot 1063 \cdot 2725164213221 \cdot 681089630669633.\]

As for how to find \((q,m_0,n_0)\), see Example 1 (2) in §8.

(2) Main Theorem 1 implies the previous theorem (Theorem 1 in §8). For the details, see Example 2 in §8.

Main Theorem 2 Assume that ERH holds. Then there exist the integers \(m_0,n_0\) and the prime number \(q\) as in Main Theorem 1.

Remark 2 “ERH” means the extended Riemann hypothesis for \(k(\zeta_n, \sqrt[p]{\zeta})\) with every square free integers \(n > 0\).

3 The framework
Let \(p\) be a prime with \(p \equiv 5 \pmod{8}\) and put \(k := \mathbb{Q}(\sqrt{p})\). Let \(\alpha \in \mathcal{O}_k \setminus \mathbb{Z}\) with \(\alpha^2 - 4 \not\in \mathbb{Z}\). Define the polynomial \(f_\alpha(X)\) by
\[f_\alpha(X) := X^4 - TX^3 + (N + 2)X^2 - TX + 1,\]
where \(N := N_{k/\mathbb{Q}}(\alpha)\), \(T := \text{Tr}_{k/\mathbb{Q}}(\alpha)\). From the assumptions \(\alpha \in \mathcal{O}_k \setminus \mathbb{Z}\) and \(\alpha^2 - 4 \not\in \mathbb{Z}\), \(f_\alpha(X)\) is irreducible over \(\mathbb{Q}\) (cf. [2] Proposition 2.1(1))). Let \(L\) be the splitting field of \(f_\alpha(X)\) over \(\mathbb{Q}\). We can easily verify that \(T^2 - 4N > 0\). Hence if
\[\alpha^2 - 4 > 0 \quad \text{and} \quad (N + 4)^2 - 4T^2 \in p\mathbb{Q}\]
hold, then \(L\) is a real cyclic quartic field with \(k \subset L\) (cf. [2] Proposition 2.1 (2), Lemma 2.4)). Moreover \(L\) is not contained in \(\mathbb{Q}(\zeta_p + \zeta_p^{-1})\) since 4 \(\mid [\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = (p - 1)/2\), and hence \(L \not\subset \mathbb{Q}(\zeta_p)\). Put \(\zeta := \zeta_p, \ \omega := \zeta + \zeta^{-1}\) and \(\tilde{L} := L(\zeta)\). Since \(\text{Gal}(\tilde{L}/\mathbb{Q}) \simeq C_{p-1} \times C_2\), \(\tilde{L}\) has two quadratic subfields other than \(k\). We denote them by \(K\) and \(K'\). Then we see that \(\text{Gal}(\tilde{L}/K) \simeq \text{Gal}(\tilde{L}/K') \simeq C_{p-1}\). Let \(\tau\) and \(\tau'\) be a generator of \(\text{Gal}(\tilde{L}/K)\) and \(\text{Gal}(\tilde{L}/K')\), respectively, whose restrictions to \(\mathbb{Q}(\zeta)\) are the generator \(\delta\) of \(\mathbb{Q}(\zeta)/\mathbb{Q}\), and put \(\tau_0 := \tau\frac{\zeta + \zeta^{-1}}{2}, \ \tau'_0 := \tau'\frac{\zeta + \zeta^{-1}}{2}\). Then \(Q(\omega_0)\) is the unique subfield of \(\mathbb{Q}(\zeta)\) of degree \((p - 1)/4\), where
\[\omega_0 := \zeta + \zeta^2 + \zeta^3 - \zeta^4 = \zeta + \zeta^2 + \zeta^3 + \zeta^4.\]
Since \(\text{Gal}(K(\omega)/\mathbb{Q}(\omega_0)) \simeq C_2 \times C_2\), \(K(\omega)/\mathbb{Q}(\omega_0)\) has three proper subextensions \(\mathbb{Q}(\omega), K(\omega_0)\) and \(K'(\omega_0)\). Put \(K_0 := K(\omega_0)\) and \(K'_0 := K'(\omega_0)\). (See Figure 1.)
In the following, we will construct an unramified cyclic extension of $K_0$ of degree $p$. (We can do the same argument when $K_0$ is replaced by $K_0'$.) Let $\varepsilon, \varepsilon^{-1}, \eta, \eta^{-1}$ be the roots of $f_\alpha(X)$ with $\varepsilon + \varepsilon^{-1} = \alpha$, $\eta + \eta^{-1} = \alpha$ (cf. [2, Lemmas 2.2, 2.3]). Then we may assume that

\[ \tau : \varepsilon \mapsto \eta \mapsto \varepsilon^{-1} \mapsto \eta^{-1}, \]

\[ \tau' : \varepsilon \mapsto \eta^{-1} \mapsto \varepsilon^{-1} \mapsto \eta. \]

(cf. [3 Lemma 1]). Since $(p - 1)/4$ is odd, we may assume

\[ \tau_0 : \varepsilon \mapsto \eta \mapsto \varepsilon^{-1} \mapsto \eta^{-1}, \]

\[ \tau'_0 : \varepsilon \mapsto \eta^{-1} \mapsto \varepsilon^{-1} \mapsto \eta. \]

Here we may assume that

\[ \zeta^\tau = \zeta^t, \quad \zeta^{\tau'} = \zeta^t, \]

where $\iota$ is a primitive root modulo $p$. Setting $\iota_0 := \iota^{\frac{3}{4}p}$, we have

\[ \text{Gal}(K_0(\zeta)/K_0) = \langle \tau_0 \rangle, \quad \zeta^{\tau_0} = \zeta^{\iota_0}. \]

We define an element $t(K_0) \in \mathbb{Z}[\text{Gal}(K_0(\zeta)/K_0)]$ by

\[ t(K_0) := \iota_0^3 + \tau_0 \rho_0^2 + \tau_0^2 \rho_0 + \tau_0^3 \in \mathbb{Z}[\text{Gal}(K_0(\zeta)/K_0)], \]

and a subset $T(K_0)$ of $\mathbb{Z}[\text{Gal}(K_0(\zeta)/K_0)]$ by

\[ T(K_0) := \{ t'(K_0) \in \mathbb{Z}[\text{Gal}(K_0(\zeta)/K_0)] \mid 3n \in (\mathbb{Z}/p\mathbb{Z})^\times \text{ s.t. } t'(K_0) \equiv nt(K_0) \pmod{p} \}. \]

Moreover, we define a subset $\mathcal{M}_\tau$ of $\widetilde{L}^\times$ by

\[ \mathcal{M}_\tau := \{ \gamma \in \widetilde{L}^\times \mid \gamma^{t(K_0)} \notin \widetilde{L}^p \}. \]

**Proposition 1** For any $\gamma \in \mathcal{M}_\tau$ and $t'(K_0) \in T(K_0)$, $\widetilde{L}(\sqrt[p]{\gamma^{t'(K_0)}})/K_0$ is a cyclic extension of degree $4p$. 

---

**Fig. 1** A diagram of $\widetilde{L}/\mathbb{Q}$

\[ K_0(\zeta) = K_0'(\zeta) = L(\zeta) = \widetilde{L} \]

\[ K(\omega) = K'(\omega) \]

\[ K_0 \]

\[ k = \mathbb{Q}(\sqrt[p]{\alpha}) \]

\[ k_0 = \mathbb{Q}(\omega_0) \]

\[ k \]

\[ L \]

\[ K' \]

\[ L(\omega) \]

\[ Q(\omega) \]

\[ Q(\zeta) \]

\[ \mathbb{Q}(\zeta) \]

\[ \mathbb{Q}(\omega) \]

\[ \mathbb{Q} \]
Proof From a direct calculation, we have
\[(\tau_0 - \alpha)\ell(K_0) \equiv \tau_0 \ell(K_0) - \alpha \ell(K_0) = 1 - \ell_0^4 \equiv 0 \pmod p.\]
This implies \(\gamma^{*}(K_0)(\tau_0 - \alpha) \in \tilde{L}_p^p\). By [6, Proposition 1.1], therefore, \(\tilde{L}(\sqrt[p]{\gamma^{*}(K_0)})/K_0\) is a cyclic extension of degree 4p.

\[\square\]

**Remark 3** Let \(\gamma \in \mathcal{M}_p\). Then it follows from the definition of \(T(K_0)\) that
\[
\tilde{L}(\sqrt[p]{\gamma^{*}(K_0)}) = \tilde{L}(\sqrt[p]{\gamma^{*}(K_0)})
\]
for any \(\tau'(K_0) \in T(K_0)\).

Now assume
\[
\varepsilon \in \mathcal{M}_p
\]
and put \(\beta := \sqrt[p]{\varepsilon^{*}(K_0)}\). Then by Proposition [6], \(\tilde{L}(\beta)/K_0\) is a cyclic extension of degree 4p. Let \(E\) be the unique subextension of \(\tilde{L}(\beta)/K_0\) such that \(E/K_0\) is a cyclic extension of degree p. (See Figure 2.) Since \(\varepsilon\) is a unit, we see by Kummer theory that
\[
E/K_0 \text{ is unramified } \iff \tilde{L}(\beta)/K_0 \text{ is unramified}
\]
\[
\iff 3x \in \tilde{L}^* \text{ s.t. } x^p \equiv \varepsilon^{*}(K_0) \pmod {p(\zeta_p - 1)\mathcal{O}_L}
\]
(cf. [13, Exercise 9.3 (b)]). Thus, under the assumption
\[
3x \in \tilde{L}^* \text{ s.t. } x^p \equiv \varepsilon^{*}(K_0) \pmod {p(\zeta_p - 1)\mathcal{O}_L},\]
\(E/K_0\) is an unramified cyclic extension of degree p, and hence the class number of \(K_0\) is divisible by \(p\).

**Fig. 2** A diagram of \(\tilde{L}(\beta)/K_0\)

---

**Lemma 1** Assume that \((N + 4)^2 - 4T^2 \equiv 0 \pmod {p^5}\). Then there exists \(x \in \tilde{L}^*\) such that
\[
x^p \equiv \varepsilon^{*}(K_0) \pmod {p(\zeta_p - 1)\mathcal{O}_L},
\]
that is, \(\text{[A3]}\) holds.

**Proof** By \((N + 4)^2 - 4T^2 \equiv 0 \pmod {p^5}\) and \(p\mathcal{O}_{\tilde{L}} = (\zeta_p - 1)^{p-1}\mathcal{O}_{\tilde{L}}\), we have
\[
(\alpha^2 - 4)(\overline{\alpha}^2 - 4) = (N + 4)^2 - 4T^2 \equiv 0 \pmod {(\zeta_p - 1)^{5(p-1)/2}\mathcal{O}_{\tilde{L}}}.
\]
Hence we have
\[
\alpha^2 - 4 \equiv 0 \pmod {(\zeta_p - 1)^{5(p-1)/2}\mathcal{O}_{\tilde{L}}}
\]
or
\[
\overline{\alpha}^2 - 4 \equiv 0 \pmod {(\zeta_p - 1)^{5(p-1)/2}\mathcal{O}_{\tilde{L}}}.
\]
Since the ideal \((\zeta_p - 1)^{5(p-1)/2}O_L\) is invariant under the action of \(\text{Gal}(\tilde{L}/\mathbb{Q})\), we have
\[
\alpha^2 - 4 \equiv \beta^2 - 4 \equiv 0 \pmod{\langle \zeta_p - 1 \rangle^{5(p-1)/2}O_L},
\]
and hence,
\[
\varepsilon = \frac{\alpha + \sqrt{\alpha^2 - 4}}{2} \equiv \frac{\alpha}{2} \pmod{\langle \zeta_p - 1 \rangle^{5(p-1)/4}O_L}.
\]
By \(\tau_0 = \tau_{\frac{p-1}{2}}\), therefore, we have
\[
\varepsilon^{\tau_0} \equiv \frac{\alpha}{2} \pmod{\langle \zeta_p - 1 \rangle^{5(p-1)/4}O_L}.
\]

Now we have \(t_0^2 = t\frac{p-1}{p} \equiv -1 \pmod{p}\). Let us express \(t_0^2 = ps - 1\) for some \(s \in \mathbb{Z}\). Then by (3.2) and (3.3), we have
\[
\varepsilon^{t(K_0)} \equiv \left(\frac{\alpha}{2}\right)^{t_0^2 + \tau_0 + \tau_0}\equiv \left(\frac{\alpha}{2}\right)^{t_0} \cdot \left(\frac{\alpha}{2}\right)^{\frac{p-1}{2}} \cdot \frac{\alpha}{2}
\]
\[
= \left\{\left(\frac{\alpha}{2}\right)^{t_0} \cdot \frac{\alpha}{2}\right\}^{ps} \pmod{\langle \zeta_p - 1 \rangle^{5(p-1)/4}O_L}.
\]
Hence by
\[
\langle \zeta_p - 1 \rangle^{\frac{5(p-1)}{4}}O_L = p\langle \zeta_p - 1 \rangle^{\frac{5}{4}}O_L \subset p\langle \zeta_p - 1 \rangleO_L,
\]
we get the assertion. \(\square\)

In \([6]\) we will show that \(\alpha = \alpha(m,n)\) with \((m,n) \in \mathcal{N}\), which is defined in \(\S 2\), satisfies conditions \([A1], [A2]\) and \([A3]\).

### 4 The fundamental unit of \(\mathbb{Q}(\sqrt{p})\) and Lucas sequences

In this section, let \(p\) be a prime with \(p \equiv 1 \pmod{4}\). Then the norm of the fundamental unit
\[
u_p = \frac{t + b\sqrt{p}}{2} \quad (t, b \in \mathbb{Z}, \ t, b > 0)
\]
of \(\mathbb{Q}(\sqrt{p})\) is equal to \(-1\) (see, for example, \([11]\) p.279, Theorem 11.5.4, \([12]\) p.316, Exercise 5]). By using the trace \(t\) of \(\nu_p\), we define two sequences \(\{\mathcal{F}_n\}, \{\mathcal{L}_n\}\) by \([11]\). The sequences \(\{\mathcal{F}_n\}\) and \(\{\mathcal{L}_n\}\) are called the Lucas sequence and the companion Lucas sequence, respectively, associated to the characteristic polynomial \(P(X) = X^2 - tX - 1\), which are known to satisfy the following properties:
\[
\mathcal{F}_n = \frac{u_p^n - \overline{u}_p^n}{u_p - \overline{u}_p}, \quad \mathcal{L}_n = u_p^n + \overline{u}_p^n, \quad (4.1)
\]
\[
\mathcal{L}_n^2 - b^2p\mathcal{F}_n^2 = (-1)^n 4, \quad (4.2)
\]
\[
\mathcal{F}_{n+m} = \mathcal{F}_n\mathcal{F}_{m+1} + \mathcal{F}_{n-1}\mathcal{F}_m, \quad (4.3)
\]
\[
\mathcal{L}_{n+m} = (-1)^n \mathcal{L}_{n-m} = b^2p\mathcal{F}_n\mathcal{F}_m, \quad (4.4)
\]
where \(\overline{u}_p\) denotes the Galois conjugate of \(u_p\) (see, for example, \([10]\) Chap. 2, IV]).

**Lemma 2** For any integer \(n \in \mathbb{Z}\), we have the following:
1. \(\mathcal{F}_{2n+1} = \mathcal{F}_{n+1}^2 + \mathcal{F}_n^2\).
2. \(\mathcal{F}_n^2 - \mathcal{F}_{n+1}^2 = (-t\mathcal{L}_{2n+1} - 4(-1)^n)/b^2p\).
3. \(\mathcal{F}_n\mathcal{F}_{n+1} = (\mathcal{L}_{2n+1} - (-1)^n t)/b^2p\).
Proof (1) The assertion follows from (4.3) immediately.

(2) From (4.4), we get

\[ L_{2n} - (-1)^n L_0 = b^2 p F_n^2, \]
\[ L_{2n+2} - (-1)^{n+1} L_0 = b^2 p F_{n+1}^2, \]

and so

\[ L_{2n} - L_{2n+2} - \{(-1)^n - (-1)^{n+1}\} L_0 = b^2 p (F_n^2 - F_{n+1}^2). \]

Since \( L_0 = 2 \) and \( L_{2n+2} = t L_{2n+1} + L_2n \), we obtain

\[-t L_{2n+1} - 4(-1)^n = b^2 p (F_n^2 - F_{n+1}^2).\]

(3) From (4.4) and \( L_1 = t \), we get

\[ L_{2n+1} - (-1)^n t = b^2 p F_{n+1} F_n \]
as desired. \( \Box \)

**Lemma 3** The period of \( \{F_n\} \mod p^2 \) (resp. \( \{L_n\} \mod p^2 \)) divides \( p^2 (p - 1) \) (resp. \( p(p - 1) \)).

**Proof** For any integer \( n \geq 4 \), we have

\[ u_p^n = 2^{-n} (t + b \sqrt{p})^n \]
\[ \equiv 2^{-n} \left( t^n + \binom{n}{1} t^{n-1} b \sqrt{p} + \binom{n}{2} t^{n-2} b^2 p + \binom{n}{3} t^{n-3} b^3 p \sqrt{p} + \binom{n}{4} t^{n-4} b^4 p^2 \right), \]

\[ \overline{u}_p^n = 2^{-n} (t - b \sqrt{p})^n \]
\[ \equiv 2^{-n} \left( t^n - \binom{n}{1} t^{n-1} b \sqrt{p} + \binom{n}{2} t^{n-2} b^2 p - \binom{n}{3} t^{n-3} b^3 p \sqrt{p} + \binom{n}{4} t^{n-4} b^4 p^2 \right) \]
(mod \( bp^2 \sqrt{p} \mathcal{O}_k \)),

and hence

\[ u_p^n - \overline{u}_p^n \equiv 2^{-n+1} \left( \binom{n}{1} t^{n-1} b \sqrt{p} + \binom{n}{3} t^{n-3} b^3 p \sqrt{p} \right) \mod \( bp^2 \sqrt{p} \mathcal{O}_k \). \]

Therefore, we get

\[ F_n = \frac{u_p^n - \overline{u}_p^n}{u_p^n - \overline{u}_p^n} \equiv 2^{-n+1} \left( \binom{n}{1} t^{n-1} + \binom{n}{3} t^{n-3} b^3 \right) \mod p^2. \]

Assume that integers \( m, n \) satisfy \( m \equiv n \pmod{p^2 (p - 1)} \). Then we have

\[ \binom{m}{1} \equiv \binom{n}{1}, \quad \binom{m}{3} \equiv \binom{n}{3} \pmod{p^2} \]

and \( 2^m \equiv 2^n, t^m \equiv t^n \pmod{p^2} \) since \( 2 \) and \( t \) are two invertible elements of \( \mathbb{Z}/p^2 \mathbb{Z} \) and the order of the cyclic group \( \mathbb{Z}/p^2 \mathbb{Z}^\times \) is \( p(p - 1) \). It concludes that \( F_m \equiv F_n \pmod{p^2} \), and the period of \( \{F_m\} \pmod{p^2} \) divides \( p^2 (p - 1) \). Similarly, by using

\[ L_n = u_p^n + \overline{u}_p^n \equiv 2^{-n+1} \left( t^n + \binom{n}{2} t^{n-2} b^2 p \right) \pmod{p^2}, \]

and

\[ \binom{n}{2} \equiv \binom{m}{2} \pmod{p} \]

for integers \( m, n \) satisfying \( m \equiv n \pmod{p(p - 1)} \), we see that the period of \( \{L_m\} \pmod{p^2} \) divides \( p(p - 1) \). \( \Box \)
Now we define two integers $A, B \in \mathbb{Z}$ by
\[ p = A^2 + B^2, \ A \equiv -1 \pmod{4}. \tag{4.5} \]
The sign of $B$ will be determined after the following lemma.

**Lemma 4** Under the above notation, either $p \mid At + 2B$ or $p \mid At - 2B$ but not both holds.

**Proof** Since $p = A^2 + B^2$ and $t^2 + 4 = b^2 p$, we have
\[
\begin{align*}
(A + 2B)(A - 2B) &= A^2 t^2 - 4B^2 = (p - B^2)(b^2 p - 4) - 4B^2 = p(b^2 p - 4 - b^2 B^2). \tag{4.6}
\end{align*}
\]
Assume that both $p \mid At + 2B$ and $p \mid At - 2B$ hold. Then $4B$ is divisible by $p$, and so is $B$. This leads a contradiction. \qed

Determine the even integer $B$ to satisfy conditions (4.5) and $p \mid At + 2B$.

**Lemma 5** Under the above notation, we have
\[ bp \geq |At \pm 2B|. \tag{4.7} \]

**Proof** We see
\[
\begin{align*}
(bp)^2 - (At \pm 2B)^2 &= b^2 p \cdot p - (A^2 t^2 \pm 4ABt + 4B^2) \\
&= (t^2 + 4)(A^2 + B^2) - (A^2 t^2 \pm 4ABt + 4B^2) \\
&= B^2 t^2 + 4A^2 \pm 4ABt \\
&= (Bt \mp 2A)^2 \geq 0.
\end{align*}
\]
From this together with $bp > 0$, we obtain (4.7). \qed

**Lemma 6** Under the above notation, we have
\[
\sqrt{\frac{bp - (At + 2B)}{2p}} \quad \text{and} \quad \sqrt{\frac{bp + (At + 2B)}{2p}} = \frac{|Bt - 2A|}{2p}.
\]

**Proof** As we have seen in the proof of Lemma 5, the equation
\[
(bp)^2 - (At + 2B)^2 = (Bt - 2A)^2
\]
holds. Then we get the assertion. \qed

**Definition 1** Define two real numbers $x_0, y_0 \in \mathbb{R}$ by
\[
x_0 := \sqrt{\frac{bp + (At + 2B)}{2p}} \quad \text{and} \quad y_0 := \kappa \sqrt{\frac{bp - (At + 2B)}{2p}}.
\]
Here, $\kappa$ is equal to 1 or $-1$ which satisfies
\[
x_0 y_0 = \frac{Bt - 2A}{2p}.
\]
Namely, $y_0$ and $Bt - 2A$ are the same signs.

**Lemma 7** Under the above notation (especially, we assume that $p \mid At + 2B$), we have $x_0, y_0 \in \mathbb{Z}$. 

Lemma 8
Under the above notation, we have

\[ x_0^2 = \frac{bp + (At + 2B)}{2p}, \quad \frac{bp - (At + 2B)}{2p} = \left( \frac{Bt - 2A}{2p} \right)^2. \]  (4.8)

it is sufficient to show that \( x_0^2 = \frac{(bp + (At + 2B))}{2p} \) and \( y_0^2 = \frac{(bp - (At + 2B))}{2p} \) are coprime. Assume, on the contrary, that \( (x_0^2, y_0^2) \neq 1 \). Then there exists a prime \( \ell \) such that

\[ \ell \mid x_0^2 \quad \text{and} \quad \ell \mid y_0^2 \]  (4.9)

Then we have

\[ \ell \mid x_0^2 + y_0^2 = b \quad \text{and} \quad \ell \mid x_0^2 - y_0^2 = \frac{At + 2B}{p}. \]  (4.10)

From these and (4.9), we have

\[ 0 \equiv -4p \pmod{\ell}, \]

and so either \( \ell = 2 \) or \( \ell = p \) holds. In the case where \( \ell = p \), we have \( p^2 \mid p(b^2 - 4 - b^2B^2) \) because of \( p \mid b \). Then by (4.10), we have \( p^2 \mid At + 2B \). This implies \( p \mid x_0^2 = \frac{(At + 2B)}{2p} \), which contradicts to (4.9). In the case where \( \ell = 2 \), (4.10) and 2 \mid A imply both 2 \mid b and 2 \mid t. Moreover, 2 \mid A and 2 \mid B imply \( 2^2 \mid Bt - 2A \). Thus \( (Bt - 2A)/2p \) is odd. Then by (4.8), we have \( 2 \mid x_0^2y_0^2 \) which contradicts (4.9). Therefore, \( x_0^2 = \frac{(bp + (A + 2B))}{2p} \) and \( y_0^2 = \frac{(bp - (At + 2B))}{2p} \) are coprime. The proof is complete. \( \square \)

Lemma 8 Under the above notation, we have

\[ bpF_{4n+1} \equiv L_{4n+1}A - 2B = 2p(x_0F_{2n} \pm y_0F_{2n+1})^2. \]  (4.11)

Proof By Lemma 2, we have

\[
2p(x_0F_{2n} \pm y_0F_{2n+1})^2 = 2p(x_0^2F_{2n}^2 + y_0^2F_{2n+1}^2 \pm 2x_0y_0F_{2n}F_{2n+1}) \\
= 2p\left( \frac{bp + (At + 2B)}{2p}F_{2n}^2 + \frac{bp - (At + 2B)}{2p}F_{2n+1}^2 \pm \frac{Bt - 2A}{p}F_{2n}F_{2n+1} \right) \\
= bp(F_{2n}^2 + F_{2n+1}^2) + (At + 2B)(F_{2n}^2 - F_{2n+1}^2) \pm 2(Bt - 2A)F_{2n}F_{2n+1} \\
= bpF_{4n+1} + (At + 2B)\frac{F_{2n}^2 + F_{2n+1}^2 - 4}{b^2p} \pm 2(Bt - 2A)\frac{L_{4n+1} - t}{b^2p} \\
= bpF_{4n+1} + \frac{1}{b^2p}(t^2 + 4)\left( \mp L_{4n+1}A - 2B \right) \\
= bpF_{4n+1} \mp L_{4n+1}A - 2B.
\]

The proof is complete. \( \square \)

5 Quadratic subfields

The aim of this section is to determine the quadratic subfields of \( \bar{L} \). Let the notations be as in §3. For simplicity, we assume that the primitive root \( \iota \) modulo \( p \) defined in (5.1) satisfies

\[ t \equiv -2i \mp \iota \pmod{p}. \]  (5.1)

Indeed, for any primitive roots \( \iota \) modulo \( p \), we have \( \iota^\frac{p-1}{p} \equiv -1 \pmod{p} \), which implies that either \( t \equiv 2i \mp \iota \pmod{p} \) or \( t \equiv -2i \mp \iota \pmod{p} \) holds by using \( t^2 \equiv -4 \pmod{p} \). If \( t \equiv 2i \mp \iota \pmod{p} \), then we replace \( \iota \) by \( -\iota \) which is also a primitive root modulo \( p \).

We recall that the actions of \( \tau \) and \( \tau' \) on \( \epsilon, \epsilon^{-1}, \eta \) and \( \eta^{-1} \) are as follows:

\[
\tau : \epsilon \mapsto \eta \mapsto \epsilon^{-1} \mapsto \eta^{-1}, \\
\tau' : \epsilon \mapsto \eta^{-1} \mapsto \epsilon^{-1} \mapsto \eta.
\]
Here we put

\[ S_0 := \sum_{k=0}^{p-2} \zeta^k, \quad S_1 := \sum_{k=0}^{p-2} \zeta^{k}, \quad S_2 := \sum_{k=0}^{p-2} \zeta^k, \quad S_3 := \sum_{k=0}^{p-2} \zeta^k. \]

Then we can verify that

\[ \tau, \tau' : S_0 \mapsto S_1 \mapsto S_2 \mapsto S_3 \mapsto S_0. \]  \hspace{1cm} (5.2)

Moreover we define the elements \( \lambda, \mu \in L(\zeta) \) by

\[ \lambda := (\varepsilon - \varepsilon^{-1})(S_0 - S_2) + (\eta - \eta^{-1})(S_1 - S_3), \]

\[ \mu := (\varepsilon - \varepsilon^{-1})(S_1 - S_3) + (\eta - \eta^{-1})(S_0 - S_2). \]

**Lemma 9** We have \( \lambda \in K, \mu \in K' \).

**Proof** By (5.2), we can verify \( \lambda = \tau \) and \( \mu = \tau' \). So the assertion follows. \( \square \)

In the following, we will compute \( \lambda \) and \( \mu \). Let \( \chi_{-p} \) be a character modulo \( p \) of order 4 with \( \chi_{-p}(1) = 1 \). Now we consider the Gauss sums \( G(\chi_{-p}) \) and \( G(\overline{\chi_{-p}}) \) of \( \chi_{-p} \) and \( \overline{\chi_{-p}} = \chi_{-p}^3 \), respectively. Then we have

\[ G(\chi_{-p}) := \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi_{-p}(a)\zeta^a = (S_0 - S_2) + i(S_1 - S_3), \]

\[ G(\overline{\chi_{-p}}) := \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi_{-p}(a)\zeta^a = (S_0 - S_2) - i(S_1 - S_3), \]

and hence,

\[ S_0 - S_2 = \frac{1}{2} (G(\chi_{-p}) + G(\overline{\chi_{-p}})), \]  \hspace{1cm} (5.3)

\[ S_1 - S_3 = \frac{1}{2i} (G(\chi_{-p}) - G(\overline{\chi_{-p}})). \]  \hspace{1cm} (5.4)

Moreover we see from \( p \equiv 5 \) (mod 8) that

\[ G(\chi_{-p})G(\overline{\chi_{-p}}) = \chi_{-p}(-1)p = -p, \]  \hspace{1cm} (5.5)

([H Theorem 1.1.4 (a)]). Let

\[ J(\chi_{-p}, \chi_{-p}) := \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi_{-p}(a)\chi_{-p}(1 - a) \]

be the Jacobi sum of \( \chi_{-p} \). Then we can write

\[ J(\chi_{-p}, \chi_{-p}) = c_4 + id_4, \]  \hspace{1cm} (5.6)

where \( c_4 \) and \( d_4 \) are rational integers such that \( c_4^2 + d_4^2 = p, c_4 \equiv -1 \) (mod 4) and \( d_4 \equiv c_4 \frac{1}{2} \) (mod 4) (H Theorems 3.2.1, 3.2.2, Table 3.2.1]). By using notation in ([I, 4.2.5], we have \( c_4 = A \). Moreover, it follows from the definition of \( B \) that \( -A \equiv 2B \) (mod \( p \)). From this together with \( d_4 \equiv c_4 \frac{1}{2} \) and (5.1), we have \( d_4 = B \).

On the other hand, let \( \chi_p \) be the character modulo \( p \) of order 2, namely, \( \chi_p(a) = (\frac{a}{p}) \) for any \( a \in (\mathbb{Z}/p\mathbb{Z})^\times \). Noting that \( p \equiv 5 \) (mod 8) and \( \chi_p^2 = \chi_p \), we have

\[ G(\chi_p) = \sqrt{p}, \]

\[ J(\chi_{-p}, \chi_p) = \frac{G(\chi_{-p})^2}{G(\chi_{-p}^2)} = \frac{G(\chi_{-p})^2}{G(\chi_p)}, \]  \hspace{1cm} ([H Theorem 1.2.4, 2.1.3]). From these relations together with (5.6), we obtain

\[ G(\chi_{-p})^2 = G(\chi_p)J(\chi_{-p}, \chi_{-p}) = \sqrt{p}(A + iB), \]  \hspace{1cm} (5.7)
and hence by (5.5),
\[ G(\chi_p) = \frac{G(\chi_p)G(\chi_p)}{G(\chi_p)} = \frac{p^2}{\sqrt{p(A+iB)}} = \sqrt{p}(A-iB). \] (5.8)

Thus it follows from (5.5), (5.7) and (5.8) that
\[ (G(\chi_p) + G(\chi_p))^2 = 2\sqrt{p}A - 2p, \] (5.9)
\[ (G(\chi_p) - G(\chi_p))^2 = 2\sqrt{p}A + 2p. \] (5.10)

**Lemma 10** The following hold:

1. \((\varepsilon - \varepsilon^{-1})^2(S_0 - S_2)^2 + (\eta - \eta^{-1})^2(S_1 - S_3)^2 = -\frac{1}{2}\text{Tr}_{k/\mathbb{Q}}\{(\alpha^2 - 4)(p - \sqrt{p}A)\}.
2. \((\varepsilon - \varepsilon^{-1})^2(S_1 - S_3)^2 + (\eta - \eta^{-1})^2(S_0 - S_2)^2 = -\frac{1}{2}\text{Tr}_{k/\mathbb{Q}}\{(\alpha^2 - 4)(p + \sqrt{p}A)\}.
3. \((\varepsilon - \varepsilon^{-1})(\eta - \eta^{-1})(S_0 - S_2)(S_1 - S_3) = \sqrt{\frac{p}{2}}\sqrt{(\alpha^2 - 4)(\bar{\alpha}^2 - 4)}.

**Proof** (1) Recall \(\varepsilon + \varepsilon^{-1} = \alpha, \eta + \eta^{-1} = \bar{\alpha}\). Then we have
\[ (\varepsilon - \varepsilon^{-1})^2 = \alpha^2 - 4, \ (\eta - \eta^{-1})^2 = \bar{\alpha}^2 - 4, \] (5.11)
and hence by (5.3), (5.4), (5.9) and (5.10),
\[ \begin{aligned}
(\varepsilon - \varepsilon^{-1})^2(S_0 - S_2)^2 + (\eta - \eta^{-1})^2(S_1 - S_3)^2 &= \frac{1}{4}\{(\alpha^2 - 4)(G(\chi_p) + G(\chi_p))^2 - (\bar{\alpha}^2 - 4)(G(\chi_p) - G(\chi_p))^2\} \\
&= \frac{1}{4}\{(\alpha^2 - 4)(2\sqrt{p}A - 2p) - (\bar{\alpha}^2 - 4)(2\sqrt{p}A + 2p)\} \\
&= -\frac{1}{2}\{(\alpha^2 - 4)(p - \sqrt{p}A) + (\bar{\alpha}^2 - 4)(p + \sqrt{p}A)\} \\
&= -\frac{1}{2}\text{Tr}_{k/\mathbb{Q}}\{(\alpha^2 - 4)(p - \sqrt{p}A)\}.
\end{aligned} \]
(2) The assertion follows from a similar calculation to that of (1)
(3) Since \((\varepsilon - \varepsilon^{-1})(\eta - \eta^{-1}) > 0\) (Lemma 2), it follows from (5.11) that
\[ (\varepsilon - \varepsilon^{-1})(\eta - \eta^{-1}) = \sqrt{(\alpha^2 - 4)(\bar{\alpha}^2 - 4)}. \]

Then by (5.3), (5.4), (5.7) and (5.8), we have
\[ \begin{aligned}
(\varepsilon - \varepsilon^{-1})(\eta - \eta^{-1})(S_0 - S_2)(S_1 - S_3) &= \sqrt{(\alpha^2 - 4)(\bar{\alpha}^2 - 4)} \cdot \frac{1}{4}\{(\alpha^2 - 4)G(\chi_p)^2 - G(\chi_p)^2\} \\
&= \frac{1}{4}\sqrt{(\alpha^2 - 4)(\bar{\alpha}^2 - 4)} \cdot 2\sqrt{p}Bi \\
&= \frac{\sqrt{p}B}{2} \sqrt{(\alpha^2 - 4)(\bar{\alpha}^2 - 4)},
\end{aligned} \]
as desired. \(\square\)

From now on, let the situation be as in our main theorems. Namely, we define an element \(\alpha \in k\) by
\[ \alpha = \alpha(m, n) := L_nL_m + (L_mF_n - 2F_m)b\sqrt{p}, \]
for \(m, n \in \mathbb{Z}\). Then we have the following lemma.

**Lemma 11** Assume that both \(m\) and \(n\) are odd. Then we have
\[ (N + 4)^2 - 4T^2 = L_p^2b^2p(L_mF_n - 2F_m)^2. \]
Especially, \((N + 4)^2 - 4T^2 \in p\mathbb{Q}^2\).
Proof It follows from (1.2) that
\[
N = \frac{\mathcal{L}_m^2 - (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 b^2 p}{4} = \frac{(b^2 \mathcal{F}_m^2 - 4) \mathcal{L}_m^2 - (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 b^2 p}{4} \tag{5.12}
\]
\[
= -\mathcal{L}_m^2 + \mathcal{L}_m \mathcal{F}_n \mathcal{F}_m b^2 p - \mathcal{F}_m^2 b^2 p = -(\mathcal{F}_m^2 b^2 p - 4) + \mathcal{L}_m \mathcal{F}_n \mathcal{F}_m b^2 p - \mathcal{F}_m^2 b^2 p
\]
\[
= \mathcal{F}_m b^2 p (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m) + 4.
\]
Hence by using \(T^2 - (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 b^2 p = 4N\) and (1.2), we have
\[
(N + 4)^2 - 4T^2 = (N + 4)^2 - 4 \left((\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 b^2 p + 4N\right)
\]
\[
= (N - 4)^2 - 4(\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 b^2 p
\]
\[
= \mathcal{F}_m^2 b^2 p (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 - 4(\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 b^2 p
\]
\[
= (\mathcal{F}_m^2 b^2 p - 4)(\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 b^2 p
\]
\[
= \mathcal{L}_m^2 (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 b^2 p,
\]
as desired. \(\square\)

Remark 4 From the proof of Lemma 11 we have
\[
f_{\alpha}(X) := X^4 - TX^3 + (N + 2)X^2 - TX + 1
\]
\[
= X^4 - \mathcal{L}_n \mathcal{L}_m X^3 + (\mathcal{F}_m b^2 p (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m) + 6)X^2 - \mathcal{L}_n \mathcal{L}_m X + 1,
\]
for odd integers \(m\) and \(n\).

Proposition 2 For any odd integers \(m, n\) with \(n > 3\), we have
\[
(K, K') = \begin{cases} 
(Q(\sqrt{D_{m,n}}), Q(\sqrt{pD_{m,n}})) & \text{if } n \equiv 1 \pmod{4}, \\
(Q(\sqrt{pD_{m,n}}), Q(\sqrt{D_{m,n}})) & \text{if } n \equiv 3 \pmod{4},
\end{cases}
\]
where \(D_{m,n}\) is defined as in §1.

Proof By (1.2), we have
\[
\alpha^2 - 4 = \frac{1}{4} \left\{ \mathcal{L}_n \mathcal{L}_m + (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)b\sqrt{p}\right\}^2 - 4
\]
\[
= \frac{1}{4} \left\{ \mathcal{L}_m^2 \mathcal{L}_m + (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 b^2 p + 2\mathcal{L}_n \mathcal{L}_m (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)b\sqrt{p}\right\} - 4
\]
\[
= \frac{1}{4} \left\{ (b^2 \mathcal{F}_m^2 - 4) \mathcal{L}_m^2 + (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2 b^2 p + 2\mathcal{L}_n \mathcal{L}_m (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)b\sqrt{p}\right\} - 4
\]
\[
= \frac{1}{4} \left\{ 2b^2 \mathcal{F}_m^2 \mathcal{L}_m^2 - 4\mathcal{L}_m \mathcal{F}_n \mathcal{F}_m b^2 p + 2\mathcal{L}_n \mathcal{L}_m (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)b\sqrt{p} - 4(\mathcal{L}_m^2 - b^2 \mathcal{F}_m^2 + 4)\right\}
\]
\[
= \frac{1}{2} \left\{ b^2 \mathcal{F}_m^2 \mathcal{L}_m^2 - 2\mathcal{L}_m \mathcal{F}_n \mathcal{F}_m b^2 p + \mathcal{L}_n \mathcal{L}_m (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)b\sqrt{p}\right\}.
\]
Then we have
\[
\text{Tr}_{k/Q}\{(\alpha^2 - 4)(p + \sqrt{p}A)\} = b^2 p^2 \mathcal{F}_m^2 \mathcal{L}_m^2 - 2\mathcal{L}_m \mathcal{F}_n \mathcal{F}_m b^2 p^2 \pm \mathcal{L}_n \mathcal{L}_m b^2 p (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)A
\]
\[
= b^2 p^2 \mathcal{F}_n \mathcal{L}_m (\mathcal{F}_n \mathcal{L}_m - 2\mathcal{F}_m) \pm \mathcal{L}_n \mathcal{L}_m b^2 p (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)A
\]
\[
= (\mathcal{F}_n \mathcal{L}_m - 2\mathcal{F}_m)b^2 p \mathcal{L}_m (b\mathcal{F}_n \pm \mathcal{L}_n)A.
\]
On the other hand, it follows from Lemma 11 that
\[
(\alpha^2 - 4)(\alpha^2 - 4) = (N + 4)^2 - 4T^2 = \mathcal{L}_m^2 b^2 p (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m)^2.
\]
Here we recall
\[
b\mathcal{L}_m (\mathcal{L}_m \mathcal{F}_n - 2\mathcal{F}_m) > 0.
\]
as we have seen in §1. Then we have
\[ \sqrt{(\alpha^2 - 4)(\beta^2 - 4)} = L_m b\sqrt{p(L_mF_n - 2F_m)}. \]

From this together with (5.13) and Lemma 10 (1), (3), we have
\[ \lambda^2 = \left( (\varepsilon - \varepsilon^{-1})(S_0 - S_2) + (\eta - \eta^{-1})(S_1 - S_3) \right)^2 \]
\[ = -\frac{1}{2} Tr_{k/Q} \{(\alpha^2 - 4)(p - \sqrt{p}A)\} + \sqrt{p} B \sqrt{(\alpha^2 - 4)(\beta^2 - 4)} \]
\[ = -\frac{1}{2} (F_n L_m - 2F_m) bp L_m(bp F_n - L_n A) + L_m bp B(L_m F_n - 2F_m) \]
\[ = -\frac{1}{2} (F_n L_m - 2F_m) bp L_m(bp F_n - L_n A - 2B). \]

By using Lemma 10 (2), (3), we obtain
\[ \mu^2 = -\frac{1}{2} (F_n L_m - 2F_m) bp L_m(bp F_n + L_n A - 2B) \] (5.15)
similarly.

Assume that \( n \equiv 1 \pmod{4} \) (resp. \( n \equiv -1 \pmod{4} \)). Then by Lemmas 3, 8 and (5.14) (resp. 5.15), we have \( \lambda^2 \in D_{m,n} Q^2 \) (resp. \( \mu^2 \in D_{m,n} Q^2 \)). Hence \( \sqrt{D_{m,n}} \in K \) (resp. \( \sqrt{D_{m,n}} \in K' \)) by Lemma 9. On the other hand, we have \( \sqrt{D_{m,n}} \not\in \mathbb{Q} \) because of \( D_{m,n} < 0 \). Thus we get \( K = \mathbb{Q}(\sqrt{D_{m,n}}) \) (resp. \( K' = \mathbb{Q}(\sqrt{D_{m,n}}) \)).

6 Proof of Main Theorem 1

Let the notations be as in §2. Namely, we consider the polynomial \( f_\alpha(X) \) for \( \alpha = \alpha(m,n) \). Before the proof of Main Theorem 1 we show the following three lemmas.

Lemma 12 Assume that two odd integers \( m, n \) satisfy \( (L_m F_n - 2F_m)b \equiv 0 \pmod{p^2} \). Then there exists \( x \in \mathcal{L}^\times \) such that
\[ x^p \equiv e^{t(K_0)} \pmod{p(\zeta^p - 1)O_L}, \]
that is, (A3) holds.

Proof We get the assertion from Lemmas 11 and 1.

Lemma 13 Let \( i, j \) be integers which are not divisible by \( p \). If \( \varepsilon^i \eta^j \in L^p \), then we have \( \varepsilon, \eta \in L^p \).

Proof Let \( k_1 \) be the subfield \( \mathbb{Q}(\zeta) \) of degree 4. We denote
\[ \text{Gal}(Lk_1/k) \simeq \langle \sigma \rangle \times \langle \sigma' \rangle \simeq C_2 \times C_2, \]
where \( \varepsilon^\sigma = \varepsilon^{-1}, \eta^\sigma = \eta, \varepsilon'^\sigma = \varepsilon \) and \( \eta'^\sigma = \eta^{-1} \). If \( \varepsilon^i \eta^j \in L^p \), then so are \( (\varepsilon^i \eta^j)^\sigma = \varepsilon^{-i} \eta^j \), their ratio \( \varepsilon^{2i} \) and their product \( \eta^{2j} \). Since \( \text{gcd}(2i, p) = \text{gcd}(2j, p) = 1 \), we conclude that both \( \varepsilon \) and \( \eta \) are \( p \)th powers in \( L \).

Lemma 14 If \( \varepsilon, \eta \not\in L^p \), then we have \( e^{t(K_0)} \not\in \mathcal{L}^p \) for any \( t(K_0) \in T(K_0) \).

Proof It is sufficient to show that \( e^{t(K_0)} \not\in \mathcal{L}^p \). Since
\[ e^{t(K_0)} = e^{\frac{2}{5}t_0 \eta^2 e^{-i_0 \eta} - 1} = e^{i_0 t_0 + 1} \eta^{2 - 1} \]
and
\[ t_0^2 - 1 = \frac{t_0 + 1}{2} - 1 \equiv -2 \not\equiv 0 \pmod{p}, \]
it holds from Lemma 13 that \( e^{t(K_0)} \not\in L^p \). Then by \( p \not\mid [\mathcal{L} : L] \), we get \( e^{t(K_0)} \not\in \mathcal{L}^p \).
Proof of Main Theorem 4 Let $m_0, n_0$ be integers and $q$ a prime number satisfying the conditions (i), (ii) in Main Theorem 1 and let

$$(m, n) \in N := \{(m, n) \in \mathbb{Z}^2 \mid m \equiv m_0 \pmod{N_q}, \ n \equiv n_0 \pmod{N_q}, \ n > 3\}.$$ 

Since $m_0 \equiv n_0 \equiv 1 \pmod{2}$ and $N_q$ is even, both $m$ and $n$ are odd. It holds that

$$\mathcal{L}_m(\mathcal{L}_m F_n - 2F_m) > 0,$$

as we have stated in §1. Then by $\mathcal{L}_n > 0$, both $\mathcal{L}_n \mathcal{L}_m$ and $(\mathcal{L}_m F_n - 2F_m) b \sqrt{p}$ have the same signs. Hence by

$$|\mathcal{L}_n \mathcal{L}_m| \geq |\mathcal{L}_n F_n| = \left|(t^5 + 5t^3 + 5t) \mathcal{L}_m\right| \geq 11,$$

it holds that

$$|\alpha| = \frac{|\mathcal{L}_n \mathcal{L}_m| + |\mathcal{L}_m F_n - 2F_m| b \sqrt{p}}{2} \geq \frac{11}{2} > 2.$$ 

Thus we obtain $\alpha^2 - 4 > 0$. From this together with Lemma 11 it follows that $\alpha$ satisfies (A1). Moreover, we see from Lemma 3 that

$$F_m \equiv F_{m_0}, \quad L_m \equiv L_{m_0}, \quad F_n \equiv F_{n_0} \mod{p^2},$$

hence by Lemma 12 a root $\varepsilon$ of $f_{\alpha}(X)$ satisfies (A3).

Next, let us prove that the condition (A2) holds. Let $d$ be the discriminant of the characteristic polynomial $P(X) = X^2 - tX - 1$. Then we have $d = t^2 + 4 = b^2 p$. It is known ([10], pp.65–66]) that the periods of $\{F_n\}$ mod $q$ and $\{L_n\}$ mod $q$ divide $q - 1$ (resp. $2(q + 1)$) if $\left(\frac{2}{q}\right) = 1$ (resp. $\left(\frac{2}{q}\right) = -1$).

Since $q \nmid 2bp$, we get $\left(\frac{4}{q}\right) = \left(\frac{2}{q}\right)$ and $\left(\frac{2}{q}\right)$. By the definition of $N_q$, we have

$$F_m \equiv F_{m_0}, \quad L_m \equiv L_{m_0}, \quad F_n \equiv F_{n_0}, \quad L_n \equiv L_{n_0} \mod{q^2},$$

and therefore $f_{\alpha, q}(X) = f_{\alpha_0, q}(X) \in \mathbb{F}_q[X]$. By the assumption (ii) of Main Theorem 4 we have $f_{\alpha, q}(a) = f_{\alpha_0, q}(a) = 0$ for some $i \in \{1, 2, 4\}$ and $a \in \mathbb{F}_{q^i} \setminus \mathbb{F}_{q^i}^p$. If $p \nmid q^i - 1$, then we have $\mathbb{F}_{q^i}^p = \mathbb{F}_{q^i}$ and this is a contradiction because $a \in \mathbb{F}_{q^i} \setminus \mathbb{F}_{q^i}^p$. We get $p \mid q^i - 1$. Now, we assume that one of $\varepsilon, \varepsilon^{-1}, \eta, \eta^{-1}$ (hence all of $\varepsilon, \varepsilon^{-1}, \eta, \eta^{-1}$) is contained in $L$. Then we have $a \in \mathbb{F}_{q^i}^p$ where $f := [O_L / \mathbb{Q} : \mathbb{Z}/q\mathbb{Z}]$ for a prime ideal $\mathbb{P}$ of $L$ above $q$. If $i \geq f$, then this is a contradiction because $a \in \mathbb{F}_{q^i}^p$. In the case $i < f$, we write $a = b^p$ for some $b \in \mathbb{F}_{q^i}$. We get $a^{f/i} = N_{\mathbb{F}_{q^i}/\mathbb{F}_{q^i}}(b)^p$. Since $f/i \in \{2, 4\}$ and $p \mid q^i - 1$, this implies $a \in \mathbb{F}_{q^i}^p$ and it is a contradiction. Thus none of $\varepsilon, \varepsilon^{-1}, \eta, \eta^{-1}$ is contained in $L$. By Lemma 14 therefore, (A2) holds.

As for the infiniteness of the set $\{(k_0(\sqrt{d_{m_0, n}}), k_0(\sqrt{pD_{m_0, n}})) \mid (m, n) \in N\}$, it is enough to prove that the set of pairs

$$\{(\mathbb{Q}(\sqrt{d_{m_0, n}}), \mathbb{Q}(\sqrt{pD_{m_0, n}})) \mid n \equiv n_0 \pmod{N_q}, \ n > 3\}$$

is infinite. For an integer $a$, let $s(a)$ denote the square free integer satisfying $a = s(a) A^2$ for some $A \in \mathbb{N}$, and assume that the set

$$\{(\mathbb{Q}(\sqrt{d_{m_0, n}}), \mathbb{Q}(\sqrt{pD_{m_0, n}})) \mid n \equiv n_0 \pmod{N_q}, \ n > 3\}$$

is finite. Then the set $\{s(D_{m_0, n}) \mid n \equiv n_0 \pmod{N_q}, \ n > 3\}$ is finite. Since there are infinitely many integers $n$ satisfying $n \equiv n_0$ (mod $N_q$) and $n > 3$, there exists an integer $\ell$ such that $N_{\ell} := \{n \in \mathbb{Z} \mid n \equiv n_0 \pmod{N_q}, \ n > 3, \ s(D_{m_0, n}) = \ell\}$ is infinite. For any integer $n \in N_{\ell}$, let $D_{m_0, n} = \ell A^2$. Then by (A2), we have

$$L_{m_0}^4 - L_{m_0}^2 c_n^2 = L_{m_0}^2 b \mathcal{F}_{m_0}^2 - 4$$

$$= p (L_{m_0} b \mathcal{F}_{m_0})^2 - 4L_{m_0}^4$$

$$= p (2b \mathcal{F}_{m_0} L_{m_0} - \ell A^2)^2 - 4L_{m_0}^4$$

$$= p \ell^2 A^4 - 4bp \mathcal{F}_{m_0} \mathcal{L}_{m_0} A^2_n + 4b^2 p \mathcal{F}_{m_0} \mathcal{L}_{m_0} - 4L_{m_0}^4.$$
This implies that infinitely many pairs \((A_n, L_n)\) are integer solutions of the equation
\[
E_{ma}^4 Y^2 = p^2X^4 + 4bp_z^2X^2 + 4b^2pF_{ma}^2 - 4L_{ma}^4.
\]
The discriminant of the quartic polynomial on the right side is
\[
2^{14}p^3 \ell^6 E_{ma}^{10} (p^2pF_{ma} - L_{ma}^2) = 2^{16}p^3 \ell^6 E_{ma}^{10} \not= 0,
\]
by (1.2) and the assumption \(m_0 \equiv 1 \pmod{2}\). Hence the equation has only finitely many integer solutions by Siegel's theorem. This is a contradiction, and the proof is complete.

\[\square\]

7 Proof of Main Theorem 2

In this section, we prove Main Theorem 2. Let \(q \not= 2\) be a prime number and \(F_q\) be the finite field with the cardinality \(q^r\). We denote by \(g\) a generator of the cyclic group \(F_q^\times\). Put
\[
Y_q := \{(g^n - g^{-m})g^n - (g^m + g^{-m}) | n, m \in \mathbb{Z}, n \equiv m \equiv 1 \pmod{2}\}.
\]
The set \(Y_q\) does not depend on \(g\) because other generators are given by \(g^s\) with \((s, q^r - 1) = 1\). First, we show the following lemma.

Lemma 15 Let \(q \not= 2\) be a prime number with \(q^r > 45\). Then we have \(Y_q = F_{q^r}\).

Proof Put \(k = (g^m - g^{-m})g^n - (g^m + g^{-m}), m = 2u + 1, n = 2v + 1 (u, v \in \mathbb{Z})\) and \(X = g^n, Y = g^v\). Then we have
\[
f(X, Y) := g^3X^4Y^2 - gY^2 - g^2X^4 - kgX^2 - 1 = 0.
\]
By the definition of \(Y_q\), we easily see that \(Y_q = F_{q^r}\) if and only if
\[
S_k := \{(X, Y) \in \mathbb{F}_{q^r}^2 | f(X, Y) = 0, XY \not= 0\} \not= \emptyset
\]
for any \(k \in F_{q^r}\). Because if \(S_k \not= \emptyset\) for \(k \in F_{q^r}\), then there exist integers \(u, v\) satisfying \(f(g^n, g^v) = 0\). This implies
\[
g^{2m}g^n - g^n - g^{2m} - kg^m - 1 = 0,
\]
where \(m = 2u + 1\) and \(n = 2v + 1\), and we get
\[
k = (g^m - g^{-m})g^n - (g^m + g^{-m}),
\]
and hence \(k \in Y_q\).

(i) Consider the case \(k \not= \pm 2\). By putting \(Y = Z/(g^3X^4 - g)\), we get
\[
f(X, Y) = -(g^3X^4 - g)^{-1}(g^5X^8 + g^4kX^6 - g^2kX^2 - g - Z^2).
\]
Put
\[
C_k : Z^2 = g(X)
\]
with
\[
g(X) = g^5X^8 + g^4kX^6 - g^2kX^2 - g = (g^3X^4 - g)(1 + gkX^2 + g^2X^4).
\]
Since \(g\) is a generator of \(F_{q^r}^\times\), if there exists \(X_0 \in F_{q^r}\) satisfying
\[
g^3X_0^4 - g = (gX_0^3 + 1)(gX_0^2 - 1) = 0,
\]
then we get \(gX_0^2 + 1 = 0\). For such an \(X_0\) and any \(Y \in F_{q^r}\), we have \(f(X_0, Y) = k - 2 \not= 0\). Therefore, for any \((X, Y) \in \mathbb{F}_{q^r}^2\) such that \(f(X, Y) = 0\), we have \(g^3X^4 - g \not= 0\). We conclude that there is one-to-one correspondence between the sets \(S_k\) and \(\{(X, Z) \in C_k(F_{q^r}) | XZ \not= 0\}\) by \((X, Y) \mapsto (X, Y(g^3X^4 - g))\). Since \(k \not= \pm 2\), we have \(C_k\) is a smooth (hyperelliptic) curve of genus 3 with the discriminant \(-2^{12}g^{12}(k - 2)^6(k + 2)^6\). Let \(\tilde{C}_k\) be the smooth projective curve by adding two infinite points. Since the leading coefficient \(g^9\) of \(g(X)\) is not a square, these infinite points are not rational, and hence we get \(\tilde{C}_k(F_{q^r}) = C_k(F_{q^r})\). By a consequence of Weil’s theorem, we have
\[
2\tilde{C}_k(F_{q^r}) = 2C_k(F_{q^r}) \geq q^r + 1 - 6\sqrt{q^r}.
\]
Since
\[ \sharp\{(0, Z) \in C_k(\mathbb{F}_{q^r})\} = \sharp\{Z \in \mathbb{F}_{q^r} \mid Z^2 + g = 0\} \leq 2, \]
\[ \sharp\{(X, 0) \in C_k(\mathbb{F}_{q^r})\} = \sharp\{X \in \mathbb{F}_{q^r} \mid 1 + gkX^2 + g^2X^4 = 0\} \leq 4, \]
we have
\[ \sharp\{(X, Z) \in C_k(\mathbb{F}_{q^r}) \mid XZ \neq 0\} \geq q^r + 1 - 6\sqrt{q^r} - 6, \]
and hence \(\{(X, Z) \in C_k(\mathbb{F}_{q^r}) \mid XZ \neq 0\} \neq \emptyset\) if \(q^r > 45\). We conclude that \(S_k \neq \emptyset\) if \(q^r > 45\).

(ii) Consider the case \(k = 2\). We note that
\[ f(X, Y) = (gX^2 + 1)(g^2X^2Y^2 - gX^2 - gY^2 - 1) \]
in this case.

If \(q^r \equiv 3 \pmod{4}\), then we have \(gX_0^2 + 1 = 0\) for \(X_0 := \pm g^{(q^r-3)/4} \in \mathbb{F}_{q^r}\). Hence we have \(f(X_0, Y) = 0\) for any \(Y \in \mathbb{F}_{q^r}\).

If \(q^r \equiv 1 \pmod{4}\), then we have \(g^3X^4 - g = g(gX^2 - 1)(gX^2 + 1) \neq 0\) for any \(X \in \mathbb{F}_{q^r}\). By putting \(Y = Z/g(gX^2 - 1)\), we get
\[ f(X, Y) = \frac{gX^2 + 1}{g(gX^2 - 1)}((g^3X^4 - g) - Z^2). \]

Put
\[ C_2 : Z^2 = g^3X^4 - g. \]
There is one-to-one correspondence between the sets \(S_2\) and \(\{(X, Z) \in C_2(\mathbb{F}_{q^r}) \mid XZ \neq 0\}\) by \((X, Y) \mapsto (X, g(gX^2 - 1)Y)\). Since \(C_2\) is a smooth curve of genus 1, by similar arguments of (i), we have
\[ \sharp C_2(\mathbb{F}_{q^r}) = \sharp\tilde{C}_2(\mathbb{F}_{q^r}) \geq q^r + 1 - 2\sqrt{q^r}. \]

Since
\[ \sharp\{(0, Z) \in C_2(\mathbb{F}_{q^r})\} = \sharp\{Z \in \mathbb{F}_{q^r} \mid Z^2 + g = 0\} = 0, \]
\[ \sharp\{(X, 0) \in C_2(\mathbb{F}_{q^r})\} = \sharp\{X \in \mathbb{F}_{q^r} \mid g^3X^4 - g = 0\} = 0, \]
we have
\[ \sharp\{(X, Z) \in C_2(\mathbb{F}_{q^r}) \mid XZ \neq 0\} \geq q^r + 1 - 2\sqrt{q^r} = (\sqrt{q^r} - 1)^2 > 0. \]

We conclude that \(S_2 \neq \emptyset\) for any prime number \(q\).

(iii) Consider the case \(k = -2\). By putting \(Y = Z/g(gX^2 + 1)\), we get
\[ f(X, Y) = \frac{gX^2 - 1}{g(gX^2 + 1)}((g^3X^4 - g) - Z^2). \]

Put
\[ C_{-2} : Z^2 = g^3X^4 - g. \]
If \(q^r \equiv 3 \pmod{4}\), then we have \(gX_0^2 + 1 = 0\) for \(X_0 := \pm g^{(q^r-3)/4} \in \mathbb{F}_{q^r}\). Hence we have
\[ f(X_0, Y) = -((gX_0^2 - 1)^2 - Y^2(g^3X^4 - g)) = -(gX_0^2 - 1)^2 = -4 \neq 0, \]
for any \(Y \in \mathbb{F}_{q^r}\). Therefore, for any \((X, Y) \in \mathbb{F}_{q^r}^2\), such that \(f(X, Y) = 0\), we have \(gX^2 + 1 \neq 0\). We conclude that there is one-to-one correspondence between the sets \(S_{-2}\) and \(\{(X, Z) \in C_{-2}(\mathbb{F}_{q^r}) \mid XZ \neq 0\}\) by \((X, Y) \mapsto (X, g(gX^2 + 1)Y)\). In this case, we have
\[ \sharp C_{-2}(\mathbb{F}_{q^r}) = \sharp\tilde{C}_{-2}(\mathbb{F}_{q^r}) \geq q^r + 1 - 2\sqrt{q^r} \]
and
\[ \sharp\{(0, Z) \in C_{-2}(\mathbb{F}_{q^r})\} = \sharp\{Z \in \mathbb{F}_{q^r} \mid Z^2 + g = 0\} = 2, \]
\[ \sharp\{(X, 0) \in C_{-2}(\mathbb{F}_{q^r})\} = \sharp\{X \in \mathbb{F}_{q^r} \mid g^3X^4 - g = 0\} = 2, \]
and hence
\[ \sharp \{(X, Z) \in C_{-2}(\mathbb{F}_{q^r}) \mid XZ \neq 0 \} \geq q^r + 1 - 2\sqrt{q^r} - 4. \]

Thus we have \( \{(X, Z) \in C_{-2}(\mathbb{F}_{q^r}) \mid XZ \neq 0 \} \neq \emptyset \) if \( q^r > 9 \).

If \( q^r \equiv 1 \pmod{4} \), then we have \( gX^2 + 1 \neq 0 \) for any \( X \in \mathbb{F}_{q^r} \). By the same argument of (ii) in the case \( q^r \equiv 1 \pmod{4} \), we have
\[ \sharp \{S_{-2} \cup \{(X, Z) \in C_{-2}(\mathbb{F}_{q^r}) \mid XZ \neq 0 \} \} > 0. \]

We conclude that \( S_{-2} \neq \emptyset \) if \( q^r > 9 \).

By (i), (ii) and (iii), we conclude that \( Y_q = \mathbb{F}_{q^r} \) for any prime number \( q \) with \( q^r > 45 \). \( \square \)

**Proposition 3** Assume that ERH holds. Then there exists odd integers \( m, n \) and a prime number \( q \) such that \( q \nmid 2bp, q^2 \neq 1 \pmod{p} \) and \( f_{\alpha, q}(a) = 0 \) for some \( a \in \mathbb{F}_{q^r} \setminus \mathbb{F}_{q^r}^* \), where \( \alpha := \alpha(m, n) \) and \( f = [\mathcal{O}_L/\mathbb{Q} : \mathbb{Z}/q\mathbb{Z}] \) for a prime ideal \( \mathcal{Q} \) of \( L \) above \( q \).

**Proof** We use a result proved by Lenstra [9 (4.8)] for \( k = \mathbb{Q}(\sqrt{\sigma}) \). Let \( \sigma \) and \( \sigma' \) be generators of the cyclic groups \( \text{Gal}(\bar{L}/L) \simeq C_{p-1/2} \) and \( \text{Gal}(\bar{L}/\mathbb{Q}(\zeta_p)) \simeq C_2 \), respectively, and put \( \tau := \sigma^{(p-1)/4} \sigma' \). Consider the set \( M = M(k, \bar{L}, \{\zeta\}, \langle u_q, \{ \rangle \} ) \) of primes \( q \) of \( k \) satisfying \( (\mathbb{Q}, \bar{L}/k) = \tau \) and \( (\mathcal{O}_k/q) / \mathbb{Z} = \langle u_q \pmod{q} \rangle \) (see [9 p.203]). Let \( \ell \) be a prime number, and assume \( L_\ell := \mathbb{Q}(\zeta, \sqrt{u_\ell}) \subset \bar{L} \) and \( \tau \in \text{Gal}(\bar{L}/L) \). By the definition of \( \tau \), the fixed field of \( \langle \tau \rangle \) coincides with \( K(\zeta) = K(\zeta' \zeta) \). We have \( L_\ell \subset K(\omega) = K'(\omega) \). Since the field \( K(\omega) \) is abelian extension over \( \mathbb{Q} \), \( L_\ell/\mathbb{Q} \) is also abelian extension. This is a contradiction, because we have
\[ \mathbb{Q} \subset k = \mathbb{Q}(u_q) \subset \mathbb{Q}(\sqrt{u_\ell}) \subset L, \]
but \( \mathbb{Q}(\sqrt{u_\ell})/k \) is not a Galois extension for any prime number \( \ell \geq 3 \), and \( \mathbb{Q}(\sqrt{u_\ell})/\mathbb{Q} \) is not a Galois extension since the Galois conjugate \( \overline{u_\ell} \) satisfies \( \overline{u_\ell} = -u_\ell \) (see the beginning of [4] and \( -1/u_\ell \notin \mathbb{Q}(\sqrt{u_\ell}) \). We conclude that there is no prime number \( \ell \) satisfying \( L_\ell \subset \bar{L} \) and \( \tau \in \text{Gal}(\bar{L}/L) \). By Lenstra’s result (4.8), the set \( M \) is infinite. Choose \( q \in M \) which is unramified in \( \bar{L}/k \) and satisfies \( q \nmid 2bp, q^2 > 45 \) for the prime number \( q \) such that \( q \nmid q \). Since \( q, \mathbb{Q}(\zeta(p)/k) \) is the restriction of \( \sigma^{1/2} \in \text{Gal}(\bar{L}/L) \) to \( \mathbb{Q}(\zeta) \) and \( (q, L/k) \) is the restriction of \( \sigma' \in \text{Gal}(\bar{L}/\mathbb{Q}(\zeta)) \) to \( L \), we see that \( q \) is totally decomposed in \( \mathbb{Q}(\zeta + \zeta^{-1})/k \) and not decomposed in both \( \mathbb{Q}(\zeta(p)/k) \) and \( L/k \). Put \( \tau := [\mathcal{O}_k/q : \mathbb{Z}/\mathbb{Z}] \) and \( f := [\mathcal{O}_L/\mathbb{Q} : \mathbb{Z}/\mathbb{Z}] \). Then we have \( f = 2r \) and the order of \( q \) in \( \mathbb{F}_{q^r}^* \) is \( 2r \) (hence, \( q^{2r} \equiv 1 \pmod{p} \), \( q^{2r} \equiv 1 \pmod{p} \) and \( q^2 \equiv 1 \pmod{p} \)). On the other hand, since \( u_\ell \overline{u_\ell} = -1 \), for odd integers \( m, n \), we have
\[
\alpha(m, n) = \frac{L_nL_m + (L_mF_n - 2F_m)b\sqrt{\sigma}}{2} \equiv L_n u_p^n - F_n (u_p - \overline{u_p}) \equiv (u_p^n + \overline{u_p^n})u_p^n - (u_p^n - \overline{u_p^n}) \equiv (u_p^n - u_p^{-m})u_p^n - (u_p^n + u_p^{-m}).
\]
Since \( u_\ell \pmod{q} = (\mathcal{O}_k/q)^{\times} \simeq \mathbb{F}_{q^r}^* \), \( q^r \geq q > 45 \), by Lemma [15] we get
\[
\{ \alpha = \alpha(m, n) \pmod{q} \in \mathcal{O}_k/q \mid n \equiv m \equiv 1 \pmod{2} \} = \mathcal{O}_k/q.
\]
From [16] and
\[ f_{\alpha}(X) \equiv (X^2 - \alpha X + 1)(X^2 - \overline{\alpha} X + 1) \pmod{q}, \]
it is enough to show
\[ \{ \beta \in \mathbb{F}_{q^r} \mid a^2 - \beta a + 1 = 0 \text{ for some } a \in \mathbb{F}_{q^r} \setminus \mathbb{F}_{q^r}^* \} \neq \emptyset. \]
Put $F_{q^f}^Z = (g)$ and $x_s := g^s$ for $s \in \{1, 2, \ldots, q^f - 1\}$. Since $\text{Gal}(F_{q^f}/\mathbb{F}_{q^f})$ is generated by Frobenius $q$, which is defined by $x^{\text{Frob}_q} = x^{q^f}$ for any $x \in F_{q^f}$, we have

$$N_{F_{q^f}/\mathbb{F}_{q^f}}(x_s) = \iff x_s^{1 + q^f} = 1$$

$$\iff g^{n(1 + q^f)} = 1$$

$$\iff s = (q^f - 1)u, \ u \in \{1, 2, \ldots, q^f + 1\}.$$

Therefore $N_{F_{q^f}/\mathbb{F}_{q^f}}(x_s) = 1$ and $x_s \notin \mathbb{F}_{q^f}$ if and only if $s = (q^f - 1)u, \ u \in \{1, 2, \ldots, q^f + 1\}$ and $p \nmid u$. Since $q^f \nmid 1 \pmod{p}$, we have $F_{q^f} = \mathbb{F}_{q^f}$. Hence if $x_s \notin \mathbb{F}_{q^f}$, then $x_s \notin F_{q^f}$, and both $x_s$ and $x_{sq^f}$ have the same minimal polynomial over $\mathbb{F}_{q^f}$.

Therefore, we conclude

$$\# \{ \beta \in F_{q^f} | a^2 - \beta a + 1 = 0 \text{ for some } a \in F_{q^f} \setminus \mathbb{F}_{q^f} \} = \frac{1}{2} \left( q^f + 1 - \frac{q^f + 1}{p} \right) = \frac{1}{2p} (q^f + 1)(p - 1) > 0,$$

and the proof is complete. \hfill \Box

**Lemma 16** If $p^r \ | \ n$, then $p^r \ | \ F_n$.

**Proof** Since

$$u_p - \overline{u}_p = b\sqrt{p},$$

$$u_p^n - \overline{u}_p^n = 2^{-n}\{(t + b\sqrt{p})^n - (t - b\sqrt{p})^n\}$$

$$\equiv 2^{-n}\{(t^n + nt^{n-1}b\sqrt{p}) - (t^n - nt^{n-1}b\sqrt{p})\}$$

$$\equiv 2^{-n+1}nt^{n-1}b\sqrt{p} \pmod{p^{r+1}b\mathcal{O}_k},$$

we have

$$F_n = \frac{u_p^n - \overline{u}_p^n}{u_p - \overline{u}_p} \equiv 2^{-n+1}nt^{n-1}b \equiv 0 \pmod{p^r\mathcal{O}_k}.$$

Therefore, we have $p^r \ | \ F_n$. \hfill \Box

**Proof of Main Theorem** Under the ERH, there exist odd integers $m, n$ and a prime number $q$ satisfying the conditions in Proposition 6. Since $q^2 \nmid 1 \pmod{p}$, there exists $c \in \mathbb{Z}$ such that $p^2c \equiv 1 \pmod{2(q^2 - 1)}$. Put $m_0 := p^2cm$ and $n_0 := p^2cn$. Then both $m_0$ and $n_0$ are odd. We prove that $m_0, n_0$ satisfy the conditions (i), (ii) of Main Theorem 8. Since $p^2 \ | \ m_0, p^2 \ | \ n_0$, we get $p^2 \ | \ F_{m_0}, p^2 \ | \ F_{n_0}$ by Lemma 16 and hence $m_0, n_0$ satisfy the condition (i). Since the periods of $\{F_n\}$ mod $q$ and $\{L_n\}$ mod $q$ divide $2(q^2 - 1)$ (pp.65–66), and $m_0 = p^2cm \equiv m \pmod{2(q^2 - 1)}$ and $n_0 = p^2cn \equiv n \pmod{2(q^2 - 1)}$, we have

$$F_{m_0} \equiv F_m, \quad L_{m_0} \equiv L_m, \quad F_{n_0} \equiv F_n, \quad L_{n_0} \equiv L_n \pmod{q}.$$

Therefore $f_{\alpha, q}(X) = f_{\alpha, q}(X) (\in \mathbb{F}_q[X])$ for $\alpha_0 := \alpha(m_0, n_0)$ and $\alpha := \alpha(m, n)$. We know that $m_0, n_0$ satisfy the condition (ii) for $i = f$. The proof is complete. \hfill \Box

8 Examples

**Example 1** (1) Let $p = 5$. Then the fundamental unit of $k$ is $u_p = (1 + \sqrt{5})/2$, and hence $t = b = 1$. So the sequences $\{F_n\}$ and $\{L_n\}$ are the same as the Fibonacci numbers $\{F_n\}$ and the Lucas numbers $\{L_n\}$, respectively. Now we will verify that any pair of integers $m_0$ and $n_0$ in Table 1 and a prime number $q = 11$ satisfy the conditions (i), (ii) of the Main Theorem 8.

| $m_0 \mod 50$ | 7 | 17 | 27 | 37 | 47 |
|---------------|---|----|----|----|----|
| $n_0 \mod 100$ | 31 | 11 | 91 | 71 | 51 |

Table 1 $p = 5, q = 11$
Since $b = 1$, the condition (i) in the Main Theorem 1 is equivalent to $F_{m_0} \equiv 2F_{m_0}L^{-1}_{m_0} \pmod{5^2}$ (Note that $p \nmid L_{m_0}$ from (4.2)). We see that $\{F_{m_0}\} \pmod{5^2}$ is 100 periodic and $\{2F_{m_0}L^{-1}_{m_0}\} \pmod{5^2}$ is 25 periodic. Hence any pair of integers $m_0$ and $n_0$ from Table 2 and 3 satisfy the condition (i) of the Main Theorem 1.

Table 2 $2F_{m_0}L^{-1}_{m_0} \mod 25$

| $m_0 \mod 50$ | 7 | 17 | 27 | 37 | 47 |
|---------------|---|---|---|---|---|
| $2F_{m_0}L^{-1}_{m_0} \mod 25$ | 19 | 14 | 9 | 4 | 24 |

Table 3 $F_{n_0} \mod 25$

| $n_0 \mod 100$ | 11 | 31 | 51 | 71 | 91 |
|---------------|---|---|---|---|---|
| $F_{n_0} \mod 25$ | 14 | 19 | 24 | 4 | 9 |

Next, both $\{F_{n_0}\} \pmod{11}$ and $\{L_{n_0}\} \pmod{11}$ are 10 periodic. Since $F_{m_0} \equiv 2 \pmod{11}$, $L_{m_0} \equiv 7 \pmod{11}$ for $m_0$ with $m_0 \equiv 7 \pmod{10}$ and $F_{n_0} \equiv L_{n_0} \equiv 1 \pmod{11}$ for $n_0$ with $n_0 \equiv 1 \pmod{10}$, we have

$$f_{\alpha}(X) \equiv X^4 + 4X^3 + 3X^2 + 4X + 1 \equiv (X - 5)(X - 7)(X - 8)(X - 9) \pmod{11},$$

and $\alpha := 5, 7, 8, 9 \pmod{11} \notin (\mathbb{F}_{13}^\times)^5 = (2^5) = \{\pm 1\}$. Therefore, the condition (ii) holds for $i = 1$.

(2) Let $p = 13$. Then the fundamental unit of $k$ is $\omega_p = (3 + \sqrt{13})/2$. We will verify that any pair of integers $m_0$ and $n_0$ in Table 4 and a prime number $q = 53$ satisfy the conditions (i), (ii) of the Main Theorem 1.

Table 4 $p = 13, q = 53$

| $m_0 \mod 2 \times 13^2$ | 15 | 41 | 67 | 93 | 119 | 145 | 171 | 197 | 223 | 249 | 275 | 301 | 327 |
|---------------------------|---|---|---|---|----|----|----|----|----|----|----|----|----|
| $n_0 \mod 2 \times 13^2$ | 55 | 263 | 471 | 3 | 211 | 419 | 627 | 159 | 367 | 579 | 107 | 315 | 523 |

Since $b = 1$, the condition (i) in the Main Theorem 1 is equivalent to $F_{n_0} \equiv 2F_{m_0}L^{-1}_{m_0} \pmod{13^2}$. We see that $\{F_{n_0}\} \pmod{13^2}$ is 676 (= $2^2 \times 13^2$) periodic and $\{2F_{m_0}L^{-1}_{m_0}\} \pmod{13^2}$ is 169 (= $13^2$) periodic. Hence any pair of integers $m_0$ and $n_0$ in Table 3 satisfies the condition (i) of the Main Theorem 1 from Tables 5 and 6.

Table 5 $2F_{m_0}L^{-1}_{m_0} \mod 13^2$

| $m_0 \mod 2 \times 13^2$ | 15 | 41 | 67 | 93 | 119 | 145 | 171 | 197 | 223 | 249 | 275 | 301 | 327 |
|---------------------------|---|---|---|---|----|----|----|----|----|----|----|----|----|
| $2F_{m_0}L^{-1}_{m_0} \mod 13^2$ | 127 | 88 | 49 | 10 | 140 | 101 | 62 | 23 | 153 | 114 | 75 | 36 | 166 |

Table 6 $F_{n_0} \mod 13^2$

| $n_0 \mod 2 \times 13^2$ | 3 | 55 | 107 | 159 | 211 | 263 | 315 | 367 | 419 | 471 | 523 | 575 | 627 |
|---------------------------|---|---|---|---|----|----|----|----|----|----|----|----|----|
| $F_{n_0} \mod 13^2$ | 10 | 127 | 75 | 23 | 140 | 88 | 36 | 153 | 101 | 49 | 166 | 114 | 62 |
Next, both \( \{F_{n_0}\} \mod 53 \) and \( \{L_{n_0}\} \mod 53 \) are 26 periodic. Since \( F_{m_0} \equiv 24 \mod 53 \), \( L_{m_0} \equiv 8 \mod 53 \) for \( m_0 \equiv 15 \mod 26 \) and \( F_{n_0} \equiv 10 \mod 53 \), \( L_{n_0} \equiv 36 \mod 53 \) for \( n_0 \equiv 3 \mod 26 \), we have

\[
f_{n_0}(X) \equiv X^4 + 30X^3 + 26X^2 + 30X + 1
\]

\[
\equiv (X - 22)(X - 24)(X - 41)(X - 42) \mod (53)
\]

and \( a := 22, 24, 41, 42 \) mod 11 \( \not\in (\mathbb{F}_5^2)^{13} = \langle 2^{13} \rangle = \{1, 23, 30, 52\} \). Therefore, the condition (ii) holds for \( i = 1 \).

**Example 2** Main Theorem \([1]\) implies the previous theorem (Theorem \([1]\) in \([1]\)). Indeed, for \( p = 5 \), we can check that any pairs \( (m_0, n_0) \in \{(1, 97), (1, 103), (1, 197), (1, 203)\} \) and \( q = 61 \) satisfy the conditions (i), (ii) as follows.

(i) Since \( m_0 = 1 \), we have \( F_{m_0} = F_1 = 1 \) and \( L_{m_0} = L_1 = 1 \). Furthermore, we have \( F_{n_0} = F_{n_0} \equiv 2 \mod 5^2 \) since \( n_0 \equiv \pm 3 \mod 100 \). Therefore, the condition (i) holds.

(ii) The polynomials \( f_{n_0, 61}(X) \in \mathbb{F}_{61}[X] \) for \( \alpha_0 = \alpha(m_0, n_0) \) are

\[
f_{n_0, 61}(X) = \begin{cases} 
(X - 10)(X - 30)(X - 55)(X - 59) & \text{if } (m_0, n_0) = (1, 97), \\
(X - 26)(X - 33)(X - 37)(X - 54) & \text{if } (m_0, n_0) = (1, 103), \\
(X - 7)(X - 24)(X - 28)(X - 35) & \text{if } (m_0, n_0) = (1, 197), \\
(X - 2)(X - 6)(X - 31)(X - 51) & \text{if } (m_0, n_0) = (1, 203). 
\end{cases}
\]

The condition (ii) holds for \( i = 1 \) since

\[
(\mathbb{F}_5^2)^{15} = \{1, 11, 13, 14, 21, 29, 32, 40, 47, 48, 50, 60\}.
\]

Therefore Main Theorem \([1]\) implies that the class numbers of both imaginary quadratic fields \( \mathbb{Q}(\sqrt{2 - F_{n_0}}) \) and \( \mathbb{Q}(\sqrt{5(2 - F_{n_0})}) \) are divisible by 5 for any

\[
n \in \{n \in \mathbb{Z} \mid n \equiv 97, 103, 197, 203 \pmod{N_q}, \ n > 3\}.
\]

By the definition of \( N_q \) and \( q = 61 \equiv 1 \pmod{5} \), we have

\[
N_q = \text{lcm}(p^2(p - 1), q - 1) = 300.
\]

Then we have

\[
\{n \in \mathbb{Z} \mid n \equiv 97, 103, 197, 203 \pmod{N_q}, \ n > 3\} = \{n \in \mathbb{N} \mid n \equiv \pm 3 \pmod{100}, \ n \not\equiv 0 \pmod{3}\}
\]

\[\supset \{n \in \mathbb{N} \mid n \equiv \pm 3 \pmod{500}, \ n \not\equiv 0 \pmod{3}\}, \]

and hence we get the set of pairs which is given in Theorem \([1]\).

**Acknowledgements** The authors would like to thank Toru Komatsu for useful advices. They would also like to thank Takuya Yamauchi for his polite suggestions on the proof of Lemma \([15]\).

**References**

1. Alaca, S., Williams, K. S.: Introductory Algebraic Number Theory. Cambridge University Press, Cambridge (2004)
2. Aoki, M., Kishi, Y.: On systems of fundamental units of certain quartic fields. Int. J. Number Theory 11, no. 7, 2019–2035 (2015)
3. Aoki, M., Kishi, Y.: An infinite family of pairs of imaginary quadratic fields with both class numbers divisible by five, J. Number Theory 176, 333–343 (2017)
4. Berndt, B. C., Evans, R. J., Williams, K. S.: Gauss and Jacobi sums. Canadian Mathematical Society Series of Monographs and Advanced Texts 21, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York (1998)
5. Izuka, Y., Konome, Y., Nakano, S.: On the class number divisibility of pairs of quadratic fields obtained from points on elliptic curves. J. Math. Soc. Japan 68, 899–915 (2016)
6. Imaoka, M., Kishi, Y.: On dihedral extensions and Frobenius extensions. Galois Theory and Modular Forms, Dev. Math. 11, 195–220, Kluwer Acad. Publ., Boston, MA (2004)
7. 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, 129–136 (2002)
8. Komatsu, T.: An infinite family of pairs of imaginary quadratic fields with ideal classes of a given order. Int. J. Number Theory 13, no. 2, 253–260 (2017)
9. Lenstra, H. W. Jr.: On Artin’s conjecture and Euclid’s algorithm in global fields. Invent. Math. 42, 201–224 (1977)
10. Ribenboim, P.: The new book of prime number records. Springer-Verlag, New York (1996)
11. Scholz, A.: Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. J. Reine Angew. Math. 166, 201-203 (1932)
12. Takagi, T.: Elementary Number Theory Lecture, Second Edition (Japanese), Kyoritsu Shuppan (1971)
13. Washington, L. C.: Introduction to Cyclotomic Fields, Graduate Texts in Mathematics 83, Springer-Verlag, New York (1982)