On the class groups of certain imaginary cyclic fields of 2-power degree

Humio Ichimura and Hiroki Sumida-Takahashi

Abstract

Let p be an odd prime number and 2^{e+1} be the highest power of 2 dividing $p-1$. For $0 \leq n \leq e$, let k_n be the real cyclic field of conductor p and degree 2^n. For a certain imaginary quadratic field L_0, we put $L_n = L_0 k_n$. For $0 \leq n \leq e-1$, let $\mathcal{F}_n$ be the imaginary quadratic subextension of the imaginary $(2,2)$-extension L_{n+1}/k_n with $\mathcal{F}_n \neq L_{n+1}$. We study the Galois module structure of the 2-part of the ideal class group of the imaginary cyclic field $\mathcal{F}_n$. This generalizes a classical result of Rédei and Reichardt for the case $n = 0$.

1 Introduction

Let $e \geq 2$ be a fixed integer, and let $p = 2^{e+1}q + 1$ be a prime number with $2 \nmid q$. For each $0 \leq n \leq e+1$, we denote by k_n the subfield of of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ of degree 2^n. Here, for an integer $m \geq 2$, ζ_m denotes a primitive mth root of unity. We denote by $\mathbb{P}$ the set of prime numbers ℓ satisfying

$$\left(\frac{p}{\ell}\right) = -1 \quad \text{and} \quad \ell \equiv \pm 1 \bmod 8. \tag{1.1}$$

Let $L_0 = \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2\ell})$ for $\ell \in \mathbb{P}$, and put $L_n = L_0 k_n$. For each $0 \leq n \leq e$, L_{n+1}/k_n is a $(2,2)$-extension with quadratic subextensions L_{n+1} and k_{n+1}. The subject of this paper is the third quadratic subextension $\mathcal{F}_n$ of L_{n+1}/k_n. It is a cyclic field of degree 2^{n+1}, whose conductor is $8p$ or $8p\ell$

2020 *Mathematics Subject Classification*: Primary 11R18; Secondary 11R23, 11Y40.
Key word and phrases: ideal class group, 2-part, imaginary cyclic field.

according as $L_0 = \mathbb{Q}(\sqrt{\pm 2})$ or $\mathbb{Q}(\sqrt{-2\ell})$. When $n = 0$, we have accordingly $\mathcal{F}_0 = \mathbb{Q}(\sqrt{\pm 2p})$ or $\mathbb{Q}(\sqrt{-2p\ell})$. The cyclic field $\mathcal{F}_n$ is imaginary when L_0 is an imaginary quadratic field and $0 \le n \le e-1$ or when $L_0 = \mathbb{Q}(\sqrt{2})$ and $n = e$. For a number field N, h_N and A_N denote the class number and the 2-part of the ideal class group Cl_N of N in the usual sense, respectively. For a CM field N, let Cl_N^- be the kernel of the norm map $Cl_N \to Cl_{N^+}$, and let $h_N^- = |Cl_N^-|$ be the relative class number and A_N^- the 2-part of Cl_N^-, respectively. Here, N^+ is the maximal real subfield of N. When $N = \mathcal{F}_n$ is imaginary, we put $h_n = h_N$, $h_n^- = h_N^-$, $A_n = A_N$ and $A_n^- = A_N^-$, for brevity. Since $\mathcal{F}_n^+ = k_n$ and the class number h_{k_n} is odd (Washington [15, Theorem 10.4]), we see that

$$\mathrm{ord}_2(h_n) = \mathrm{ord}_2(h_n^-) \quad \text{and} \quad A_n = A_n^-,$$

where $\mathrm{ord}_2(*)$ is the 2-adic additive valuation on $\mathbb{Q}$ with $\mathrm{ord}_2(2) = 1$. The main purpose of this paper is to study the Galois module structure of the class group A_n for those n where $\mathcal{F}_n$ is imaginary. When $n = 0$, it is well known that

$$A_0 \cong \mathbb{Z}/2^j \quad \text{or} \quad \mathbb{Z}/2 \oplus \mathbb{Z}/2^j \tag{1.2}$$

with $j \ge 2$ according as $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$, which is due to Rédei and Reichardt [13]. We generalize this result for the case $n \ge 1$. There are many other results on the 2-part of the class group of $\mathcal{F}_0$ or other quadratic fields such as [1, 7, 9, 11, 16].

To state our results, let us introduce some notation. Let $\Gamma_n = \mathrm{Gal}(\mathcal{F}_n/\mathbb{Q})$ and $R_n = \mathbb{Z}_2[\Gamma_n]$, where $\mathbb{Z}_2$ is the ring of 2-adic integers. We fix a generator γ_n of the cyclic group Γ_n of order 2^{n+1}. Let $\Lambda = \mathbb{Z}_2[[T]]$ be the 2-adic power series ring with indeterminate T. We identify the group ring R_n with $\Lambda/((1+T)^{2^{n+1}} - 1)$ by the correspondence $\gamma_n \leftrightarrow 1 + T$:

$$R_n = \Lambda/((1+T)^{2^{n+1}} - 1).$$

The class group A_n is naturally regarded as a module over R_n, and hence as a module over Λ. We see that $(1+T)^{2^n} + 1$ annihilates the Λ-module $A_n = A_n^-$.

The class number h_n is always even when $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ (and $0 \le n \le e-1$) by Proposition 1.1 in the below. We define an integer $\bar{h}_n$ by

$$\bar{h}_n = h_n \quad \text{or} \quad \frac{h_n}{2} \tag{1.3}$$

according as $L_0 = \mathbb{Q}(\sqrt{\pm 2})$ or $\mathbb{Q}(\sqrt{-2\ell})$. There are many cases where $\mathrm{ord}_2(\bar{h}_n) \geq 2^n + 1$. For instance, this inequality holds when $n = 0$ by (1.2). In such a case, we put

$$s_n = \left\lceil \frac{\mathrm{ord}_2(\bar{h}_n)}{2^n} \right\rceil \tag{1.4}$$

and

$$a_n = 2^n s_n - \mathrm{ord}_2(\bar{h}_n) \quad \text{and} \quad b_n = 2^n - a_n. \tag{1.5}$$

Here, $\lceil x \rceil$ denotes the smallest integer $\geq x$. Then, $s_n \geq 2$, $a_n \geq 0$ and $b_n \geq 1$. For instance, when $n = 0$, we have

$$s_0 = \mathrm{ord}_2(\bar{h}_0), \quad a_0 = 0, \quad b_0 = 1. \tag{1.6}$$

Further, we define an ideal Θ_n of Λ by

$$\Theta_n = (2^{s_n},\, 2^{s_n-1}T^{b_n},\, (1+T)^{2^n} + 1) \subset \Lambda. \tag{1.7}$$

We easily see that

$$\Lambda/\Theta_n \cong (\mathbb{Z}/2^{s_n-1})^{\oplus a_n} \oplus (\mathbb{Z}/2^{s_n})^{\oplus b_n} \tag{1.8}$$

as abelian groups. For the ideal Θ_n, we often write $\Theta_n(d)$ with $d = -2$, 2 or -2ℓ when they are associated to $L_0 = \mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2\ell})$, respectively.

Let κ_p be the smallest nonnegative integer κ such that p splits completely in $\mathbb{Q}(2^{1/2^{e-\kappa+1}})$. It is known that $0 \leq \kappa_p \leq e$ and that for any i with $0 \leq i \leq e$, there exist infinitely many prime numbers p of the form $p = 2^{e+1}q + 1$ with $2 \nmid q$ for which $\kappa_p = i$ ([5, Lemma 1]). We put

$$\tilde{f} = e - \kappa_p + 1 \ (\geq 1) \quad \text{and} \quad f = \min\{\tilde{f}, e\}$$

When $\kappa_p \geq 2$, we have $f = \tilde{f} \leq e - 1$. In the following, we simply write "$f \leq n \leq e-1$" when $\kappa_p \geq 2$ and $f \leq n \leq e-1$. It is known that the prime 2 splits completely in $k_{\tilde{f}}/\mathbb{Q}$ and the primes over 2 remain prime in $k_{e+1}/k_{\tilde{f}}$ ([5, Lemma 3]).

Now we can state our results. As the case $L_0 = \mathbb{Q}(\sqrt{2})$ is dealt with in [5], L_0 denotes $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$ in the rest of this section unless otherwise stated. As we mentioned before, $\mathcal{F}_n$ is imaginary for $0 \leq n \leq e-1$. For a finite abelian group A and an integer $t \geq 1$, let

$$r_{2^t}(A) = \dim_{\mathbb{F}_2} 2^{t-1}A/2^tA$$

be the 2^t-rank of A.

Proposition 1.1. *The 2-rank $r_2(A_n)$ equals 2^n or $1+2^n$ when $0 \le n \le f-1$ and 2^f or $1+2^f$ when $f \le n \le e-1$ according as $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$.*

Proposition 1.2. *The 4-rank $r_4(A_n)$ is positive if and only if $0 \le n \le f-1$.*

Let $\bar{h}_n$ be, as in (1.3), h_n or half of h_n. When $0 \le n \le f-1$, it follows from these propositions that $\mathrm{ord}_2(\bar{h}_n) \ge 2^n + 1$, and hence the integers s_n, a_n, b_n and the ideal Θ_n of Λ are defined by (1.4), (1.5) and (1.7).

Theorem 1.1. *When $f \le n \le e-1$, the Λ-module A_n is isomorphic to*

$$\Lambda/(2,\, T^{2^f}) \quad \text{or} \quad \Lambda/(2,\, T) \oplus \Lambda/(2,\, T^{2^f})$$

according as $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$.

Theorem 1.2. *When $0 \le n \le f-1$, the Λ-module A_n is isomorphic to*

$$\Lambda/\Theta_n(-2) \quad \text{or} \quad \Lambda/(2,\, T) \oplus \Lambda/\Theta_n(-2\ell)$$

according as $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$.

When $n = 0$, we see from (1.6) and (1.8) that Theorem 1.2 is a Galois module version of the classical result (1.2) of Rédei and Reichardt for the imaginary quadratic field $\mathcal{F}_0$. Thus Theorem 1.2 combined with (1.8) is a generalization of (1.2). For comparison, we recall here some results in [5, Theorems 1, 2, Proposition 2] for the case $L_0 = \mathbb{Q}(\sqrt{2})$. In this case, $\mathcal{F}_n$ is imaginary only when $n = e$.

Theorem 1.3 ([5])**.** *Let $L_0 = \mathbb{Q}(\sqrt{2})$.*

(i) *Assume that $\kappa_p \ge 1$. Then, the Λ-module A_e is isomorphic to $\Lambda/(2, T^{2^{e-\kappa_p+1}})$.*

(ii) *Assume that $\kappa_p = 0$. Then, $r_2(A_e) = 2^e$, and $\mathrm{ord}_2(\bar{h}_e) = 5$ when $e = 2$ and $\mathrm{ord}_2(\bar{h}_e) \ge 2^e + 2$ when $e \ge 3$. Further, the Λ-module A_e is isomorphic to $\Lambda/\Theta_e(2)$.*

By definition, the integers s_n, a_n and b_n depend on L_0. We computed the values of $\mathrm{ord}_2(\bar{h}_n)$ for various L_0. We are surprised to find that there are several cases where these integers behave in quite a regular way when n moves and that they do not depend on the choice of L_0. (See Tables 3 and 4 in Section 8.) For instance, for $p = 65537 = 2^{16} + 1$, we have $e = 15$, $\kappa_p = 5$, $f = 11$ and

$$\mathrm{ord}_2(\bar{h}_n) = 12,\ 20,\ 36,\ 68,\ 132,\ 260,\ 516,\ 1028$$

with $n = 3, 4, 5, 6, 7, 8, 9, 10$, respectively, when $L_0 = \mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-2\ell})$ for $\ell \in \mathbb{P}$ with $\ell < 1000$. There are 42 such L_0's. By (1.4) and (1.5), this implies that

$$(s_n,\, a_n,\, b_n) = (2, 2^n - 4, 4) \quad \text{and} \quad \mathrm{ord}_2(\bar{h}_n) = 2^n + 4$$

for these n and L_0. In particular, it follows from (1.8) that the 4-rank $r_4(A_n)$ equals 4 for these n and L_0. On the other hand, the value $\mathrm{ord}_2(\bar{h}_0)$ ranges over the integers $2 \sim 8$, $\mathrm{ord}_2(\bar{h}_1) = 4 \sim 10$ and $\mathrm{ord}_2(\bar{h}_2) = 8 \sim 13$. Further, for various numerical data, see Section 8. These examples lead us to prove the following theorems on the 4-rank of A_n. By virtue of Proposition 1.2, it suffices to deal with the case where $f \geq 2$ and $0 \leq n \leq f - 1$. Thus, we assume $f \geq 2$ in the following. Further, by Theorem 1.2 and (1.8), we already know that $r_4(A_n) \leq 2^n$ and that the following equivalence holds for these n:

$$\begin{aligned} r_4(A_n) < 2^n &\iff s_n = 2 \text{ and } b_n < 2^n \\ &\iff \mathrm{ord}_2(\bar{h}_n) < 2^{n+1}. \end{aligned} \tag{1.9}$$

To state the theorems, it is convenient to divide the set $\mathbb{P}$ of prime numbers ℓ satisfying (1.1) into two classes. Let $\mathbb{P}_+$ (resp. $\mathbb{P}_-$) be the subset of $\mathbb{P}$ consisting of those ℓ with $\ell \equiv 1 \bmod 8$ (resp. $\ell \equiv -1 \bmod 8$).

Theorem 1.4. *When the base field L_0 moves over the quadratic fields $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-2\ell})$ with $\ell \in \mathbb{P}_+$, the following assertions hold.*

(i) *For $0 \leq n \leq f - 1$, the 4-rank $r_4(A_n)$ depends only on n, and not on individual L_0's.*

(ii) *Assume that there exists some $1 \leq n \leq f - 1$ for which $r_4(A_n) < 2^n$ (or equivalently, $s_n = 2$ and $b_n < 2^n$). Let $n_p^+ \geq 1$ be the smallest such integer, and put $b_p^+ = b_{n_p^+}$ $(< 2^{n_p^+})$. Then, $b_p^+ \geq 2^{n_p^+ - 1}$, and*

$$(s_n,\, a_n,\, b_n) = (2,\, 2^n - b_p^+,\, b_p^+) \quad \textit{and} \quad \mathrm{ord}_2(\bar{h}_n) = 2^n + b_p^+$$

for any n with $n_p^+ \leq n \leq f - 1$ and for $L_0 = \mathbb{Q}(\sqrt{-2})$ and $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ with any $\ell \in \mathbb{P}_+$. Further, $r_4(A_n) = 2^n$ for $0 \leq n \leq n_p^+ - 1$.

Theorem 1.5. *When the base field L_0 moves over the quadratic fields $\mathbb{Q}(\sqrt{-2\ell})$ with $\ell \in \mathbb{P}_-$, the following assertions hold.*

(i) *For $0 \leq n \leq f - 1$, the 4-rank $r_4(A_n)$ depends only on n, and not on*

individual L_0's.

(ii) *Assume that there exists some $1 \le n \le f-1$ for which $r_4(A_n) < 2^n$ (or equivalently, $s_n = 2$ and $b_n < 2^n$). Let $n_p^- \ge 1$ be the smallest such integer, and put $b_p^- = b_{n_p^-}$ $(< 2^{n_p^-})$. Then, $b_p^- \ge 2^{n_p^- - 1}$, and*

$$(s_n,\, a_n,\, b_n) = (2,\, 2^n - b_p^-,\, b_p^-) \quad \textit{and} \quad \mathrm{ord}_2(\bar{h}_n) = 2^n + b_p^-$$

for any n with $n_p^- \le n \le f-1$ and for $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ with any $\ell \in \mathbb{P}_-$. Further, $r_4(A_n) = 2^n$ for $0 \le n \le n_p^- - 1$.

For the above mentioned example $p = 65537$, we have $(n_p^+, b_p^+) = (n_p^-, b_p^-) = (3, 4)$. We will see in Section 8 that there are cases where $(n_p^+, b_p^+) \ne (n_p^-, b_p^-)$. In contrast to Theorem 1.4, Theorem 1.5 does not deal with $\mathbb{Q}(\sqrt{2})$. This is because when $L_0 = \mathbb{Q}(\sqrt{2})$, $\mathcal{F}_n$ is imaginary only for $n = e$. The following theorem recovers this weak point when $\kappa_p = 0$.

Theorem 1.6. *Let $L_0 = \mathbb{Q}(\sqrt{2})$, and assume that $\kappa_p = 0$ (so that $f = e$).*

(i) *Assume that $r_4(A_e) < 2^{e-1}$. Let $n_1 \ge 1$ be the smallest integer such that $b_e < 2^{n_1}$. Then, the assumption of Theorem 1.5(ii) is satisfied, and the assertion of Theorem 1.5(ii) holds with $(n_p^-,\, b_p^-) = (n_1,\, b_e)$.*

(ii) *Assume that $r_4(A_e) \ge 2^{e-1}$. Then, we have $r_4(A_n) = 2^n$ for any $0 \le n \le e-1$ and for $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ with any $\ell \in \mathbb{P}_-$. Hence, the assumption of Theorem 1.5(ii) is not satisfied.*

We will see in Section 8 that there are cases where the assumption in Theorem 1.4(ii) or Theorem 1.5(ii) is not satisfied and that the two cases in Theorem 1.6 actually occur. We know that $r_4(A_1) = 1$ or 2 by (1.9) (and $f \ge 2$). We can determine $r_4(A_1)$ as follows.

Theorem 1.7. (I) *When $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$ with $\ell \in \mathbb{P}_+$, we have $r_4(A_1) = 2$. Hence, under the assumption of Theorem 1.4(ii), we have $n_p^+ \ge 2$ and $b_p^+ \ge 2$.*

(II) *When $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ with $\ell \in \mathbb{P}_-$, we have $r_4(A_1) = 2$ if and only if $e \ge 3$. Hence, under the assumption of Theorem 1.5(ii), we have $n_p^- = 1$ and $b_p^- = 1$ when $e = 2$, and $n_p^- \ge 2$ and $b_p^- \ge 2$ when $e \ge 3$.*

This paper is organized as follows. In Section 2, we give some propositions and remarks related to the theorems. In Section 3, we show some technical lemmas which are necessary to prove the theorems. In Section 4, we study

some basic properties of the tower $k_{e+1}/\mathbb{Q}$, which are key for proving our results. We prove Theorems 1.1, 1.2, 1.4 and 1.5 in Section 5, Theorem 1.6 in Section 6, and Theorem 1.7 in Section 7. In Section 8, we give several numerical data related to Theorems 1.1–1.7.

2 Related propositions and remarks

Let $p = 2^{e+1}q + 1$ be a prime number with $2 \nmid q$. Letting $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$ with $\ell \in \mathbb{P}$, we use the same notation as in Section 1. In particular, for $0 \le n \le e+1$, k_n is the subfield of $\mathbb{Q}(\zeta_p)$ of degree 2^n, and $L_n = L_0 k_n$. We see from the class number formula [15, Theorem 4.17] that the relative class numbers $h^-_{L_n}$ and $h^-_n = h^-_{\mathcal{F}_n}$ are related by

$$h^-_n = 2 \times \frac{h^-_{L_{n+1}}}{h^-_{L_n}}, \tag{2.1}$$

for $0 \le n \le e$. Here, we have used the fact that the unit indices of L_n and $\mathcal{F}_n$ are 1 (Conner and Hurrelbrink [2, Lemma 13.5]). We see that the class numbers $h^-_{L_n}$ enjoy Iwasawa type "class number formula" from (2.1) and our results on the class group A_n.

Proposition 2.1. *For $f+1 \le n \le e$, $\mathrm{ord}_2(h^-_{L_n})$ equals $(2^f-1)n+\nu$ or $2^f n+\nu$ according as $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$ with some integer ν depending on p and L_0.*

Proposition 2.2. *Under the setting and the assumption in Theorem 1.4(ii) or 1.5(ii), for $n^\pm_p + 1 \le n \le f$, $\mathrm{ord}_2(h^-_{L_n})$ equals $2^n + (b^\pm_p - 1)n + \nu$ or $2^n + b^\pm_p n + \nu$ according as $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$ ($\ell \in \mathbb{P}_\pm$) with some integer ν depending on p and L_0.*

For example, when $p = 65537$, we have $\mathrm{ord}_2(h^-_{L_n}) = 2^n + 4n + \nu$ with $4 \le n \le 11$ and $\mathrm{ord}_2(h^-_{L_n}) = 2^{11}n + \nu'$ with $12 \le n \le 15$ for every $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ with $\ell \in \mathbb{P}$.

Proofs of Propositions 2.1 and 2.2. For $f+1 \le n \le e$, we see from (2.1) that

$$\mathrm{ord}_2(h_{L^-_n}) = \sum_{j=f}^{n-1} \mathrm{ord}_2\left(\frac{h^-_n}{2}\right) + \mathrm{ord}_2(h_{L^-_f}).$$

By Propositions 1.1 and 1.2, $\mathrm{ord}_2(h_n^-) = 2^f$ or $2^f + 1$ according as $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$. From this, we obtain Proposition 2.1. Under the setting and the assumption of Theorem 1.4(ii) or Theorem 1.5(ii), we see from the theorem that for $n_p^{\pm} \leq n \leq f-1$, $\mathrm{ord}_2(h_n^-) = 2^n + b_p^{\pm}$ or $2^n + b_p^{\pm} + 1$ according as $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$. From this and (2.1), we obtain Proposition 2.2. □

Remark 2.1. Let us refer to the papers of Ferrero [3] and Kida [8]. Let $\mathbb{B}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_2$-extension, and $\mathbb{B}_n$ its nth layer with $n \geq 0$. Let N be an imaginary quadratic field, and put $N_n = N\mathbb{B}_n$ with $0 \leq n \leq \infty$. Let F_n be the imaginary quadratic subextension of the $(2,2)$-extension $N_{n+1}/\mathbb{B}_n$ with $F_n \neq N_{n+1}$. Ferrero and Kida independently computed the Iwasawa lambda invariant of the cyclotomic $\mathbb{Z}_2$-extension N_∞/N by studying the 2-part of the class group of F_n for sufficiently large n. Propositions 2.1 and 2.2 for the finite tower L_e/L_0 are analogous to the above classical result for the $\mathbb{Z}_2$-tower N_∞/N.

Remark 2.2. In Proposition 2.2, the "μ-invariant" is positive ! This is because the prime 2 splits completely in $k_f/\mathbb{Q}$ and ramifies in L_0. Let us recall here a paper [6] of Iwasawa, where he constructed (non-cyclotomic) $\mathbb{Z}_p$-extensions with positive μ-invariants. Our reason for positive μ is almost the same to that in [6].

Remark 2.3. Iwasawa type "class number formula" is already known for a finite tower inside the pth cyclotomic field in Example in Lehmer [10, page 607], a table in Schoof [12, Appendix] and [4, Theorem 3]. For this "formula", the "μ-invariant" is zero.

Remark 2.4. For $0 \leq n \leq e-1$, we see that p splits completely in $\mathbb{Q}(2^{1/2^{n+1}})/\mathbb{Q}$ if and only if $0 \leq n \leq f-1$. This is because p splits completely in $\mathbb{Q}(2^{1/2^{\tilde{f}}})$ and the primes over p remains prime in $\mathbb{Q}(2^{1/2^{e+1}})/\mathbb{Q}(2^{1/2^{\tilde{f}}})$ ([5, Lemma 3]). Therefore, Proposition 1.2 says that the 4-rank of A_n is positive if and only if p splits completely in $\mathbb{Q}(2^{1/2^{n+1}})$. This assertion is analogous to several classical results on "governing field" for the 2-part of the class group of quadratic fields such as those in [1, 11, 16].

Remark 2.5. Under the setting and the assumption of Theorem 1.4(ii) or Theorem 1.5(ii), the theorem implies that $r_4(A_n) = 2^n$ for $0 \leq n \leq n_p^{\pm} - 1$ and $r_4(A_n) = b_p^{\pm}$ for $n_p^{\pm} \leq n \leq f-1$. On the other hand, Yue [18] generalized

a result of Rédei [14] and gave a formula for the 4-rank of the class group of a relative quadratic extension. It would be possible to derive Proposition 1.2 and the above mentioned result on $r_4(A_n)$ from his formula using the results in Sections 3 and 4 and Lemmas 5.1, 5.2 of this paper.

3 Some lemmas

In this section, we collect several lemmas which are necessary to prove the theorems. Some of them are known to specialists. For a number field N, let $\mathcal{O}_N$ be the ring of integers of N, and $E_N = \mathcal{O}_N^\times$ the group of units of N. The following lemma is given in [5, Lemma 6].

Lemma 3.1. *Let k be a totally real number field of degree n. Assume that the narrow class number of k is odd and that the prime 2 splits completely in k; $2 = \mathfrak{q}_1 \cdots \mathfrak{q}_n$. Then, the map*

$$E_k \to (\mathcal{O}_k/4)^\times = (\mathcal{O}_k/\mathfrak{q}_1^2)^\times \oplus \cdots \oplus (\mathcal{O}_k/\mathfrak{q}_n^2)^\times; \quad \epsilon \to \epsilon \bmod 4$$

is surjective.

For a CM field N with its maximal real subfield N^+, an ideal class $c \in Cl_N$ is ambiguous when $c^J = c$ where J is the nontrivial automorphism of N over N^+. The number of ambiguous classes is denoted by $a(N)$, and is given by the following lemma (see Yokoi [17]).

Lemma 3.2. *For a CM field N,*

$$a(N) = h_{N^+} \times \frac{2^{t_N - 1}}{[E_{N^+} : E_{N^+} \cap \mathcal{N}(N^\times)]}.$$

Here, t_N is the number of prime divisors of N^+ (finite or infinite) which are ramified in N, and $\mathcal{N}$ is the norm map form N to N^+.

Let $\mathcal{M}/F$ be the Hilbert 2-class field of a number field F, namely, the class field corresponding to $A_F = Cl_F(2)$. Via the reciprocity law map, we identify A_F with $\mathrm{Gal}(\mathcal{M}/F)$:

$$A_F = \mathrm{Gal}(\mathcal{M}/F); \quad c \leftrightarrow \rho_c.$$

Here, ρ_c is the Frobenius automorphism associated to the ideal class c. Let K/F be an unramified quadratic extension, and let $B = \mathrm{Gal}(\mathcal{M}/K) \subset A_F$.

Clearly, $B^2 \subseteq A_F^2$. For an abelian group A, let ${}_2A$ be the subgroup of A consisting of elements $c \in A$ with $c^2 = 1$. The following lemma has its origin in [13], and is used repeatedly for studying the 4-rank of quadratic fields.

Lemma 3.3. *Under the above setting, the following three conditions are equivalent with each other.*

(i) *The unramified quadratic extension K/F extends to an unramified cyclic quartic extension.*

(ii) *For any $c \in {}_2A_F$, the automorphism ρ_c is trivial on K.*

(iii) $B^2 \subsetneq A_F^2$.

PROOF. First, we show (i) $\Rightarrow$ (ii). Assume that K/F extends to an unramified cyclic quartic extension N/F. Then, for $c \in {}_2A_F$, the restriction $\rho_{c|N} \in \mathrm{Gal}(N/F)$ is trivial or of order 2. This implies that the restriction $\rho_{c|K}$ to the quadratic subextension K of the cyclic extension N/F is trivial. Next, to show (ii) $\Rightarrow$ (iii), assume to the contrary that $B^2 = A_F^2$. Choose an element $c \in A_F$ such that ρ_c is nontrivial on K. Then, as $B^2 = A_F^2$, there exists $c_1 \in B$ with $c_1^2 = c^2$. Let $d = cc_1^{-1}$. Then, $d^2 = 1$ and hence $d \in {}_2A_F$. However, we see that ρ_d is nontrivial on K because ρ_c is nontrivial and ρ_{c_1} is trivial on K. Finally, to show (iii) $\Rightarrow$ (i), assume again to the contrary that K/F never extends to an unramified cyclic quartic extension. Let M_A/F (resp. M_B/K) be the subextension of $\mathcal{M}/F$ (resp. $\mathcal{M}/K$) corresponding to A_F^2 (resp. B^2) by Galois theory. As $B \subset A_F$, we have $M_A \subseteq M_B$. Let N/K be a quadratic subextension of M_B/K. Then, from the assumption, we see that the abelian quartic extension N/F is a $(2,2)$-extension. This implies that $N \subseteq M_A$, and hence $M_B \subseteq M_A$. Therefore, we obtain $M_A = M_B$, and hence $B^2 = A_F^2$. □

Remark 3.1. Let $\mathfrak{q}_i$ $(1 \leq i \leq r)$ be some prime ideals of F, and let t be an odd integer. When ${}_2A_F$ is generated by the ideal classes $[\mathfrak{q}_i^t]$, the condition (ii) in Lemma 3.3 holds if and only if these prime ideals $\mathfrak{q}_i$ split in K/F.

The following lemma is well known ([15, Exercise 9.3]).

Lemma 3.4. *Let $\mathfrak{q}$ be a prime ideal of F over 2. Let $K = F(\sqrt{w})$ be a quadratic extension with $w \in F^\times$ relatively prime to $\mathfrak{q}$. Let $a \geq 1$ be an integer with $\mathfrak{q}^a \| 2$. Then,* (i) *the prime ideal $\mathfrak{q}$ is unramified in K if and only if $w \equiv u^2 \bmod \mathfrak{q}^{2a}$ for some $u \in \mathcal{O}_F$, and* (ii) *it splits in K if and only if $w \equiv u^2 \bmod \mathfrak{q}^{2a+1}$ for some $u \in \mathcal{O}_F$.*

As in Section 1, let $\Lambda = \mathbb{Z}_2[[T]]$. Let A be a finite cyclic Λ-module with $\bar{h} = |A|$. Denote by $I_A \subset \Lambda$ the annihilator of the Λ-module A so that $A \cong \Lambda/I_A$ as Λ-modules. Assume that (i) $j = (1+T)^{2^n}$ acts on A via (-1)-multiplication and that (ii) $r_2(A) = 2^n$ but $\mathrm{ord}_2(\bar{h}) \geq 2^n+1$. The assumption (i) implies that $(1+T)^{2^n} + 1 \in I_A$. As in (1.4) and (1.5), we put

$$s = \left\lceil \frac{\mathrm{ord}_2(\bar{h})}{2^n} \right\rceil, \quad a = 2^n s - \mathrm{ord}_2(\bar{h}), \quad b = 2^n - a,$$

so that we have $s \geq 2$, $a \geq 0$ and $b \geq 1$. The following algebraic assertion is essentially contained in [5, Proposition 3].

Lemma 3.5. *Under the above setting and assumptions, we have*

$$I_A = (2^s,\, 2^{s-1}T^b, (1+T)^{2^n} + 1),$$

and hence

$$A \cong (\mathbb{Z}/2^{s-1})^{\oplus a} \oplus (\mathbb{Z}/2^s)^{\oplus b} \tag{3.1}$$

as abelian groups.

Proof. We can write

$$A = \bigoplus_{i=1}^{r} (\mathbb{Z}/2^i)^{\oplus t_i}$$

as abelian groups for some integers $r \geq 1$, $t_i \geq 0$ $(1 \leq i \leq r-1)$ and $t_r \geq 1$. As the 2-rank of A is 2^n, we have

$$\sum_{i=1}^{r} t_i = 2^n, \quad \text{and} \quad \sum_{i=1}^{r} i t_i = \mathrm{ord}_2(\bar{h}). \tag{3.2}$$

We see that $r \geq 2$ as $\mathrm{ord}_2(\bar{h}) \geq 2^n + 1$. We observe that

$$B := A^{2^{r-2}} = (\mathbb{Z}/2)^{\oplus t_{r-1}} \oplus (\mathbb{Z}/4)^{\oplus t_r}, \quad \text{and} \quad 1 \leq t_{r-1} + t_r \leq 2^n.$$

Let $I_B \subset \Lambda$ be the annihilator of the cyclic Λ-module B. Then, we see immediately from [5, Proposition 3] that $t_{r-1} + t_r = 2^n$ and

$$I_B = (4,\, 2T^{t_r},\, (1+T)^{2^n} + 1). \tag{3.3}$$

It follows from (3.2) that $t_i = 0$ for $1 \le i \le r-2$ and that

$$t_{r-1} + t_r = 2^n \quad \text{and} \quad (r-1)t_{r-1} + rt_r = \mathrm{ord}_2(\bar{h}).$$

Then, noting that $t_r \ge 1$, we observe that $r = s$, $t_{r-1} = a$ and $t_r = b$ from the very definitions of s, a and b. Therefore, we obtain the assertion (3.1) on the abelian group A. Noting that $B = A^{2^{r-2}}$ with $r = s$, we see from (3.3) that the ideal I of Λ generated by 2^s, $2^{s-1}T^b$ and $(1+T)^{2^n}+1$ is contained in I_A. Since the abelian group Λ/I is isomorphic to the righthand side of (3.1), we obtain $I = I_A$. □

4 Arithmetic of the tower $k_e/\mathbb{Q}$

We use the same notation as in the previous sections. In particular, $p = 2^{e+1}q + 1$ is a prime number with $2 \nmid q$, and k_n is the subfield of $\mathbb{Q}(\zeta_p)$ of degree 2^n. In what follows, we let

$$h = h_{k_e}$$

be the class number of k_e, which is odd by [15, Theorem 10.4]. The class number of k_n for $n \le e$ is a divisor of h because $k_e/\mathbb{Q}$ is totally ramified at p. Let $\mathfrak{p}_n$ be the unique prime ideal of k_n over p, so that we have $(p) = \mathfrak{p}_n^{2^n}$. For $0 \le n \le e$, there is an element d_n of k_n such that $k_{n+1} = k_n(\sqrt{d_n})$. The element d_n is totally positive when $0 \le n \le e-1$, and it is totally negative when $n = e$. Since k_{n+1}/k_n is ramified only at $\mathfrak{p}_n$ and h is odd, we can choose d_n so that it satisfies

$$(d_n) = \mathfrak{p}_n^h \quad \text{and} \quad d_n \equiv u^2 \bmod 4 \tag{4.1}$$

for some $u \in \mathcal{O}_{k_n}$. Here, the last congruence holds by Lemma 3.4(i). Further, as 2 splits completely in $k_{\tilde{f}}/\mathbb{Q}$ and the primes over 2 remain prime in $k_{e+1}/k_{\tilde{f}}$ ([5, Lemma 3]), we see from Lemma 3.4(ii) that

$$d_n \equiv 1 \bmod 8 \quad \text{for } 0 \le n \le \tilde{f}-1 \tag{4.2}$$

but

$$d_n \not\equiv u^2 \bmod 8 \quad \text{for } \tilde{f} \le n \le e \tag{4.3}$$

for any $u \in \mathcal{O}_{k_n}$. Further, we have

$$\mathcal{F}_n = k_n(\sqrt{2d_n}), \quad k_n(\sqrt{-2d_n}) \quad \text{or} \quad k_n(\sqrt{-2\ell d_n})$$

according as $L_0 = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$.

We put $G_n = \mathrm{Gal}(k_n/\mathbb{Q})$, which is a cyclic group of order 2^n. We fix a prime ideal $\mathfrak{q}_f$ of k_f over 2, and for $0 \leq n \leq f$, we put $\mathfrak{q}_n = N_{f/n}\mathfrak{q}_f$. Here, $N_{f/n}$ denotes the norm map from k_f to k_n. Then, $\mathfrak{q}_n$ is a prime ideal of k_n over 2, and

$$(2) = \prod_{\sigma \in G_n} \mathfrak{q}_n^{\sigma}.$$

When ($f \leq e-1$ and) $f+1 \leq n \leq e$, we denote the unique prime ideal of k_n over $\mathfrak{q}_f^{\sigma}$ with $\sigma \in G_f$ by the same symbol $\mathfrak{q}_f^{\sigma}$. Now, we choose and fix a prime number $\ell \in \mathbb{P}$. We put

$$2^* = \begin{cases} -2, & \text{when } L_0 = \mathbb{Q}(\sqrt{-2}) \text{ or } \mathbb{Q}(\sqrt{-2\ell}) \text{ with } \ell \in \mathbb{P}_+, \\ 2, & \text{when } L_0 = \mathbb{Q}(\sqrt{2}) \text{ or } \mathbb{Q}(\sqrt{-2\ell}) \text{ with } \ell \in \mathbb{P}_-, \end{cases}$$

and

$$\ell^* = \begin{cases} \ell, & \text{when } \ell \in \mathbb{P}_+, \\ -\ell, & \text{when } \ell \in \mathbb{P}_-. \end{cases}$$

Then, we have

$$2^*\ell^* = -2\ell, \quad \ell^* \equiv 1 \bmod 8, \quad \text{and} \quad \left(\frac{\ell^*}{p}\right) = -1$$

for every ℓ in $\mathbb{P} = \mathbb{P}_+ \sqcup \mathbb{P}_-$. As $h_{k_{e+1}}$ is odd, the narrow class number of k_f is odd. Therefore, by Lemma 3.1, we can choose an element ω of k_f such that $\mathfrak{q}_f^h = (\omega)$ and

$$\frac{\omega}{(2^*)^h} \equiv 1 \bmod \mathfrak{q}_f^2 \quad \text{and} \quad \omega \equiv 1 \bmod (\mathfrak{q}_f^{\sigma})^2$$

for $\sigma \in G_f$ with $\sigma \neq 1_f$. Here, 1_n denotes the identity element of G_n. For $0 \leq n \leq f-1$, we put $\omega_n = N_{f/n}\omega$. Then we see that $\mathfrak{q}_n^h = (\omega_n)$ and

$$\frac{\omega_n}{(2^*)^h} \equiv 1 \bmod \mathfrak{q}_n^2 \quad \text{and} \quad \omega_n \equiv 1 \bmod (\mathfrak{q}_n^{\sigma})^2 \tag{4.4}$$

for $\sigma \in G_n$ with $\sigma \neq 1_n$. When $f \leq n \leq e$ and $L_0 = \mathbb{Q}(\sqrt{\pm 2})$, we simply set $\omega_n = \omega$. When $f \leq n \leq e$ and $L_0 = \mathbb{Q}(\sqrt{-2\ell})$, we set $\omega_n = \omega$ or $\ell^*\omega$ according as ω is a quadratic residue module $\mathfrak{p}_f$ or not, so that ω_n is a quadratic residue module $\mathfrak{p}_n$ by (1.1). Then, in any case, we see that ω_n satisfies the congruence (4.4) for any $0 \leq n \leq e$ as $\ell^* \equiv 1 \bmod 8$ and that

$$\omega_n \equiv N_{f/n}\omega_f \bmod (k_n^{\times})^2 \tag{4.5}$$

for $0 \leq n \leq f-1$. From the above, we obtain

Lemma 4.1. *When $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ with $\ell \in \mathbb{P}$, ω_n is a quadratic residue modulo $\mathfrak{p}_n$ for each $0 \leq n \leq e$.*

Let V_n be the submodule of $k_n^\times/(k_n^\times)^2$ generated by the class $[\omega_n]$ over the group ring $\mathbb{F}_2[G_n]$, and let W_n be the submodule of $k_n^\times/(k_n^\times)^2$ generated by the class $[\ell^*]$ and V_n. (We need the module W_n only for the case $L_0 = \mathbb{Q}(\sqrt{-2\ell})$.) We denote by $\widetilde{V}_n$ and $\widetilde{W}_n$ the images of V_n and W_n under the lifting map $k_n^\times/(k_n^\times)^2 \to \mathcal{F}_n^\times/(\mathcal{F}_n^\times)^2$, respectively.

Lemma 4.2. *Under the above setting, we have*

$$\dim_{\mathbb{F}_2} V_n = \dim_{\mathbb{F}_2} \widetilde{V}_n = 2^n \quad or \quad 2^f,$$

and

$$\dim_{\mathbb{F}_2} W_n = \dim_{\mathbb{F}_2} \widetilde{W}_n = 2^n + 1 \quad or \quad 2^f + 1$$

according as $0 \leq n \leq f-1$ or $f \leq n \leq e$.

Proof. We show the assertion only for W_n. The assertion for V_n is shown similarly. We easily see that

$$\dim_{\mathbb{F}_2} \widetilde{W}_n \leq \dim_{\mathbb{F}_2} W_n \leq 2^n + 1 \quad \text{or} \quad 2^f + 1.$$

Hence, it suffices to show that the dimension of $\widetilde{W}_n$ equals $2^n + 1$ or $2^f + 1$. We show it only for case $n = e$. It is shown similarly for the other cases. Put

$$x = \ell^s \times \prod_{\sigma \in G_f} (\omega_f^\sigma)^{t_\sigma} \in k_f^\times$$

with $s, t_\sigma = 0, 1$. Assume that x is a square in $\mathcal{F}_e$. Then, as $\mathcal{F}_e = k_e(\sqrt{-2\ell d_e})$, we observe that x or $y = -2\ell d_e x$ is a square in k_e. When x is a square in k_e, the ideal

$$(x) = (\ell)^{s+u} \times \prod_{\sigma \in G_f} (\mathfrak{q}_f^\sigma)^{ht_\sigma}$$

is a square of an ideal of k_e. Here, $u = 0$ or $\sum_{\sigma \in G_f} t_\sigma$ according as $\omega_f = \omega$ or $\ell^*\omega$. However, since ℓ and 2 are unramified in k_e and $h = h_{k_e}$ is odd, we see that $s + u$ is even and $t_\sigma = 0$ for $\sigma \in G_f$, from which follows $s = 0$. Further, since $\mathfrak{p}_e^h \| y$ and h is odd, y is not a square in k_e. □

By Lemma 4.2 and (4.5), we see that the lifting map $k_n^\times/(k_n^\times)^2 \to k_{n+1}^\times/(k_{n+1}^\times)^2$ induces an injection $V_n \to V_{n+1}$, which is bijective for $f \le n \le e-1$. Therefore, letting $V = V_f$, we regard V_n as a submodule of V when $0 \le n \le f-1$, and we identify V_n with V when $f+1 \le n \le e$. We denote the group ring $\mathbb{F}_2[G_f]$ by $\mathcal{R}$:

$$\mathcal{R} = \mathbb{F}_2[G_f].$$

We also see from Lemma 4.2 that $V = V_f = \mathcal{R} \cdot \omega_f$ is free and cyclic over $\mathcal{R}$, and we fix an isomorphism

$$\iota : V \to \mathcal{R} \tag{4.6}$$

sending ω_f to the identity element 1_f of G_f. For $0 \le n \le f$, we denote the element of $\mathcal{R}$ corresponding to the norm map $N_{f/n}$ from k_f to k_n also by $N_{f/n}$. Let $J_n = (N_{f/n})$ be the ideal of $\mathcal{R}$ generated by $N_{f/n}$. Then, by the definition of V_n and (4.5), we obtain

$$\iota(V_n) = J_n \tag{4.7}$$

for $0 \le n \le f$. Let ρ be a generator of the cyclic group G_f of order 2^f. For $0 \le i \le 2^f$, let U_i be the ideal of $\mathcal{R}$ generated by $(1+\rho)^i$. We have a filtration

$$U_0 = \mathcal{R} \supset U_1 \supset \cdots \supset U_{2^f-1} \supset U_{2^f} = \{0\}.$$

Lemma 4.3. (i) *The ideals U_i are all the ideals of $\mathcal{R}$, and $\dim_{\mathbb{F}_2} U_i = 2^f - i$ as a vector space over $\mathbb{F}_2$. In particular, the ideals of $\mathcal{R}$ are parametrized by their dimensions over $\mathbb{F}_2$.*

(ii) *For $0 \le n \le f$, $J_n = U_{2^f-2^n}$ and $\dim_{\mathbb{F}_2} J_n = 2^n$. In particular, $J_0 = U_{2^f-1}$ is the smallest nontrivial ideal of $\mathcal{R}$.*

Proof. The first assertion is shown in [5, Lemma 8]. Let us show

$$N_{f/n} = \sum_{j=0}^{2^{f-n}-1} (1+\rho^{2^n})^j = (1+\rho)^{2^f-2^n}.$$

This is obvious for $n = f$. If this holds for n ($\le f$), then we see that

$$N_{f/(n-1)} = (1+\rho^{2^{n-1}})N_{f/n} = (1+\rho)^{2^{n-1}}(1+\rho)^{2^f-2^n} = (1+\rho)^{2^f-2^{n-1}},$$

and hence the equality holds for $n-1$. Therefore, we obtain the second assertion. □

Consider an element α of k_f of the form

$$\alpha = \prod_{\sigma \in G_f} (\omega_f^\sigma)^{a_\sigma} \quad \text{with} \quad a_\sigma = 0,\, 1$$

such that

$$\alpha \equiv 1 \bmod (\mathfrak{q}_f^\sigma)^3 \quad \text{or} \quad \frac{\alpha}{(2^*)^h} \equiv 1 \bmod (\mathfrak{q}_f^\sigma)^3 \tag{4.8}$$

according as $a_\sigma = 0$ or 1. Let Q be the submodule of V generated by the classes $[\alpha]$ for all such α. We easily see that Q is a $\mathcal{R}$-submodule of V. Since

$$(2^*)^h \equiv N_{f/0}\omega_f \bmod (\mathbb{Q}^\times)^2, \tag{4.9}$$

we see that $[2^*] \in Q$ and that Q is nontrivial. We put $\mathcal{Q} = \iota(Q) \subseteq \mathcal{R}$. This is a nontrivial ideal of $\mathcal{R}$. The following simple lemma on the ideal $\mathcal{Q}$ plays a crucial role for showing Theorems 1.4–1.6.

Lemma 4.4. *The ideal $\mathcal{Q}$ depends only on whether $2^* = -2$ or 2, and not on individual L_0's.*

Proof. The element $\omega \in k_f$ defined by (4.4) depends only on whether $2^* = -2$ or 2. Since $\omega_f = \omega$ or $\ell^*\omega$ and $\ell^* \equiv 1 \bmod 8$, the submodule Q of V consisting of elements α satisfying (4.8) depends only on the value 2^*. Hence, the ideal $\mathcal{Q}$ also depend only on the value of 2^*. □

5 Proofs of Theorems 1.1, 1.2, 1.4 and 1.5

First, we introduce some notation which we use in Sections 5 and 6. The prime ideals $\mathfrak{p}_n$ and $\mathfrak{q}_n^\sigma$ of k_n ramify in $\mathcal{F}_n$, where σ runs over the Galois group G_n (resp. G_f) when $0 \le n \le f-1$ (resp. $f \le n \le e$). We denote by $\mathfrak{P}_n$ and $\mathfrak{Q}_n^\sigma$ the prime ideals of $\mathcal{F}_n$ over $\mathfrak{p}_n$ and $\mathfrak{q}_n^\sigma$, so that we have $\mathfrak{p}_n = \mathfrak{P}_n^2$ and $\mathfrak{q}_n^\sigma = (\mathfrak{Q}_n^\sigma)^2$ in $\mathcal{F}_n$, respectively. When $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ with $\ell \in \mathbb{P}$, the prime number ℓ remains in k_n by (1.1), and ramifies in $\mathcal{F}_n$. We denote by $\mathfrak{L}_n$ the prime ideal of $\mathcal{F}_n$ over (ℓ), so that we have $(\ell) = \mathfrak{L}_n^2$ in $\mathcal{F}_n$. For $0 \le n \le e$, we put

$$M_n^1 = \mathcal{F}_n(\sqrt{\alpha} \;\big|\; [\alpha] \in \widetilde{V}_n).$$

When $L_0 = \mathbb{Q}(\sqrt{-2\ell})$, we put

$$M_n^0 = \mathcal{F}_n(\sqrt{\ell^*}) \quad \text{and} \quad M_n^2 = M_n^0 M_n^1 = \mathcal{F}_n(\sqrt{\alpha} \;\big|\; [\alpha] \in \widetilde{W}_n).$$

These extensions of $\mathcal{F}_n$ play an important role for proving our theorems.

In the rest of this section, we prove Theorems 1.1, 1.2, 1.4 and 1.5 for $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$. So, n runs over $0 \leq n \leq e-1$. We begin with showing Proposition 1.1.

Proof of Proposition 1.1. We show the assertion only for $L_0 = \mathbb{Q}(\sqrt{-2\ell})$. It is shown similarly for $L_0 = \mathbb{Q}(\sqrt{-2})$. We use Lemma 3.2 for the imaginary cyclic field $\mathcal{F}_n = k_n(\sqrt{-2\ell d_n})$ noting that $\mathcal{F}_n^+ = k_n$. Let g_n be the number of ambiguous classes in A_n, namely g_n is the 2-part of the ambiguous class number $a(\mathcal{F}_n)$. Let r be the 2-rank of $A_{\mathcal{F}_n}$. Then we see that $g_n = 2^r$ because a class $c \in A_n = A_n^-$ is ambiguous if and only if $c^2 = 1$. Let $E_{k_n}^+$ be the subgroup of E_{k_n} consisting of totally positive units. Then it follows that

$$E_{k_n}^2 \subseteq E_{k_n} \cap \mathcal{N}(\mathcal{F}_n^\times) \subseteq E_{k_n}^+.$$

Since the class number of the imaginary cyclic field k_{e+1} is odd, so is the narrow class number of k_n. Therefore, a unit $\epsilon \in E_{k_n}$ is totally positive if and only if it is a square in k_n ([2, Corollary 13.10]). Hence, $E_{k_n} \cap \mathcal{N}(\mathcal{F}_n^\times)$ coincides with $E_{k_n}^2$, and

$$[E_{k_n} : E_{k_n} \cap \mathcal{N}(\mathcal{F}_n^\times)] = 2^{2^n}.$$

The primes of $\mathcal{F}_n^+ = k_n$ ramified in $\mathcal{F}_n$ are prime divisors over p, ℓ and 2 and infinite prime divisors. The number $t_{\mathcal{F}_n}$ of all such primes equals

$$t_{\mathcal{F}_n} = 1 + 1 + 2^n + 2^n \quad \text{or} \quad 1 + 1 + 2^f + 2^n$$

according as $0 \leq n \leq f-1$ or $f \leq n \leq e-1$. Accordingly, we see from Lemma 3.2 that $g_n = 2^{2^n+1}$ or 2^{2^f+1}. Now, we obtain the assertion as $g_n = 2^r$. □

Lemma 5.1. (i) *The case $L_0 = \mathbb{Q}(\sqrt{-2})$. The group ${}_2A_n$ is generated by the ideal class $[\mathfrak{Q}_n^h]$ over $\mathbb{F}_2[G_n]$.*

(ii) *The case $L_0 = \mathbb{Q}(\sqrt{-2\ell})$. The group ${}_2A_n$ is generated by the ideal classes $[\mathfrak{P}_n^h]$ and $[\mathfrak{Q}_n^h]$ over $\mathbb{F}_2[G_n]$.*

Proof. We show the assertion for the case where $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ and $n = f$. It is shown similarly for the other cases. We already know that $(\mathfrak{P}_f^h)^2 = \mathfrak{p}_f^h$ and $(\mathfrak{Q}_f^h)^2 = \mathfrak{q}_f^h$ are principal ideals. Let S_f be the subgroup of

${}_2A_f$ generated by the classes $[\mathfrak{P}_f^h]$ and $[\mathfrak{Q}_f^h]$ over $\mathbb{F}_2[G_f]$. By Proposition 1.1, it suffices to show that the 2-rank of S_f equals 2^f+1. Assume that

$$(\mathfrak{P}_f^h)^s \prod_{\sigma\in G_f} (\mathfrak{Q}_f^{\sigma h})^{t_\sigma} = (\alpha)$$

for some $\alpha \in \mathcal{F}_f^\times$ with $s,\, t_\sigma = 0,\, 1$. Then it follows that

$$(\alpha^2) = (\mathfrak{p}_f^h)^s \prod_{\sigma\in G_f} (\mathfrak{q}_f^{\sigma h})^{t_\sigma} = (a)$$

for some $a \in k_f^\times$ because $h = h_{k_e}$. We see that $a\epsilon = \alpha^2$ for some unit ϵ of k_f because the unit index of $\mathcal{F}_f$ is 1 ([2, Corollary 13.10]). Therefore, since $\mathcal{F}_f = k_f(\sqrt{-2\ell d_f})$, $a\epsilon$ or $a\epsilon \times (-2\ell d_f)$ is a square in k_f. This implies that the principal ideal (a) or $(2a\ell d_f)$ of k_f is a square in the group of ideals k_f. For the first case, we see that $s = t_\sigma = 0$ for all σ in G_f since h is odd. The second case is impossible because l remains prime in k_f. Thus, we have shown that the 2-rank of S_f is 2^f+1. □

Lemma 5.2. (i) *The case $L_0 = \mathbb{Q}(\sqrt{-2})$. The extension $M_n^1/\mathcal{F}_n$ is the class field corresponding to A_n/A_n^2.*

(ii) *The case $L_0 = \mathbb{Q}(\sqrt{-2\ell})$. The extension $M_n^2/\mathcal{F}_n$ is the class field corresponding to A_n/A_n^2, and the subextension $M_n^1/\mathcal{F}_n$ is the maximal intermediate field of $M_n^2/\mathcal{F}_n$ in which the prime ideal $\mathfrak{P}_n$ over p splits completely.*

Proof. We show the assertion (ii) for $L_0 = \mathbb{Q}(\sqrt{-2\ell})$. The assertion (i) is shown similarly. We see from Lemma 4.2 that the 2-rank of the abelian group $\mathrm{Gal}(M_n^2/\mathcal{F}_n)$ of exponent 2 equals 2^n+1 or 2^f+1 according as $0 \le n \le f-1$ or $f \le n \le e-1$. Then, we observe from Proposition 1.1 that for showing the first assertion of (ii), it suffices to show that the extension $M_n^2/\mathcal{F}_n$ is unramified. To show that it is unramified, it suffices to show that the subextensions $\mathcal{F}_n(\sqrt{\ell^*})/\mathcal{F}_n$ and $\mathcal{F}_n(\sqrt{\omega_n^\sigma})/\mathcal{F}_n$ $(\sigma \in G_n)$ are unramified. As $\mathcal{F}_n/\mathbb{Q}$ is a Galois extension, $\mathcal{F}_n(\sqrt{\omega_n^\sigma})/\mathcal{F}_n$ is unramified if and only if so is $\mathcal{F}_n(\sqrt{\omega_n})/\mathcal{F}_n$. Since $\ell^* \equiv 1 \bmod 8$, $\mathcal{F}_n(\sqrt{\ell^*})/\mathcal{F}_n$ is unramified outside ℓ by Lemma 3.4. It is unramified also at ℓ since $\mathcal{F}_n/k_n$ is ramified at ℓ. It follows that $\mathcal{F}_n(\sqrt{\omega_n})/\mathcal{F}_n$ is unramified outside 2 even for the case $\omega_n = \ell^*\omega$. As $\mathcal{F}_n = k_n(\sqrt{2^*\ell^* d_n})$, we have

$$\mathcal{F}_n(\sqrt{\omega_n}) = \mathcal{F}_n(\sqrt{x}) \quad \text{with} \quad x = \frac{\omega_n}{(2^*)^h} \times (\ell^* d_n)^{-1}.$$

Therefore, by (4.1), (4.4) and Lemma 3.4, we see that $\mathcal{F}_n(\sqrt{\omega_n})/\mathcal{F}_n$ is unramified also at 2. Thus, we obtain the first assertion of Lemma 5.2(ii). The element ℓ^* is a quadratic nonresidue modulo $\mathfrak{P}_n$ by (1.1), while ω_n is a quadratic residue modulo $\mathfrak{P}_n$ by Lemma 4.1. Therefore, the second assertion of (ii) follows from the first one. □

We denote by $\mathcal{M}_n = \mathcal{M}_{\mathcal{F}_n}$ the Hilbert 2-class field of $\mathcal{F}_n$, so that we can identify $\mathrm{Gal}(\mathcal{M}_n/\mathcal{F}_n)$ with the class group A_n. When $L_0 = \mathbb{Q}(\sqrt{-2\ell})$, we put

$$B_n = \mathrm{Gal}(\mathcal{M}_n/M_n^0) \quad \text{and} \quad C_n = \langle [\mathfrak{P}_n^h] \rangle.$$

We see that B_n is a Λ-submodule of $A_n = \mathrm{Gal}(\mathcal{M}_n/\mathcal{F}_n)$ because M_n^0 is Galois over $\mathbb{Q}$. The group C_n is also a Λ-submodule of A_n because the ideal $\mathfrak{P}_n$ is invariant under the action of $\Gamma_n = \mathrm{Gal}(\mathcal{F}_n/\mathbb{Q})$. It follows that

$$C_n \cong \Lambda/(2, T).$$

Proposition 5.1. (i) *The case $L_0 = \mathbb{Q}(\sqrt{-2})$. The Λ-module A_n is cyclic.*

(ii) *The case $L_0 = \mathbb{Q}(\sqrt{-2\ell})$. We have a decomposition $A_n = B_n \oplus C_n$ of Λ-modules. The Λ-module B_n is cyclic, and $\dim_{\mathbb{F}_2} B_n/B_n^2 = 2^n$ or 2^f according as $0 \le n \le f-1$ or $f \le n \le e-1$.*

Proof. We show the assertion (ii). The assertion (i) is shown similarly. By Lemma 5.2(ii), we see that $\mathfrak{P}_n$ remains prime in the quadratic extension $M_n^0/\mathcal{F}_n$. This implies that $[\mathfrak{P}_n] \notin B_n = \mathrm{Gal}(\mathcal{M}_n/M_n^0)$. It follows that $B_n \cap C_n = \{0\}$, and hence $A_n = B_n \oplus C_n$. We observe that the quadratic extension $M_n^0/\mathcal{F}_n$ does not satisfy the condition (ii) of Lemma 3.3 since $[\mathfrak{P}_n^h] \in {}_2A_n$ and $\mathfrak{P}_n$ remains prime in $M_n^0/\mathcal{F}_n$. Hence, we obtain $A_n^2 = B_n^2$ by Lemma 3.3. From this and Lemma 5.2(ii), we see that the intermediate field of $\mathcal{M}_n/M_n^0$ corresponding to B_n^2 coincides with $M_n^2 = M_n^0 M_n^1$. Therefore, we obtain an isomorphism

$$B_n/B_n^2 = \mathrm{Gal}(M_n^2/M_n^0) \cong \mathrm{Gal}(M_n^1/\mathcal{F}_n),$$

which is compatible with the action of Γ_n. The submodule $\widetilde{V}_n$ of $\mathcal{F}_n^\times/(\mathcal{F}_n^\times)^2$ is naturally regarded as a module over $R_n = \mathbb{Z}_2[\Gamma_n]$, and hence as a module over Λ. The module $\widetilde{V}_n$ is cyclic over Λ since V_n is cyclic over $\mathbb{F}_2[G_n]$. The Kummer pairing

$$\mathrm{Gal}(M_n^1/\mathcal{F}_n) \times \widetilde{V}_n \to \{\pm 1\}; (g, [v]) \to \langle g, v \rangle = (v^{1/2})^{g-1}$$

is nondegenerate and satisfies $\langle g^\gamma, v^\gamma \rangle = \langle g, v \rangle$ for $\gamma \in \Gamma_n$. Therefore, we obtain an isomorphism

$$\mathrm{Gal}(M_n^1/\mathcal{F}_n) \cong H = \mathrm{Hom}(\widetilde{V}_n, \{\pm 1\}), \tag{5.1}$$

which is compatible with the action of Γ_n. Here, $\gamma \in \Gamma_n$ acts on $f \in H$ by the rule $f^\gamma([v]) = f([v]^{\gamma^{-1}})$. Since the Λ-module $\widetilde{V}_n$ is cyclic, we see from (5.1) that $\mathrm{Gal}(M_n^1/\mathcal{F}_n)$ is cyclic over Λ. Hence, so is B_n/B_n^2. It follows that B_n is cyclic over Λ by Nakayama's lemma. The assertion on the dimension of B_n/B_n^2 over $\mathbb{F}_2$ follows from Lemma 4.2 and (5.1). □

Lemma 5.3. *An unramified quadratic extension $N/\mathcal{F}_n$ extends to an unramified cyclic quartic extension if and only if (a) the prime ideals $\mathfrak{Q}_n^\sigma$ ($\sigma \in G_n$) of $\mathcal{F}_n$ over 2 split in N and (b) $N \subseteq M_n^1$ for the case $L_0 = \mathbb{Q}(\sqrt{-2\ell})$.*

Proof. We show the assertion only when $L_0 = \mathbb{Q}(\sqrt{-2\ell})$. It is shown similarly when $L_0 = \mathbb{Q}(\sqrt{-2})$. By Lemma 5.1, the group ${}_2A_n$ is generated by the classes $[\mathfrak{P}_n^h]$ and $[(\mathfrak{Q}_n^\sigma)^h]$ with $\sigma \in G_n$. Then, because of Lemma 3.3 combined with Remark 3.1, we observe that $N/\mathcal{F}_n$ extends to an unramified cyclic quartic extension if and only if the prime ideals $\mathfrak{P}_n$ and $\mathfrak{Q}_n^\sigma$ with $\sigma \in G_n$ split in N. On the other hand, by Lemma 5.2(ii), $\mathfrak{P}_n$ splits in N if and only if $N \subseteq M_n^1$. Thus, we obtain the assertion. □

Lemma 5.4. *The quadratic extension $\mathcal{F}_n(\sqrt{2^*})/\mathcal{F}_n$ extends to an unramified cyclic quartic extension if and only if $0 \le n \le f-1$.*

Proof. We show the assertion when $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ using Lemma 5.3. It is shown similarly when $L_0 = \mathbb{Q}(\sqrt{-2})$. We see that $\mathcal{F}_n(\sqrt{2^*}) \subseteq M_n^1$ by (4.9), and hence the condition (b) in Lemma 5.3 is satisfied. As $\mathcal{F}_n = k_n(\sqrt{2^*\ell^* d_n})$, we have

$$\mathcal{F}_n(\sqrt{2^*}) = \mathcal{F}_n(\sqrt{\ell^* d_n}).$$

By Lemma 3.4 and the congruences (4.2), (4.3), we observe that the prime ideals $\mathfrak{Q}_n^\sigma$ of $\mathcal{F}_n$ over 2 split in $\mathcal{F}_n(\sqrt{2^*})/\mathcal{F}_n$ if and only if $0 \le n \le f-1$. Therefore, we obtain the assertion from Lemma 5.3. □

Let $N_{n,4}/\mathcal{F}_n$ be the composite of all unramified quadratic extensions $N/\mathcal{F}_n$ which extends to an unramified cyclic quartic extension. We see that an unramified quadratic extension $N/\mathcal{F}_n$ extends to an unramified cyclic

quartic extension if and only if $N \subseteq N_{n,4}$ and that $N_{n,4}$ is Galois over $\mathbb{Q}$. We have $N_{e,4} \subseteq M_n^1$ by Lemma 5.3.. Let $V_{n,4}$ be the submodule of V_n such that

$$N_{n,4} = \mathcal{F}_n(\sqrt{\alpha} \;\big|\; [\alpha] \in V_{n,4}),$$

and let

$$\mathcal{R}_{n,4} = \iota(V_{n,4}) \subseteq \mathcal{R} = \mathbb{F}_2[G_f].$$

Here, ι is the fixed isomorphism from $V = V_f$ to $\mathcal{R} = \mathbb{F}_2[G_f]$ in (4.6). As $N_{n,4}$ is Galois over $\mathbb{Q}$, $\mathcal{R}_{n,4}$ is an ideal of $\mathcal{R}$.

Lemma 5.5. (i) *When $0 \le n \le f-1$, the ideal $\mathcal{R}_{n,4}$ coincides with $\mathcal{Q} \cap J_n$ and it is nontrivial. When $f \le n \le e-1$, $\mathcal{R}_{n,4} = \{0\}$.*

(ii) *For each n, the ideal $\mathcal{R}_{n,4}$ depends only on whether $2^* = -2$ or 2, and not on individual L_0's.*

Proof. By Lemma 5.4, $V_{n,4}$ contains the class $[2^*]$ if and only if $0 \le n \le f-1$. By (4.9), we have $\iota([2^*]) = N_{f/0} \in \mathcal{R}$. Therefore, $\mathcal{R}_{n,4}$ contains the ideal $J_0 = (N_{f/0})$ if and only if $0 \le n \le f-1$. On the other hand, J_0 is the smallest nontrivial ideal of $\mathcal{R}$ by Lemma 4.3. This implies that $\mathcal{R}_{n,4}$ is nontrivial if and only if $0 \le n \le f-1$. Let $0 \le n \le f-1$. Let $[\alpha]$ be a nontrivial element of V_n, so that $N = \mathcal{F}_n(\sqrt{\alpha})$ is a quadratic subextension of $M_n^1/\mathcal{F}_n$. Here,

$$\alpha = \prod_{\sigma \in G_f} (\omega_f^\sigma)^{a_\sigma} \quad \text{with} \quad a_\sigma = 0,\, 1,$$

and the elements a_σ satisfy

$$\sum_{\sigma \in G_f} a_\sigma \sigma \in J_n = (N_{f/n}).$$

By Lemma 5.3, $N/\mathcal{F}_n$ extends to an unramified cyclic quartic extension if and only if the prime ideals $\mathfrak{Q}_n^\sigma$ of $\mathcal{F}_n$ over 2 split in $N/\mathcal{F}_n$. For an element $x \in k_n$ relatively prime to $\mathfrak{q}_n^\sigma = \mathfrak{Q}_n^\sigma \cap k_n$, we observe from Lemma 3.4 that the following equivalence holds:

$$\text{the ideal } \mathfrak{Q}_n^\sigma \text{ splits in } \mathcal{F}_n(\sqrt{x})/\mathcal{F}_n \Longleftrightarrow x \equiv 1 \bmod (\mathfrak{q}_n^\sigma)^3.$$

This is because the prime ideal $\mathfrak{q}_n$ of k_n is of degree one for $0 \le n \le f-1$ and ramifies in $\mathcal{F}_n$. Now, we can write

$$N = \mathcal{F}_n(\sqrt{\alpha}) = \mathcal{F}_n(\sqrt{\beta}) \quad \text{with} \quad \beta = \frac{\alpha}{(2^*)^h} \times (\ell^* d_n)^{-1}.$$

As $0 \leq n \leq f-1$, $\ell^* d_n \equiv 1 \bmod 8$ by (4.2). Therefore, because of the above equivalence, we see from (4.8) or the definition of the submodule Q of V that the prime ideals $\mathfrak{Q}_n^\sigma$ with $\sigma \in G_n$ split in $N/\mathcal{F}_n$ if and only if $[\alpha] \in Q \cap V_n$. Then, it follows that $V_{n,4} = Q \cap V_n$, and hence $\mathcal{R}_{n,4} = \mathcal{Q} \cap J_n$ by (4.7). Thus, we obtain the first assertion (i). The assertion (ii) follows from (i) and Lemma 4.4. □

Lemma 5.6. *If $\mathcal{Q} \cap J_{f-1} = J_{f-1}$, then the 4-rank $r_4(A_n)$ equals 2^n for any $0 \leq n \leq f-1$.*

Proof. If $\mathcal{Q} \cap J_{f-1} = J_{f-1}$, then we see from Lemma 5.5 that $\mathcal{R}_{n,4} = \mathcal{Q} \cap J_n = J_n$ for $0 \leq n \leq f-1$. It follows from (4.7) that $V_n = V_{n,4}$. This implies that $r_4(A_n)$ equals $\dim_{\mathbb{F}_2} V_n = 2^n$ by Lemma 4.2 □

Proof of Proposition 1.2. Proposition 1.2 follows from Lemma 5.5. □

Proof of Theorem 1.1. We show the assertion when $L_0 = \mathbb{Q}(\sqrt{-2\ell})$. It is shown similarly when $L_0 = \mathbb{Q}(\sqrt{-2})$. By Proposition 5.1, the Λ-module A_n is a product of the cyclic Λ-module B_n and $C_n = \Lambda/(2, T)$. By Propositions 1.1 and 1.2, $B_n \cong (\mathbb{Z}/2)^{2^f}$ as abelian groups. This implies that the cyclic Λ-module B_n is isomorphic to $\Lambda/(2, T^{2^f})$. □

Proof of Theorem 1.2. We show the assertion when $L_0 = \mathbb{Q}(\sqrt{-2\ell})$. It is shown similarly when $L_0 = \mathbb{Q}(\sqrt{-2})$. By Proposition 5.1, the Λ-module A_n is a product of the cyclic Λ-module B_n and $C_n = \Lambda/(2, T)$. The 2-rank of B_n equals 2^n by Proposition 1.1, and $|B_n| \geq 2^{n+1}$ by Proposition 1.2. This implies that the cyclic Λ-module B_n satisfies the assumptions of Lemma 3.5. Hence, we obtain the assertion from Lemma 3.5. □

Proof of Theorem 1.4. Because of Lemma 5.5(ii) and the definition of 2^*, the ideal $\mathcal{R}_{n,4} = \mathcal{Q} \cap J_n$ depends only on n when the base field L_0 moves over $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$ with $\ell \in \mathbb{P}_+$. Therefore, we obtain the assertion (i) of Theorem 1.4. We see that $\mathcal{Q} \cap J_{f-1}$ is nontrivial by Lemma 5.5(i). By Lemma 4.3(ii), this implies that $\mathcal{Q} \cap J_{f-1} \supseteq J_0$. If $\mathcal{Q} \cap J_{f-1} = J_{f-1}$, then $r_4(A_n) = 2^n$ for any $0 \leq n \leq f-1$ by Lemma 5.6. Therefore, under the assumption of Theorem 1.4(ii), we have $J_0 \subseteq \mathcal{Q} \cap J_{f-1} \subsetneq J_{f-1}$. It follows from Lemma 4.3 that there exists an integer m_0 $(1 \leq m_0 \leq f-1)$ such that

$$J_{m_0-1} \subseteq \mathcal{Q} \cap J_{f-1} \subsetneq J_{m_0}. \tag{5.2}$$

Then, by Lemma 5.5, we see that $\mathcal{R}_{n,4} = J_n$ for $0 \le n \le m_0 - 1$ and $\mathcal{R}_{n,4} = \mathcal{Q} \cap J_{f-1} \subsetneq J_n$ for $m_0 \le n \le f-1$. Therefore, we see from Lemma 4.3(ii) that $r_4(A_n) = 2^n$ for $0 \le n \le m_0 - 1$, and that $r_4(A_n) < 2^n$ for $m_0 \le n \le f-1$. Hence, the integer m_0 is nothing but the integer n_p^+ in Theorem 1.4. Now, by Lemma 5.5(i), we obtain the assertion of Theorem 1.4(ii) on (s_n, a_n, b_n) and $\mathrm{ord}_2(\bar{h}_n)$ with $n_p^+ = m_0$ and $b_p^+ = \dim_{\mathbb{F}_2} \mathcal{Q} \cap J_{f-1}$. Further, we obtain $b_p^+ \ge 2^{n_p^+ - 1}$ from (5.2) and Lemma 4.3. □

Proof of Theorem 1.5. Theorem 5 is shown similarly to Theorem 1.4 by using Lemma 5.5. □

6 Proof of Theorem 1.6

We see in the following lemma that many of the assertions shown in Section 4 when $L_0 = \mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-2\ell})$ hold also when $L_0 = \mathbb{Q}(\sqrt{2})$ and $\kappa_p = 0$. In the following, we let $L_0 = \mathbb{Q}(\sqrt{2})$, and assume that $\kappa_p = 0$. Recall that $\mathcal{F}_n$ is imaginary only when $n = e$.

Lemma 6.1. *Under the above assumption, the following assertions hold on the imaginary cyclic field $\mathcal{F}_e$.*

(i) $r_2(A_e) = 2^e$ *and* $r_4(A_e) \ge 1$.

(ii) *The group ${}_2A_e$ is generated by the ideal class $[\mathfrak{Q}_e^h]$ over $\mathbb{F}_2[G_e]$.*

(iii) *The extension $M_e/\mathcal{F}_e$ is the class field corresponding to A_e/A_e^2.*

(iv) *The class group A_e is cyclic over Γ_e.*

Proof. These assertions are shown in [5] except for the second assertion (ii). We can show (ii) using $r_2(A_e) = 2^e$ in a way similar to Lemma 5.1. □

Proof of Theorem 1.6. As $\kappa_p = 0$, we have $\tilde{f} = e + 1$ and $f = e$. Similarly to Section 5, let $N_{e,4}/\mathcal{F}_e$ be the composite of all unramified quadratic extensions over $\mathcal{F}_e$ which extends to an unramified cyclic quartic extension. Let $V_{e,4}$ be the submodule of V_e such that

$$N_{e,4} = \mathcal{F}_e(\sqrt{\alpha} \;\big|\; [\alpha] \in V_{e,4}),$$

and $\mathcal{R}_{e,4} = \iota(V_{e,4}) \subseteq \mathcal{R} = \mathbb{F}_2[G_e]$. Here, ι is the isomorphism from $V = V_e$ to $\mathcal{R} = \mathbb{F}_2[G_e]$ in (4.6). We see that $N_{e,4}$ is Galois over $\mathbb{Q}$, and hence $\mathcal{R}_{e,4}$ is an ideal of $\mathcal{R}$. By Lemmas 3.3 and 6.1(ii), we see that an unramified quadratic extension $N/\mathcal{F}_e$ extends to an unramified cyclic quartic extension if and only

if the ideals $\mathfrak{Q}_e^\sigma$ ($\sigma \in G_e$) of $\mathcal{F}_e$ split in N. Hence, we obtain $\mathcal{R}_{e,4} = \mathcal{Q}$ from Lemma 3.4 and (4.8) similarly to Lemma 5.5.

First, we assume that $r_4(A_e) < 2^{e-1}$ and show Theorem 1.6(i). By Theorem 1.3 and (1.8), the assumption implies that $s_e = 2$ and $b_e = \dim_{F_2} \mathcal{Q} < 2^{e-1}$. For $1 \le n \le e-1$, we observe from Lemma 4.3 that $b_e = \dim_{F_2} \mathcal{Q} < 2^n$ if and only if $\mathcal{Q} \subsetneq J_n$. Hence, by the definition of the integer n_1, we have $J_{n_1-1} \subseteq \mathcal{Q} \subsetneq J_{n_1}$. Therefore, we see that $\mathcal{Q} \cap J_n = J_n$ for $n \le n_1 - 1$ and that $\mathcal{Q} \cap J_n = \mathcal{Q} \subsetneq J_n$ for $n_1 \le n \le e-1$. Because of Lemma 5.5, it follows from this that $n_1 = n_p^-$ and that $b_e = \dim_{\mathbb{F}_2} \mathcal{Q} = b_p^-$. Thus, we obtain Theorem 1.6(i).

Next, assume that $r_4(A_e) \ge 2^{e-1}$ and show Theorem 1.6(ii). Since $\mathcal{R}_{e,4} = \mathcal{Q}$, we see from the assumption that $\mathcal{Q} \supseteq J_{e-1}$ by Lemma 4.3. Therefore, $\mathcal{Q} \cap J_n = J_n$ for $n \le e-1$. Hence, we obtain Theorem 1.6(ii) by Lemma 5.5. □

7 Proof of Theorem 1.7

As in the previous sections, we let $p \equiv 1 \bmod 8$ and we use the same notation. For a number field N, let $\tilde{A}_N$ be the 2-part of the ideal class group of N in the narrow sense. Clearly, $\tilde{A}_N$ coincides with the usual class group A_N when N is a CM field. When N is a quadratic field of discriminant d, we write $\tilde{A}(d) = \tilde{A}_N$ and we let $h^+(d)$ be the narrow class number of N. It is well known that the $\tilde{A}(-8p)$ and $\tilde{A}(8p)$ are cyclic by Gauss and that $4|h^+(-8p)$ and $4|h^+(8p)$ by Rédei and Reichardt [13, 14]. Morton [11, Theorems 2, 3] obtained the following theorem on 8-divisibility on these class numbers, which is a key for proving Theorem 1.7. For some related results on 8-divisibility, see also [7, 16].

Theorem 7.1 ([11]). *We have $8|h^+(-8p)$ if and only if p splits completely in $\mathbb{Q}(\sqrt[4]{2})$. We have $8|h^+(8p)$ if and only if p splits completely in $\mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$.*

Proof of Theorem 1.7. First, we prove Theorem 1.7(I). By Theorem 1.4(i), it suffices to deal with the case where $L_0 = \mathbb{Q}(\sqrt{-2})$ and $\mathcal{F}_0 = \mathbb{Q}(\sqrt{-2p})$. We already know that $L_1 = \mathcal{F}_0(\sqrt{-2}) = \mathbb{Q}(\sqrt{-2}, \sqrt{p})$ is an unramified extension over $\mathcal{F}_0$ and that $L_1/\mathcal{F}_0$ extends to an unramified cyclic quartic extension by Lemma 5.4. Let ω_1 be the element of $k_1 = \mathbb{Q}(\sqrt{p})$ defined in Section 4, which satisfies the congruence (4.4) with $2^* = -2$. Then,

we observe that $N = L_1(\sqrt{\omega_1})/L_1$ is an unramified quadratic extension because of $\mathfrak{q}_1^h = (\omega_1)$ and (4.4). Here, $\mathfrak{q}_1$ is a prime ideal of k_1 over 2 and $h = h_{k_e}$ is the class number of k_e. Further, we easily see that $N/\mathcal{F}_0$ is a cyclic quartic extension using $\omega_1\omega_1^\sigma = (-2)^h$ where σ is the nontrivial automorphism of $k_1/\mathbb{Q}$. On the other hand, we see that p splits completely in $\mathbb{Q}(\sqrt[4]{2})$ as we are assuming $f \geq 2$ in Theorems 1.4–1.7. Therefore, by virtue of Theorem 7.1, the unramified cyclic quartic extension $N/\mathcal{F}_0$ extends to an unramified cyclic extension of degree 8. By Lemma 5.1(i), the class group ${}_2A_0 = {}_2A_{\mathcal{F}_0}$ is generated by the class $[\mathfrak{Q}_0^h]$, where $\mathfrak{Q}_0$ is the prime ideal of $\mathcal{F}_0$ over 2. Then, we see that the last condition on $N/\mathcal{F}_0$ is equivalent to saying that the prime ideal $\mathfrak{Q}_0$ splits completely in N similarly to Lemma 3.3. Let $\tilde{\mathfrak{q}}_1$ and $\tilde{\mathfrak{q}}_1^\sigma$ be the prime ideals of L_1 over $\mathfrak{q}_1$ and $\mathfrak{q}_1^\sigma$, so that we have $\mathfrak{Q}_0 = \tilde{\mathfrak{q}}_1\tilde{\mathfrak{q}}_1^\sigma$ in L_1. Now, we see that the condition on $N/\mathcal{F}_0$ is equivalent to saying that the prime ideals $\tilde{\mathfrak{q}}_1$ and $\tilde{\mathfrak{q}}_1^\sigma$ of L_1 split in $N = L_1(\sqrt{\omega_1})$. By Lemma 3.4, this is equivalent to

$$\frac{\omega_1}{(-2)^h} \equiv 1 \bmod \mathfrak{q}_1^3 \quad \text{and} \quad \omega_1 \equiv 1 \bmod (\mathfrak{q}_1^\sigma)^3.$$

This congruence means that $\alpha = \omega_1 = N_{f/1}\omega_f$ satisfies the congruence (4.8), which is equivalent to $Q \supseteq V_1$, where Q is the submodule of $V = V_f$ defined just after (4.8). Therefore, we obtain $\mathcal{Q} \supseteq J_1$ and $\mathcal{R}_{1,4} = J_1$. This implies that $r_4(A_1) = \dim_{\mathbb{F}_2} J_1 = 2$.

Next, let us show Theorem 1.7(II). We use the real quadratic field $K = \mathbb{Q}(\sqrt{2p})$ and the narrow class group $\tilde{A}_K = \tilde{A}(8p)$ in place of $\mathcal{F}_0 = \mathbb{Q}(\sqrt{-2p})$ and the usual class group A_0 in the above argument. We see that $E = K(\sqrt{2}) = K(\sqrt{p})$ is an unramified quadratic extension of K. Let ω_1 be the element defined in Section 4, which satisfies (4.4) with $2^* = 2$. Then, we can show that $E(\sqrt{\omega_1})/K$ is a cyclic quartic extension unramified at all finite primes. By Theorem 7.1, the extension $E(\sqrt{\omega_1})/K$ extends to a cyclic extension of degree 8 unramified at all finite primes if and only if $p \equiv 1 \bmod 16$. Let $\mathfrak{q}$ be the unique prime ideal of K over 2, and let $\tilde{\mathfrak{q}}_1$ and $\tilde{\mathfrak{q}}_1^\sigma$ be the prime ideals of E over $\mathfrak{q}_1$ and $\mathfrak{q}_1^\sigma$. Then, we see that ${}_2\tilde{A}_K$ is a cyclic group generated by the narrow ideal class $[\mathfrak{q}]$ and that $\mathfrak{q} = \tilde{\mathfrak{q}}_1\tilde{\mathfrak{q}}_1^\sigma$ in E. Now, we can prove Theorem 1.7(II) similarly to Theorem 1.7(I) using the quadratic extension $E(\sqrt{\omega_1})/E$ in place of $L_1(\sqrt{\omega_1})/L_1$. □

8 Numerical data

In the previous sections, we were working with a fixed e and prime numbers p of the form $p = 2^{e+1}q + 1$. In this section, we deal with various e and various primes p, and we put

$$e_p = \mathrm{ord}_2(p-1) - 1 \quad \text{and} \quad f_p = \min\{e_p - \kappa_p + 1, e_p\},$$

so that we have $p = 2^{e_p+1}q + 1$ with $2 \nmid q$.

In Table 1 (resp. Table 2), we give the number of prime numbers $p < 10^5$ with $(e_p, \kappa_p) = (e, \kappa)$ (resp. $f_p = f$). In view of Theorems 1.4 and 1.5, those p with relatively large f_p are of interest. By Table 2, there are 15 primes $p < 10^5$ with $f_p \geq 5$. For these p, we compute the values $\mathrm{ord}_2(\bar{h}_n)$ by using 2-adic analytic class number formula when $L_0 = \mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-2\ell})$ for $\ell \in \mathbb{P}$ with $l < 1000$, and we obtain Tables 3–5. Tables 3 and 4 are direct data on the values $\mathrm{ord}_2(\bar{h}_n)$ for prime numbers $p = 65537$ and 25601 with $(e_p, \kappa_p, f_p) = (15, 5, 11)$ and $(9, 4, 6)$, respectively. In the tables, the data in the row $\ell = *1$ are those corresponding to the case $L_0 = Q(\sqrt{-2})$. By virtue of Theorem 1.2 and (1.8), we see from Table 4 that when $p = 25601$ and $L_0 = \mathbb{Q}(\sqrt{-2})$,

$$\begin{aligned} &A_0 \cong \mathbb{Z}/16, \quad A_1 \cong (\mathbb{Z}/8)^{\oplus 2}, \quad A_2 \cong (\mathbb{Z}/4)^{\oplus 2} \oplus (\mathbb{Z}/8)^{\oplus 2}, \\ &A_3 \cong (\mathbb{Z}/4)^{\oplus 5} \oplus (\mathbb{Z}/8)^{\oplus 3}, \\ &A_n \cong \begin{cases} (\mathbb{Z}/2)^{\oplus(2^n-10)} \oplus (\mathbb{Z}/4)^{\oplus 10} & \text{for} \quad 4 \leq n \leq 5 \\ (\mathbb{Z}/2)^{\oplus 64} & \text{for} \quad 6 \leq n \leq 8. \end{cases} \end{aligned}$$

As we mentioned in Section 1, direct data on the values $\mathrm{ord}_2(\bar{h}_n)$ and resulting data on the abelian groups A_n such as above have led us to prove Theorems 1.4–1.6. From Tables 3, 4 and the equivalence (1.9), we see that the both prime numbers satisfy the assumptions of Theorems 1.4(ii) and 1.5(ii) and obtain the value $n_p^{\pm}$. We obtain the value $b_p^{\pm}$ by Theorem 1.2 and (1.8). For instance, $(n_p^+, b_p^+) = (4, 10)$ for $p = 25601$. For the remaining 13 primes p, we see from the corresponding data on $\mathrm{ord}_2(\bar{h}_n)$ that the assumptions of Theorems 1.4(ii) and 1.5(ii) are satisfied and obtain $n_p^{\pm}$ and $b_p^{\pm}$. Table 5 lists the values $n_p^{\pm}$ and $b_p^{\pm}$ for these 15 prime numbers.

In Table 5, the maximal value of $n_p^{\pm}$ is 4. We search for prime numbers p with $n_p^{\pm} \geq 5$. We have $n_p^{\pm} = 5$ if and only if $r_4(A_4) \geq 2^4$ and $2^4 < r_4(A_5) < 2^5$. By (1.9), the last condition is equivalent to

$$\mathrm{ord}_2(\bar{h}_4) \geq 32 \quad \text{and} \quad 32 < \mathrm{ord}_2(\bar{h}_5) < 64.$$

For $L_0 = \mathbb{Q}(\sqrt{-2})$ and $p < 10^9$ with $f_p \geq 5$, we compute the order of A_4 and obtain Table 6 on the number of such p with $\mathrm{ord}_2(\bar{h}_4) = i$ ($i \geq 17$). There are 98813 such prime numbers. In the table, the number of such p with $\mathrm{ord}_2(\bar{h}_4) = 17 = 2^4 + 1$ is zero! Here, see Theorem 1.7 once more. Among 98813 prime numbers in the table, there are only six primes with $\mathrm{ord}_2(\bar{h}_4) \geq 32$. These primes are candidates of primes with $n_p^+ \geq 5$. By further computation on $\mathrm{ord}_2(\bar{h}_5)$ for the six prime numbers, we obtain Table 7. The table contains the values of $\mathrm{ord}_2(\bar{h}_5)$ also when $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ for the first three prime numbers $\ell \in \mathbb{P}_+$. We find three primes with $n_p^+ = 5$, the ones with $\mathrm{ord}_2(\bar{h}_5) = 48$ and 49. In the table, those p with the mark $-$ do not satisfy the assumption of Theorem 1.4(ii). Hence, for these p, $r_4(A_n) = 2^n$ with $0 \leq n \leq f_p - 1$.

Table 8 gives some data related to Theorem 1.6 for the nine prime numbers $p = p_{4,i}$ in [5, Table 2]. Here, $p_{4,i}$ denotes the minimum prime number p satisfying $(e_p, \kappa_p, \mathrm{ord}_2(h_4)) = (4, 0, i)$ for $L_0 = \mathbb{Q}(\sqrt{2})$. For such p, we have $f_p = e = 4$. By Theorem 1.3 and (1.8), we see that the assumption of Theorem 1.6(i) is satisfied if and only if $17 < i < 24$. Among those p in Table 8, there are six ones satisfying this condition. For these six ones, we list (n_1, b_e) in the table. In the table, those ones with the mark $-$ do not satisfy the assumption of Theorem 1.6(i), and hence they do not satisfy the assumption of Theorem 1.5(ii) by Theorem 1.6(ii). The table also gives the basic data $\mathrm{ord}_2(\bar{h}_n)$ with $0 \leq n \leq f_p - 1 = 3$ when $L_0 = \mathbb{Q}(\sqrt{-2\ell})$ for the first three prime numbers $\ell \in \mathbb{P}_-$. Then, we obtain the values n_p^- and b_p^- in Theorem 1.5, and we can re-check the equality $(n_p^-, b_p^-) = (n_1, b_4)$ in Theorem 1.6(i) for the six ones.

Table 1: The number of prime numbers with $(e_p, \kappa_p) = (e, \kappa)$.

e \ κ	0	1	2	3	4	5	6	7	8	9	10	11	total
0	2399	2409	0	0	0	0	0	0	0	0	0	0	4808
1	0	0	2399	0	0	0	0	0	0	0	0	0	2399
2	308	287	601	0	0	0	0	0	0	0	0	0	1196
3	66	76	151	296	0	0	0	0	0	0	0	0	589
4	20	17	37	70	155	0	0	0	0	0	0	0	299
5	4	2	10	23	44	71	0	0	0	0	0	0	154
6	0	1	3	2	12	15	42	0	0	0	0	0	75
7	0	0	1	0	4	2	8	17	0	0	0	0	32
8	0	0	0	0	0	2	1	4	9	0	0	0	16
9	0	0	0	0	2	0	0	0	4	8	0	0	14
10	0	0	0	1	0	0	0	0	1	1	1	0	4
11	0	0	0	0	0	0	0	0	0	0	1	2	3
12	0	0	0	0	0	0	0	0	0	0	0	1	1
13	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	1	0	0	0	0	0	0	1
total	2797	2792	3202	392	217	91	51	21	14	9	2	3	9591

Table 2: The number of prime numbers with $f_p = f$.

f	0	1	2	3	4	5	6	7	8	9	10	11	total
	7207	1202	894	218	55	9	4	0	1	0	0	1	9591

Table 3: $\mathrm{ord}_2(\bar{h}_n)$ for $p = 65537$ ($f_p = 11$).

l \ n	0	1	2	3	4	5	6	7	8	9	10	11∼14
∗1	5	6	8	12	20	36	68	132	260	516	1028	2048
41	2	4	10	12	20	36	68	132	260	516	1028	2048
73	3	5	8	12	20	36	68	132	260	516	1028	2048
89	5	5	8	12	20	36	68	132	260	516	1028	2048
113	3	7	8	12	20	36	68	132	260	516	1028	2048
137	2	4	10	12	20	36	68	132	260	516	1028	2048
313	2	4	13	12	20	36	68	132	260	516	1028	2048
337	8	5	8	12	20	36	68	132	260	516	1028	2048
401	2	4	10	12	20	36	68	132	260	516	1028	2048
409	2	4	9	12	20	36	68	132	260	516	1028	2048
433	2	4	10	12	20	36	68	132	260	516	1028	2048
449	2	4	9	12	20	36	68	132	260	516	1028	2048
457	2	4	10	12	20	36	68	132	260	516	1028	2048
521	2	4	10	12	20	36	68	132	260	516	1028	2048
569	2	4	10	12	20	36	68	132	260	516	1028	2048
577	4	5	8	12	20	36	68	132	260	516	1028	2048
601	4	5	8	12	20	36	68	132	260	516	1028	2048
641	2	4	9	12	20	36	68	132	260	516	1028	2048
857	2	4	9	12	20	36	68	132	260	516	1028	2048
881	3	6	8	12	20	36	68	132	260	516	1028	2048
929	2	4	11	12	20	36	68	132	260	516	1028	2048
7	2	4	10	12	20	36	68	132	260	516	1028	2048
23	2	4	10	12	20	36	68	132	260	516	1028	2048
31	3	6	8	12	20	36	68	132	260	516	1028	2048
47	3	6	8	12	20	36	68	132	260	516	1028	2048
127	4	6	8	12	20	36	68	132	260	516	1028	2048
151	2	4	11	12	20	36	68	132	260	516	1028	2048
167	2	4	10	12	20	36	68	132	260	516	1028	2048
223	7	6	8	12	20	36	68	132	260	516	1028	2048
271	3	7	8	12	20	36	68	132	260	516	1028	2048
311	2	4	10	12	20	36	68	132	260	516	1028	2048
359	2	4	11	12	20	36	68	132	260	516	1028	2048
383	3	6	8	12	20	36	68	132	260	516	1028	2048
463	3	10	8	12	20	36	68	132	260	516	1028	2048
607	3	6	8	12	20	36	68	132	260	516	1028	2048
727	2	4	10	12	20	36	68	132	260	516	1028	2048
743	2	4	10	12	20	36	68	132	260	516	1028	2048
823	2	4	10	12	20	36	68	132	260	516	1028	2048
863	3	6	8	12	20	36	68	132	260	516	1028	2048
887	2	4	11	12	20	36	68	132	260	516	1028	2048
983	2	4	11	12	20	36	68	132	260	516	1028	2048
991	3	6	8	12	20	36	68	132	260	516	1028	2048

Table 4: $\mathrm{ord}_2(\bar{h}_n)$ for $p = 25601$ ($f_p = 6$).

l \ n	0	1	2	3	4	5	6∼8	l \ n	0	1	2	3	4	5	6∼8
$*1$	4	6	10	19	26	42	64	31	3	7	8	12	20	36	64
41	2	4	8	16	26	42	64	47	3	6	8	12	20	36	64
73	3	5	9	17	26	42	64	71	2	4	12	12	20	36	64
89	5	5	9	17	26	42	64	103	2	4	10	12	20	36	64
97	2	4	8	16	26	42	64	151	2	4	10	12	20	36	64
193	2	4	8	16	26	42	64	191	3	7	8	12	20	36	64
241	2	4	8	16	26	42	64	199	2	4	12	12	20	36	64
281	4	5	9	17	26	42	64	239	3	6	8	12	20	36	64
313	2	4	8	16	26	42	64	263	2	4	10	12	20	36	64
337	4	5	9	17	26	42	64	271	3	6	8	12	20	36	64
593	3	6	11	18	26	42	64	311	2	4	10	12	20	36	64
641	2	4	8	16	26	42	64	359	2	4	12	12	20	36	64
761	2	4	8	16	26	42	64	367	3	6	8	12	20	36	64
769	2	4	8	16	26	42	64	431	3	8	8	12	20	36	64
809	2	4	8	16	26	42	64	503	2	4	12	12	20	36	64
929	2	4	8	16	26	42	64	599	2	4	10	12	20	36	64
953	2	4	8	16	26	42	64	647	2	4	10	12	20	36	64
977	2	4	8	16	26	42	64	719	5	7	8	12	20	36	64
								727	2	4	10	12	20	36	64
								743	2	4	15	12	20	36	64
								751	3	6	8	12	20	36	64
								823	2	4	10	12	20	36	64
								863	3	6	8	12	20	36	64
								919	2	4	10	12	20	36	64
								967	2	4	15	12	20	36	64
								991	3	6	8	12	20	36	64

Table 5: $(n_p^{\pm}, b_p^{\pm})$ with $f_p \geq 5$.

f_p	p	e_p	κ_p	(n_p^+, b_p^+)	(n_p^-, b_p^-)
11	65537	15	5	(3,4)	(3,4)
8	59393	10	3	(2,2)	(2,3)
6	6529	6	1	(3,5)	(3,4)
6	25601	9	4	(4,10)	(3,4)
6	50177	9	4	(2,2)	(2,2)
6	96001	7	2	(2,2)	(2,3)
5	15809	5	0	(2,3)	(2,2)
5	21569	5	1	(2,3)	(2,2)
5	35201	6	2	(3,5)	(2,2)
5	45697	6	2	(3,6)	(2,2)
5	50753	5	1	(3,6)	(4,10)
5	53633	6	2	(2,2)	(2,2)
5	83777	5	0	(2,3)	(3,5)
5	92737	5	0	(3,4)	(3,6)
5	93377	5	0	(2,2)	(2,2)

Table 6: The number of primes with the $\mathrm{ord}_2(\bar{h}_4) = i$ ($p < 10^9,\ f_p \geq 5$).

i	17	18	19	20	21	22	23	24	25	26
	0	48078	25053	12771	6409	3281	1576	822	384	212
i	27	28	29	30	31	32	33	34	≥ 35	
	120	56	24	13	8	2	2	2	0	

Table 7: $\mathrm{ord}_2(\bar{h}_n)$ for six primes with the $\mathrm{ord}_2(\bar{h}_4) \geq 32$.

p	e_p	κ_p	(n_p^+, b_p^+)			
l \ n	0	1	2	3	4	5
676199297	6	1	(5,16)			
$*1$	4	6	10	18	32	48
73	4	6	10	18	32	48
113	4	5	9	17	32	48
137	2	4	8	16	33	48
816873089	6	2	–			
$*1$	4	6	10	18	32	32
17	2	4	8	16	35	32
89	8	5	9	17	32	32
97	2	4	8	16	33	32
574717313	6	1	(5,17)			
$*1$	4	6	10	18	33	49
73	8	7	12	20	33	49
193	2	4	8	16	32	49
233	4	5	9	17	37	49
640935553	6	0	(5,17)			
$*1$	5	10	12	20	33	49
17	2	4	8	16	32	49
41	2	4	8	16	32	49
89	3	6	18	20	33	49
156731329	5	0	–			
$*1$	7	8	12	20	34	
41	2	4	8	16	32	
89	4	5	9	17	33	
97	2	4	8	16	32	
579604033	5	0	–			
$*1$	4	6	10	18	34	
41	2	4	8	16	32	
73	4	8	14	22	35	
89	3	9	10	18	34	

Table 8: $\mathrm{ord}_2(\bar{h}_n)$ for $p_{4,i}$.

$p_{4,i}$	e_p	κ_p	(n_1, b_e)	i	$p_{4,i}$	e_p	κ_p	(n_1, b_e)	i
l \ n	0	1	2	3	l \ n	0	1	2	3
2593	4	0	(2,2)	18	598817	4	0	(3,7)	23
7	2	6	6	10	31	3	6	11	15
23	2	6	6	10	103	2	4	8	15
127	4	4	6	10	127	5	6	10	15
26849	4	0	(2,3)	19	31649	4	0	–	24
31	5	8	7	11	31	3	6	12	16
71	2	4	7	11	167	2	4	8	17
79	4	6	7	11	223	10	9	12	16
10657	4	0	(3,4)	20	476513	4	0	–	25
7	2	4	12	12	23	2	4	8	16
31	3	8	8	12	31	3	9	10	17
47	3	6	8	12	103	2	4	8	16
68449	4	0	(3,5)	21	572321	4	0	–	26
7	2	4	8	13	31	3	7	10	19
79	3	8	9	13	71	2	4	8	16
103	2	4	8	13	103	2	4	8	16
138977	4	0	(3,6)	22					
7	2	4	8	14					
23	2	4	8	14					
47	3	8	14	14					

References

[1] H. Cohn and J. C. Lagarias, On the existence of fields governing the 2-invariants of the classgroup $\mathbb{Q}(\sqrt{dp})$ as p varies, Math. Comp., **41** (1983), no. 164, 711–730.

[2] P. E. Conner and J. Hurrelbrink, Class Number Parity, World Scientific, Singapore, 1988.

[3] B. Ferrero, The cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields, Amer. J. Math., **102** (1980), no. 3, 447–459.

[4] H. Ichimura, Relative class numbers inside the pth cyclotomic field, Osaka J. Math., **57** (2020), no. 4, 945–959.

[5] H. Ichimura and H. Sumida-Takahashi, On the class group of an imaginary cyclic field of conductor $8p$ and 2-power degree, to appear in Tokyo J. Math. Doi:10.3836/tjm/1502179326.

[6] K. Iwasawa, On the μ-invariants of $\mathbb{Z}_\ell$-extensions, Number Theory, Algebraic Geometry and Commutative Algebra, in honor of Yasuo Akizuki, pp. 1–11, Kinokuniya, Tokyo, 1973.

[7] P. Kaplan, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-gruppe de classes est cyclique et réciprocité biquadratique, J. Math. Soc. Japan, **25** (1973), no. 4, 596–608.

[8] Y. Kida, On cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields, Tohoku Math. J., **31** (1979), no. 1, 91–96.

[9] P. Koymans and D. Milovic, On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-2p})$ for primes $p \equiv 1 \bmod 4$, Int. Math. Res. Not. IMRN, 2019, no. 23, 7406–7427.

[10] D. H. Lehmer, Prime factors of cyclotomic class numbers, Math. Comp., **31** (1977),no. 138, 599–607.

[11] P. Morton, The quadratic number fields with cyclic 2-classgroups, Pacific J. Math., **108** (1983), no. 1, 165–175.

[12] R. Schoof, Minus class groups of the fields of ℓth roots of unity, Math. Comp., **67** (1998), no. 223, 1225–1245.

[13] L. Rédei and H. Reichardt, Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. Reine Angew. Math., **170** (1934), 69–74.

[14] L. Rédei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratishen Zahlkörper, J. Reine. Angew. Math., **171** (1934), 55–60.

[15] L. C. Washington, Introduction to Cyclotomic Fields, 2nd ed., Springer, New York, 1997.

[16] Y. Yamamoto, Divisibility by 16 of class number of quadratic fields whose 2-class groups are cyclic, Osaka J. Math., **21** (1984), no. 1, 1–22.

[17] H. Yokoi, On the class number of a relatively cyclic number field, Nagoya Math. J., **29** (1967), 31–44.

[18] Q. Yue, The generalized Rédei-matrix, Math. Z., **261** (2009), no. 1, 23–37.