On the class group of an imaginary cyclic field of conductor $8p$ and 2-power degree

Humio Ichimura and Hiroki Sumida-Takahashi

Abstract

Let $p = 2^{e+1}q + 1$ be an odd prime number with $2 \nmid q$. Let K be the imaginary cyclic field of conductor p and degree 2^{e+1}. We denote by $\mathcal{F}$ the imaginary quadratic subextension of the imaginary (2, 2)-extension $K(\sqrt{2})/K^+$ with $\mathcal{F} \neq K$. We determine the Galois module structure of the 2-part of the class group of $\mathcal{F}$.

1 Introduction

For a prime number p with $p \equiv 3 \bmod 4$, let $F = \mathbb{Q}(\sqrt{-2p})$. It is well known that the 2-part of the class group of F is nontrivial and cyclic by Gauss, and that $4|h_F$ if and only if p splits in $\mathbb{Q}(\sqrt{2})$ by Rédei and Reichardt [11]. Here, h_N denotes the class number of a number field N. There are many other papers and related results on the 2-part of the class group of a quadratic field such as [1, 6, 8, 9, 12, 15, 19].

In this paper, we give a generalization of the classical results on $F = \mathbb{Q}(\sqrt{-2p})$ for a general odd prime number p and an imaginary cyclic field of conductor $8p$ and 2-power degree. Let $e \geq 0$ be a fixed integer, and let $p = 2^{e+1}q+1$ denote an odd prime number with $2 \nmid q$. Let K be the imaginary subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ of degree 2^{e+1}. Here, for an integer m, ζ_m denotes a primitive mth root of unity. The extension $K(\sqrt{2})/K^+$ is an imaginary (2, 2)-extension, where N^+ denotes the maximal real subfield of a CM-field N. We denote by $\mathcal{F} = \mathcal{F}_p$ the imaginary quadratic intermediate

2010 Mathematics Subject Classification: 11R18, 11R23
Keywords and phrases: class group, 2-part, imaginary cyclic field

field of $K(\sqrt{2})/K^+$ with $\mathcal{F} \neq K$. We see that $\mathcal{F}$ is an imaginary cyclic field of conductor $8p$ and degree 2^{e+1}. For the case $e = 0$, we have $K = \mathbb{Q}(\sqrt{-p})$ and $\mathcal{F} = \mathbb{Q}(\sqrt{-2p})$. For a number field N, Cl_N and $A_N = Cl_N(2)$ denote the ideal class group of N in the usual sense and its 2-part, respectively. When N is a CM-field, let Cl_N^- be the kernel of the norm map $Cl_N \to Cl_{N^+}$ and $h_N^- = |Cl_N^-|$ the relative class number of N. Further, A_N^- denotes the 2-part of Cl_N^-. We have $A_{\mathcal{F}} = A_{\mathcal{F}}^-$ because $F^+ = K^+$ and h_{K^+} is odd (Washington [13, Theorem 10.4(b)]). We study the Galois module structure of $A_{\mathcal{F}}$.

Let $\Gamma = \mathrm{Gal}(\mathcal{F}/\mathbb{Q})$ and $R = \mathbb{Z}_2[\Gamma]$, where $\mathbb{Z}_2$ is the ring of 2-adic integers. We choose and fix a generator γ of the cyclic group Γ of order 2^{e+1}. Let $\Lambda = \mathbb{Z}_2[[T]]$ be the power series ring with indeterminate T. In all what follows, we identify R with $\Lambda/((1+T)^{2^{e+1}} - 1)$ by the correspondence $\gamma \leftrightarrow 1+T$:

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

The group $A_{\mathcal{F}}$ is naturally regarded as a module over R, and hence as a module over Λ. The following assertion generalizes the classical fact due to Gauss that $A_{\mathcal{F}}$ is a cyclic group when $e = 0$ and $\mathcal{F} = \mathbb{Q}(\sqrt{-2p})$.

Proposition 1. *Under the above setting, the class group $A_{\mathcal{F}}$ is cyclic over Λ.*

We denote by $I_{\mathcal{F}}$ $(\subseteq \Lambda)$ the annihilator of the cyclic Λ-module $A_{\mathcal{F}}$, so that we have an isomorphism $A_{\mathcal{F}} \cong \Lambda/I_{\mathcal{F}}$ of Λ-modules. We see that

$$(1+T)^{2^e} + 1 \in I_{\mathcal{F}} \tag{1}$$

because the complex conjugation $\gamma^{2^e} = (1+T)^{2^e}$ acts on $A_{\mathcal{F}} = A_{\mathcal{F}}^-$ via (-1)-multiplication. When $e = 0$, the classical fact due to Gauss implies that $I_{\mathcal{F}} = (2^s, 2+T)$ with $s = \mathrm{ord}_2(h_{\mathcal{F}})$ and hence

$$A_{\mathcal{F}} \cong \Lambda/(2^s, 2+T) \ (\cong \mathbb{Z}/2^s). \tag{2}$$

Here, $\mathrm{ord}_2(*)$ denotes the additive 2-adic valuation on $\mathbb{Q}$ with $\mathrm{ord}_2(2) = 1$.

We generalize the fact (2) for the case $e \geq 1$. To state our results, we need some more preliminaries. We denote by $\kappa = \kappa_p$ the smallest nonnegative integer with $0 \leq \kappa \leq e+1$ such that p splits completely in $\mathbb{Q}(2^{1/2^{e-\kappa+1}})$. By definition, we have $\kappa_p = 0$ if and only if p splits completely in $\mathbb{Q}(2^{1/2^{e+1}})$. Thus, when $e = 0$, the condition $\kappa_p = 0$ is nothing but the one in the old paper [11] which we mentioned at the beginning of this section. On the value κ_p, the following assertion holds.

Lemma 1. *When $e = 1$, we have $\kappa_p = e + 1 = 2$. When $e \geq 2$, for each i with $0 \leq i \leq e$ (resp. $i = e+1$), there exist infinitely many (resp. no) prime numbers p such that $p = 2^{e+1}q + 1$ with $2 \nmid q$ and $\kappa_p = i$.*

We have $\mathrm{ord}_2(h_{\mathcal{F}}) = \mathrm{ord}_2(h_{\mathcal{F}}^-)$ as h_{K^+} is odd. On the value $\mathrm{ord}_2(h_{\mathcal{F}})$, we show the following assertion.

Proposition 2. (I) *When $e = 1$, we have* $\mathrm{ord}_2(h_{\mathcal{F}}) = 1$.

(II) *When $e \geq 2$ and $\kappa = \kappa_p \geq 1$, we have* $\mathrm{ord}_2(h_{\mathcal{F}}) = 2^{e-\kappa+1}$.

(III) *When $\kappa = 0$,* $\mathrm{ord}_2(h_{\mathcal{F}}) = 2^e + 1 = 5$ *for the case $e = 2$ and* $\mathrm{ord}_2(h_{\mathcal{F}}) \geq 2^e + 2$ *for the case $e \geq 3$.*

When $e = 1$, there is nothing to do on the structure of the class group $A_{\mathcal{F}}$ because of Proposition 2(I). So we let $e \geq 2$ in the following. When $e \geq 2$ and $\kappa_p = 0$, we put

$$s_p = \left\lceil \frac{\mathrm{ord}_2(h_{\mathcal{F}})}{2^e} \right\rceil$$

and

$$a_p = 2^e s_p - \mathrm{ord}_2(h_{\mathcal{F}}) \quad \text{and} \quad b_p = 2^e(1 - s_p) + \mathrm{ord}_2(h_{\mathcal{F}}).$$

Here, $\lceil x \rceil$ denotes the smallest integer $\geq x$. We easily see that $s_p \geq 2$ by Proposition 2(III) and that $a_p \geq 0$, $b_p \geq 1$ and $a_p + b_p = 2^e$. Further, when $e = 2$, we have $s_p = 2$, $a_p = 3$ and $b_p = 1$ by Proposition 2(III). The following assertions on $A_{\mathcal{F}}$ and its annihilator $I_{\mathcal{F}}$ are the main results of the paper. They generalize the classical result (2).

Theorem 1. *Let $e \geq 2$ and $\kappa = \kappa_p \geq 1$. Then*

$$I_{\mathcal{F}} = (2,\, T^{2^{e-\kappa+1}}), \quad \textit{and hence} \quad A_{\mathcal{F}} \cong (\mathbb{Z}/2)^{\oplus 2^{e-\kappa+1}}$$

as abelian groups.

Theorem 2. *Let $e \geq 2$ and $\kappa_p = 0$. Then*

$$I_{\mathcal{F}} = (2^{s_p},\, 2^{s_p-1}T^{b_p},\, (1+T)^{2^e} + 1),$$

and hence

$$A_{\mathcal{F}} \cong (\mathbb{Z}/2^{s_p-1})^{\oplus a_p} \oplus (\mathbb{Z}/2^{s_p})^{\oplus b_p} \tag{3}$$

as abelian groups.

Corollary 1. *Let $e = 2$ and $\kappa_p = 0$. Then*

$$A_{\mathcal{F}} \cong (\mathbb{Z}/2)^{\oplus 3} \oplus \mathbb{Z}/4$$

as abelian groups.

For a finite abelian group A and an integer $t \geq 1$, we denote by

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

the 2^t-rank of A. Here, $\mathbb{F}_2$ is the finite field with two elements. The following assertion is an immediate consequence of Theorems 1 and 2. It is a generalization of the classical result of Rédei and Reichardt for the case $e = 0$.

Corollary 2. *When $e \geq 2$, the 4-rank $r_4(A_{\mathcal{F}})$ is positive if and only if $\kappa_p = 0$.*

Remark 1. In [17, 18], Yue generalized a result of Rédei [12] and gave a formula for the 4-rank of the class group of a relative quadratic extension E/F. It is possible to show Corollary 2 using his formula.

Remark 2. Let $e \geq 2$. For $x > 0$, let $P_e(x)$ be the set of prime numbers $p = 2^{e+1}q + 1 < x$ with $2 \nmid q$. We put

$$\theta_e = \lim_{x \to \infty} \frac{|\{p \in P_e(x) \mid r_4(A_{\mathcal{F}}) > 0\}|}{|P_e(x)|}.$$

We see that $\theta_e = 2^{-e}$ from Corollary 2 and the Chebotarev density theorem.

When $e = 0$, this type of density results are already obtained for prime numbers p such that ($p \equiv 3 \bmod 4$ and) $2^s | h_{\mathcal{F}}$ with $s = 2$, 3 and 4 by Rédei-Reichardt [11], Morton [9] and Milovic [8], respectively.

This paper is organized as follows. In §2, we show Lemma 1 and Proposition 2. We show Theorems 1 and 2, respectively, in §3 and §4. Proposition 1 is shown in §5. In §6, we consider which unramified quadratic extension over $\mathcal{F}$ extends to an unramified cyclic quartic extension. In §7, we give some numerical data on $\mathrm{ord}_2(h_{\mathcal{F}})$ and the class group $A_{\mathcal{F}}$.

2 Proof of Proposition 2

Let $p = 2^{e+1}q + 1$, K, $\mathcal{F}$ and $\kappa = \kappa_p$ be as in §1. We begin by showing Lemma 1 in §1.

Proof of Lemma 1. When $e = 1$ (and hence $p \equiv 5 \bmod 8$), p does not split in $\mathbb{Q}(\sqrt{2})$ and hence $\kappa_p = e + 1 = 2$. Let us deal with the case $e \geq 2$. As $p \equiv 1 \bmod 8$, p splits in $\mathbb{Q}(\sqrt{2})$ and hence $\kappa_p \leq e$. Fixing i with $0 \leq i \leq e$, let $k = \mathbb{Q}(\zeta_{2^{e+1}},\, 2^{1/2^{e-i+1}})$. We put

$$L = k(\zeta_{2^{e+2}},\, 2^{1/2^{e-i+2}}), \quad L_1 = k(\zeta_{2^{e+2}}), \quad L_2 = k(2^{1/2^{e-i+2}}).$$

We see that L is a (2, 2)-extension over k, and that L_1 and L_2 are two of the three quadratic intermediate fields of L/k. Let L_3 be the third intermediate field of L/k. By the Chebotarev density theorem, there exist infinitely many prime ideals $\mathfrak{P}$ of L_3 which is degree one over $\mathbb{Q}$ and remains prime in the quadratic extension L/L_3. Let $\wp = \mathfrak{P} \cap k$. Then the prime ideal $\wp$ of k remains prime in L_1, L_2 and splits in L_3. For the prime number $p = \wp \cap \mathbb{Q}$, we see that $p = 1 + 2^{e+1}q$ with $2 \nmid q$ and $\kappa_p = i$. $\square$

To show Proposition 2 on the class number $h_{\mathcal{F}}$, it suffices to deal with the relative class number $h_{\mathcal{F}}^-$ as h_{K^+} is odd. We see that the unit index of our imaginary abelian field $\mathcal{F}$ is 1 by Conner and Hurrelbrink [2, Lemma 13.5]. Then it follows from the class number formula [13, Theorem 4.17] that

$$h_{\mathcal{F}}^- = 2 \times \prod_{\delta} \left(-\frac{1}{2} B_{1,\delta\psi} \right). \tag{4}$$

Here, δ runs over the odd Dirichlet characters of conductor p and order 2^{e+1}, and ψ is the even Dirichlet character of conductor 8 and order 2. In the following, we regard these characters to be $\bar{\mathbb{Q}}_2$-valued, where $\bar{\mathbb{Q}}_2$ is a fixed algebraic closure of the 2-adic rationals $\mathbb{Q}_2$. Let $\omega = \omega_4$ be the Teichmüller character of conductor 4. We put $\mathcal{O} = \mathcal{O}[\delta] = \mathbb{Z}_2[\zeta_{2^{e+1}}]$. Iwasawa constructed a power series $G_{\delta\omega}(T)$ in the power series ring $\mathcal{O}[[T]]$ related to the 2-adic L-function $L_2(s,\, \delta\omega)$ by

$$G_{\delta\omega}((1+4p)^s - 1) = \frac{1}{2} L_2(s,\, \delta\omega) \tag{5}$$

for $s \in \mathbb{Z}_2$. The power series $G_{\delta\omega}(T)$ also satisfies

$$G_{\delta\omega}(-(1+4p)^s - 1) = \frac{1}{2} L_2(s, \delta\psi\omega) \tag{6}$$

for $s \in \mathbb{Z}_2$. For (5) and (6), see Iwasawa [5, §6, Lemma 3] or [13, Theorem 7.10]. By a theorem of Ferrero and Washington ([13, Theorem 7.15]), we have $2 \nmid G_{\delta\omega}$. Then it follows that

$$G_{\delta\omega}(T) = P(T)u(T)$$

for some distinguished polynomial $P(T) \in \mathcal{O}[T]$ and a unit $u(T)$ of $\mathcal{O}[[T]]$ from [13, Theorem 7.3]. The degree λ_p of $P(T)$ is the Iwasawa lambda invariant of the power series $G_{\delta\omega}$. It follows from (5), (6) and [13, Theorem 5.11] that

$$\begin{aligned} G_{\delta\omega}(0) &= \frac{1}{2}L_2(0,\,\delta\omega) = -\frac{1}{2}(1-\delta(2))B_{1,\delta} \\ &= -\frac{1}{2}(1-\zeta_{2^{e+1}})B_{1,\delta} \times \frac{1-\delta(2)}{1-\zeta_{2^{e+1}}} \end{aligned} \tag{7}$$

and that

$$G_{\delta\omega}(-2) = \frac{1}{2}L_2(0,\,\delta\psi\omega) = -\frac{1}{2}(1-\delta\psi(2))B_{1,\delta\psi} = -\frac{1}{2}B_{1,\delta\psi}. \tag{8}$$

Further, it is known that

$$\frac{1}{2}(1-\zeta_{2^{e+1}})B_{1,\delta} \in \mathcal{O}^{\times}. \tag{9}$$

(See Hasse [3, Satz 32] or [4, Lemma 7].)

Lemma 2. *On the lambda invariant λ_p, we have*

$$\lambda_p = \begin{cases} 2^{\mathrm{ord}_2(q+1)-1} - 1, & \text{for } e = 0 \\ 2^{e-1} - 1, & \text{for } e \geq 1. \end{cases} \tag{10}$$

Proof. Let K_∞/K be the cyclotomic $\mathbb{Z}_2$-extension over K, and let λ_K be the Iwasawa lambda invariant of the ideal class group of K_∞. The invariant λ_K equals $2^e\lambda_p$ by a theorem of Wiles [14, Theorem 6.2] (Iwasawa main conjecture). On the other hand, it is an immediate consequence of the formula (II) in Kida [7, §6] that λ_K equals 2^e times of the right-hand side of (10). Thus we obtain the assertion. □

Lemma 3. *Let D_p be the decomposition field of the prime 2 in the cyclic extension $K/\mathbb{Q}$ of degree 2^{e+1}, and let i be an integer with $0 \leq i \leq e+1$. Then the following three conditions are equivalent to each other.*

(I) *The value $\delta(2)$ is a primitive 2^ith root of unity.*

(II) $[D_p : \mathbb{Q}] = 2^{e-i+1}$.

(III) $\kappa_p = i$.

Proof. As the character δ has order 2^{e+1}, the equivalence (I) $\Leftrightarrow$ (II) follows immediately from the reciprocity law for $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. The condition (I) is equivalent to the condition that the congruence $x^{2^{e-i+1}} \equiv 2 \bmod p$ has a solution but (for the case $i \geq 1$) $y^{2^{e-(i-1)+1}} \equiv 2 \bmod p$ has no solution. We easily see that the last condition is equivalent to $\kappa_p = i$. $\square$

Proof of Proposition 2(I). Let $e = 1$. Then the power series $G_{\delta\omega}$ is a unit of $\mathcal{O}[[T]]$ by Lemma 2. Then it follows from (8) that $\dfrac{1}{2}B_{1,\delta\psi}$ is a unit of $\mathcal{O}$. Therefore, we obtain the assertion from the class number formula (4). $\square$

In the following, we assume that $e \geq 2$. Then the degree λ_p of $P(T)$ is positive by Lemma 2. By (7) and Lemma 3, we obtain the following:

Lemma 4. *The polynomial $P(T)$ is divisible by T if and only if $\kappa_p = 0$.*

Proof of Proposition 2(II), (III). For an integer $i \geq 0$, we put $\pi_i = \zeta_{2^{i+1}} - 1$. Then π_e is a uniformizer of $\mathcal{O} = \mathbb{Z}_2[\zeta_{2^{e+1}}]$. First, let us show the assertion (II) for the case $\kappa = \kappa_p \geq 1$. It follows from (7), (9) and Lemma 3 that

$$P(0) \sim G_{\delta\omega}(0) \sim \alpha = \pi_{\kappa-1}/\pi_e.$$

Here, for elements x and y of $\bar{\mathbb{Q}}_2^\times$, we write $x \sim y$ when x/y is a 2-adic unit. We see that $P(-2) \sim P(0)$ because $P(T) \in \mathcal{O}[T]$ and $P(0) \sim \alpha$ is a divisor of $2/\pi_e$. Hence, $G_{\delta\omega}(-2) \sim P(-2) \sim \alpha$. Then we see from (4) and (8) that

$$h_{\mathcal{F}}^- \sim 2 \times (\pi_{\kappa-1}/\pi_e)^{2^e} \sim 2 \times 2^{2^{e-\kappa+1}} \times 2^{-1} = 2^{2^{e-\kappa+1}}.$$

Next, we show the assertion (III) when $\kappa = 0$ and $e \geq 3$. Then $\lambda_p \geq 3$ by Lemma 2. It follows from Lemma 4 that $P(T) = TQ(T)$ for some distinguished polynomial $Q(T) \in \mathcal{O}[T]$ of degree $\lambda_p - 1 \geq 2$. Since $Q(-2)$ is divisible by π_e, it follows from (4) and (8) that $h_{\mathcal{F}}^-$ is divisible by

$$2 \times (-2)^{2^e} \times \pi_e^{2^e} \sim 2^{2^e+2}.$$

Finally, we show (III) when $\kappa = 0$ and $e = 2$. We have $P(T) = T$ by Lemmas 2 and 4. Then we obtain the assertion from (4) and (8). $\square$

3 Proof of Theorem 1

First, we recall a formula for the number of "ambiguous" classes of a CM-field. Let N be a CM-field. An ideal class $c \in Cl_N$ is ambiguous when $c^J = c$, where J is the nontrivial automorphism of N over N^+ (the complex conjugation). Let $a(N)$ be the number of ambiguous classes of N. For a number field L, we denote by $\mathcal{O}_L$ and $E_L = \mathcal{O}_L^\times$ the ring of integers and the group of units of L, respectively. It is known that

$$a(N) = h_{N^+} \times \frac{2^{t_N - 1}}{[E_{N^+} : E_{N^+} \cap \mathcal{N}(N^\times)]}. \tag{11}$$

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^+. For this formula, see Yokoi [16] for example.

Lemma 5. *The 2-rank $r_2(A_{\mathcal{F}})$ equals 2^e or $2^{e-\kappa+1}$ according as $\kappa = \kappa_p = 0$ or $\kappa \geq 1$.*

Proof. We use the above formula for $N = \mathcal{F}$ noting that $\mathcal{F}^+ = K^+$. We put $r = r_2(A_{\mathcal{F}})$ for brevity. Let $B_{\mathcal{F}}$ be the ambiguous classes in $A_{\mathcal{F}}$. Then $b(\mathcal{F}) = |B_{\mathcal{F}}|$ is nothing but the 2-part of $a(\mathcal{F})$. We see that a class c in $A_{\mathcal{F}}$ is ambiguous ($c^J = c$) if and only if $c^2 = 1$ as $A_{\mathcal{F}} = A_{\mathcal{F}}^-$. It follows that $b(\mathcal{F}) = 2^r$. As $\mathcal{F}$ is a CM-field, every element $x \in \mathcal{N}(\mathcal{F}^\times)$ is totally positive. It follows that

$$(E_{K^+})^2 \subseteq E_{K^+} \cap \mathcal{N}(\mathcal{F}^\times) \subseteq \{\epsilon \in E_{K^+} \bigm| \epsilon \text{ is totally positive}\}.$$

As h_K is odd ([13, Theorem 10.4(b)]), we see from [2, Corollary 13.10] that a unit ϵ of K^+ is totally positive if and only if ϵ is a square in K^+. Therefore, $E_{K^+} \cap \mathcal{N}(\mathcal{F}^\times)$ coincides with $(E_{K^+})^2$, and hence

$$[E_{K^+} : E_{K^+} \cap \mathcal{N}(\mathcal{F}^\times)] = 2^{2^e} \tag{12}$$

by the Dirichlet unit theorem. The primes of $K^+ = \mathcal{F}^+$ ramified in $\mathcal{F}$ are those over p or 2 and the infinite prime divisors. By Lemma 3, we see that $2\mathcal{O}_{K^+}$ is a product of 2^e (resp. $2^{e-\kappa+1}$) prime ideals of K^+ when $\kappa = 0$ (resp. $\kappa \geq 1$). Hence, it follows that

$$t_{\mathcal{F}} = 1 + 2^e + 2^e \text{ or } 1 + 2^{e-\kappa+1} + 2^e$$

according as $\kappa = 0$ or $\kappa \geq 1$. Accordingly, we obtain from (11) and (12) that $b(\mathcal{F}) = 2^{2^e}$ or $2^{2^{e-\kappa+1}}$. Thus we have shown that $r = 2^e$ or $2^{e-\kappa+1}$ according as $\kappa = 0$ or $\kappa \geq 1$. $\square$

Proof of Theorem 1. By Proposition 2(II) and Lemma 5, we see that the abelian group $A_{\mathcal{F}}$ is isomorphic to $2^{e-\kappa+1}$ copies of $\mathbb{Z}/2$. The assertion on the annihilator $I_{\mathcal{F}}$ of the cyclic Λ-module $A_{\mathcal{F}}$ follows from this. $\square$

4 Proof of Theorem 2

Let $e \geq 2$ and $\kappa = \kappa_p = 0$. We already know that

$$r_2(A_{\mathcal{F}}) = 2^e \quad \text{and} \quad A_{\mathcal{F}} = A_{\mathcal{F}}^{-}.$$

The proof of Theorem 2 is based upon Propositions 1, 2 and the following purely algebraic assertion.

Proposition 3. *Let A be a cyclic module over $R = \Lambda/((1+T)^{2^e} - 1)$ with a generator g, and let I_A be the annihilator of the Λ-module A (so that $A \cong \Lambda/I_A$ as Λ-modules). Assume that $g^{\gamma^{2^e}} = g^{-1}$ and that*

$$A \cong (\mathbb{Z}/2)^{\oplus \ell} \oplus (\mathbb{Z}/4)^{\oplus m}$$

with $m \geq 1$ and $1 \leq \ell + m \leq 2^e$. Then we have $\ell + m = 2^e$ and

$$I_A = (4,\, 2T^m,\, (1+T)^{2^e} + 1).$$

Proof of Theorem 2. We write

$$A_{\mathcal{F}} = A_{\mathcal{F}}^{-} \cong \bigoplus_{i=1}^{s} (\mathbb{Z}/2^i)^{t_i}$$

for some integers $s \geq 1$ and $t_i \geq 0$ $(1 \leq i \leq s)$ with $t_s \geq 1$. As $r_2(A_{\mathcal{F}}) = 2^e$, these integers s and t_i satisfy

$$\sum_{i=1}^{s} t_i = 2^e \quad \text{and} \quad \sum_{i=1}^{s} it_i = \mathrm{ord}_2(h_{\mathcal{F}}).$$

Further, we see that $s \geq 2$ since $\mathrm{ord}_2(h_{\mathcal{F}}) \geq 2^e + 1$ by Proposition 2(III). Assume that $t_i \geq 1$ for some i with $i \leq s-2$. Then it follows that

$$A_{\mathcal{F}}^{2^{s-2}} \cong (\mathbb{Z}/2)^{\oplus t_{s-1}} \oplus (\mathbb{Z}/4)^{\oplus t_s}$$

and $t_{s-1}+t_s<2^e$. This is impossible by Proposition 3 because $A_{\mathcal{F}}=A_{\mathcal{F}}^-$ is cyclic over Λ by Proposition 1. Therefore, we observe that

$$A_{\mathcal{F}} \cong (\mathbb{Z}/2^{s-1})^{\oplus a} \oplus (\mathbb{Z}/2^s)^{\oplus b}$$

for some integers a and b such that $a \geq 0$, $b \geq 1$, $a+b=2^e$ and $(s-1)a+sb=\mathrm{ord}_2(h_{\mathcal{F}})$. We see that $s=s_p$, $a=a_p$ and $b=b_p$ from the last four conditions, and thus we obtain the second assertion (3) of Theorem 2. Further, by Proposition 3, the annihilator of $A_{\mathcal{F}}^{2^{s-2}}$ equals $(4,\, 2T^{b_p},\, (1+T)^{2^e}+1)$. It follows from this and (1) that the ideal I of Λ generated by 2^{s_p}, $2^{s_p-1}T^{b_p}$ and $(1+T)^{2^e}+1$ is contained in the annihilator $I_{\mathcal{F}}$ of $A_{\mathcal{F}}$. Since $\Lambda/I \cong A_{\mathcal{F}}$ as abelian groups by (3), we obtain $I=I_{\mathcal{F}}$. $\square$

Proof of Proposition 3. As $m \geq 1$, the module A^2 is nontrivial. Let J_1 be the annihilator of the Λ-module $A^2=\Lambda\cdot g^2$. As A^2 is isomorphic to $(\mathbb{Z}/2)^{\oplus m}$ as abelian groups, we see that $J_1=(2,\, T^m)$ and that

$$A^2=\langle g^2\rangle \times \langle g^{2T}\rangle \times \cdots \times \langle g^{2T^{m-1}}\rangle. \tag{13}$$

Here, $\langle * \rangle$ denotes the cyclic group generated by $*$. It follows that $g^{2T^m}=1$ and hence $2T^m \in I_A$. The assumption $g^{\gamma^{2^e}}=g^{-1}$ implies that $(1+T)^{2^e}+1 \in I_A$. As the ideal I_A contains 4 and $2T^m$, it follows that

$$T^{2^e} \equiv 2+\sum_{i=1}^{m-1} 2a_iT^i \bmod I_A \tag{14}$$

for some $a_i \in \mathbb{Z}$. Let ${}_2A$ be the elements x of A with $x^2=1$. Then, noting that $A^2 \subseteq {}_2A$, we put $B={}_2A/A^2$. We see from $J_1=(2,\, T^m)$ that m is the smallest integer with $g^{T^m} \in {}_2A$, and hence that the Λ-module B is generated by the class $[g^{T^m}]$. Further, $B \cong (\mathbb{Z}/2)^{\oplus \ell}$ as abelian groups. Let J_2 be the annihilator of B. Then, from the above, we observe that

$$J_2=\{\alpha \in \Lambda \mid g^{T^m\alpha} \in A^2\}=(2,\, T^\ell)$$

and that $g^{T^{m+\ell}} \in A^2=\Lambda\cdot g^2$. Because of (13), this implies that

$$T^{m+\ell} \equiv \sum_{i=0}^{m-1} 2b_iT^i \bmod I_A$$

for some $b_i \in \mathbb{Z}$. Now assume that $m + \ell < 2^e$. Then, as $2T^m \in I_A$, we observe that

$$T^{2^e} = T^{m+\ell}T^{2^e-(m+\ell)} \equiv \sum_{i=1}^{m-1} 2c_i T^i \bmod I_A$$

for some $c_i \in \mathbb{Z}$ with $1 \leq i \leq m-1$. It follows from (14) that

$$2 \equiv \sum_{i=1}^{m-1} 2d_i T^i \bmod I_A$$

for some $d_i \in \mathbb{Z}$, and hence

$$2f(T) \in I_A \quad \text{with} \quad f(T) = 1 - \sum_{i=1}^{m-1} d_i T^i.$$

This implies that $2 \in I_A$ because the polynomial $f(T)$ is a unit of Λ. However, this contradicts the assumption $m \geq 1$. Thus we obtain $m + \ell = 2^e$.

Let $I = (4,\, 2T^m,\, (1+T)^{2^e} + 1)$. We already know that $I \subseteq I_A$. Using $m+\ell = 2^e$, we see that Λ/I is isomorphic to A as an abelian group. Therefore, we obtain $I_A = I$. $\square$

5 Proof of Proposition 1

In this section, we construct the class field corresponding to $A_{\mathcal{F}}/A_{\mathcal{F}}^2$ and show Proposition 1. We begin with the following lemma.

Lemma 6. *Let k be a totally real number field of degree n. Assume that the narrow class number $\tilde{h}_k$ of k is odd and that the prime number 2 splits completely in k; $2 = \mathfrak{L}_1 \cdots \mathfrak{L}_n$. Then the natural map*

$$\varphi : E_k \to (\mathcal{O}_k/4\mathcal{O}_k)^\times = \bigoplus_{j=1}^{n} (\mathcal{O}_k/\mathfrak{L}_j^2)^\times$$

induced by reduction modulo 4 is surjective.

Proof. We write $E = E_k$ for brevity. By the second assumption, we see that $(\mathcal{O}_k/4\mathcal{O}_k)^\times$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus n}$ as an abelian group. If a unit $\epsilon \in E$ satisfies $\epsilon \equiv 1 \bmod 4$, then $k(\sqrt{\epsilon})/k$ is unramified outside the infinite prime divisors by [13, Exercise 9.3]. As $\tilde{h}_k$ is odd, this implies that ϵ is a square in k. It follows that $\ker\varphi = E^2$. Now, we see that φ is surjective because E/E^2 is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\oplus n}$ as an abelian group by the Dirichlet unit theorem. $\square$

Let $p = 2^{e+1}q+1$ be an odd prime number, and we use the same notation as in the previous sections. We choose and fix a totally negative element d of K^+ with $(d,\, 2) = 1$ and $K = K^+(\sqrt{d})$. We have

$$d \equiv u^2 \bmod 4 \tag{15}$$

for some $u \in K^+$ by [13, Exercise 9.3] since K/K^+ is unramified at the primes over 2. Let $\wp$ be the unique prime ideal of K^+ over p. We put $h^+ = h_{K^+}$ for brevity. In addition to (15), we may as well assume that

$$(d) = \wp^{h^+}$$

since h^+ is odd and K/K^+ is ramified only at $\wp$ (and the infinite prime divisors). We see that $\mathcal{F} = K^+(\sqrt{2d})$ from the definition of $\mathcal{F}$ and that the quadratic extension $\mathcal{F}(\sqrt{2}) = \mathcal{F}(\sqrt{d})$ over $\mathcal{F}$ is unramified.

For brevity, we put

$$r = 2^e \quad \text{or} \quad 2^{e-\kappa+1}$$

according as $\kappa = 0$ or $\kappa = \kappa_p \geq 1$. By Lemma 5, $r = r_2(A_{\mathcal{F}})$. Let k be the intermediate field of the cyclic extension $K^+/\mathbb{Q}$ with $[k : \mathbb{Q}] = r$. The cyclic group $\mathrm{Gal}(k/\mathbb{Q})$ of order r is generated by $\rho = \gamma_{|k}$ where γ is the generator of $\Gamma = \mathrm{Gal}(\mathcal{F}/\mathbb{Q})$ fixed in §1. By Lemma 3, the prime 2 splits completely in k. We choose a prime ideal $\mathfrak{q}$ of k over 2. We put $\mathfrak{q}_i = \mathfrak{q}^{\rho^{i-1}}$ for each $1 \leq i \leq r$, so that we have a decomposition $2 = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ in k. As h_K is odd, the narrow class number $\tilde{h}_k$ of k is odd. Therefore, by Lemma 6, we can choose a generator $w = w_1 \in k^\times$ of the principal ideal $\mathfrak{q}_1^{h^+}$ such that

$$\frac{w}{2^{h^+}} \equiv 1 \bmod \mathfrak{q}_1^2 \quad \text{and} \quad w \equiv 1 \bmod \mathfrak{q}_j^2 \quad \text{for } 2 \leq j \leq r.$$

We put $w_i = w^{\rho^{i-1}}$ for each i with $1 \leq i \leq r$. Then we see that for each i,

$$\frac{w_i}{2^{h^+}} \equiv 1 \bmod \mathfrak{q}_i^2, \quad \text{and} \quad w_i \equiv 1 \bmod \mathfrak{q}_j^2 \quad \text{for any } j \neq i, \tag{16}$$

and that

$$2^{h^+} = w_1 \cdots w_r. \tag{17}$$

As $\mathcal{F} = K^+(\sqrt{2d})$ and h^+ is odd, $\mathcal{F}(\sqrt{w_i}) = \mathcal{F}(\sqrt{w_i/2^{h^+}d})$. Therefore, we see from (15) and (16) that

$$L = \mathcal{F}(\sqrt{w_i} \mid 1 \leq i \leq r)$$

is an unramified extension over $\mathcal{F}$ by [13, Exercise 9.3].

We put $X = \mathcal{F}^\times/(\mathcal{F}^\times)^2$ for brevity, and let V be the subgroup of X generated by r elements $[w_i]$ $(1 \leq i \leq r)$. Here, $[x]$ denotes the class in X containing an element $x \in \mathcal{F}^\times$. These groups are naturally regarded as vector spaces over $\mathbb{F}_2$.

Lemma 7. *Under the above setting, the demension of the vector space V equals r.*

Proof. We put

$$x = \prod_{i=1}^{r} w_i^{s_i}$$

with $0 \leq s_i \leq 1$. If x is a square in $\mathcal{F}$, then we see that x or $2dx$ is a square in K^+ because $x \in K^+$ and $\mathcal{F} = K^+(\sqrt{2d})$. If x is a square in K^+, then $\prod_i(\mathfrak{q}_i\mathcal{O}_{K^+})^{h^+s_i}$ is a square of an ideal of K^+. It follows that $s_i = 0$ since h^+ is odd and the prime ideal $\mathfrak{q}_i$ remains prime in K^+/k. If $2dx$ is a square in K^+, then we obtain $K = K^+(\sqrt{d}) = K^+(\sqrt{2x})$. However, this is impossible because K/K^+ is ramified at $\wp$ but $K^+(\sqrt{2x})/K^+$ is unramified at $\wp$. Thus we obtain the assertion. $\square$

From Lemmas 5 and 7, we obtain:

Proposition 4. *Under the above setting, the unramified extension $L/\mathcal{F}$ corresponds to the class group $A_\mathcal{F}/A_\mathcal{F}^2$.*

Proof of Proposition 1. The group X is naturally regarded as a module over $R = \mathbb{Z}_2[\Gamma]$. Then V is a cyclic R-submodule of X generated by $[w]$. By Proposition 4, the class group $A_\mathcal{F}/A_\mathcal{F}^2$ is isomorphic to the Galois group $G = \mathrm{Gal}(L/\mathcal{F})$ via the reciprocity law map which is compatible with the action of Γ. The Kummer pairing

$$G \times V \to \mu_2;\ (g, [v]) \to \langle g, v\rangle = (\sqrt{v})^{g-1}$$

is nondegenerate and satisfies $\langle g^\delta, v^\delta\rangle = \langle g, v\rangle$ for $g \in G$, $[v] \in V$ and $\delta \in \Gamma$. Therefore, we obtain an isomorphism

$$G \cong H = \mathrm{Hom}(V, \mu_2)$$

of R-modules. Here, $\delta \in \Gamma$ acts on $f \in H$ by the rule $f^\delta([v]) = f([v]^{\delta^{-1}})$. As V is cyclic over R, so is the Galois group G. Therefore, we see that $A_\mathcal{F}/A_\mathcal{F}^2$ is cyclic over R from the above. This implies that $A_\mathcal{F}$ is cyclic over R by Nakayama's lemma ([13, Lemma 13.16]). $\square$

6 Unramified cyclic quartic extension

In this section, we consider which unramified quadratic extension over $\mathcal{F}$ extends to an unramified cyclic quartic extension when $r_4(A_\mathcal{F}) \geq 1$. We use the same notation as in the previous sections. In the following, we let $e \geq 2$ and $\kappa = \kappa_p = 0$ in view of Corollary 2. Let $\Gamma^+ = \mathrm{Gal}(K^+/\mathbb{Q})$, $\rho = \gamma_{|K^+}$ and $R^+ = \mathbb{F}_2[\Gamma^+]$. Let W be the subgroup of $X^+ = (K^+)^\times/((K^+)^\times)^2$ generated by the classes $[w_i]$ in X^+. The group X^+ is naturally regarded as a module over R^+, and W as an R^+-submodule of X^+. In this section, we use Γ^+, R^+ and W instead of Γ, R and V. This is justified because the inclusion map $K^+ = \mathcal{F}^+ \to \mathcal{F}$ induces an isomorphism between the abelian groups W and V because of Lemma 7. The module W is cyclic over R^+ with a generator $[w]$ similary to V. Further, it follows from Lemma 7 that $\dim_{\mathbb{F}_2} W = \dim_{\mathbb{F}_2} R^+ = 2^e$. Hence, the cyclic R^+-module W is also free over R^+. Namely we have

$$W = R^+ \cdot [w] \cong R^+. \tag{18}$$

This is the advantage of using W in place of V.

Let U_i be the principal ideal of R^+ generated by $(1+\rho)^i$ for $0 \leq i \leq 2^e$. We have a filtration

$$U_0 = R \supset U_1 \supset \cdots \supset U_{2^e-1} \supset U_{2^e}. \tag{19}$$

We see that

$$(1+\rho)^{2^e-1} = \sum_{t=0}^{2^e-1} \rho^t \ (:= \mathrm{Tr}) \quad \text{and} \quad (1+\rho)^{2^e} = 0. \tag{20}$$

It follows that

$$U_{2^e-1} = \{0, \mathrm{Tr}\} \quad \text{and} \quad U_{2^e} = \{0\}. \tag{21}$$

Lemma 8. *The ideals U_i are all the ideals of R^+ and $\dim_{\mathbb{F}_2} U_i = 2^e - i$.*

Proof. We see from (20) that the homomorphism $\varphi : \mathbb{F}_2[T] \to R^+$ sending $1+T$ to ρ induces an isomorphism

$$\mathbb{F}_2[T]/(T^{2^e}) \cong R^+.$$

From this we obtain the assertion. $\square$

For each j with $0 \leq j \leq 2^e$, letting $i = 2^e - j$, we put

$$L_j = \mathcal{F}(\sqrt{w^x} \mid x \in U_i).$$

From (17) with $r = 2^e$, (19) and (21), we have

$$L_0 = \mathcal{F} \subset L_1 = \mathcal{F}(\sqrt{2}) \subset \cdots \subset L_{2^e-1} \subset L_{2^e} = L.$$

Proposition 5. *Let $e \geq 2$ and $\kappa_p = 0$.*

(I) *When $r_4(A_{\mathcal{F}}) = j$ with $1 \leq j \leq 2^e$, an unramified quadratic extension $E/\mathcal{F}$ extends to an unramified quartic cyclic extension if and only if $E \subseteq L_j$.*

(II) *The unramified extension $\mathcal{F}(\sqrt{2})/\mathcal{F}$ extends to an unramfied quartic cyclic extension.*

Proof. First we show the assertion (I). Let $E_1/\mathcal{F}$ and $E_2/\mathcal{F}$ be quadratic extensions contained in L with $E_1 \neq E_2$, and let $E_3/\mathcal{F}$ be the third quadratic extension in the $(2,2)$-extension $E_1E_2/\mathcal{F}$. We see that if both of E_1 and E_2 extend to unramified quartic cyclic extensions, then E_3 has the same property. Let N_j be the composite of all unramified quadratic extensions $E/\mathcal{F}$ which extends to an unramfied quartic cyclic extension. Then, from the above and $j = r_4(A_{\mathcal{F}})$, we see that $\mathrm{Gal}(N_j/\mathcal{F}) \cong (\mathbb{Z}/2)^{\oplus j}$. Further, we see that N_j is Galois over $\mathbb{Q}$. Let W_j be the submodule of W such that

$$N_j = \mathcal{F}(\sqrt{v} \mid [v] \in W_j).$$

As N_j is Galois over $\mathbb{Q}$, W_j is an R^+-submodule of W with $\dim_{\mathbb{F}_2}(W_j) = j$. Then we see from (18) and Lemma 8 that $W_j = U_iW = U_i\cdot[w]$ with $i = 2^e - j$. Therefore, we obtain $N_j = L_j$. Thus we have shown the assertion (I). The assertion (II) follows from (I) because $r_4(A_{\mathcal{F}}) \geq 1$ by Corollary 2. $\square$

7 Numerical data

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

and various prime numbers $p < 10^6$ (or 10^7), and we put $e_p = \mathrm{ord}_2(p-1)-1$ so that $p = 2^{e_p+1}q+1$ with $2 \nmid q$. Further, $\mathcal{F} = \mathcal{F}_p$, $\kappa = \kappa_p$, $A_{\mathcal{F}}$ and $h_{\mathcal{F}}$ are the same as in §1. In Table 1, we give the number of prime numbers p with $(e_p, \kappa_p) = (e, \kappa)$ for $p < 10^6$. For instance, on the row for $e = 4$, we see that the ratio $155 : 150 : 312 : 621 : 1218$ is approximately equal to $1 : 1 : 2 : 4 : 8$. This is because of the Chebotarev density theorem on the ray class group of $M_e = \mathbb{Q}(\zeta_{2^{e+1}})$ corresponding to the abelian extension $M_e(2^{1/2^{e+1}})/M_e$.

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

$e \backslash \kappa$	0	1	2	3	4	5	6	7	8	9	total
0	19669	19653	0	0	0	0	0	0	0	0	39322
1	0	0	19623	0	0	0	0	0	0	0	19623
2	2471	2426	4894	0	0	0	0	0	0	0	9791
3	600	609	1206	2434	0	0	0	0	0	0	4849
4	155	150	312	621	1218	0	0	0	0	0	2456
5	38	34	69	174	294	624	0	0	0	0	1233
6	11	12	24	29	71	149	322	0	0	0	618
7	0	1	3	11	22	41	83	146	0	0	307
8	3	1	1	0	7	18	18	33	72	0	153
9	0	0	1	2	2	2	2	10	19	34	72

$e \backslash \kappa$	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	total
10	1	0	1	1	1	5	7	15	0	0	0	0	0	0	0	31
11	0	0	1	2	1	1	1	4	15	0	0	0	0	0	0	25
12	0	0	0	0	1	0	0	1	2	5	0	0	0	0	0	9
13	0	0	0	0	0	0	0	0	1	1	2	0	0	0	0	4
14	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	2
15	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

In the following, we let $e_p \geq 2$ because $2 \| h_{\mathcal{F}}$ when $e_p = 1$ by Proposition 2(I). When $\kappa_p \geq 1$, we have $A_{\mathcal{F}} \cong (\mathbb{Z}/2)^{\oplus r}$ with $r = 2^{e_p-\kappa_p+1}$ and the 4-rank $r_4(A_{\mathcal{F}}) = 0$ by Theorem 1. On the other hand, when $\kappa_p = 0$, we have $r_4(A_{\mathcal{F}}) > 0$ by Corollary 2. Therefore, we see from Table 1 that there are $3278 = 2471 + 600 + 155 + 38 + 11 + 3$ prime numbers p with $r_4(A_{\mathcal{F}}) > 0$ in the range $p < 10^6$.

We already know the precise structure of $A_{\mathcal{F}}$ when $\kappa_p = 0$ and $e_p = 2$

by Corollary 1. When $e_p \geq 3$, to know the structure of $A_{\mathcal{F}}$, we need to know the value $t_p = \mathrm{ord}_2(h_{\mathcal{F}})$ in view of Theorem 2. By Proposition 2(III), $t_p \geq 2^{e_p+2}$. We computed t_p for $p < 10^6$ with $e_p \geq 3$ and $\kappa_p = 0$ by the class number formula (4). Let $n_{e,t}$ be the number of prime numbers p with $(e_p, \kappa_p, t_p) = (e, 0, t)$ in the range. Let $p_{e,t}$ be the minimum prime number p satisfying $(e_p, \kappa_p, t_p) = (e, 0, t)$. In Table 2, we give $n_{e,t}$ and $p_{e,t}$ for each e and t.

Table 2: The exponent of 2-class number and the minimum primes.

e	t	$n_{e,t}$	$p_{e,t}$	e	t	$n_{e,t}$	$p_{e,t}$	e	t	$n_{e,t}$	$p_{e,t}$
3	10	309	337	4	18	85	2593	5	34	18	15809
	11	112	43441		19	31	26849		35	8	131009
	12	80	39761		20	21	10657		36	1	868801
	13	49	28657		21	13	68449		37	6	83777
	14	25	12049		22	8	138977		38	4	92737
	15	5	79889		23	2	598817		39	1	470081
	16	11	34961		24	6	31649				
	17	7	44497		25	1	476513				
	18	2	57457		26	2	572321				

e	t	$n_{e,t}$	$p_{e,t}$	e	t	$n_{e,t}$	$p_{e,t}$
6	66	6	266369	8	258	3	115201
	67	2	195457				
	68	2	299393				
	70	1	710273				

By Theorem 2, the 8-rank $r_8(A_{\mathcal{F}})$ is positive if and only if $t > 2^{e+1}$. In Table 2, we see that the condition $t > 2^{e+1}$ is satisfied only when $(e, t) = (3, 17)$ or $(3, 18)$ and that there are $9 = 7+2$ prime numbers with $r_8(A_{\mathcal{F}}) > 0$ in the range $p < 10^6$. These prime numbers are $p = 44497$, 79697, 103409, 162257, 717841, 797201 and 921841 with $(e, t) = (3, 17)$, and $p = 57457$ and 875377 with $(e, t) = (3, 18)$. By Theorem 2, we have

$$A_{\mathcal{F}} \cong (\mathbb{Z}/4)^{\oplus 7} \oplus \mathbb{Z}/8 \quad \text{or} \quad A_{\mathcal{F}} \cong (\mathbb{Z}/4)^{\oplus 6} \oplus (\mathbb{Z}/8)^{\oplus 2}.$$

according as $t = 17$ or 18.

Further, we computed t_p for $p < 10^7$ with $e_p = 3$ and $\kappa_p = 0$. Let $n'_{3,t}$ be the number of prime numbers with $(e_p, \kappa_p, t_p) = (3, 0, t)$ in the range. In Table 3, we give $n'_{3,t}$, $p_{3,t}$ and the structure of $A_{\mathcal{F}}$ for each t.

Table 3: The exponent of 2-class number ($p < 10^7$).

t	$n'_{3,t}$	$p_{3,t}$	$A_{\mathcal{F}}$
10	2610	337	$(\mathbb{Z}/2)^{\oplus 6} \oplus (\mathbb{Z}/4)^{\oplus 2}$
11	1164	43441	$(\mathbb{Z}/2)^{\oplus 5} \oplus (\mathbb{Z}/4)^{\oplus 3}$
12	707	39761	$(\mathbb{Z}/2)^{\oplus 4} \oplus (\mathbb{Z}/4)^{\oplus 4}$
13	321	28657	$(\mathbb{Z}/2)^{\oplus 3} \oplus (\mathbb{Z}/4)^{\oplus 5}$
14	194	12049	$(\mathbb{Z}/2)^{\oplus 2} \oplus (\mathbb{Z}/4)^{\oplus 6}$
15	94	79889	$(\mathbb{Z}/2) \oplus (\mathbb{Z}/4)^{\oplus 7}$
16	75	34961	$(\mathbb{Z}/4)^{\oplus 8}$
17	37	44497	$(\mathbb{Z}/4)^{\oplus 7} \oplus (\mathbb{Z}/8)$
18	7	57457	$(\mathbb{Z}/4)^{\oplus 6} \oplus (\mathbb{Z}/8)^{\oplus 2}$
19	10	2347409	$(\mathbb{Z}/4)^{\oplus 5} \oplus (\mathbb{Z}/8)^{\oplus 3}$
20	3	3295249	$(\mathbb{Z}/4)^{\oplus 4} \oplus (\mathbb{Z}/8)^{\oplus 4}$
21	3	3238801	$(\mathbb{Z}/4)^{\oplus 3} \oplus (\mathbb{Z}/8)^{\oplus 5}$
22	1	5897329	$(\mathbb{Z}/4)^{\oplus 2} \oplus (\mathbb{Z}/8)^{\oplus 6}$
26	1	6765169	$(\mathbb{Z}/8)^{\oplus 6} \oplus (\mathbb{Z}/16)^{\oplus 2}$

Among 5227 prime numbers, there is only one prime number such that the 16-rank of $A_{\mathcal{F}}$ is positive.

References

[1] H. Cohn and J. C. Lagarias, On the existence of fields governing the 2-invariants of the classgroup of $\mathbb{Q}(\sqrt{dp})$ 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] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952. Reprinted with an introduction by J. Martine; Springer, Berlin, 1985.

[4] H. Ichimura, Triviality of Stickelberger ideals of conductor p, J. Math. Sci. Univ. Tokyo, **13** (2006), no. 4, 617-628.

[5] K. Iwasawa, Lectures on p-Adic L-Functions, Annals of Math. Stud., No. 74. Princeton Univ. Press, Princeton, N. J.; Univ. Tokyo Press, Tokyo, 1972.

[6] H. Jung and Q. Yue, 8-ranks of class groups of imaginary quadratic number fields and their densities, J. Korean Math. Soc., **48** (2011), no. 6, 1249-1268.

[7] Y. Kida, Cyclotomic $\mathbb{Z}_2$-extension of J-fields, J. Number Theory, **14** (1982), no. 3, 340-352.

[8] D. Milovic, On the 16-rank of class groups of $\mathbb{Q}(\sqrt{-8p})$ for $p \equiv -1 \bmod 4$, Geom. Funct. Anal., **27** (2017), no. 4, 973-1016.

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

[10] W. Narkiewicz, Elementrary and Analytic Theory of Algebraic Numbers (3rd ed.), Springer, Berlin, 2004.

[11] L. Rédei und H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe im quadratischer Zahlkörper, J. Reine Angew. Math., **170** (1933), 69-74.

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

[13] L. C. Washington, Introduction to Cyclotomic Fields (2nd. ed.), Springer, New York, 1987.

[14] A. Wiles, Iwasawa conjecture for totally real fields, Ann. of Math., **131** (1990), no. 3, 493-540.

[15] 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.

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

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

[18] Q. Yue, Class groups under relative quadratic extensions, Acta Arith., **150** (2011), no. 4, 399-414.

[19] L. Zhang and Q. Yue, Another case of a Scholz's theorem on class groups, Int. J. Number Theory, **4** (2008), no. 3, 459-501.