Note on class number parity of an abelian field of prime conductor

Shoichi Fujima* and Humio Ichimura**

Abstract

Let $n \geq 1$ be an integer and let $2^e$ be the highest power of 2 dividing $n$. For a prime number $p = 2n\ell + 1$ with an odd prime number $\ell$, let $N$ be the imaginary abelian field of conductor $p$ and degree $2^{e+1}\ell$ over $\mathbb{Q}$. We show that for $n \leq 30$, the relative class number $h_N^-$ of $N$ is odd when 2 is a primitive root modulo $\ell$ except for the case where $(n, \ell) = (27, 3)$ and $p = 163$ with the help of computer.

1. Introduction

For an odd prime number $p$, let $h_p^-$ denote the relative class number of the $p$th cyclotomic field $\mathbb{Q}(\zeta_p)$. When $p$ is of the form $p = 2\ell + 1$ with an odd prime number $\ell$, it is conjectured that $h_p^-$ is odd. There are many results related to the conjecture. In particular, it is known that $h_p^-$ is odd when 2 is a primitive root modulo $\ell$. This is first proved by Davis [4], and several different proofs are given, for instance, in Metsänkylä [17, Corollary 1] and Stevenhagen [20, Corollary 2.3]. This result is extended to the case where $p$ is of the form $p = 2^{e+1}\ell + 1$ with an odd prime number $\ell$ when $e = 1$ by [17, Corollary 2] and when $2 \leq e \leq 4$ by the authors [7, Theorem 1].

In this paper, we deal with a more general case. Let $n \geq 2$ be a fixed integer, and let $2^e$ be the highest power of 2 dividing $n$. We consider a prime number $p$ of the form $p = 2n\ell + 1$ with an odd prime number $\ell$. It is conjectured that there exist infinitely many such $p$ and $\ell$ by Hardy and Littlewood [8, Conjecture D]. Let $k$ and $F$ be the imaginary (resp. real) subfield of $\mathbb{Q}(\zeta_p)$ with degree $2^{e+1}\ell$ (resp. $\ell$) over $\mathbb{Q}$, and set $N = kF$. For a number field $M$, let $h_M$ be the class number of $M$ in the usual sense. When $M$ is an imaginary abelian field, let $h_M^+ = h_M/h_M^+$ be the relative class number of $M$. Here, $M^+$ denotes the maximal real subfield of $M$. Our target is the relative class number $h_N^-$ of $N$. This is nothing but $h_p^-$ when $n$ is a power of 2. In addition to the case $n = 2^e$ with $0 \leq e \leq 4$, it is known that for $n = 3$ or 5, $h_N^-$ is odd.
when 2 is a primitive root modulo ℓ ([11, Remark 2], [12, Corollary 1]). In this paper, we generalize these results on the parity of $h_N^-$ as follows, with the help of computer.

**Theorem.** Under the above setting, let $n \leq 30$. Then the relative class number $h_N^-$ is odd whenever 2 is a primitive root modulo $\ell$ except for the case where $(n, \ell) = (27, 3)$ and $p = 163$. For the exceptional case, $h_N^-$ is even.

It is known that when 2 is a primitive root modulo $\ell$, $h_N^-$ is odd if and only if $h_F$ is odd by Cornacchia [2, Theorem 1]:

$$2 \nmid h_N^- \iff 2 \nmid h_F.$$  \hfill (1.1)

(See [10, Theorem 4], for an alternative proof.) On the parity of $h_F$, we showed in [12, Theorem 2] the following:

**Proposition 1.** Under the above setting, $h_F$ is odd if the following two conditions are satisfied.

(i) 2 is a primitive root modulo $\ell$.

(ii) $p = 2n\ell + 1 > (2n - 1)^{\phi(2n)}$ where $\phi(*)$ is the Euler function.

By virtue of Proposition 1 and the equivalence (1.1), for proving the Theorem, it suffices to show that the class number $h_F$ or $h_N^-$ is odd for all prime numbers $p = 2n\ell + 1$ such that 2 is a primitive root modulo $\ell$ and $p < m_n = (2n - 1)^{\phi(2n)}$. This method is effective for very small $n$. Actually, when $n \leq 5$ (and hence $m_n \leq 6551$), we can use the tables in Cornacchia [3] and Koyama and Yoshino [15] on real abelian fields of prime conductor $< 10000$ with even class number. However, the value $m_n$ is, in general, so large ($m_{20} \sim 10^{49.16}$ for instance) that it is hopeless to deal with the class numbers for all such large $p$’s. We, therefore, prepare a refined version of this proposition (Proposition 3 in §3) which involves a smaller number of smaller prime numbers, and prove the theorem with the powerful help of computer.

**Remark 1.** When $n$ is not so small and $\ell$ is relatively small compared to $n$, there do exist several examples of $(n, \ell)$ other than $(27, 3)$ such that (i) $p = 2n\ell + 1$ is a prime number, (ii) 2 is a primitive root modulo $\ell$ but (iii) $h_N^-$ is even (or equivalently $h_F$ is even), such as $(n, \ell) = (46, 3), (58, 3), (94, 5), (216, 5)$. We can find them in the tables in [3] and [15] mentioned above. However, when $n = 2^e$, in spite of our vigorous computation in [7], we could not find any example of $(n, \ell)$ satisfying the above three conditions (i)–(iii).

**Remark 2.** There are several other results on indivisibility of the class numbers $h_F$ and $h_N^-$ such as [11, 12, 13, 14, 16].

2. **Criterion**

Let $n$ and $e$ be as in §1. We assume that $n \geq 2$ in all what follows because the Theorem is already settled for the case $n = 1$ by [4]. Let $p = 2n\ell + 1$ be a prime number with an odd prime number $\ell$, and let $k$, $F$ and $N = kF$ be the subfields of $\mathbb{Q}(\zeta_p)$ defined in §1. For simplicity, we assume that

$$\ell \nmid n$$
Note on class number parity of an abelian field of prime conductor

in this section. (The assumption is harmless because in the range of our computation, the case where \( \ell \) divides \( n \) is so rare.) For \( x \in \mathbb{Z} \), we denote by \( s_p(x) \) the unique integer such that \( s_p(x) \equiv x \mod p \) and \( 0 \leq s_p(x) \leq p - 1 \). We fix a primitive root \( g \) modulo \( p \). We put

\[
x_u = \sum_{v=0}^{n-1} s_p(g^{2nu+\ell v})
\]

for each \( 0 \leq u \leq \ell - 1 \), and

\[
G(T) = G_{n,\ell}(T) = \sum_{u=0}^{\ell-1} x_u T^u \in \mathbb{Z}[T].
\]

Further, let \( \Phi_\ell(T) \) denote the \( \ell \)th cyclotomic polynomial. Let \( D(T) \) be the greatest common divisor of \( G(T) \mod 2 \) and \( \Phi_\ell(T) \mod 2 \) in \( \mathbb{F}_2[T] \) where \( \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} \):

\[
D(T) = \gcd(G(T) \mod 2, \Phi_\ell(T) \mod 2).
\]

The following lemma is a consequence of the classical class number formula for \( h_N^{-} \).

**Lemma 1.** Under the above setting, assume that \( \ell \mid n \). Then \( h_N^{-} \) is even if and only if \( \deg D(T) \geq 1 \). Moreover, when \( 2 \) is a primitive root modulo \( \ell \), \( h_N^{-} \) is even if and only if the following congruences hold:

\[
x_0 \equiv x_1 \equiv \cdots \equiv x_{\ell-1} \mod 2.
\]

**Proof.** By [21, Theorem 10.4(b)], we know that \( h_k^{-} \) is odd. Hence, the parity of \( h_N^{-} \) coincides with that of the ratio \( h_N^{-}/h_k^{-} \). The unit index of an imaginary abelian field of conductor \( p \) is 1 by Hasse [9, Satz 23]. Therefore, it follows from the class number formula [21, Theorem 4.17] that

\[
h_N^{-}/h_k^{-} = p^\delta \prod_{\varphi: \chi} \left( -\frac{1}{2} B_1,\varphi\chi \right)
\]

where \( \delta = 1 \) or 0 according as \( n \) is a power of 2 or not, and \( \varphi \) (resp. \( \chi \)) runs over the odd (resp. even) Dirichlet characters of conductor \( p \) and order \( 2^{e+1} \) (resp. \( \ell \)). Further,

\[
B_1,\psi = \frac{1}{f} \sum_{a=1}^{f-1} a \psi(a)
\]

denotes the generalized Bernoulli number associated to a Dirichlet character \( \psi \) of conductor \( f \). Because of the assumption \( \ell \mid n \), we see that the integers \( 2nu + \ell v \) with \( 0 \leq u \leq \ell - 1 \) and \( 0 \leq v \leq 2n - 1 \) constitute a complete set of representatives of the additive group \( \mathbb{Z}/2nf\mathbb{Z} \). It follows that

\[
\{ g^{2nu+\ell v} \mod p \mid 0 \leq u \leq \ell - 1, 0 \leq v \leq 2n - 1 \} = (\mathbb{Z}/p\mathbb{Z})^\times.
\]
We fix characters $\varphi$ and $\chi$ in the class number formula (2.2), and we put $\xi = \zeta_{2^{n-1}} = \varphi(g^f)$ and $\zeta_\ell = \chi(g^{2n})$. Clearly, these are primitive $2^{r+1}$st and $\ell$th roots of unity, respectively. Noting that $g^{f_n} \equiv 1 \mod p$ and $\xi^n = 1$, we observe that

$$\frac{1}{2} B_{1, \varphi \chi} = \frac{1}{2p} \sum_{u=0}^{\ell-1} \sum_{v=0}^{2n-1} s_p(g^{2nu+\ell v}) \xi^v \zeta_\ell^u$$

$$= \frac{1}{2p} \sum_{u=0}^{\ell-1} \sum_{v=0}^{n-1} (s_p(g^{2nu+\ell v}) \xi^v - s_p(-g^{2nu+\ell v}) \xi^v) \zeta_\ell^u$$

$$= \frac{1}{2p} \sum_{u=0}^{\ell-1} \sum_{v=0}^{n-1} s_p(g^{2nu+\ell v}) \xi^v \zeta_\ell^u \in \mathbb{Q}(\zeta_{2^{n+1}}, \zeta_\ell).$$

Here, the last equality holds because $s_p(-x) = p - s_p(x)$ for an integer $x$ with $p \nmid x$. Let $\mathcal{O}$ be the product of prime ideals of $\mathbb{Q}(\zeta_{2^{n+1}}, \zeta_\ell)$ over 2. Then, as $\xi \equiv 1 \mod \mathcal{O}$, we see from the above that

$$\frac{1}{2} B_{1, \varphi \chi} \equiv G(\zeta_\ell) \mod \mathcal{O} \quad \text{with} \quad \zeta_\ell = \chi(g^{2n}).$$

Therefore, from the class number formula (2.2), we obtain the first assertion of Lemma 1. The second one follows immediately from the first one because $\Phi_\ell \mod 2$ is irreducible over $\mathbb{F}_2$ when 2 is a primitive root modulo $\ell$. \hfill \qed

3. Refined version of Proposition 1

To give a refined version of Proposition 1, let us recall some notation and results in [12]. Let $I$ be the set of integers $i$ with $0 \leq i \leq n - 1$, and for each $a \in I$, let $I_a = I \setminus \{a\}$. We denote by $\Psi$ (resp. $\Psi_a$) the set of all maps from $I$ (resp. $I_a$) to $\{0, 1\}$. We choose and fix a primitive $2n$th root of unity $\epsilon = \zeta_{2n}$. We put

$$\alpha(\kappa) = \sum_{i \in I} \kappa(i) \epsilon^i \quad \text{and} \quad \beta(a, \kappa) = \sum_{i \in I_a} \kappa(i) \epsilon^i$$

for each $\kappa \in \Psi$ and each pair $(a, \kappa) \in I \times \Psi_a$, respectively. Fixing a map $\kappa_0 \in \Psi_0$, we define elements $X_\kappa$ and $Y_{a, \kappa}$ of the 2nd cyclotomic field $\mathbb{Q}(\zeta_{2n})$ by

$$X_\kappa = 2\alpha(\kappa) - 1 - 2\beta(0, \kappa_0) \quad \text{and} \quad Y_{a, \kappa} = \epsilon^a + 2\beta(a, \kappa) - 1 - 2\beta(0, \kappa_0)$$

for $\kappa \in \Psi$ and for a pair $(a, \kappa) \in I \times \Psi_a$ with $(a, \kappa) \neq (0, \kappa_0)$, respectively. We have shown that $X_{\kappa} \neq 0$ and that $Y_{a, \kappa} \neq 0$ if $a \neq 0$ for any choice of $\kappa_0 \in \Psi_0$ in [12, Lemma 8]. (See the proof of the assertions (i) and (iii) of [12, Lemma 8].) In [12, Lemma 8], we further showed that we can choose $\kappa_0 \in \Psi_0$ so that

$$Y_{0, \kappa} \neq 0 \quad \text{for any} \ \kappa \in \Psi_0 \ \text{with} \ a \neq 0. \quad (3.1)$$

We fix such a map $\kappa_0$. Then the norms $\text{Nr}(X_\kappa)$ and $\text{Nr}(Y_{a, \kappa})$ are non-zero integers because of (3.1), where $\text{Nr}$ denotes the norm map from $\mathbb{Q}(\zeta_{2n})$ to $\mathbb{Q}$. Let $P_1^0(\kappa_0)$ be
Because of (3.2), we have some (a,κ) ≠ (0,κ0). The set \( P^0_n(κ_0) \) is finite because \( \text{Nr}(X_n) \neq 0 \) and \( \text{Nr}(Y_{a,κ}) \neq 0 \). Let \( P_n(κ_0) \) be the subset of \( P^0_n(κ_0) \) consisting of prime numbers \( p \in P^0_n(κ_0) \) of the form \( p = 2n\ell + 1 \) with an odd prime number \( \ell \) such that \( \ell \nmid n \) and 2 is a primitive root modulo \( \ell \). Of course, the sets \( P^0_n(κ_0) \) and \( P_n(κ_0) \) depend on the choice of the map \( κ_0 \). The set \( P_n(κ_0) \) is more convenient than \( P^0_n(κ_0) \) for showing the Theorem with the help of computer. The following assertion is a refined version of Proposition 1.

**Proposition 2.** Let \( n \geq 2 \) be a fixed integer, and let \( κ_0 \in Ψ_0 \) be a map satisfying (3.1). Let \( p = 2n\ell + 1 \) be a prime number where \( \ell \) is an odd prime number such that 2 is a primitive root modulo \( \ell \).

(I) The class number \( h_γ \) is odd if \( p \not\in P^0_n(κ_0) \).

(II) When \( \ell \nmid n \), \( h_γ \) is odd if \( p \not\in P_n(κ_0) \).

The assertion (I) is a consequence of Theorem 2(II) and Remark 6 of [12] combined with the equivalence (1.1). The assertion (II) follows immediately from (I).

**Remark 3.** In [12, Lemma 9], we showed that if \( p = 2n\ell + 1 \) satisfies condition (ii) of Proposition 1, then \( p \not\in P^0_n(κ_0) \) for any \( κ_0 \in Ψ_0 \) satisfying the condition (3.1). In this sense, Proposition 2 is sharper than Proposition 1.

In all what follows, we choose \( κ_0 \in Ψ_0 \) so that

\[
κ_0(i) = 0 \quad \text{for all } i ∈ I_0. \tag{3.2}
\]

When \( n = 2^e r^f \) with some odd prime number \( r \), this \( κ_0 \) satisfies the condition (3.1) because of the following lemma. Therefore, when \( 2 \leq n \leq 30 \) (the range of our computation), the above choice of \( κ_0 \) is justified except for \( n = 15, 21 \) and 30. For \( n = 15, 21 \) and 30, we computed all the norms \( \text{Nr}(Y_{a,κ}) \) for \( κ \neq κ_0 \), and checked that they are not zero and hence (3.1) is satisfied. Thus, the choice (3.2) of \( κ_0 \) is justified in the range of our computation.

**Lemma 2.** Assume that \( n = 2^e r^f \) for some odd prime number \( r \) and integers \( e, f \geq 0 \). Then the above map \( κ_0 \) satisfies the condition (3.1).

**Proof.** Let \( n = 2^e r^f \) be as above, and let \( Φ_{2n}(T) \) be the 2n-th cyclotomic polynomial. First we assume that \( f \geq 1 \). We have

\[
Φ_{2n}(T) = \frac{T^{2^e r^f} + 1}{T^{2^e r^{f-1}} + 1} = T^{n - 2^e r^{f-1}} - T^{n - 2^e r^{f-1}} + \cdots. \tag{3.3}
\]

Because of (3.2), we have

\[
Y_{0,κ} = 2 \sum_{i=1}^{n-1} κ(i)ε^i = 2ε \times \sum_{i=0}^{n-2} κ(i + 1)ε^i.
\]

Therefore, it suffices to show that if a polynomial \( F(T) = \sum_{i=0}^{n-2} a_i T^i \in Ζ[T] \) with \( a_i = 0 \) or 1 satisfies \( F(ε) = 0 \), then \( F(T) = 0 \). We see that \( F(ε) = 0 \) if and only if \( F(T) \)
is divisible by $\Phi_{2n}(T)$ as $\Phi_{2n}$ is irreducible. Let $F(T) = \sum_{i=0}^{n-2} a_i T^i$ be a polynomial in $\mathbb{Z}[T]$ with $a_i = 0$ or 1, and assume that $F(T)$ is divisible by $\Phi_{2n}(T)$ but $F(T) \neq 0$. Put $m = \deg F(T)$. When $m \leq n - 2^e r^f - 1$, it follows that $m = n - 2^e r^f - 1$ and $\Phi_{2n}(T) = F(T)$ from the assumption and the irreducibility of $\Phi_{2n}$. This is impossible as the $(n - 2^{e+1} r^f - 1)$th coefficient of $\Phi_{2n}(T)$ is $-1$ by (3.3). When $n - 2^e r^f - 1 < m \leq n - 2$, we have

$$F(T) = \Phi_{2n}(T) \times (T^{m-n} + 2^e r^f - 1 + \text{lower terms}).$$

By (3.3), we see that from the product $\Phi_{2n}(T) \times T^{m-n} + 2^e r^f - 1$ appears the polynomial

$$T^m - T^{m-2^e r^f - 1} + \cdots.$$  

On the other hand, we see that the term $T^{m-2^e r^f - 1}$ does not appear from $\Phi_{2n}(T)$ times the lower terms in (3.4) because for $j < m - n + 2^e r^f - 1$,

$$n - 2^e r^f - 1 + j > m - 2^e r^f - 1 \quad \text{and} \quad n - 2^{e+1} r^f - 1 + j < m - 2^e r^f - 1.$$

Therefore, the $(m - 2^e r^f - 1)$th coefficient of the right-hand side of (3.4) is $-1$, and hence the equality (3.4) is impossible. Thus we obtain the assertion when $f \geq 1$. It is shown similarly when $f = 0$. \hfill \Box

4. Computation

First of all, we settle the case where $\ell$ divides $n$. There exist 11 pairs $(n, \ell)$ of an integer $2 \leq n \leq 30$ and an odd prime number $\ell$ dividing $n$ for which $p = 2n\ell + 1$ is a prime number and $2$ is a primitive root modulo $\ell$: $(n, \ell) = (3, 3), (6, 3), (10, 5), (12, 3), (15, 5), (18, 3), (21, 3), (25, 5), (26, 13), (27, 3)$ and $(30, 3)$. We see from the tables in [3] and [15] that among them, $2 \nmid h_F$ (or equivalently $2 \nmid h^-F$) except for the case where $(n, \ell) = (27, 3)$ and $p = 163$ and $h_F$ is even for the exceptional case.

In what follows, we confine ourselves to the case $\ell \mid n$ so that we can use Lemma 1 and Proposition 2(II). For each $2 \leq n \leq 30$, we computed the finite set $P_n = P_n(\kappa_0)$ in §3 for the map $\kappa_0$ defined in (3.2), and at the same time verified that the condition (3.1) is satisfied also for $n = 15, 21$ and 30. In Table 1, we give some data of the set $P_n$: the minimal and the maximal prime numbers contained in the set and the number of elements of the set. In particular, $P_n$ is the empty set for $n = 2, 3$. In Table 1, we find that the maximal prime number contained in the set $P_n$ is about the square root of the value $\mathfrak{m}_n = (2n - 1)^{\Theta(2n)}$ which appeared in condition (ii) of Proposition 1. This shows that Proposition 2 is much more sharper and fits to computation better than Proposition 1.

For each prime number $p = 2n\ell + 1 \in P_n = P_n(\kappa_0)$, we checked $h^-F$ is odd using Lemma 1 and obtain the theorem. Namely, we computed the coefficients $x_u$ of the polynomial $G(T) = G_{n, \ell}(T)$ defined in (2.1) for $x_0, x_1, x_2, \cdots$, until we find the first integer $j_0 \geq 1$ such that $x_{j_0} \neq x_0 \mod 2$. For each $9 \leq n \leq 30$, for which $|P_n| \geq 10$, we give in Table 2 the maximal value of $j_0$ when $p$ runs over the set $P_n$. Further, we give Tables 3 and 4 to show how the values of $j_0$ are distributed when $n = 29$ and $n = 30$ for example.
Note on class number parity of an abelian field of prime conductor

n’s, we find that the values of $j_0$ are distributed almost similarly. Tables 3 and 4 seem to suggest that the coefficients $x_n$ behave random modulo 2.

Let us explain our computation more precisely. We fix an integer $n \geq 2$, and let $\epsilon = \zeta_{2n}$. Let $\kappa_0 \in \Psi_0$ be the map defined in (3.2). We put

$$\mathbb{X}_n = \{X_\kappa \mid \kappa \in \Psi \} \cup \{Y_{a,\kappa} \mid (a, \kappa) \in I \times \Psi_a \text{ with } (a, \kappa) \neq (0, \kappa_0)\}.$$  

We put

$$U = \{\pm 1\} \times \{0, 1\} \times \cdots \times \{0, 1\}$$

and

$$V = U \setminus (\{\pm 1\} \times \{0, \cdots, 0\}).$$

For each $x = (x_0, x_1, \cdots, x_{n-1})$ in the set $U$ and each $a \in I_0$, we define integers $f(x)$, $g(x)$ and $h_a(x)$ in $\mathbb{Q}(\epsilon)$ by

$$f(x) = 2 \sum_{i \neq 0} x_i \epsilon^i, \quad g(x) = x_0 + f(x), \quad h_a(x) = x_0 + \epsilon^a + 2 \sum_{i \neq 0, a} x_i \epsilon^i.$$  

We put

$$Y_n = \{f(x) \mid x \in V\} \cup \{g(x), h_a(x) \mid x \in U, a \in I_0\}.$$  

Because of (3.2), we see that $\mathbb{X}_n = \mathbb{Y}_n$ with the correspondence

$$Y_{0,\kappa} \leftrightarrow f(x), \quad X_\kappa \leftrightarrow g(x), \quad Y_{a,\kappa} \leftrightarrow h_a(x),$$

for $a \neq 0$. Here $Y_{0,\kappa} = f(x)$ for some $x \in V$ because $\kappa \neq \kappa_0$.

For an element

$$\alpha = \sum_{i=0}^{n-1} a_i \epsilon^i \in \mathbb{Q}(\epsilon),$$

the norm $\text{Nr}(\alpha)$ is calculated as follows. We regard $\mathbb{Q}(\epsilon)$ as a vector space over $\mathbb{Q}$ with a basis

$$B = \{\epsilon^i \mid 0 \leq i \leq \phi(2n) - 1\}.$$  

Let $M_\alpha$ be the matrix representing the linear transformation of $\mathbb{Q}(\epsilon)$ sending each element $v$ to $\alpha v$ with respect to the basis $B$. Then we have

$$\text{Nr}(\alpha) = \det M_\alpha,$$  

(4.1)

for which see Fröhlich and Taylor [5, I, (1.27a)].

As $\text{Nr}(\alpha) = \text{Nr}(\epsilon \alpha) = \text{Nr}(\overline{\alpha})$, we have

$$\text{Nr}(\alpha) = \text{Nr}(-a_{n-1} + \sum_{i=1}^{n-1} a_{n-i} \epsilon^i) = \text{Nr}(a_0 - \sum_{i=1}^{n-1} a_{n-i} \epsilon^i),$$

(4.2)

where $\overline{\alpha}$ is the complex conjugate of $\alpha$. It enables us to eliminate duplication of elements of $\mathbb{Y}_n$ which give same norm values. We define a subset $\mathbb{Y}_n'$ of $\mathbb{Y}_n$ by

$$\mathbb{Y}_n' = \{f(x) \mid x \in V'\} \cup \{g(x), h_a(x) \mid x \in U', a \in I_0\},$$

(4.3)
Shoichi Fujima and Humio Ichimura

where

\[
U' = \{1\} \times \{0, 1\} \times \cdots \times \{0, 1\} \subset U,
\]

\[
V' = \{1\} \times \{1\} \times \{0, 1\} \times \cdots \times \{0, 1\} \subset V.
\]

Then from (4.2) we see that

\[
\{\text{Nr}(\alpha) | \alpha \in Y'_n\} = \{\text{Nr}(\alpha) | \alpha \in Y_n\},
\]

and we denote this set by \(Q_n\).

The size of \(Y'_n\) is \((n + 2)2^{n-2}\). Table 5 shows the ratio of \(|Q_n|\) obtained by computation to \(|Y'_n|\) in the cases \(21 \leq n \leq 30\). We see that the frequency that different elements of \(Y'_n\) have the same norms is smaller when \(\phi(2n)/n\) is larger.

The computation consists of four steps:

(i) Compute the set \(Q_n\) of the norms of \(\alpha \in Y'_n\) for each \(n\) using (4.1) and (4.3). (For \(n = 15, 21\) and 30, we find that \(0 \notin Q_n\).)

(ii) Factor all elements in \(Q_n\) as products of prime numbers, and make the set \(R_n = \mathbb{P}_n(\kappa_0)\) of the prime factors.

(iii) We make the set \(P_n = \mathbb{P}_n(\kappa_0)\); namely we extract from the set \(R_n\) those prime numbers \(p\) of the form \(p = 2n\ell + 1\) for some odd prime number \(\ell\) such that \(\ell \nmid n\) and 2 is a primitive root modulo \(\ell\).

(iv) For each \(p = 2n\ell + 1 \in P_n\), verify the oddness of \(h_{-n}\) with the method of Lemma 1.

Steps (iii) and (iv) include computation of a primitive root modulo \(\ell\) and \(p\), respectively, so that \(\ell - 1\) and \(p - 1\) are factored there, respectively. For the factorizations, we recursively employ compositeness test by Miller-Rabin method [18, 19] followed by Pollard’s \(\rho\) method (Brent’s modified algorithm [1]) for large composite numbers (> \(2^{46}\)) or by the trial division method using a prime number table for small ones (\(< 2^{46}\)).

The computation of this paper was executed in thread-parallel in about 50 threads of CPUs (Intel Core i5 and i7) in 12 personal computers. Total computation times for step (i) increased with the size of \(Y'_n\) (namely with \(n\)), e.g., 381, 1028 and 1646 hours for \(n = 28, 29\) and 30, respectively. Steps (ii) and (iii) took 2752, 8611 and 116 hours for them, respectively. The reasons of such dispersion are considered to be both the size of the set \(Q_n\) (see Table 5) and the size of each element of \(Q_n\) (see max \(P_n\) in Table 1). For details of the computed data, see [6].

References

[1] R. P. Brent, An improved Monte-Carlo factorization algorithm, BIT 20 (1980), no. 2, 176-184.

[2] P. Cornacchia, The parity of the class number of the cyclotomic fields of prime conductor, Proc. Amer. Math. Soc., 125 (1997), no. 11, 3163-3168.
Table 1. $P_n$, results of computation.

| $n$ | $|P_n|$ | min $P_n$ | max $P_n$ |
|-----|--------|-----------|-----------|
| 2   | 0      | –         | –         |
| 3   | 0      | –         | –         |
| 4   | 1      | 1         | 41        |
| 5   | 2      | 31        | 131       |
| 6   | 3      | 61        | 349       |
| 7   | 6      | 43        | 2423      |
| 8   | 2      | 593       | 977       |
| 9   | 12     | 199       | 14347     |
| 10  | 24     | 61        | 225221    |
| 11  | 39     | 67        | 1602899   |
| 12  | 57     | 313       | 510457    |
| 13  | 218    | 79        | 229519343 |
| 14  | 295    | 1709      | 240208949 |
| 15  | 309    | 331       | 2694631   |
| 16  | 2193   | 97        | 205620281249 |
| 17  | 3116   | 103       | 911538238427 |
| 18  | 3229   | 181       | 4811374549 |
| 19  | 19609  | 191       | 44935624972739 |
| 20  | 19813  | 521       | 5857043639561 |
| 21  | 19855  | 211       | 26386938607 |
| 22  | 174679 | 1277      | 15162335762044637 |
| 23  | 214350 | 139       | 256542896059736219 |
| 24  | 204682 | 241       | 84887023671313 |
| 25  | 1123743| 151       | 692999252589011451 |
| 26  | 1783809| 157       | 53874936788992994429 |
| 27  | 178834 | 271       | 8994267451978867 |
| 28  | 10577927| 281       | 372414297099293236313 |
| 29  | 15859433| 1103      | 267581589941982610559939 |
| 30  | 6335426 | 661       | 1561846392223861 |

Table 2. Maximum value of $j_0$ when $p$ runs over the set $P_n$

| $n$ | max $j_0$ |
|-----|-----------|
| 9   | 4         |
| 10  | 7         |
| 11  | 7         |
| 12  | 6         |
| 13  | 8         |
| 14  | 8         |
| 15  | 11        |
| 16  | 10        |
| 17  | 14        |
| 18  | 11        |
| 19  | 14        |
| 20  | 20        |
| 21  | 23        |
| 22  | 24        |
| 23  | 25        |
| 24  | 26        |
| 25  | 27        |
| 26  | 28        |
| 27  | 29        |
| 28  | 30        |
| 29  | 18        |
| 30  | 19        |

Note on class number parity of an abelian field of prime conductor
Table 3. distribution of $j_0$, in the case of $n = 29$

| $j_0$ | 1     | 2     | 3     | 4     | 5     | 6     | $\geq 7$ |
|------|-------|-------|-------|-------|-------|-------|---------|
|      | $N$   |       |       |       |       |       |         |
|      | 79.28691 | 39.64737 | 10.83326 | 0.910127 | 0.495311 | 0.248169 | 0.048187 |
|      | ratio(%) | 49.99 | 25.00 | 12.51 | 6.25 | 3.12 | 1.56 | 1.56 |

Table 4. distribution of $j_0$, in the case of $n = 30$

| $j_0$ | 1     | 2     | 3     | 4     | 5     | 6     | $\geq 7$ |
|------|-------|-------|-------|-------|-------|-------|---------|
|      | $N$   |       |       |       |       |       |         |
|      | 31.68877 | 15.85324 | 7.80193 | 3.95161 | 1.97982 | 1.98825 | 1.99064 |
|      | ratio(%) | 50.02 | 25.02 | 12.47 | 6.24 | 3.12 | 1.56 | 1.56 |

Table 5. $|Y'_n|$ and $|Q_n|$.

| $n$  | $|Y'_n|$ | $|Q_n|$ | ratio(%) |
|------|---------|---------|----------|
| 21   | 12058624 | 1676404 | 13.90    |
| 22   | 25165824 | 20671408 | 82.14   |
| 23   | 52428800 | 45396278 | 86.59   |
| 24   | 109051904 | 24765506 | 22.71  |
| 25   | 226492416 | 169551023 | 74.86  |
| 26   | 469762048 | 418170490 | 89.02  |
| 27   | 973078528 | 84145767  | 27.15  |
| 28   | 2013265920 | 1763120606 | 87.58  |
| 29   | 4160749568 | 3078727486 | 73.99  |
| 30   | 8589934592 | 843901472  | 9.82   |
Note on class number parity of an abelian field of prime conductor

[3] P. Cornacchia, The 2-ideal class groups of $\mathbb{Q}(\zeta_\ell)$, Nagoya Math. J., 162 (2001), 1–18.

[4] D. Davis, Computing the number of totally positive circular units which are square, J. Number Theory, 10 (1978), no. 1, 1-9.

[5] A. Fröhlich and M. J. Taylor, Algebraic Number Theory, Cambridge Univ. Press, Cambridge, 1993.

[6] S. Fujima, Supplementary files website for this paper, http://fujima.sci.ibaraki.ac.jp/clpari/.

[7] S. Fujima and H. Ichimura, Note on the class number of the $p$th cyclotomic field, II, Experiment. Math., 27 (2018), no. 1, 111-118.

[8] G. H. Hardy and J. E. Littlewood, Some problems of “Partitio numerorum”; III: On the expression of a number as a sum of primes, Acta Math., 44 (1923), no. 1, 1-70.

[9] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademia Verlag, Berlin, 1952.

[10] H. Ichimura, On a duality of Gras between totally positive and primary cyclotomic units, Math. J. Okayama Univ., 58 (2016), 125-132.

[11] H. Ichimura, Note on Bernoulli numbers associated to some Dirichlet character of prime conductor, Arch. Math. (Basel), 107 (2016), no. 6, 595-601.

[12] H. Ichimura, Triviality of Iwasawa module associated to some abelian fields of prime conductor, Abh. Math. Semin. Univ. Hambg., 88 (2018), no. 1, 51-66.

[13] S. Jakubec, On divisibility of class number of real abelian fields of prime conductor, Abh. Math. Sem. Univ. Hamburg, 63 (1993), 67-86.

[14] S. Jakubec, M. Pasteka and A. Schinzel, Class number of real abelian fields, J. Number Theory, 148 (2015), 365-371.

[15] Y. Koyama and K. Yoshino, Prime divisors of the class numbers of the real $p^r$th cyclotomic field and characteristic polynomial attached to them, RIMS Kōkyūroku Bessatsu 12 (2009), 149-177.

[16] T. Metsänkylä, Some divisibility results for the cyclotomic class number, Tatra Mt. Math. Publ., 11 (1997), 59-68.

[17] T. Metsänkylä, On the parity of the class numbers of real abelian fields, Acta Math. Univ. Ostraviensis, 6 (1998), no. 1, 159-166.

[18] G. Miller, Riemann’s hypothesis and tests for primality, J. Comput. System Sci., 13 (1976), no. 3, 300-317.

[19] M. Rabin, Probabilistic algorithms for testing primality, J. Number Theory, 12 (1980), no. 1, 128-138.
[20] P. Stevenhagen, Class number parity of the $p$th cyclotomic field, Math. Comp., 63 (1994), no. 208, 773-784.

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