Indivisibility of the class number of a real abelian field of prime conductor

Shoichi Fujima * and Humio Ichimura **

Abstract

For a fixed integer \( n \geq 1 \), let \( p = 2n\ell + 1 \) be a prime number with an odd prime number \( \ell \) and let \( F = F_{p,\ell} \) be the real abelian field of conductor \( p \) and degree \( \ell \). When \( n \leq 21 \), we show that a prime number \( r \) does not divide the class number \( h_F \) of \( F \) whenever \( r \) is a primitive root modulo \( \ell \) with the help of computer. This generalizes a result of Jakubec and Metsänkylä for the case \( n = 1 \).

1. Introduction

We fix an integer \( n \geq 1 \), and we consider a prime number \( p \) of the form \( p = 2n\ell + 1 \) with an odd prime number \( \ell \). We denote by \( F = F_{p,\ell} \) the real abelian field of conductor \( p \) and degree \( \ell \) over \( \mathbb{Q} \). For a number field \( N \), let \( h_N \) be the class number of \( N \) in the usual sense. There are very many papers on indivisibility of the class number \( h_F \). For this, see for example, Davis [3], Jakubec [13], Jakubec, Pasteka and Schinzel [14], Metsänkylä [17], Stevenhagen [20] and many references therein. It is expected that a prime number \( r \) does not divide \( h_F \) if (a) \( r \) is a primitive root modulo \( \ell \) and (b) \( \ell \) is large enough or \( n \) is small ([17, page 495]). On this expectation, we obtained the following results in [10, Theorem 2] and [12, Theorem 2].

**Theorem 1 ([10]).** Let \( p = 2n\ell + 1 \) and \( F = F_{p,\ell} \) be as above. A prime number \( r \) does not divide \( h_F \) if the following two conditions are satisfied:

(i) \( r \) is a primitive root modulo \( \ell \).

(ii) \( \ell \) is so large that \( p = 2n\ell + 1 \) satisfies the inequality

\[
p > \begin{cases} 
\max ((nr - 2)\phi(2n), 2^{n-1}n(r - 1)), & \text{for } r \geq 3, \\
(2n - 1)^\phi(2n), & \text{for } r = 2.
\end{cases}
\]

Here, \( \phi(*) \) denotes the Euler function.
Theorem 2 ([12]). Let \( p = 2n\ell + 1 \) and \( F = F_{p,\ell} \) be as above, and assume that the prime 2 does not split in \( F \). Then a prime number \( r \) does not divide \( h_F \) when \( r \) is a primitive root modulo \( \ell \) and \( r \geq n \).

When \( n = 1 \) (resp. \( n \leq 4 \)), it is shown that a prime number \( r \) does not divide the class number of \( F_{p,\ell} \) when \( r \) is a primitive root modulo \( \ell \) and \( r \geq n \). The purpose of the present paper is to generalize these results as follows using a refined version of Theorem 1 (Theorem 4 in Section 2) and Theorem 2 with the powerful help of computer.

Theorem 3. When \( n \leq 21 \), a prime number \( r \) does not divide the class number of \( F_{p,\ell} \) whenever \( r \) is a primitive root modulo \( \ell \).

As for a larger \( n \), because of computation time, we obtain only the following partial result for some small prime number \( r \).

Proposition 1. The class number of \( F_{p,\ell} \) is not divisible by \( r \) when \( r \) is a primitive root modulo \( \ell \) for the cases where \( n = 22 \) and \( r \leq 11 \); \( n = 23 \) and \( r \leq 5 \); \( n = 24 \) and \( r \leq 13 \); \( n = 25 \) and \( r \leq 5 \); \( n = 26 \) and \( r \leq 3 \); \( n = 27 \) and \( r \leq 5 \) except for the case \((n,\ell,r) = (27,3,2)\); \( n = 30 \) and \( r \leq 5 \).

Remark 1. Using (a refined version of) Theorem 1 for the case \( r = 2 \), we already showed in [6, 7] with the help of computer that when \( n \leq 30 \), the class number of \( F_{p,\ell} \) is odd whenever 2 is a primitive root modulo \( \ell \) except for the case \((n,\ell) = (27,3)\) and \( p = 163 \). Thus for showing Theorem 3 and Proposition 1, it suffices to deal with an odd prime number \( r \).

2. Refined version of Theorem 1

Let \( n, \ell, p = 2n\ell + 1 \) and \( F = F_{p,\ell} \) be as in Section 1. Let \( r \) be a prime number with \( r \neq p, \ell \). The assumption \( r \neq p, \ell \) is satisfied when \( r \) is a primitive root modulo \( \ell \). In view of Theorem 1, we put

\[
a_n = \max((nr - 2)^{\phi(2n)}, 2^{n-1}n(r - 1)) \quad \text{or} \quad (2n - 1)^{\phi(2n)}
\]

according as \( r \geq 3 \) or \( r = 2 \). Condition (ii) of Theorem 1 reads \( p = 2n\ell + 1 > a_n \). The value \( a_n \) is so huge in general; for example, \( a_n = 321^{18} \sim 2^{150} \) for \((n,\ell) = (19,17)\). Thus Theorem 1 is not useful enough for showing Theorem 3 with the help of computer. Therefore, we need a refined version of the theorem, which involves quite technical notation.

Let \( J \) be the set of integers \( j \) with \( 0 \leq j \leq n - 1 \), and for each \( a \in J \), let \( J_a = J \setminus \{a\} \). Let \( \Psi \) (resp. \( \Psi_a \)) be the set of all the maps from \( J \) (resp. \( J_a \)) to \( \{0, 1\} \).

For an integer \( m \geq 2 \), \( \zeta_m \) denotes a primitive \( m \)th root of unity. We often write \( \epsilon = \zeta_{2m} \) for simplicity. We put

\[
\alpha(\kappa) = \sum_{j \in J} \kappa(j)\epsilon^j
\]
for each \( \kappa \in \Psi \), and

\[
\beta(a, \kappa) = \sum_{j \in J_a} \kappa(j)e^j
\]

for each \( a \in J \) and \( \kappa \in \Psi_a \). We fix a map \( \kappa_0 \in \Psi_0 \). When \( r \geq 3 \), we put

\[
X_{a, \kappa, k} = X_{a, \kappa, k}(r) = ke^a + r\beta(a, \kappa) - 1 - r\beta(0, \kappa_0)
\]

for each triple \((a, \kappa, k)\) with \( a \in J \), \( \kappa \in \Psi_a \) and \( 1 \leq k \leq r - 1 \). When \( r = 2 \), we put

\[
X_{a, \kappa} = e^a + 2\beta(a, \kappa) - 1 - 2\beta(0, \kappa_0)
\]

for each pair \((a, \kappa)\) with \( a \in J \) and \( \kappa \in \Psi_a \), and

\[
Y_{\kappa} = 2\alpha(\kappa) - 1 - 2\beta(0, \kappa_0)
\]

for each \( \kappa \in \Psi \). When \( a = 0 \), we easily see that the quantities \( X_{0, \kappa, 1} \) for the case \( r \geq 3 \) and \( X_{0, \kappa} \) for \( r = 2 \) are related by

\[
X_{0, \kappa, 1} = \frac{r}{2} X_{0, \kappa}
\]

(1)

for each \( \kappa \in \Psi_0 \). In what follows, we exclude the triple \((a, \kappa, k) = (0, \kappa_0, 1)\) when \( r \geq 3 \) and the pair \((a, \kappa) = (0, \kappa_0)\) when \( r = 2 \) because \( X_{0, \kappa, 1} = X_{0, \kappa_0} = 0 \). The following lemma on non-nullity of \( X_{a, \kappa, k} \), \( X_{a, \kappa} \), and \( Y_{\kappa} \) is essentially contained in [10, Lemma 8].

**Lemma 1.**  \( \text{(I) For any choice of } \kappa_0 \in \Psi_0, \text{ the following assertions hold.} \)

(I-i) The case \( r \geq 3 \). When \( a, k \neq (0, 1) \), \( X_{a, \kappa, k} \neq 0 \) for any \( \kappa \in \Psi_a \).

(I-ii) The case \( r = 2 \). When \( a \neq 0 \), \( X_{a, \kappa} \neq 0 \) for any \( \kappa \in \Psi_a \). Further, \( Y_{\kappa} \neq 0 \) for any \( \kappa \in \Psi \).

(II) We can choose \( \kappa_0 \in \Psi_0 \) so that

\[
X_{0, \kappa, 1} \neq 0 \quad \text{and} \quad X_{0, \kappa} \neq 0
\]

(2)

for any \( \kappa \in \Psi_0 \) with \( \kappa \neq \kappa_0 \).

**Proof.** The assertion (I) is contained in the (short) proof of [10, Lemma 8(i), (iii)]. The assertion (II) follows from [10, Lemma 8(ii)] combined with (1). \( \square \)

In the following, we choose and fix a map \( \kappa_0 \in \Psi_0 \) which satisfies (2). For an element \( x \in \mathbb{Q}((\zeta_{2n})) \), let \( \text{Nr}(x) = |\text{Nr}_{\mathbb{Q}(\zeta_{2n})/\mathbb{Q}}(x)| \) be the absolute value of the norm of \( x \) from \( \mathbb{Q}((\zeta_{2n})) \) to \( \mathbb{Q} \). Then, by Lemma 1, all the norms \( \text{Nr}(X_{a, \kappa, k}) \) with \( (a, \kappa, k) \neq (0, \kappa_0, 1) \), and \( \text{Nr}(X_{a, \kappa}) \) with \( (a, \kappa) \neq (0, \kappa_0) \) and \( \text{Nr}(Y_{\kappa}) \) are positive integers. For a positive integer \( m \), let \( \text{Supp} m \) be the set of prime numbers dividing \( m \). We put

\[
\mathbb{P}_{n, r}(\kappa_0) = \begin{cases} 
\bigcup_{(a, \kappa, k) \neq (0, \kappa_0, 1)} \text{Supp} \text{Nr}(X_{a, \kappa, k}), & \text{for } r \geq 3, \\
\bigcup_{(a, \kappa) \neq (0, \kappa_0)} \text{Supp} \text{Nr}(X_{a, \kappa}) \cup \bigcup_{\kappa \in \Psi} \text{Supp} \text{Nr}(Y_{\kappa}), & \text{for } r = 2.
\end{cases}
\]

The following is a refined version of Theorem 1. For this, see [10, Theorem 2] combined with [10, Remark 6].
Theorem 4. Let $p = 2n\ell + 1$ and $F = F_{p,\ell}$ be as in Section 1. Let $r$ be a prime number with $r \neq p, \ell$, and let $\kappa_0 \in \Psi_0$ be an arbitrary map satisfying the condition (2). Then $r \nmid h_F$ if the following three (resp. two) conditions are satisfied when $r \geq 3$ (resp. $r = 2$).

(i) $r$ is a primitive root modulo $\ell$.
(ii) $p = 2n\ell + 1 \notin \mathbb{P}_{n,r}(\kappa_0)$.
(iii) When $r \geq 3$, $p = 2n\ell + 1 > 2^{n-1}n(r - 1)$.

Remark 2. In the proof of [10, Lemma 6], we have shown that $p = 2n\ell + 1 \notin \mathbb{P}_{n,r}(\kappa_0)$ if $p > (nr - 2)^{\phi(2n)}$ or $p > (2n - 1)^{\phi(2n)}$ according as $r \geq 3$ or $r = 2$. The last condition is a part of assumption (ii) of Theorem 1, and assumptions (i) and (iii) of Theorem 4 are contained in assumptions of Theorem 1. In this sense, Theorem 4 is a refined version of Theorem 1.

At present, we have no general method to find a map $\kappa_0 \in \Psi_0$ satisfying the condition (2). However, as we see in the below, there are several cases where the “zero map” satisfies (2).

Lemma 2. Let $n \geq 2$ be an integer satisfying one of the following two conditions:

(I) $n = 2^esf$ for some odd prime number $s$ and some integers $e, f \geq 0$.
(II) $n = 15, 21$ or $30$.

Let $\kappa_0 \in \Psi_0$ be the map such that $\kappa_0(j) = 0$ for all $j \in J_0$. Then this map $\kappa_0$ satisfies (2) in Lemma 1.

In particular, when $2 \leq n \leq 30$, the above map $\kappa_0$ satisfies (2).

Proof. By (1), it suffices to deal with the quantity $X_{0,n}$ for the case $r = 2$. In [7], we have already shown the assertion when $r = 2$; the case (I) in [7, Lemma 2] and the case (II) with the help of computer (see [7, page 22]).

Remark 3. Let $p = 2n\ell + 1$ and $F = F_{p,\ell}$ be as in Section 1. In [10], we assumed that the prime 2 does not split in $F$ in several (but not all) places. In this remark, we show that

(*) Under assumptions (ii) and (iii) of Theorem 4, 2 does not split in $F$.

We proved [10, Theorem 1] for the case $r = 2$ under assumptions (i), (ii) of Theorem 1 of this paper and the third one that 2 does not split in $F$. It follows from (*) and Remark 2 that the third one is unnecessary. (For this assertion, see also [11, Lemma 1].)

To show (*), let us introduce some more notation. Let $K = \mathbb{Q}(\zeta_p)$ be the $p$th cyclotomic field, and $K^+$ the maximal real subfield of $K$. Let $g$ be a primitive root modulo $p$. We put

$$\xi = \prod_{a=0}^{n-1}(\zeta_p^{a\ell} + 1) \quad \text{and} \quad \epsilon = N_{K^+/F}(\zeta_p + \zeta_p^{-1}).$$

These cyclotomic units of $K$ and $F$ played roles in [10, 11] and [12], respectively. We easily see that the unit $\xi$ is Galois conjugate to $\epsilon$ times an element of $\mu_K$, where $\mu_K$ is
the group of roots of unity in $K$. It follows that $\xi \in \mu_K$ if and only if $\epsilon = \pm 1$. Under assumptions (ii) and (iii) of Theorem 4, we observe that $\xi \not\in \mu_K$ (and hence $\epsilon \neq \pm 1$). Actually, if $\xi$ would be a root of unity, then the congruence on $\xi$ in [10, Lemma 5] obviously holds. However, what we have proved in [10, §4] together with [10, Remark 6] is that this congruence does not hold under these assumptions. On the other hand, it is known that $\epsilon = \pm 1$ (and hence $\xi \in \mu_K$) if and only if 2 splits in $F$ ([12, Lemma 2]). Therefore, we see that 2 does not split in $F$ under assumptions (ii) and (iii) of Theorem 4.

3. Sufficient condition for $r \nmid h_F$

In this section, we give a sufficient condition for $r \nmid h_F$ (Lemma 4) in terms of a polynomial associated to some Bernoulli number.

First we recall some standard notation. Let $r$ be an arbitrary prime number. We denote by $\mathbb{Z}_r$, $\mathbb{Q}_r$, and $\bar{\mathbb{Q}}_r$ the ring of $r$-adic integers, the field of $r$-adic rationals and a fixed algebraic closure of $\mathbb{Q}_r$, respectively. Let $G$ be a finite abelian group with $r \nmid |G|$, and let $\chi$ be a $\bar{\mathbb{Q}}_r$-valued character of $G$. Let $\mathbb{Q}_r(\chi)$ be the extension of $\mathbb{Q}_r$ generated by the values of $\chi$, and $\mathcal{O}_\chi$ the ring of integers of $\mathbb{Q}_r(\chi)$. We denote by

$$
\epsilon_\chi = \frac{1}{|G|} \sum_{g \in G} \text{Tr}_{\mathbb{Q}_r(\chi)/\mathbb{Q}_r}(\chi(g)^{-1}) g \in \mathbb{Z}_r[G]
$$

the idempotent of $\mathbb{Z}_r[G]$ associated to $\chi$. Here, Tr denotes the trace map. For a module $M$ over $\mathbb{Z}_r[G]$, let $M(\chi) = M^{\epsilon_\chi}$ (or $e_\chi M$) be the $\chi$-part of $M$, which we naturally regard as a module over $\mathcal{O}_\chi$.

Let $p = 2n\ell + 1$ and $F = F_{p, \ell}$ be as in Section 1. Let $r$ be an odd prime number with $r \neq p, \ell$. (The case $r = 2$ is already dealt with in [6] and [7].) Let $\Delta = \text{Gal}(F/\mathbb{Q})$, and we fix a complete set $\Theta_F$ of representatives of the $\mathbb{Q}_r$-conjugacy classes of the nontrivial $\mathbb{Q}_r$-valued characters of $\Delta$. For a number field $N$, $A_N$ denotes the $r$-part of the ideal class group of $N$. Then we have

$$A_F = \bigoplus_{\chi \in \Theta_F} A_F(\chi)$$

because $A_F(\chi_0) = A_2$ is trivial, where $\chi_0$ is the trivial character of $\Delta$. Let $k = \mathbb{Q}(\zeta_r)$ and $G_r = \text{Gal}(k/\mathbb{Q})$. We put $L = kF = F(\zeta_r)$. Then the Galois groups $\text{Gal}(L/F)$ and $\text{Gal}(L/\mathbb{Q})$ are naturally identified with $G_r$ and $G_r \times \Delta$, respectively. Let $\omega_r$ be the $\mathbb{Q}_r$-valued character of the Galois group $G_r$ representing the Galois action on $\zeta_r$. For $\chi \in \Theta_F$, $\omega_r \chi^{-1}$ denotes the character of $G_r \times \Delta$ sending $(g, \delta) \in G_r \times \Delta$ to $\omega_r(g)\chi^{-1}(\delta)$. The $r$-part $A_L$ of the ideal class group of $L$ is naturally regarded as a module over $\mathbb{Z}_r[G_r \times \Delta]$. For each $\chi \in \Theta_F$, the following implication is shown by a standard Spiegelung argument:

$$A_L(\omega_r \chi^{-1}) = \{0\} \implies A_F(\chi) = \{0\}.$$  

For this, see [21, §10.2] or Corollary 5.4.6 in G. Gras [9, Chapter II]. Let $\chi$ be a character in $\Theta_F$. We naturally regard the characters $\omega_r$, $\chi$ and $\omega_r \chi^{-1}$ as primitive.
Dirichlet characters. We see that
\[ |A_L(\omega_r \chi^{-1})| = |\mathcal{O}_\chi / \beta_\chi \mathcal{O}_\chi| \quad \text{with} \quad \beta_\chi = \frac{1}{2} B_{1, \chi \omega_r^{-1}} \]
(6)
by the Iwasawa main conjecture (a theorem of Mazur and Wiles [16, Theorem 2]).

Here, for a Dirichlet character \( \psi \) of conductor \( f \),
\[ B_{1, \psi} = \frac{1}{f} \sum_{a=0}^{f-1} a \psi(a) \]
is the generalized Bernoulli number.

In the remainder of this section, we assume that \( \ell \nmid n \) for simplicity. This assumption is harmless because the case where \( \ell \) divides \( n \) is so rare in the range of our computation. Let \( g \) be a primitive root modulo \( p \). As we are assuming that \( \ell \nmid n \), we see that
\[ \{ g^{2nu + \ell v} \mod p \mid 0 \leq u \leq \ell - 1, 0 \leq v \leq 2n - 1 \} = (\mathbb{Z}/p\mathbb{Z})^\times. \]
(7)

For an integer \( x \in \mathbb{Z} \), let \( s_p(x) \) be the unique integer such that \( s_p(x) \equiv x \mod p \) and \( 0 \leq s_p(x) \leq p - 1 \). For an integer \( b \) with \( 1 \leq b \leq (r - 1)/2 \), we define a function \( f_b \) on \( \mathbb{Z} \) by
\[ f_b(a) = \begin{cases} 1, & \text{if } \frac{bp}{r} < s_p(a) < \frac{(r - b)p}{r}, \\ 0, & \text{otherwise}. \end{cases} \]
Clearly, we have \( f_b(a') = f_b(a) \) if \( a' \equiv a \mod p \). Further, we can easily show that
\[ f_b(-a) = f_b(a). \]
(8)

We put
\[ x_u = \sum_{b=0}^{u-1} \sum_{b=1}^{(r-1)/2} f_b(g^{2nu + \ell v}) \omega_r(b)^{-1} \in \mathbb{Z}_r \]
for each \( 0 \leq u \leq \ell - 1 \), and
\[ G(T) = G_{\ell, r}(T) = \sum_{u=0}^{\ell-1} x_u T^u \in \mathbb{Z}_r[T]. \]
(9)

The following lemma on the Bernoulli number \( \beta_\chi \) is shown later.

**Lemma 3.** Under the above notation, assume that \( r \geq 3 \) and \( \ell \nmid n \). Then we have
\[ \beta_\chi = u_\chi \cdot G_{\ell, r}(\zeta_\ell) \quad \text{with} \quad \zeta_\ell = \chi(g^{2n}) \]
where \( u_\chi = \chi(r) \omega_r(p)^{-1} \) is a root of unity.
Let \( \Phi_{\ell}(T) \) be the \( \ell \)th cyclotomic polynomial, and we put
\[
D_{\ell, r}(T) = \gcd(G(T) \mod r, \Phi_{\ell}(T) \mod r) \in \mathbb{F}_r[T]
\]
where \( \mathbb{F}_r = \mathbb{Z}/r\mathbb{Z} \).

**Lemma 4.** Under the above notation, assume that \( r \geq 3 \) and \( \ell \mid n \). Then, the following assertions hold.

1. We have \( r \mid h_F \) if \( D_{\ell, r}(T) = 1 \).
2. When \( r \) is a primitive root modulo \( \ell \), we have \( r \mid h_F \) if \( x_j \not\equiv x_0 \mod r \) for some \( 1 \leq j \leq \ell - 1 \).

**Proof.** Assume that \( D_{\ell, r}(T) = 1 \). Then, it follows from Lemma 3 that \( \beta_{\chi} \) is a unit of \( \mathcal{O}_\chi \) for every \( \chi \in \Theta_F \). This implies that for every \( \chi \in \Theta_F \), \( A_{\ell, r}(\omega_r^{-1}) \) is trivial by (6), and hence so is \( A_F(\chi) \) by (5). Now the assertion (I) follows from (4). The assertion (II) follows from (I) because \( \Phi_{\ell} \mod r \) is irreducible over \( \mathbb{F}_r \) when \( r \) is a primitive root modulo \( \ell \). \( \square \)

**Proof of Lemma 3.** For an integer \( x \), let \( \hat{s}(x) \) be the integer such that \( \hat{s}(x) \equiv x \mod rp \) and \( 0 \leq \hat{s}(x) \leq rp - 1 \). We see that
\[
\{ra + pb \mod rp \mid 0 \leq a \leq p - 1, \ 0 \leq b \leq r - 1\} = \mathbb{Z}/rp\mathbb{Z}.
\]

Then it follows that
\[
\beta_{\chi} = \frac{1}{2} B_{1, \chi} \omega_r^{-1} = \frac{1}{2rp} \sum_{a=0}^{p-1} \sum_{b=0}^{r-1} \hat{s}(ra + pb)(\chi\omega_r^{-1})(ra + pb).
\]
Noting that \( (\chi\omega_r^{-1})(ra + pb) = \chi(ra)\omega_r^{-1}(pb) \) or 0 according as \( ab \neq 0 \) or \( ab = 0 \), we see that
\[
X := \chi(r)^{-1} \omega_r(p) \cdot \beta_{\chi} = \frac{1}{2rp} \sum_{a=1}^{p-1} \sum_{b=1}^{r-1} \hat{s}(ra + pb)\chi(a)\omega_r(b)^{-1}.
\]
As \( \omega_r \) is an odd character, we observe that \( X \) equals
\[
\frac{1}{2rp} \sum_{a=1}^{p-1} \sum_{b=1}^{(r-1)/2} \{ \hat{s}(ra + pb)\omega_r(b)^{-1} + \hat{s}(ra + p(r-b))\omega_r(r-b)^{-1} \} \chi(a)
\]
\[
= \frac{1}{2rp} \sum_{a=1}^{p-1} \sum_{b=1}^{(r-1)/2} \{ \hat{s}(ra + pb) - \hat{s}(ra + p(r-b)) \} \omega_r(b)^{-1} \chi(a).
\]

For each \( 1 \leq b \leq (r-1)/2 \), we see that
\[
\hat{s}(ra + p(r-b)) = \hat{s}(\hat{s}(ra + pb) + p(r-2b))
\]
equals
\[
\hat{s}(ra + pb) + p(r-2b) \quad \text{or} \quad \hat{s}(ra + pb) + p(r-2b) - rp.
\]
We easily see that the latter case happens if and only if \( \hat{s}(ra + pb) > 2bp \). (Here, note that \( \hat{s}(ra + pb) = 2bp \) does not hold as \( 1 \leq a \leq p \).) Let us show that this is equivalent to \( f_b(a) = 1 \). Actually, if \( f_b(a) = 1 \), then \( bp < ar < (r - b)p \) by the definition of \( f_b \). It follows that \( 2bp < ar + bp < rp \) and hence \( \hat{s}(ra + pb) > 2bp \). If \( f_b(a) = 0 \), then we have

\[
0 < ar < bp \quad \text{or} \quad (r - b)p < ar < rp.
\]

In both cases, we can easily show that \( \hat{s}(ra + pb) < 2bp \).

Therefore, it follows that

\[
\hat{s}(ra + pb) - \hat{s}(ra + p(r - b)) = \hat{s}(ra + pb) - \{ \hat{s}(ra + pb) + p(r - 2b) - rp f_b(a) \} = -p(r - 2b) + rp f_b(a).
\]

Now noting that \( \sum_a \chi(a) = 0 \), we see from (10) that

\[
X = \frac{1}{2} \sum_{a=1}^{p-1} \left( \sum_{b=1}^{(r-1)/2} f_b(a) \omega_r(b)^{-1} \right) \chi(a).
\]

Because of (7), we can write \( a = s_p(g^{2nu+\ell \nu}) \) with \( 0 \leq u \leq \ell - 1 \) and \( 0 \leq v \leq 2n - 1 \). We put \( \zeta_\ell = \chi(g^{2n}) \), so that we have \( \chi(g^{2nu+\ell \nu}) = \zeta_\ell^u \). Then noting that \( g^{2n} \equiv -1 \mod p \), we observe from the above that

\[
X = \frac{1}{2} \sum_{u=0}^{\ell-1} \left( \sum_{v=0}^{2n-1} \sum_{b=1}^{(r-1)/2} f_b(g^{2nu+\ell \nu}) \omega_r(b)^{-1} \right) \zeta_\ell^u
= \frac{1}{2} \sum_{u=0}^{\ell-1} \sum_{v=0}^{u-1} \sum_{b=1}^{(r-1)/2} \left( f_b(g^{2nu+\ell \nu}) + f_b(-g^{2nu+\ell \nu}) \right) \omega_r(b)^{-1} \zeta_\ell^u
= \sum_{u=0}^{\ell-1} \sum_{v=0}^{u-1} \sum_{b=1}^{(r-1)/2} f_b(g^{2nu+\ell \nu}) \omega_r(b)^{-1} \zeta_\ell^u.
\]

Here, the last equality holds because of (8). Thus we have shown Lemma 3. \( \square \)

**Remark 4.** The condition in Lemma 4(I) or Lemma 4(II) is sufficient for \( r \nmid h_F \), but it is not a necessary condition. In other words, the converse of the implication (5) does not hold in general. Let us give some example. When \( n = 25, 61, 151, 206, 217, 247 \) and \( \ell = 3 \), we see with the help of computer that the simultaneous congruence \( x_0 \equiv x_1 \equiv x_2 \mod r \) holds for \( r = 5 \). Further, when \( n = 277 \) and \( \ell = 3 \), the congruence holds for \( r = 53 \). However, for these \( n \) and \( \ell \), \( h_F = 1 \) by a table in M. N. Gras [8].

### 4. Exceptional cases

Let \( p = 2n\ell + 1 \) and \( F = F_{p,\ell} \) be as in Section 1. For showing Theorem 3, there are two exceptional cases: the case where 2 splits in \( F \) and the case where \( \ell \) divides
Class number of a real abelian field

We can not apply Theorem 2 for the first case, and we excluded the second case in Lemma 3 for the sake of simplicity. This section is devoted to these two cases.

To deal with the first case, we use the following lemma, whose proof is given at the end of this section.

Lemma 5. Let \( p = 2n\ell + 1 \) and \( F = F_{p,\ell} \) be as above, and let \( r \) be a prime number which is a primitive root modulo \( \ell \). Assume that 2 splits in \( F \) and that \( r \) divides \( h_F \). Then \( r \) satisfies

\[
r < \sqrt{p} \times \log p / \varpi
\]

with

\[
\varpi = \exp(0.46) = 1.584073985 \cdots
\]

Let \( p = 2n\ell + 1 \) and \( F = F_{p,\ell} \) be as above. We see from Brillhart et al [2] that when \( n \leq 30 \) (the range of our computation), 2 splits in \( F \) or equivalently \( 2^{2n} \equiv 1 \mod p \) if and only if the pair \((n,\ell)\) equals one of the following 12 ones:

\begin{align*}
(5,3), (7,3), (11,31), (15,5), (15,11), (18,3), \\
(21,3), (24,5), (25,5), (26,3), (26,31), (29,19).
\end{align*}

(11)

Among them, the value \( p = 2n\ell + 1 \) is the largest when \((n,\ell) = (26,31)\) and \( p = 1613 \).

For these exceptional pairs, we see that a prime number \( r \) never divides \( h_F \) when \( r \) is a primitive root modulo \( \ell \). It is shown as follows. Let \( r \) be a prime number. Assume that, for some of the above pair \((n,\ell)\), \( r \) divides \( h_F \) and \( r \) is a primitive root modulo \( \ell \). Then we see from Lemma 5 that

\[
r < \sqrt{1613} \times \log 1613 / \varpi = 187.25 \cdots
\]

We see from a table in Koyama and Yoshino [15] on class numbers of real abelian fields of prime conductor < \( 10^4 \) that for each of the above pairs, \( h_F \) is not divisible by any prime number \( r \leq 187 \).

Let us deal with the second exceptional case where \( \ell \) divides \( n \). For \( n \leq 30 \) (the range of our computation) and an odd prime divisor \( \ell \) of \( n \), \( p = 2n\ell + 1 \) is a prime number if and only if the pair \((n,\ell)\) equals one of the following 12 ones:

\begin{align*}
(3,3), (6,3), (10,5), (12,3), (14,7), (26,13), (27,3), (30,3), \\
(15,5), (18,3), (21,3), (25,5).
\end{align*}

The last four ones are contained in (11) and are already settled above. For the remaining eight ones, we see that 2 does not split in \( F \) and that \( h_F \) is not divisible by a prime number \( r \) with \( r < n \) (except for the case \((n,\ell) = (27,3) \) and \( r = 2 \)) from the table in [15]. Hence, by virtue of Theorem 2, \( h_F \) is not divisible by a prime number \( r \) which is a primitive root modulo \( \ell \) except for the above case.
Proof of Lemma 5. Let $D_F = \pm p^{\ell-1}$ and $R_F$ be the discriminant and the regulator of $F$, respectively. By the class number formula ([21, page 38]), we have

$$\frac{2^{\ell-1}h_FR_F}{\sqrt{|D_F|}} = \prod_{\chi} L(1, \chi),$$

(12)

where $\chi$ runs over the even Dirichlet characters of conductor $p$ and order $\ell$. We have $\chi(2) = 1$ as we are assuming that 2 splits in $F$. Eddin [4] studied the value $|L(1, \psi)|$ for an even Dirichlet character $\psi$ with $\psi(2) = 1$. It follows from [4, Theorem 1.1] that

$$|L(1, \chi)| < \frac{\log p}{2}.$$

As for the regulator $R_F$, it follows from Korollar to Satz 3 of Zimmert [22] that

$$R_F \geq 0.04 \times \pi^\ell.$$

Hence, we observe from the class number formula (12) that

$$h_F < \frac{25}{\omega} \left( \frac{\sqrt{p} \log p}{4\omega} \right)^{\ell-1}.$$ 

(13)

Now, let $r$ be a prime number which is a primitive root modulo $\ell$, and assume that $r$ divides $h_F$. Then, we see from [21, Theorem 10.8] that $r^{\ell-1}$ divides $h_F$ and hence $r^{\ell-1} \leq h_F$. Therefore, we obtain the assertion from (13) noting that

$$\left( \frac{25}{\omega} \right)^{1/(\ell-1)} \leq \left( \frac{25}{\omega} \right)^{1/2} < 4.$$

5. Computation

In this section, we prove Theorem 3 and Proposition 1 with the powerful help of computer. As we mentioned in Section 1, the case $n = 1$ is already settled in [13, 17], and the case $r = 2$ in [6, 7]. For each $2 \leq n \leq 30$ and an odd prime number $r < n$, we put $P_{n,r} = \mathbb{P}_{n,r}(\kappa_0)$ where $\kappa_0 \in \Psi_0$ is the map defined in Lemma 2. We denote by $P_{n,r}$ the set of prime numbers $p$ satisfying the following two conditions:

(a) $p \in P_{0,n}$ or $p \leq 2^{n-1}n(r-1)$,
(b) $p = 2n\ell + 1$ for some odd prime number $\ell$ such that $\ell \nmid n$, $\ell \neq r$ and $r$ is a primitive root modulo $\ell$.

We give some data of the set $P_{n,r}$; the minimal and the maximal prime numbers contained in the set and the number of elements of the set, in Table 1 for $4 \leq n \leq 21$, and in Table 2 for computed cases in $n \geq 22$. The number of binary digits of the value $(nr - 2)^{\phi(2n)}$, which appeared in assumption (ii) of Theorem 1, is also shown in Table 2. We find that the number of digits of the maximal prime number contained in the set $P_{n,r}$ is about 50%-70% of that of $(nr - 2)^{\phi(2n)}$. This shows that Theorem 4 is more sharper and fits to computation better than Theorem 1.
As in the previous sections, we put $F = F_{p,\ell}$ for $p = 2n\ell + 1 \in P_{n,r}$. To prove Theorem 3, it suffices to show that $r \nmid h_F$ with $p \in P_{n,r}$ for each $2 \leq n \leq 21$ and each odd prime number $r < n$. This is because of Theorems 2 and 4 and the results in Section 4 for the exceptional cases. Similarly, to prove Proposition 1, it suffices to show $r \nmid h_F$ with $p \in P_{n,r}$ for each pair $(n,r)$ in the proposition. To show $r \nmid h_F$, we use the sufficient condition given in Lemma 4(II). Namely, we compute the coefficients $x_{j0}$ of the polynomial $G_{\ell,r}(T)$ defined in (9) for $x_0, x_1, x_2, \ldots$ until we find the first integer $j_0$ with $x_{j_0} \not\equiv x_0 \pmod{r}$. We show in Figure 1 an example of this computation, the case $(n,r) = (4,3)$. We also give Table 3 to show how the values of $j_0$ are distributed when $n = 21, 22$ and $r = 3, 5, 7$ for example. In the column $j_0$ of the table, the number of the primes $p \in P_{n,r}$ for which the value of $j_0$ equals $j$ is shown. Table 3 seems to suggest that the coefficients $x_j$ behave random modulo $r$. For the other $n$’s, we find that the values of $j_0$ are distributed almost similarly.

The computation method consists of five steps:

(i) Compute the norm $N_r(X_{a,\kappa,k})$ for each triples $(a,\kappa,k)$ with $a \in J, \kappa \in \Psi_a$ and $1 \leq k \leq r - 1$ such that $(a,\kappa,k) \neq (0,\kappa_0,1)$, and make the set of the norms.

(ii) Factor all elements in the resultant set of the previous step as products of prime numbers, and make the set $P_{n,r}^{0}$ of the prime factors.
(iii) Make the union of $P_{0,n,r}$ and the set of all prime numbers $p \leq 2^{n-1}(r-1)$.

(iv) We make the set $P_{n,r}$; namely we extract from the resultant set of the previous step those prime numbers $p$ of the form $p = 2n\ell + 1$ for some prime number $\ell$ such that $\ell \nmid n$, $\ell \neq r$ and $r$ is a primitive root modulo $\ell$.

(v) For each $p = 2n\ell + 1 \in P_{n,r}$, verify $r \nmid h_F$ using Lemma 4(II).

In Step (i) the norm $N_r(\alpha)$ for an element $\alpha \in \mathbb{Q}(\epsilon)$ is calculated by using the following formula (14). We regard $\mathbb{Q}(\epsilon)$ as a vector space over $\mathbb{Q}$ with a basis $B = \{\epsilon^i \mid 0 \leq i \leq \phi(2^n) - 1\}$.

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

$$N_r(\alpha) = \det M_\alpha,$$

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

For the factorizations, we recursively employ compositeness test by Miller-Rabin method [18, 19] followed by Pollard’s $\rho$ factorization 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 ($\leq 2^{46}$). The average of times of operations in Pollard’s $\rho$ method to factorize an integer $n$ is $O(n^{1/4})$.

All computation for Theorem 3 and some computation for Proposition 1 ($n = 22$; $(n, r) = (23, 3)$, $(24, 3)$ and $(24, 5)$) were executed in about 50 processes on 12 personal computers, whose CPUs are Intel Core i5 or i7. Among them, the case $(n, r) = (22, 11)$ had spent the longest computation time, $4.3 \times 10^8$ seconds totally, where 99.90% of the computation time were for factorization. In the case, the number of the triples $(a, \kappa, k)$ whose norms are to be computed is $n(r - 1)2^{n-1} - 1 = 461373439$, while the size of the set of norms $N_r(X_{a,\kappa, k})$ was 448424969. The construction of the set of the norms plays a role to reduce computation time to factorize. However, its effect is small (2.8% reduction in the above case) and it prevents parallel computation.

We therefore refill the remaining $(n, r)$-pairs in Proposition 1, that are some of pairs having smaller $(nr - 2)\phi(2n)$ values than that of $(n, r) = (22, 11)$, by computation using a refined method, which consists of two independent procedures:

(a) Pass all norm values generated in Step (i) through all procedures in Steps (ii),(iv) and (v) without making set in each step.

(b) Also pass all prime numbers $p \leq 2^{n-1}(r-1)$ through Steps (iv) and (v).

This method is highly suitable for parallelism so that those computation were executed in the Oakbridge-CX super computer system in the University of Tokyo. The longest computation time in those cases was $1.9 \times 10^8$ seconds, which is total of 2240 parallel MPI processes, in $(n, r) = (30, 5)$, however its elapsed time was within 45 hours.

Computation codes in this paper were written in Java(tm) Platform, where huge integer values could be handled using BigInteger class.

Acknowledgements

The authors would like to thank the referee for several valuable comments, in particular for pointing out some mistakes on the data for the exceptional pairs $(n, \ell)$ in Section 4.
### Table 1. $P_{n,r}$ in the cases of $4 \leq n \leq 21$.

| $(n,r)$ | $P_{n,r}$ | min $P_{n,r}$ | max $P_{n,r}$ |
|---------|-----------|---------------|---------------|
| (4,3)   | 2         | 41            | 137           |
| (5,3)   | 2         | 71            | 191           |
| (6,3)   | 5         | 61            | 1213          |
| (6,5)   | 4         | 277           | 1237          |
| (7,3)   | 4         | 71            | 1583          |
| (7,5)   | 35        | 43            | 748343        |
| (8,3)   | 14        | 113           | 144649        |
| (8,5)   | 37        | 113           | 803309        |
| (8,7)   | 66        | 977           | 111315377     |
| (9,3)   | 30        | 127           | 97327         |
| (9,5)   | 68        | 127           | 4832767       |
| (9,7)   | 97        | 199           | 3775743       |
|         | ...       | ...           | ...           |
| (18,3)  | 14863     | 181           | 754390467109  |
| (18,5)  | 63251     | 613           | 45930594043693 |
| (18,7)  | 62604     | 181           | 28148167729250533 |
| (18,11) | 127161    | 613           | 7328673534122958637 |
| (18,13) | 174748    | 181           | 674020573786231989293 |
| (18,17) | 231057    | 181           | 1500830985299077679949 |
| (19,3)  | 59180     | 191           | 492164961151583 |
| (19,5)  | 136979    | 647           | 145168218622596688527 |
| (19,7)  | 278757    | 191           | 750960692365039000929167 |
| (19,11) | 531783    | 647           | 3147809639477782051173589667 |
| (19,13) | 689974    | 191           | 53706047343895386002575759763 |
| (19,17) | 932190    | 191           | 7069413515268419117667013727699 |
| (20,3)  | 75762     | 281           | 106805612590361 |
| (20,5)  | 239700    | 281           | 240196071295722152281 |
| (20,7)  | 371338    | 521           | 8898885766959513262361 |
| (20,11) | 652096    | 521           | 7194644333820696710311721 |
| (20,13) | 900116    | 761           | 1504154780632502436724006841 |
| (20,17) | 1019275   | 281           | 11045446783218245494969908941 |
| (20,19) | 1238369   | 281           | 8518668606657333330802630041 |
| (21,3)  | 107467    | 211           | 4883864297047 |
| (21,5)  | 176893    | 967           | 331919777685427 |
| (21,7)  | 470426    | 211           | 128255419214243203 |
| (21,11) | 856922    | 547           | 37082828805522636739 |
| (21,13) | 1166940   | 211           | 28468603091811620599 |
| (21,17) | 1600458   | 211           | 7326879540593452298467 |
| (21,19) | 1676999   | 463           | 24970684330727130586963 |
Table 2. $P_{n,r}$ in the computed cases for $n \geq 22$, and $(nr - 2)^{\phi(2n)}$.

| $(n, r)$ | $P_{n,r}$ | $\min P_{n,r}$ | $\lceil \lg \max P_{n,r} \rceil$ | $\lceil \lg(nr - 2)^{\phi(2n)} \rceil$ |
|----------|-----------|----------------|------------------|------------------|
| (22,3)   | 6 16416   | 1277           | 59               | 120              |
| (22,5)   | 21 75450  | 1013           | 81               | 136              |
| (22,7)   | 27 27751  | 1013           | 91               | 145              |
| (22,11)  | 47 36919  | 1013           | 104              | 159              |
| (23,3)   | 9 23087   | 1427           | 71               | 134              |
| (23,5)   | -         | 139            | 88               | 151              |
| (23,11)  | 9 62595   | 241            | 56               | 99               |
| (24,3)   | 14 85374  | 337            | 61               | 111              |
| (24,7)   | -         | 241            | 77               | 119              |
| (24,13)  | -         | 1489           | 87               | 129              |
| (25,3)   | -         | 1451           | 69               | 124              |
| (25,5)   | -         | 151            | 83               | 139              |
| (26,3)   | -         | 1613           | 75               | 150              |
| (27,3)   | -         | 271            | 65               | 114              |
| (27,5)   | -         | 379            | 78               | 127              |
| (30,3)   | -         | 421            | 61               | 104              |
| (30,5)   | -         | 421            | 72               | 116              |

($\lg = \log_2$)

Table 3. Frequency distribution table of $j_0$, in $n = 21, 22$, $r = 3, 5, 7$.

| $(n, r)$ | $j_0 = 1$ | 2  | 3  | 4  | 5  | 6  | 7  | $\geq 8$ |
|----------|-----------|----|----|----|----|----|----|---------|
| (21,3)   | 71561     | 23788 | 8023 | 2779 | 872 | 288 | 112 | 44      |
| (21,5)   | 141403    | 28383 | 5669 | 1174 | 215 | 38  | 9   | 2       |
| (21,7)   | 403182    | 57674 | 8214 | 1158 | 164 | 29  | 4   | 1       |
| (22,3)   | 411045    | 137051 | 45492 | 15132 | 5024 | 1802 | 593 | 277     |
| (22,5)   | 1740141   | 348275 | 60713 | 13850 | 2806 | 536 | 101 | 28      |
| (22,7)   | 2338217   | 333729 | 47774 | 6877  | 989 | 137 | 25  | 3       |
References

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

[2] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, Jr., Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers, (2nd ed.), Contemp. Math., vol. 22, Amer. Math. Soc., Providence, RI, 1988.

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

[4] S. S. Eddin, An explicit bound for $|L(1, \chi)|$ when $\chi(2) = 1$ and $\chi$ is even, Int. J. Number Theory, 12 (2016), no. 8, 2299-2315.

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

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

[7] S. Fujima and H. Ichimura, Note on class number parity of an abelian field of prime conductor, Math. J. Ibaraki Univ., 50 (2018), 15-26.

[8] M. N. Gras, Méthodes et algorithmes pour le calcul numérique du nombre de classes et unités des extensions cubiques cycliques de $\mathbb{Q}$, J. Reine Angew. Math., 277 (1975), 89-116.

[9] G. Gras, Class Field Theory: From Theory to Practice, Springer, Berlin, (2003).

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

[11] H. Ichimura, Note on class number parity of an abelian field of prime conductor, II, Kodai Math. J., 42 (2019), no.1, 99-110.

[12] H. Ichimura, On the class number of a real abelian field of prime conductor, to appear in Acta Arith.

[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 number of the real $p$’th cyclotomic field and characteristic polynomials attached to them, RIMS Kôkyûroku Bessatsu, B12 (2009), 149-172.

[16] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, Invent. Math., 76 (1984), no. 2, 179-330.
[17] T. Metsänkylä, An application of the $p$-adic class number formula, Manuscripta Math., 93 (1997), no. 4, 481-498.

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

[19] M. O. Rabin, Probabilistic algorithm for testing primality, J. Number Theory, 12 (1980), no. 1, 128-138.

[20] P. Stevenhagen, Class number parity for the $p$th cyclotomic field, Math. Comp., 63 (1994), no. 208, 773-784.

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

[22] R. Zimmert, Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung, Invent. Math., 62 (1980), no. 3, 367-380.