Functiones et Approximatio
57.1 (2017), 93–103
doi: 10.7169/facm/1619

NOTE ON THE CLASS NUMBER OF THE pTH CYCLOTOMIC FIELD, III

Humio Ichimura

Abstract: Let $p = 2\ell^f + 1$ be a prime number with $f \geqslant 2$ and an odd prime number ℓ. For $0 \leqslant t \leqslant f$, let K_t be the imaginary subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ with $[K_t : \mathbb{Q}] = 2\ell^t$. Denote by $h^-_{p,t}$ the relative class number of K_t, and by $h^+_{p,t}$ the class number of the maximal real subfield K_t^+. It is known that the ratio $h^-_{p,f}/h^-_{p,f-1}$ is odd (and hence so is $h^+_{p,f}/h^+_{p,f-1}$) whenever 2 is a primitive root modulo ℓ^2. We show that $h^+_{p,f}/h^+_{p,f-1}$ is odd under a somewhat milder assumption on ℓ and that the ratio $h^-_{p,f-1}/h^-_{p,f-2}$ is always odd when $\ell = 3$.

Keywords: relative class number, cyclotomic field.

1. Introduction

Let p be an odd prime number. Let $K = \mathbb{Q}(\zeta_p)$ be the pth cyclotomic field, and h^-_p the relative class number of K. Here, for an integer $m \geqslant 2$, ζ_m denotes a primitive mth root of unity. When $p = 2\ell + 1$ for some odd prime number ℓ, it is conjectured that h^-_p is odd. There are several results and computations related to this conjecture, for which see Estes [3], Stevenhagen [12], Metsänkylä [10] and some references therein. In the previous papers [4, 5], we extended some of these results for prime numbers of the form $p = 2\ell^f + 1$ with $f \geqslant 2$ and $p = 2^{e+1}\ell + 1$ with $e \geqslant 1$. In what follows, let $p = 2\ell^f + 1$ be a prime number with $f \geqslant 2$ and an odd prime number ℓ. For each $0 \leqslant t \leqslant f$, we denote by K_t the imaginary subfield of K of degree $2\ell^t$ over $\mathbb{Q}$ and by $k_t = K_t^+$ the maximal real subfield of K_t. Let $h^-_{p,t}$ be the relative class number of K_t, and $h^+_{p,t}$ the class number of k_t in the usual sense. Then we have $K_f = K$, $h^-_{p,f} = h^-_p$, $K_0 = \mathbb{Q}(\sqrt{-p})$ and $k_0 = \mathbb{Q}$. Using class field theory, we can easily show that $h^{\pm}_{p,t-1}$ divides $h^{\pm}_{p,t}$ for each t. In [4], we proved that the ratio $h^-_{p,f}/h^-_{p,f-1}$ is odd whenever 2 is a primitive root modulo ℓ^2, and gave some computational results in the range $p = 2\ell^f + 1 < 2^{56}$, which suggest that $h^-_{p,t}/h^-_{p,t-1}$ might be odd if $t_0 + 1 \leqslant t \leqslant f$ with $t_0 = \mathrm{ord}_\ell(2^{\ell-1} - 1)$. It is

2010 Mathematics Subject Classification: primary: 11R18; secondary: 11R29

known that the ratio $h^+_{p,t}/h^+_{p,t-1}$ is odd if $h^-_{p,t}/h^-_{p,t-1}$ is odd (see Lemma 1 in §2), and hence it follows from the above that the ratio $h^+_{p,f}/h^+_{p,f-1}$ is odd whenever 2 is a primitive root modulo ℓ^2.

The purposes of this note are (i) to relax the assumption of the last assertion on the real class number (Proposition 1) and (ii) to deal with the case $t = f-1$ for the relative class number (Propositions 2, 3). The assertion on the real class number is given for a fixed f and varying ℓ, while the ones on the relative class number are given for a fixed ℓ and varying f.

Proposition 1. *Under the above setting, assume that $\ell \equiv 3 \bmod 4$ and the order of 2 modulo ℓ^2 is $(\ell-1)\ell/2$. Then the ratio $h^+_{p,f}/h^+_{p,f-1}$ is odd.*

Proposition 2. *Let ℓ be an odd prime number such that 2 is a primitive root modulo ℓ^2. Then the ratio $h^-_{p,f-1}/h^-_{p,f-2}$ is odd for any prime number $p = 2\ell^f+1$ if $p > (2\ell(\ell-1))^{\ell(\ell-1)}$.*

Let $\ell = 3$. By the computation of Williams and Zarnke [15], it is known that when $f \leqslant 325$, $p = 2\cdot 3^f+1$ is a prime number for

$$f = 1, 2,\ 4,\ 5,\ 6,\ 9,\ 16,\ 17,\ 30,\ 54,\ 57,\ 60,\ 65,\ 132,\ 180,\ 320.$$

We see from Proposition 2 that $h^-_{p,f-1}/h^-_{p,f-2}$ is odd if $p > 12^6$ since 2 is a primitive root modulo 9. In view of the above data, this implies that the ratio is odd when $f \geqslant 16$ as $2\cdot 3^{16}+1 > 12^6$. On the other hand, we already know by [4, Proposition 2] that $h^-_{p,t}/h^-_{p,t-1}$ is odd for any $2 \leqslant t \leqslant f$ when $p = 2\cdot 3^f+1 < 2^{56}$, namely when $f \leqslant 30$ in the above data. Therefore, we obtain the following:

Proposition 3. *When $\ell = 3$, $h^-_{p,f-1}/h^-_{p,f-2}$ is odd for any prime number $p = 2\cdot 3^f+1$.*

Remark 1.

(I) When $p = 2\ell+1$ (the case $f = 1$), it is shown in [3, 10, 12] that h^-_p is odd (and hence so is h^+_p) when $\ell \equiv 3 \bmod 4$ and the order of 2 modulo ℓ is $(\ell-1)/2$. It is not clear to us whether their methods can be applied for showing that $h^-_{p,f}/h^-_{p,f-1}$ is odd under the setting and the assumption of Proposition 1.

(II) A similar condition appears also for an odd prime number r. Let $p = 2\ell+1$ be as above, and assume that $\ell \equiv 3 \bmod 4$ and that the order of r modulo ℓ is $\ell-1$ or $(\ell-1)/2$. Then Jakubec and Trojovský [9, Theorem 1] and Trojovský [13, Theorem 1] showed that h^+_p is not divisible by r when $r \leqslant 10000$.

2. Proof of Proposition 1

For a while, we work in a more general setting. Let p be an odd prime number with $p \equiv 3 \bmod 4$, and put $K = \mathbb{Q}(\zeta_p)$ and $K_0 = \mathbb{Q}(\sqrt{-p})$. We denote by Cl_N

the ideal class group of a number field N in the usual sense. Let Cl_K^- be the kernel of the norm map $Cl_K \to Cl_{K^+}$ where N^+ is the maximal real subfield of an imaginary abelian field N. We denote by A_K^- and A_K^+ the 2-primary parts of the class groups Cl_K^- and Cl_{K^+}, respectively. The Galois group $\Delta = \mathrm{Gal}(K^+/\mathbb{Q})$ is naturally identified with $\mathrm{Gal}(K/K_0)$ as $K = K^+K_0$. We can naturally regard the groups A_K^- and A_K^+ as modules over the group ring $\mathbb{Z}[\Delta]$. We fix algebraic closures $\bar{\mathbb{Q}}$ and $\bar{\mathbb{Q}}_2$ of the rationals $\mathbb{Q}$ and the 2-adic rationals $\mathbb{Q}_2$, respectively, and we fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_2$ in all what follows. A character of Δ or a Dirichlet character of conductor p is assumed to be $\bar{\mathbb{Q}}$-valued and at the same time as $\bar{\mathbb{Q}}_2$-valued via the embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_2$. Further, a character of Δ is often regarded as an even Dirichlet character of conductor p. For a character χ of Δ, let

$$e_\chi = \frac{1}{|\Delta|} \sum_{\sigma \in \Delta} \mathrm{Tr}_\chi(\chi(\sigma^{-1}))\sigma \in \mathbb{Z}_2[\Delta] \tag{1}$$

be the idempotent of $\mathbb{Z}_2[\Delta]$ associated to χ, Tr_χ being the trace map from $\mathbb{Q}_2(\chi)$ to $\mathbb{Q}_2$. Here, $\mathbb{Z}_2$ denotes the ring of 2-adic integers and $\mathbb{Q}_2(\chi)$ the subfield of $\bar{\mathbb{Q}}_2$ generated by the values of χ over $\mathbb{Q}_2$. For a module X over $\mathbb{Z}[\Delta]$, we set $X(\chi) = \widehat{X}^{e_\chi}$ or $e_\chi \widehat{X}$, where $\widehat{X} = X \otimes_{\mathbb{Z}} \mathbb{Z}_2$. The following assertion is shown in Cornacchia [1, Theorem 1]. (See also [8, Theorem 4] for an alternative proof.)

Lemma 1. *Under the above setting, the following conditions are equivalent to each other.*

(I) *At least one of $A_K^-(\chi)$ and $A_K^-(\chi^{-1})$ is trivial.*
(II) *Both of $A_K^+(\chi)$ and $A_K^+(\chi^{-1})$ are trivial.*

The following assertion is a consequence of Lemma 1.

Lemma 2. *Under the setting of Lemma 1, assume that $-1 \equiv 2^a \bmod d$ for some $a \in \mathbb{Z}$ where d is the order of χ. Then $A_K^-(\chi)$ is trivial if and only if so is $A_K^+(\chi)$.*

Proof. Under the assumption on d, we see that χ and χ^{-1} are conjugate over $\mathbb{Q}_2$, and hence that $X(\chi) = X(\chi^{-1})$ for every $\mathbb{Z}[\Delta]$-module X. Therefore, the assertion follows from Lemma 1. ∎

Let δ be the quadratic character associated to $K_0 = \mathbb{Q}(\sqrt{-p})$. Regarding a character χ of Δ as an even Dirichlet character of conductor p, we denote by

$$B_{1,\delta\chi} = \frac{1}{p} \sum_{a=1}^{p-1} a\delta\chi(a)$$

the generalized Bernoulli number. As for the order of $A_K^-(\chi)$, Greither [6, Theorem A] proved that

$$|A_K^-(\chi)| = |\mathcal{O}_\chi / \beta_{\delta\chi^{-1}} \mathcal{O}_\chi| \qquad \text{with} \ \ \beta_{\delta\chi} = \frac{1}{2} B_{1,\delta\chi} \tag{2}$$

as a consequence of the Iwasawa main conjecture. Here, $\mathcal{O}_\chi$ is the ring of integers of $\mathbb{Q}_2(\chi)$.

We return back to the specific setting in §1 with $p = 2\ell^f + 1$ and recall what we have shown in the previous paper [4]. We use the same notation as above. In particular, $K = K_f$ and $\Delta = \mathrm{Gal}(K_f/K_0) = \mathrm{Gal}(k_f/\mathbb{Q})$. In what follows, we assume that $\mathrm{ord}_\ell(2^{\ell-1}-1) = 1$, where $\mathrm{ord}_\ell(*)$ is the additive ℓ-adic valuation with $\mathrm{ord}_\ell(\ell) = 1$. This is satisfied in the setting of Propositions 1 and 2. For an element $x \in \mathbb{Z}_p$, let $s_p(x) \in \mathbb{Z}$ be the unique integer with $s_p(x) \equiv x \bmod p$ and $0 \leqslant s_p(x) \leqslant p-1$. Fixing a primitive root g modulo p, we put

$$G_{t,j_0} = G_{t,j_0}(T) = \sum_{v=0}^{\ell-1} \left(\sum_{u=0}^{\ell^{f-t}-1} s_p(g^{2(\ell^t u + \ell^{t-1} v + j_0)}) \right) T^v \ (\in \mathbb{Z}[T])$$

for each integer $j_0 \geqslant 0$. Let χ_t be an arbitrary character of Δ with order ℓ^t for each $0 \leqslant t \leqslant f$. The value $\beta_{\delta\chi_t}$ is contained in $F_t = \mathbb{Q}(\zeta_{\ell^t})$. In [4, page 303], we have shown that

$$\mathrm{Tr}_{F_t/F_1}\left(\zeta_{\ell^t}^{-j_0}\beta_{\delta\chi_t}\right) = \frac{\ell^{t-1}}{p} G_{t,j_0}(\zeta_\ell) \tag{3}$$

with

$$\zeta_{\ell^t} = \chi_t(g^2) \qquad \text{and} \qquad \zeta_\ell = \zeta_{\ell^t}^{\ell^{t-1}} = \chi_t(g^{2\ell^{t-1}}). \tag{4}$$

What we have actually shown in the proof of the main theorem of [4] is the following. Let $\Phi_\ell = \Phi_\ell(T)$ be the ℓth cyclotomic polynomial. For a polynomial $G = G(T) \in \mathbb{Z}[T]$, let $\widetilde{G} = G \bmod 2 \in \mathbb{F}_2[T]$. Here, $\mathbb{F}_2$ is the finite field of two elements.

Lemma 3. *When $t = f$, there exists some j_0 such that $\widetilde{G}_{f,j_0}$ is not divisible by $\widetilde{\Phi}_\ell$.*

Assume that $\ell \equiv 3 \bmod 4$ and that the order of 2 modulo ℓ^2 is $(\ell-1)\ell/2$. Let D_t be the decomposition group of the prime 2 for the abelian extension $F_t/\mathbb{Q}$. Then the assumption on ℓ implies that for each $1 \leqslant t \leqslant f$, the Galois group $\mathrm{Gal}(F_t/\mathbb{Q})$ is generated by D_t and the complex conjugation. We fix a character χ_t of Δ with order ℓ^t. Then we observe from the above that any character of Δ with order ℓ^t is conjugate to χ_t or χ_t^{-1} over $\mathbb{Q}_2$. Hence, we obtain

$$X = \bigoplus_{t=1}^{f} \left(X(\chi_t) \oplus X(\chi_t^{-1})\right) \bigoplus X(\chi_0)$$

for every $\mathbb{Z}_2[\Delta]$-module X.

Proof of Proposition 1. Under the setting and assumptions of Proposition 1, assume to the contrary that $h_{p,f}^+/h_{p,f-1}^+$ is even. Then it follows from the above that at least one of $A_K^+(\chi_f)$ or $A_K^+(\chi_f^{-1})$ is nontrivial. By Lemma 1, this implies that both of $A_K^-(\chi_f)$ and $A_K^-(\chi_f^{-1})$ are nontrivial. Let $\mathfrak{P}_f$ be the prime ideal of F_f over 2 corresponding to the fixed embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_2$, and we put $\mathfrak{P}_1 = \mathfrak{P}_f \cap F_1$.

Then we see from (2) that $\beta_{\delta\chi_f} \equiv \beta_{\delta\chi_f^{-1}} \equiv 0 \bmod \mathfrak{P}_f$. Because of the assumption on ℓ, the prime ideal $\mathfrak{P}_1$ of F_1 remains prime in F_f. It follows that

$$\mathrm{Tr}_{F_f/F_1}\left(\zeta^{-1}\beta_{\delta\chi_f}\right) \equiv \mathrm{Tr}_{F_f/F_1}\left(\zeta^{-1}\beta_{\delta\chi_f^{-1}}\right) \equiv 0 \bmod \mathfrak{P}_1$$

for any ℓ^fth root ζ of unity. Therefore, we observe from (3) and (4) that $\zeta_\ell = \chi_f(g^{2\ell^{f-1}}) \bmod \mathfrak{P}_1$ and $\zeta_\ell^{-1} = \chi_f^{-1}(g^{2\ell^{f-1}}) \bmod \mathfrak{P}_1$ are roots of $\widetilde{G}_{f,j_0}$ for all j_0. On the other hand, the assumption on ℓ implies that $\widetilde{\Phi}_\ell$ is decomposed as $\widetilde{\Phi}_\ell = P(X)Q(X)$ where $P(X)$, $Q(X)$ are irreducible over $\mathbb{F}_2$ and $Q(X) = X^{(\ell-1)/2}P(1/X)$ is the reciprocal polynomial of $P(X)$. Therefore, it follows that $\widetilde{G}_{f,j_0}$ are multiple of $\widetilde{\Phi}_\ell$ for all j_0. However, this is impossible by Lemma 3. ■

3. Cyclotomic units

In what follows, we *always assume* that 2 is a primitive root modulo ℓ^2, and work under the setting of §1. Then, all characters of $\Delta = \mathrm{Gal}(K_f/K_0)$ with order ℓ^t are conjugate to χ_t over $\mathbb{Q}_2$. Hence, it follows that

$$X = \bigoplus_{t=0}^{f} X(\chi_t)$$

for every $\mathbb{Z}[\Delta]$-module X. In particular, the 2-part of the ratio $h_{p,t}^-/h_{p,t-1}^-$ equals $|A_K^-(\chi_t)|$. Thus, we obtain from Lemma 2 the equivalence

$$2 \nmid h_{p,t}^-/h_{p,t-1}^- \iff A_K^+(\chi_t) = \{0\}. \tag{5}$$

Let E be the group of units of $k_f = \mathbb{Q}(\zeta_p)^+$, and C the subgroup of E consisting of cyclotomic units of k_f in the sense of Washington [14, §8.1]. As is well known, E/C is a finite abelian group and $|E/C| = h^+$ ([14, Theorem 8.2]). Cornacchia and Greither [2, Proposition 2] proved

$$|(E/C)(\chi_t)| = |A_K^+(\chi_t)| \tag{6}$$

for each t as a consequence of the Iwasawa main conjecture.

For t with $0 \leqslant t < f$, let $N_{f,t}$ be the norm map from k_f to k_t, which is identified with the norm map from K_f to K_t. We see that

$$e_{\chi_{f-1}} = \frac{1}{\ell^2}(\ell N_{f,f-1} - N_{f,f-2}).$$

This follows from the definition (1) as follows. For each $\sigma \in \Delta$, we note that $\chi_{f-1}(\sigma) = 1$ if and only if $\sigma^\ell = 1$, and that with $1 \leqslant i \leqslant f-1$, $\chi_{f-1}(\sigma)$ is a primitive ℓ^ith root of unity if and only if the order of σ equals ℓ^{i+1}. The prime number 2 remains prime in $\mathbb{Q}(\zeta_{\ell^{f-1}})$ since 2 is a primitive root modulo ℓ^2. Hence, $\mathbb{Q}_2(\chi_{f-1}) = \mathbb{Q}_2(\zeta_{\ell^{f-1}})$ is of degree $(\ell-1)\ell^{f-2}$ over $\mathbb{Q}_2$. Put $\mathrm{Tr} = \mathrm{Tr}_{\chi_{f-1}}$ for brevity.

Then, we see that $\mathrm{Tr}(\delta) = 0$ for $\delta \in \mu_{\ell^{f-1}} \setminus \mu_\ell$, and that $\mathrm{Tr}(\delta) = (\ell-1)\ell^{f-2}$ or $-\ell^{f-2}$ for $\delta \in \mu_\ell$ according as $\delta = 1$ or not. Combining these, we can easily show the assertion from (1).

We put $\mathcal{O} = \mathbb{Z}_2[\zeta_{\ell^{f-1}}]$. Then the χ_{f-1}-part $X(\chi_{f-1})$ of a $\mathbb{Z}[\Delta]$-module X is naturally regarded as an $\mathcal{O}$-module. We see that $E(\chi_{f-1}) \cong \mathcal{O}$ as $\mathcal{O}$-modules by a theorem of Minkowski on the group of units of a Galois extension over $\mathbb{Q}$ (cf. Narkiewicz [11, Theorem 3.26]). Let g be a fixed primitive root modulo p, and put

$$\xi = {\prod_j}' \left(\zeta_p^{g^{2\ell^{f-2}j}} + 1 \right) \tag{7}$$

where j runs over the integers with $0 \leqslant j \leqslant \ell^2 - 1$ and $\ell \nmid j$. Let $\mathfrak{f} = \mathfrak{f}_2$ be the Frobenius automorphism of K_f at 2. We show the following:

Lemma 4. *If the ratio $h^-_{p,f-1}/h^-_{p,f-2}$ is even, then* $\xi^{\mathfrak{f}} \equiv \xi^2 \bmod 4$.

Proof. Put

$$\xi_1 = (\zeta_p + \zeta_p^{-1})^{\ell N_{f,f-1} - N_{f,f-2}},$$

which is an element of $C(\chi_{f-1})$. Assume that $h^-_{p,f-1}/h^-_{p,f-2}$ is even. Then, as $E(\chi_{f-1}) \cong \mathcal{O}$, we see from (5) and (6) that $C(\chi_{f-1}) \subseteq E(\chi_{f-1})^2$. Therefore, ξ_1 is a square in E, and hence $\xi_1 \in (K_f^\times)^2$. We see that ξ_1 is Galois conjugate to the element

$$\xi_2 = (\zeta_p + 1)^{\ell N_{f,f-1}} \times (\zeta_p + 1)^{-N_{f,f-2}}.$$

Thus, $\xi_2 \in (K_f^\times)^2$. Let σ be the automorphism of K_f sending ζ_p to ζ_p^g. Then we see that

$$\begin{aligned}
\xi_2 &= \left(\prod_{j=0}^{\ell-1} (\zeta_p + 1)^{\sigma^{2\ell^{f-1}j}} \right)^{\ell} \times \left(\prod_{j=0}^{\ell^2-1} (\zeta_p + 1)^{\sigma^{2\ell^{f-2}j}} \right)^{-1} \\
&= \left(\prod_{j=0}^{\ell-1} (\zeta_p + 1)^{\sigma^{2\ell^{f-1}j}} \right)^{\ell-1} \times \left({\prod_j}' (\zeta_p + 1)^{\sigma^{2\ell^{f-2}j}} \right)^{-1} \\
&\equiv \xi^{-1} \bmod (K_f^\times)^2.
\end{aligned}$$

Here, in the fourth product $\prod_j'$, j runs over the same range as in (7). Thus, it follows that $\xi = x^2$ for some $x \in K_f^\times$. As 2 is unramified in K_f, we have $x^{\mathfrak{f}} \equiv x^2 \bmod 2$. Hence,

$$\xi^{\mathfrak{f}} = (x^{\mathfrak{f}})^2 \equiv (x^2)^2 \equiv \xi^2 \bmod 4. \qquad \blacksquare$$

Let J be the set of integers with $0 \leqslant j \leqslant \ell^2 - 1$ and $\ell \nmid j$. For each $m \in J$, let $J_m = J \setminus \{m\}$ and let Ψ_m be the set of maps $\kappa : J_m \to \{0, 1\}$. For $m \in J$ and $\kappa \in \Psi_m$, we put

$$A(m, \kappa) = g^{2\ell^{f-2}m} + 2 \sum_{j \in J_m} \kappa(j) g^{2\ell^{f-2}j}.$$

Lemma 5. *Assume that there exist an integer $m_0 \in J$ and a map $\kappa_0 \in \Psi_{m_0}$ such that $A(m, \kappa) \not\equiv A(m_0, \kappa_0) \bmod p$ for all pairs $(m, \kappa) \neq (m_0, \kappa_0)$. Then the ratio $h^-_{p,f-1}/h^-_{p,f-2}$ is odd.*

Proof. Let m_0 and κ_0 be as above. Assume to the contrary that $h^-_{p,f-1}/h^-_{p,f-2}$ is even. Then by Lemma 4 we see that

$$\begin{aligned}\prod_j{}'(\zeta_p^{2g^{2\ell^{f-2}j}}+1) &\equiv \prod_j{}'(\zeta_p^{g^{2\ell^{f-2}j}}+1)^2\\ &\equiv \prod_j{}'((\zeta_p^{2g^{2\ell^{f-2}j}}+1)+2\zeta_p^{g^{2\ell^{f-2}j}}) \bmod 4.\end{aligned} \tag{8}$$

The third product is congruent to

$$\begin{aligned}\prod_j{}'(\zeta_p^{2g^{2\ell^{f-2}j}}+1) &+ 2\sum_{m\in J}\zeta_p^{g^{2\ell^{f-2}m}}\prod_{j\in J_m}(\zeta_p^{2g^{2\ell^{f-2}j}}+1)\\ &\equiv \prod_j{}'(\zeta_p^{2g^{2\ell^{f-2}j}}+1)+2\sum_{m\in J}\sum_{\kappa\in\Psi_m}\zeta_p^{A(m,\kappa)} \bmod 4.\end{aligned}$$

Therefore, it follows from (8) that

$$\sum_{m\in J}\sum_{\kappa\in\Psi_m}\zeta_p^{A(m,\kappa)} \equiv 0 \bmod 2.$$

Multiplying this by $\zeta_p^{-A(m_0,\kappa_0)}$, we obtain

$$1+\sum_{(m,\kappa)}{}'\zeta_p^{A(m,\kappa)-A(m_0,\kappa_0)} \equiv 0 \bmod 2 \tag{9}$$

where (m,κ) runs over the pairs with $(m, \kappa) \neq (m_0, \kappa_0)$. The number N of such pairs equals $|J| \times 2^{|J|-1} - 1$, and hence it is odd. Therefore, taking the trace of the left hand side of (9) to the rationals $\mathbb{Q}$, we obtain

$$(p-1)+N\times(-1) \equiv 1 \bmod 2$$

because $\zeta_p^{A(m,\kappa)-A(m_0,\kappa_0)}$ is a primitive pth root of unity by the assumption of Lemma 5. This contradicts the congruence (9). ■

As g is a primitive root modulo p, the order of $g^{2\ell^{f-2}} \bmod p$ is ℓ^2. As $p \equiv 1 \bmod \ell^f$ and $f \geqslant 2$, p splits completely in $\mathbb{Q}(\zeta_{\ell^2})$. Let $\mathfrak{P}$ be an arbitrary prime ideal of $\mathbb{Q}(\zeta_{\ell^2})$ over p, which is necessarily of degree one. Then there exists a primitive ℓ^2th root η of unity in $\mathbb{Q}(\zeta_{\ell^2})$ such that

$$\eta \equiv g^{2\ell^{f-2}} \bmod \mathfrak{P}. \tag{10}$$

For $m \in J$ and $\kappa \in \Psi_m$, we put

$$B(m,\kappa) = \eta^m + 2\sum_{j \in J_m} \kappa(j)\eta^j \ \in \mathbb{Q}(\zeta_{\ell^2}).$$

Then, by (10), we obtain the following equivalence on the condition in Lemma 5.

$$A(m,\kappa) \equiv A(m_0,\kappa_0) \bmod p \Longleftrightarrow B(m,\kappa) \equiv B(m_0,\kappa_0) \bmod \mathfrak{P}. \tag{11}$$

4. Proof of Proposition 2

Let η be the primitive ℓ^2th root of unity satisfying (10). Because of (11), we can work in the ℓ^2th cyclotomic field $\mathbb{Q}(\zeta_{\ell^2})$. We assume that 2 is a primitive root modulo ℓ^2. Then the automorphism sending η to η^2 is a generator of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^2})/\mathbb{Q})$. For each $1 \leqslant i \leqslant \ell-1$ and $1 \leqslant j \leqslant \ell$, we put

$$\eta_i = \eta^{2^{i-1}} \qquad \text{and} \qquad \eta_{i,j} = \eta_i^{1+(j-1)\ell} = \eta^{2^{i-1}(1+(j-1)\ell)}.$$

These $\ell(\ell-1)$ elements are all the primitive ℓ^2th roots of unity. Let ρ be an automorphism of $\mathbb{Q}(\zeta_{\ell^2})$ over $\mathbb{Q}(\zeta_\ell)$ sending η to $\eta^{1+\ell}$. Then, setting $\zeta_\ell = \eta^\ell$, we see that

$$\eta_{i,j}^\rho = \eta_{i,j+1} = \zeta_\ell^{2^{i-1}}\eta_{i,j}.$$

It follows that

$$\mathrm{Tr}(\eta_i) = \sum_{j=1}^{\ell} \eta_{i,j} = \eta_i \times \sum_{j=1}^{\ell} (\zeta_\ell^{2^{i-1}})^{j-1} = 0 \tag{12}$$

where Tr denotes the trace map from $\mathbb{Q}(\zeta_{\ell^2})$ to $\mathbb{Q}(\zeta_\ell)$. Regarding $\mathbb{Q}(\zeta_{\ell^2})$ as a vector space over $\mathbb{Q}$, let V be its subspace spanned by all the primitive ℓ^2th roots of unity over $\mathbb{Q}$. For each i with $1 \leqslant i \leqslant \ell-1$, let V_i be the subspace of V spanned by $\eta_{i,j}$ with $1 \leqslant j \leqslant \ell$. The following lemma on these vector spaces over $\mathbb{Q}$ is easy to show.

Lemma 6.

(I) *The automorphism ρ acts on V_i via $\zeta_\ell^{2^{i-1}}$-multiplication, and $V = V_1 \oplus V_2 \cdots \oplus V_{\ell-1}$.*

(II) *For each i, the equality* (12) *is the unique linear relation over $\mathbb{Q}$ satisfied by the elements $\eta_{i,j}$ with $1 \leqslant j \leqslant \ell$, namely* $\dim_{\mathbb{Q}} V_i = \ell - 1$.

Let I be the set of pairs (i,j) with $1 \leqslant i \leqslant \ell-1$ and $1 \leqslant j \leqslant \ell$. We identify the set I with J in §3 via the correspondence

$$(i,\, j) \longleftrightarrow 2^{i-1}(1+(j-1)\ell) \bmod \ell^2.$$

For each $(u,v) \in I$, let $I_{u,v} = I \setminus \{(u,v)\}$ and let $\Psi_{u,v}$ be the set of maps $\kappa : I_{u,v} \to \{0,\, 1\}$. For each map $\kappa \in \Psi_{u,v}$, we put

$$C(u,v,\kappa) = \eta_{u,v} + 2{\sum_{(i,j)}}' \kappa(i,j)\eta_{i,j}$$

where (i,j) runs over the set $I_{u,v}$. We choose $\kappa_0 \in \Psi_{1,1}$ so that $\kappa_0(i,1) = 1$ for $i \geqslant 2$ and $\kappa_0(i,j) = 0$ for $j \geqslant 2$, and put

$$C_0 = C(1,1,\kappa_0) = \eta_{1,1} + 2(\eta_{2,1} + \cdots + \eta_{\ell-1,1}).$$

The triple $(1,1,\kappa_0)$ plays the role of the pair (m_0,κ_0) in Lemma 5.

Lemma 7. *For $(u,v) \in I$ and $\kappa \in \Psi_{u,v}$, we have $C(u,v,\kappa) \neq C_0$ if $(u,v,\kappa) \neq (1,1,\kappa_0)$.*

Proof. We fix a triple (u,v,κ) with $(u,v,\kappa) \neq (1,1,\kappa_0)$. For each i with $i \neq u$, we define an element X_i of V_i by

$$X_i = (\kappa(i,1) - 1)\eta_{i,1} + \sum_{j=2}^{\ell} \kappa(i,j)\eta_{i,j}.$$

Further, we define elements Y_1 and Z_1 of V_1 when $(u,v) \neq (1,1)$ by

$$Y_1 = (2\kappa(1,1) - 1)\eta_{1,1} + 2\sum_{j=2}^{\ell} \kappa(1,j)\eta_{1,j}, \quad \text{for } u \neq 1,$$

$$Z_1 = (2\kappa(1,1) - 1)\eta_{1,1} + \eta_{1,v} + 2\sum_{j\neq 1,v} \kappa(1,j)\eta_{1,j}, \quad \text{for } v \neq 1,$$

and elements Y_u and Z_u of V_u when $u \neq 1$ by

$$Y_u = -\eta_{u,1} + 2\sum_{j=2}^{\ell} \kappa(u,j)\eta_{u,j}, \quad \text{for } v = 1,$$

$$Z_u = 2(\kappa(u,1) - 1)\eta_{u,1} + \eta_{u,v} + 2\sum_{j\neq 1,v} \kappa(u,j)\eta_{u,j}, \quad \text{for } v \neq 1.$$

By Lemma 6(II), we see that $X_i = 0$ if and only if $\kappa(i,1) - 1 = \kappa(i,j)$ for $2 \leqslant j \leqslant \ell$. As the value of κ is 0 or 1, we obtain the equivalence

$$X_i = 0 \Longleftrightarrow \kappa(i,1) = 1 \text{ and } \kappa(i,j) = 0 \text{ for } 2 \leqslant j \leqslant \ell. \tag{13}$$

Similarly, we can show that $Y_k \neq 0$ and $Z_k \neq 0$ with $k = 1$, u from Lemma 6(II).

First, we deal with the case $(u,v) = (1,1)$. We have

$$C(1,1,\kappa) - C_0 = 2\sum_{j=2}^{\ell} \kappa(1,j)\eta_{1,j} + 2\sum_{i=2}^{\ell-1} X_i. \tag{14}$$

Assume that $C(1,1,\kappa) = C_0$. Then it follows from (14) and Lemma 6(I) that

$$\sum_{j=2}^{\ell} \kappa(1,j)\eta_{1,j} = X_2 = \cdots = X_{\ell-1} = 0.$$

From Lemma 6(II) and (13), we obtain $\kappa = \kappa_0$, which contradicts the assumption $(u, v, \kappa) = (1, 1, \kappa) \neq (1, 1, \kappa_0)$. Next, let $u = 1$ and $v \neq 1$. Then we have

$$C(1, v, \kappa) - C_0 = Z_1 + 2 \sum_{i=2}^{\ell-1} X_i. \tag{15}$$

As $Z_1 \neq 0$, we see that $C(1, v, \kappa) \neq C_0$ from Lemma 6(I). Finally, let $u \neq 1$. We have

$$C(u, v, \kappa) - C_0 = \begin{cases} Y_1 + Y_u + 2 \sum_{i \neq 1, u} X_i, & \text{for } v = 1 \\ Y_1 + Z_u + 2 \sum_{i \neq 1, u} X_i, & \text{for } v \geqslant 2. \end{cases} \tag{16}$$

Hence, $C(u, v, \kappa) \neq C_0$ as $Y_1 \neq 0$. ■

Proof of Proposition 2. For each element $\alpha = \sum_\xi a_\xi \xi$ in V with $\xi \in \mu_{\ell^2} \setminus \mu_\ell$ and $a_i \in \mathbb{Q}$, we have

$$|\iota(\alpha)| \leqslant \sum_\xi |a_\xi|$$

for any embedding ι of $\mathbb{Q}(\zeta_{\ell^2})$ into the complex numbers $\mathbb{C}$. It follows that

$$N(\alpha) \leqslant \left(\sum_\xi |a_\xi| \right)^{\ell(\ell-1)}, \tag{17}$$

where N denotes the norm map from $\mathbb{Q}(\zeta_{\ell^2})$ to $\mathbb{Q}$. For $(u, v, \kappa) \neq (1, 1, \kappa_0)$, we obtain

$$1 \leqslant N(C(u, v, \kappa) - C_0) \leqslant (2\ell(\ell-1))^{\ell(\ell-1)}$$

from Lemma 7 and the estimate (17) because the coefficients of the primitive ℓ^2th roots $\eta_{i,j}$ of unity in (14), (15) and (16) are 0, ± 1 or ± 2. Hence, if $p > (2\ell(\ell-1))^{\ell(\ell-1)}$, we see that

$$C(u, v, \kappa) \not\equiv C_0 \bmod \mathfrak{P}$$

for $(u, v, \kappa) \neq (1, 1, \kappa_0)$. Here, $\mathfrak{P}$ is an arbitrary prime ideal of $\mathbb{Q}(\zeta_{\ell^2})$ over p. Therefore, by Lemma 5 and the equivalence (11), we obtain the assertion. ■

Remark 2. In [7], Horie studied the non-ℓ-part of the class numbers of the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$. We have used some of his ideas/techniques for showing Proposition 2.

Corrigendum. In the previous paper [4, §4], we gave five tables; Tables 3, 4, 5, 6 and 7. However, their labeling is wrong, and it is necessary to change Table n to Table $n-2$ for each $3 \leqslant n \leqslant 7$ except for the one in the first line of [4, Proposition 3]. Further, in Table 7, the entry for the column $r = 7$ and the row $j_0 = 2$ is incorrect and it should be changed to 4.

Acknowledgement. The author is grateful to the referee for several valuable comments, in particular for pointing out a mistake in the first version of the paper.

References

[1] P. Cornacchia, *The parity of class number of the cyclotomic fields of prime conductor,* Proc. Amer. Math. Soc., **125** (1997), 3163-3168.

[2] P. Cornacchia and C. Greither, *Fitting ideals of class groups of real fields of prime power conductor,* J. Number Theory, **73** (1998), 459-471.

[3] D. Estes, *On the parity of the class number of the field of q th roots of unity,* Rocky Mountain J. Math., **19** (1989), 675-689.

[4] S. Fujima and H. Ichimura, *Note on the class number of the pth cyclotomic field,* Funct. Approx. Comment. Math., **52.2** (2015), 299-309.

[5] S. Fujima and H. Ichimura, *Note on the class number of the pth cyclotomic field, II,* Experiment. Math., doi:10.1080/10586458.2016.1230528.

[6] C. Greither, *Class groups of abelian extensions and the main conjecture,* Ann. Inst. Fourier, **42** (1996), 449-499.

[7] K. Horie, *Ideal class groups of the Iwasawa-theoretical extensions of the rationals,* J. London Math. Soc., **66** (2002), 257-275.

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

[9] S. Jakubec and P. Trojovský, *On divisiblity of the class number h^+ of the real cyclotomic fields $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ by primes $p < 5000$,* Abh. Math. Univ. Hamburg, **67** (1997), 269-280.

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

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

[12] P. Stevenhagen, *Class number parity of the pth cyclotomic field,* Math. Comp., **63** (1994), 773-784.

[13] P. Trojovský, *On divisibility of the class number h^+ of the real cyclotomic field $\mathbb{Q}(\zeta_q + \zeta_q^{-1})$ by primes $q < 10000$,* Math. Slovaca, **50.5** (2000), 541-555.

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

[15] H.C. Williams and C.R. Zarnke, *Some prime numbers of the forms $2A3^n + 1$ and $2A3^n - 1$,* Math. Comp., **26** (1972), 995-998.

Address: Humio Ichimura: Faculty of Science, Ibaraki University, Bunkyo 2-1-1, Mito, 310-8512, Japan.

E-mail: humio.ichimura.sci@vc.ibaraki.ac.jp

Received: 22 July 2016; **revised:** 6 September 2016