ACTA ARITHMETICA
150.3 (2011)

# On the class group of a cyclotomic $\mathbb{Z}_p \times \mathbb{Z}_\ell$-extension

by

Humio Ichimura (Mito)

**1. Introduction.** Let $p$ be an odd prime number, and $\ell$ a prime number with $p \neq \ell$. For a number field $F$, let $F_\infty/F$ be the cyclotomic $\mathbb{Z}_p$-extension, and $F_n$ its $n$th layer with $F_0 = F$. It is a well known theorem of Washington [18] that when $F$ is an abelian field, the $\ell$-part of the class number $h_{F_n}$ of $F_n$ is stable for sufficiently large $n$. For an abelian field $F$, we denote by $f_F$ the conductor of $F$. In what follows, let $F$ be a *real* abelian field. For simplicity, we always assume that $p^2 \nmid f_F$. For $0 \leq n \leq \infty$, denote by $F_n^{(\ell)}$ the cyclotomic $\mathbb{Z}_\ell$-extension over $F_n$. In particular, $F_\infty^{(\ell)}$ is the cyclotomic $\mathbb{Z}_p \times \mathbb{Z}_\ell$-extension over $F$. For an integer $n < \infty$, let $M_n/F_n^{(\ell)}$ be the maximal pro-$\ell$ abelian extension unramified outside $\ell$, and $M_\infty = \bigcup_{n \geq 0} M_n$. Using the above theorem of Washington, Friedman [2] proved the following:

Proposition. *For a real abelian field $F$, we have $M_\infty = M_n F_\infty^{(\ell)}$ for a sufficiently large $n$.*

When $F$ is a real abelian field with $\ell \nmid f_F$ and $\ell \nmid [F : \mathbb{Q}]$, an explicit version of Washington's theorem was obtained by Horie [9, 10, 11]. Namely, he gave an explicit constant $\boldsymbol{m} = \boldsymbol{m}_{F,p,\ell}$ depending on $F$, $p$ and $\ell$ such that the ratio $h_{F_n}/h_{F_{n-1}}$ is not divisible by $\ell$ for all $n > \boldsymbol{m}$. The purpose of this paper is to obtain an explicit version of Friedman's result (under the same assumption on $F$).

Before giving our results, let us introduce some notation. We put $n_0 = \mathrm{ord}_p(\ell^{p-1} - 1)$, where $\mathrm{ord}_p(*)$ is the normalized $p$-adic additive valuation. When $\ell = 2$, let $A_p$ be the number of $p$th roots $\zeta$ of unity such that $\mathrm{Tr}(\zeta) \equiv 0 \bmod 2$, and let $B_p = p - A_p$. Here, Tr is the trace map from $\mathbb{Q}_2(\zeta_p)$ to $\mathbb{Q}_2$, $\mathbb{Q}_2$ being the field of 2-adic rationals. Further, for an integer $k \geq 2$, $\zeta_k$ denotes a primitive $k$th root of unity. We define an integer $\varpi_{p,\ell} \geq 1$ as follows. We set $\varpi_{p,\ell} = 1$ when $\ell$ is a primitive root modulo $p^2$. Otherwise,

2010 *Mathematics Subject Classification*: 11R18, 11R23.
*Key words and phrases*: class group, cyclotomic $\mathbb{Z}_p \times \mathbb{Z}_\ell$-extension.

DOI: 10.4064/aa150-3-4

we put

$$\varpi_{p,\ell} = \begin{cases} (p-1-[p/\ell]) \cdot p^{n_0-1} & \text{if } \ell > 2 \text{ or } n_0 > 1, \\ \min(A_p, B_p) & \text{if } \ell = 2 \text{ and } n_0 = 1. \end{cases}$$

Here, $[x]$ denotes the largest integer $\leq x$. For a real abelian field $F$, let $m = m_F$ be the non-$p$-part of the conductor $f_F$. We put

$$N_{F,p,\ell} = (\ell\phi(m)(p-1)\varpi_{p,\ell})^{\phi(p-1)}$$

where $\phi(*)$ is the Euler function.

THEOREM 1. *Let $F$ be a real abelian field with $\ell \nmid f_F$, $p^2 \nmid f_F$ and $\ell \nmid [F:\mathbb{Q}]$. We have $M_\infty = M_n F_\infty^{(\ell)}$ when $p^{n+1-n_0} > N_{F,p,\ell}$.*

The following is an immediate consequence of Theorem 1.

COROLLARY. *Under the setting of Theorem 1, the ratio $h_{F_n}/h_{F_{n-1}}$ is not divisible by $\ell$ when $p^{n+1-n_0} > N_{F,p,\ell}$.*

When $m = 1$, the assertion of the Corollary was given in [13, Theorem 1(I)]. It was used to show with the help of computer that when $p$ is an odd prime number with $p \leq 509$, the ratio $h_{p^n}/h_p$ is odd for any $n \geq 1$ where $h_{p^n}$ is the class number of $\mathbb{Q}(\zeta_{p^{n+1}})$ ([13, Theorem 2]).

The Corollary is quite similar to an assertion obtained directly from [11, Proposition 3] which is given in a more general setting. (A correction to this proposition is given in [12, p. 823].) Actually, applying [11, Proposition 3] to the setting of the Corollary, we see that $h_{F_n}/h_{F_{n-1}}$ is not divisible by $\ell$ if

$$p^{n+1-n_0} > (\ell(p-1)^3\phi(m)p^{n_0-1})^{\phi(p-1)}.$$

We see that the Corollary is a little sharper than this result. Horie proved [11, Proposition 3] by using (a) some tools in Leopoldt [15], in particular, Leopoldt's algebraic intepretation of the analytic class number formula for a real abelian field and (b) his new idea and technique for a very subtle treatment on cyclotomic units. We show Theorem 1 using Horie's idea and technique and some tools in modern theory of cyclotomic fields, in particular, the structure theorem of local units modulo cyclotomic units and the Iwasawa main conjecture.

REMARK 1. When $p = 3$, Friedman and Sands [3] gave an explicit version of the theorems of Washington and Friedman. Their method depends on the fact that the roots of unity in $\mathbb{Z}_3$, the ring of 3-adic integers, are $\pm 1$. A reason that we excluded the case $p = 2$ is that their method can apply also to this case. The method of Horie [9, 10, 11] and this paper is completely different from theirs.

This paper is organized as follows. In Section 2, we give (1) a "$\Delta$-decomposed version" (Theorem 2) of Theorem 1 in terms of the lambda invariant associated to an $\ell$-adic $L$-function, and (2) another version (Theorem 3) of Theorem 1 in terms of minus class groups. In Section 3, we prove Theorem 2 postponing the proof of a key lemma (Lemma 3). In Section 5, we prove Lemma 3 after preparing several lemmas in Section 4.

## 2. Theorems

**2.1. $\Delta$-decomposed version of Theorem 1.** We denote by $\mathbb{Z}_\ell$ and $\mathbb{Q}_\ell$ the ring of $\ell$-adic integers and the field of $\ell$-adic rationals, respectively, and by $\bar{\mathbb{Q}}_\ell$ a fixed algebraic closure of $\mathbb{Q}_\ell$. Let $G$ be a finite abelian group and $\chi$ a $\bar{\mathbb{Q}}_\ell$-valued character of $G$. Let $X$ be a module over $\mathbb{Z}_\ell[G]$. When $\ell \nmid |G|$, let $X(\chi)$ be the $\chi$-component of $X$. Then we have a canonical decomposition

$$X = \bigoplus_{\chi} X(\chi)$$

where $\chi$ runs over a complete set of representatives of the $\mathbb{Q}_\ell$-conjugacy classes of the $\bar{\mathbb{Q}}_\ell$-valued characters of $G$. Letting $\tilde{X} = X \otimes \mathbb{Q}_\ell$, we denote by $\tilde{X}(\chi)$ the $\chi$-component of the $\mathbb{Q}_\ell[G]$-module $\tilde{X}$. For the definition of the $\chi$-component and some of its properties, see Tsuji [17, Section 2].

Let $F$ be a real abelian field (with $p^2 \nmid f_F$). For a while, we do not assume that $\ell \nmid f_F$ and $\ell \nmid [F : \mathbb{Q}]$. Let $\Delta = \mathrm{Gal}(F/\mathbb{Q})$, and let $\Delta_\ell$ and $\Delta_0$ be the $\ell$-part and the non-$\ell$-part of $\Delta$, respectively. Let $\Gamma_n = \mathrm{Gal}(F_n/F) = \mathrm{Gal}(F_n^{(\ell)}/F_0^\ell)$. We put

$$\mathcal{G}_n = \mathrm{Gal}(M_n/F_n^{(\ell)}) \quad \text{and} \quad \tilde{\mathcal{G}}_n = \mathcal{G}_n \otimes \mathbb{Q}_\ell.$$

It is known that $\mathcal{G}_n$ is a free $\mathbb{Z}_\ell$-module of finite rank. This follows from Iwasawa [14, Theorem 18] and Ferrero and Washington [1, Theorem]. We naturally regard the groups $\mathcal{G}_n$ and $\tilde{\mathcal{G}}_n$ as modules over the groups defined above. To prove Theorem 1, it suffices to show that $\mathcal{G}_n(\psi_n) = \{0\}$ for each $\bar{\mathbb{Q}}_\ell$-valued character of $\Gamma_n$ of order $p^n$ (when $p^{n+1-n_0} > N_{F,p,\ell}$). This is equivalent to the condition $\dim \tilde{\mathcal{G}}_n(\psi_n) = 0$ as $\mathcal{G}_n$ is free over $\mathbb{Z}_\ell$. Here, $\dim(*)$ denotes the dimension over $\mathbb{Q}_\ell$.

Let $\tilde{\ell} = \ell$ or 4 according as $\ell \geq 3$ or $\ell = 2$, and let $\omega_{\tilde{\ell}} : (\mathbb{Z}/\tilde{\ell})^\times \to \mathbb{Z}_\ell^\times$ be the Teichmüller character of conductor $\tilde{\ell}$. For a Dirichlet character $\chi$, we denote by $f_\chi$ the conductor of $\chi$. Let $\chi$ be a nontrivial $\bar{\mathbb{Q}}_\ell$-valued even Dirichlet character such that $\ell^2 \nmid f_\chi$ (resp. $8 \nmid f_\chi$) when $\ell \geq 3$ (resp. $\ell = 2$). Namely, $\chi$ is of the first kind. We denote by $\mathcal{O}_\chi = \mathbb{Z}_\ell[\chi]$ the subring of $\bar{\mathbb{Q}}_\ell$ generated by the values of $\chi$ over $\mathbb{Z}_\ell$, and by $\Omega_\chi$ the field of fractions of $\mathcal{O}_\chi$. Iwasawa constructed a power series $g_\chi(T) \in \mathcal{O}_\chi[[T]]$ associated to the $\ell$-adic $L$-function $L_\ell(s,\chi)$ by

$$g_\chi((1+c_\chi)^s - 1) = \frac{1}{2} L_\ell(s,\chi), \tag{1}$$

where $c_\chi$ is the least common multiple of $\tilde{\ell}$ and the conductor of $\chi$. By [1], $g_\chi(T)$ is not divisible by $\ell$. Let $\lambda_\chi$ be the $\lambda$-invariant of the power series $g_\chi$. We have $\lambda_\chi = 0$ if and only if

$$g_\chi(0) = \frac{1}{2}L_\ell(0,\chi) = -(1-(\chi\omega_{\tilde{\ell}}^{-1})(\ell))\cdot\frac{1}{2}B_{1,\chi\omega_{\tilde{\ell}}^{-1}} \tag{2}$$

is an $\ell$-adic unit. Here, $B_{1,\chi\omega_{\tilde{\ell}}^{-1}}$ is the generalized Bernoulli number.

Let $F$ be again a real abelian field (with $p^2 \nmid f_F$). For $\bar{\mathbb{Q}}_\ell$-valued characters $\varpi$ and $\varphi$ of $\Delta_\ell$ and $\Delta_0$, we regard the character $\chi = \varpi\varphi\psi_n$ of $\mathrm{Gal}(F_n/\mathbb{Q}) = \Delta\times\Gamma_n$ as a primitive Dirichlet character and use the above notation. Then it is known that the Iwasawa main conjecture for the minus class groups (= Mazur and Wiles [16, Theorem] and Wiles [20, Theorem 6.2]) implies

$$\dim\tilde{\mathcal{G}}_n(\psi_n) = \sum_{\varpi,\varphi}[\Omega_{\varpi\varphi\psi_n}:\mathbb{Q}_\ell]\cdot\lambda_{\varpi\varphi\psi_n},$$

where $\varpi$ (resp. $\varphi$) runs over a complete set of representatives of the $\mathbb{Q}_\ell$-conjugacy classes of the $\bar{\mathbb{Q}}_\ell$-valued characters of $\Delta_\ell$ (resp. $\Delta_0$). For this, see Greenberg [6, 7]; [6, Proposition 1] for the case $\ell\ge 3$; and [6, Proposition 2] and some arguments in pp. 42–43 of [7] for the case $\ell = 2$.

*Proof of Proposition.* It follows from [2] that $\lambda_{\varpi\varphi\psi_n} = 0$ for sufficiently large $n$. Hence, we obtain the assertion. ∎

In what follows, unless otherwise stated, we always assume that $\ell\nmid f_F$, $p^2\nmid f_F$ and $\ell\nmid[F:\mathbb{Q}]$. Then the above formula for $\dim\tilde{\mathcal{G}}(\psi_n)$ becomes

$$\dim\tilde{\mathcal{G}}_n(\psi_n) = \sum_{\varphi}[\Omega_{\varphi\psi_n}:\mathbb{Q}_\ell]\cdot\lambda_{\varphi\psi_n}$$

where $\varphi$ runs over a complete set of representatives of the $\mathbb{Q}_\ell$-conjugacy classes of the $\bar{\mathbb{Q}}_\ell$-valued characters of $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. As the invariant $\lambda_{\varphi\psi_n}$ depends only on the characters $\varphi$ and $\psi_n$, we may and will replace the base field $F$ with the real abelian field corresponding to $\varphi$.

Now, let $\varphi$ be a $\bar{\mathbb{Q}}_\ell$-valued even Dirichlet character of order $d = d_\varphi$, $F = F_\varphi$ the real abelian field corresponding to $\varphi$, and $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. We can regard $\varphi$ as an injective homomorphism $\Delta\to\bar{\mathbb{Q}}_\ell^\times$. Let $m = m_\varphi$ be the non-$p$-part of the conductor of $\varphi$. We put

$$N_\varphi = (\ell\phi(m)(p-1)\varpi_{p,\ell})^{\phi(p-1)}.$$

From what we have remarked above, Theorem 1 is an immediate consequence of the following

THEOREM 2. *Under the above setting, assume that $\ell\nmid m$, $\ell\nmid d$ and $p^2\nmid f_\varphi$. Then $\lambda_{\varphi\psi_n} = 0$ for any $\psi_n$ when $p^{n+1-n_0} > N_\varphi$.*

In some cases, the assertion of Theorem 2 holds for a wider class of Dirichlet characters because of the following lemma.

LEMMA 1. *Let $\varphi$ and $\psi_n$ be as in Theorem 2. Let $\varpi$ be a $\bar{\mathbb{Q}}_\ell$-valued even Dirichlet character with $\ell \nmid f_\varpi$ and $p^2 \nmid f_\varpi$ whose order is a power of $\ell$. Assume that the sets of prime numbers dividing the conductors $f_{\varphi\psi_n}$ and $f_{\varpi\varphi\psi_n}$ coincide. Then the condition $\lambda_{\varphi\psi_n} = 0$ implies $\lambda_{\varpi\varphi\psi_n} = 0$.*

*Proof.* We put $\chi = \varphi\psi_n$, $m_1 = f_{\varpi\chi}$ and $m_2 = f_\chi$ for brevity. We see that $m_2$ divides $m_1$ since the order of $\varpi$ is a power of $\ell$ and that of $\chi$ is not divisible by $\ell$. As $m_1$ (resp. $m_2$) is relatively prime to $\ell$, the conductor of $\varpi\chi\omega_{\tilde{\ell}}^{-1}$ (resp. $\chi\omega_{\tilde{\ell}}^{-1}$) is $m_1\tilde{\ell}$ (resp. $m_2\tilde{\ell}$). We have

$$\frac{1}{2}B_{1,\varpi\chi\omega_{\tilde{\ell}}^{-1}} = \frac{1}{2m_1\tilde{\ell}}\sum_{a=1}^{m_1\tilde{\ell}} a \cdot \varpi\chi\omega_{\tilde{\ell}}^{-1}(a), \qquad \frac{1}{2}B_{1,\chi\omega_{\tilde{\ell}}^{-1}} = \frac{1}{2m_1\tilde{\ell}}\sum_{a=1}^{m_1\tilde{\ell}} a \cdot \chi\omega_{\tilde{\ell}}^{-1}(a)$$

where $a$ runs over the integers with $1 \le a \le m_1\tilde{\ell}$ and $(a, m_1\ell) = 1$. The first equality is just the definition, and the second one holds because of $m_2 \mid m_1$ and the assumption on $m_1$ and $m_2$. Since $\varpi\chi\omega_{\tilde{\ell}}^{-1}(\ell) = \chi\omega_{\tilde{\ell}}^{-1}(\ell) = 0$, we see from (2) that it suffices to show

$$\frac{1}{2}B_{1,\varpi\chi\omega_{\tilde{\ell}}^{-1}} \equiv \frac{1}{2}B_{1,\chi\omega_{\tilde{\ell}}^{-1}} \bmod \mathcal{L}$$

where $\mathcal{L}$ is the prime ideal of the $\ell$-adic field $\Omega_{\varpi\chi\omega_{\tilde{\ell}}^{-1}}$. We prove this congruence when $\ell = 2$. For the case $\ell \ge 3$, it is shown similarly. As the characters $\varpi\chi\omega_4^{-1}$ and $\chi\omega_4^{-1}$ are odd, we see that

$$\begin{aligned}(3)\qquad \frac{1}{2}B_{1,\varpi\chi\omega_4^{-1}} &= \frac{1}{8m_1}\Big\{\sum_{a=1}^{2m_1} a \cdot \varpi\chi\omega_4^{-1}(a) - \sum_{a=1}^{2m_1}(4m_1 - a) \cdot \varpi\chi\omega_4^{-1}(a)\Big\} \\ &= \frac{1}{4m_1}\sum_{a=1}^{2m_1} a \cdot \varpi\chi\omega_4^{-1}(a) - \frac{1}{2}\sum_{a=1}^{2m_1} \varpi\chi\omega_4^{-1}(a)\end{aligned}$$

and that

$$(4)\qquad \frac{1}{2}B_{1,\chi\omega_4^{-1}} = \frac{1}{4m_1}\sum_{a=1}^{2m_1} a \cdot \chi\omega_4^{-1}(a) - \frac{1}{2}\sum_{a=1}^{2m_1} \chi\omega_4^{-1}(a).$$

Let $X$ (resp. $Y$) be the difference of the first (resp. second) terms of the right hand sides of (3) and (4). It suffices to show that $X \equiv Y \equiv 0 \bmod \mathcal{L}$. Since the order of $\varpi$ is a power of $\ell = 2$, the prime ideal $\mathcal{L}$ divides $\varpi(a) - 1$. As $a\omega_4^{-1}(a) \equiv 1 \bmod 4$, it follows that

$$a \cdot \varpi\omega_4^{-1}(a) - a \cdot \omega_4^{-1}(a) \equiv \varpi(a) - 1 \bmod 4\mathcal{L}.$$

Now, we see that

$$X \equiv \sum_{a=1}^{2m_1}(\varpi\chi(a) - \chi(a)) \equiv \sum_{a=1}^{2m_1}(\varpi(a) - 1)\chi(a) \equiv 0 \bmod \mathcal{L}.$$

Similarly, we can show $Y \equiv 0 \bmod \mathcal{L}$. ∎

REMARK 2. The assumption in Lemma 1 is satisfied when the conductor of $\varpi$ equals $p$. Therefore, the assertions of Theorems 1 and 2 hold for the real abelian field $F = \mathbb{Q}(\zeta_p)^+$ even if $\ell$ divides $[F : \mathbb{Q}]$.

**2.2. Another version of Theorem 1.** In this subsection, we give another formulation of Theorem 1. Let $F$ be, as before, a real abelian field with $p^2 \nmid f_F$ and $\ell \nmid f_F$. We use the same notation as in Subsection 2.1. We put $L = F(\zeta_{\tilde{\ell}})$ and $L_n = F_n(\zeta_{\tilde{\ell}})$ for $0 \le n \le \infty$, so that $L_\infty/L$ is the cyclotomic $\mathbb{Z}_p$-extension. For an integer $j \ge 0$, denote by $L_{n,j}$ the $j$th layer of the cyclotomic $\mathbb{Z}_\ell$-extension $L_n^{(\ell)}/L_n$. Let $h_{n,j}^-$ be the relative class number of $L_{n,j}$. Let $A_{n,j}$ be the $\ell$-part of the ideal class group of $L_{n,j}$, and let $X_n = \varprojlim A_{n,j}$ be the projective limit of $A_{n,j}$ with respect to the relative norms $L_{n,j+1} \to L_{n,j}$ for $j \ge 0$. The class group $A_{n-1,j}$ is naturally regarded as a subgroup of $A_{n,j}$. Actually, it is a direct summand of $A_{n,j}$ (cf. [19, Lemma 16.15]). Hence, $X_{n-1}$ is also a direct summand of $X_n$. We put

$$B_{n,j} = A_{n,j}/A_{n-1,j} \quad \text{and} \quad Y_n = X_n/X_{n-1} = \varprojlim B_{n,j}.$$

For a while, assume that $\ell \ge 3$. Let $\omega_\ell$ be, as before, the Teichmüller character of conductor $\ell$. We identify $G = \mathrm{Gal}(L/F) = \mathrm{Gal}(L_n/F_n)$ with the multiplicative group $(\mathbb{Z}/\ell)^\times$ through the Galois action on $\zeta_\ell$, and regard $\omega_\ell$ as a character of $G$. We denote by $Y_n(\omega_\ell)$ the $\omega_\ell$-component of the $\mathbb{Z}_\ell[G]$-module $Y_n$. We obtain the following assertion from Theorems 1 and 2.

THEOREM 3. *Let $F$ be a real abelian field with $\ell \nmid f_F$, $p^2 \nmid f_F$ and $\ell \nmid [F : \mathbb{Q}]$. When $p^{n+1-n_0} > N_{F,p,\ell}$, the following assertions hold.*

- (I) *For $\ell \ge 3$, the class group $Y_n(\omega_\ell)$ is trivial, and hence $B_{n,j}(\omega_\ell)$ is trivial for all $j \ge 0$.*
- (II) *For $\ell = 2$, the ratio $h_{n,j}^-/h_{n-1,j}^-$ is odd for all $j \ge 0$.*

*Proof.* First, let $\ell \ge 3$. As in Subsection 2.1, let $\chi = \varphi\psi_n$ be a $\bar{\mathbb{Q}}_\ell$-valued character of $\mathrm{Gal}(F_n/\mathbb{Q}) = \Delta \times \Gamma_n$. Regarding $\omega_\ell\chi^{-1}$ as a character of $\mathrm{Gal}(L_n/\mathbb{Q})$, we denote by $X_n(\omega_\ell\chi^{-1})$ (resp. $Y_n(\omega_\ell\chi^{-1})$) the $\omega_\ell\chi^{-1}$-component of the $\mathrm{Gal}(L_n/\mathbb{Q})$-module $X_n$ (resp. $Y_n$). We easily see that

$$Y_n(\omega_\ell) = \sum_{\varphi,\,\psi_n} Y_n(\omega_\ell(\varphi\psi_n)^{-1}) = \sum_{\varphi,\,\psi_n} X_n(\omega_\ell(\varphi\psi_n)^{-1})$$

where $\varphi$ (resp. $\psi_n$) runs over a complete set of representatives of the $\mathbb{Q}_\ell$-conjugacy classes of the $\bar{\mathbb{Q}}_\ell$-valued characters of $\Delta$ (resp. of $\Gamma_n$ of order $p^n$). It is known that $X_n(\omega_\ell\chi^{-1})$ is a finitely generated free module over $\mathcal{O}_\chi$ (cf. [19, Corollary 13.29]). Let $\lambda_\chi^*$ be the free rank of the $\mathcal{O}_\chi$-module $X_n(\omega_\ell\chi^{-1})$. By the Iwasawa main conjecture, the lambda invariant $\lambda_\chi^*$ equals the invariant $\lambda_\chi$ associated to the power series $g_\chi(T)$. Therefore, we immediately obtain the assertion from Theorems 1 and 2.

Let us deal with the case $\ell = 2$. We see that the unit index of $L_{n,j}$ equals 1 by Hasse [8, Satz 22]. Hence, it follows from the class number formula [19, Theorem 4.17] that

$$h_{n,j}^-/h_{n-1,j}^- = \prod_{\varphi,\psi_n,\theta}\left(-\frac{1}{2}B_{1,\varphi\psi_n\theta\omega}\right)$$

where $\varphi$ (resp. $\psi_n$) runs over the $\bar{\mathbb{Q}}_2$-valued characters of $\Delta$ (resp. of $\Gamma_n$ of order $p^n$), and $\theta$ runs over the $\bar{\mathbb{Q}}_2$-valued even Dirichlet characters of conductor dividing $2^{j+2}$. Further, $\omega = \omega_4$ is the Teichmüller character of conductor 4. Let $\chi = \varphi\psi_n$ and let $g_\chi \in \mathcal{O}_\chi[[T]]$ be the power series defined by (1). By [19, Theorem 7.10], it also satisfies

$$g_\chi(\zeta_\theta(1+c_\chi)^s - 1) = \frac{1}{2}L_2(s, \chi\theta)$$

where $\zeta_\theta$ is a 2-power root of unity associated to $\theta$. By Theorem 2, $g_\chi$ is a unit of $\mathcal{O}_\chi[[T]]$ and hence

$$g_\chi(\zeta_\theta - 1) = \frac{1}{2}L_2(0, \chi\theta) = -\frac{1}{2}B_{1,\varphi\psi_n\theta\omega}$$

is a 2-adic unit. Therefore, we obtain the assertion. ∎

Remark 3. (I) Because of Remark 2 or Lemma 1, the assertion of Theorem 3 holds for $F = \mathbb{Q}(\zeta_p)^+$ even if $\ell$ divides $[F:\mathbb{Q}]$.

(II) When $F = \mathbb{Q}(\zeta_p)^+$, a weaker version of Theorem 3 was given in [13, Theorem 3].

**3. Proof of Theorem 2.** In what follows, we fix characters $\varphi$ and $\psi_n$ in Theorem 2, and use the same notation as in Theorem 2. For brevity, we write

$$\chi = \varphi\psi_n.$$

Let $e_\varphi$ and $e_{\psi_n}$ be the idempotents of $\mathbb{Z}_\ell[\Delta]$ and $\mathbb{Z}_\ell[\Gamma_n]$ corresponding to $\varphi$ and $\psi_n$, respectively:

$$e_\varphi = \frac{1}{d}\sum_{\delta\in\Delta} \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi(\delta)^{-1})\delta,$$

$$e_{\psi_n} = \frac{1}{p^n}\sum_{\gamma\in\Gamma_n} \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_{p^n})/\mathbb{Q}_\ell}(\psi_n(\gamma)^{-1})\gamma.$$

Choose $\tilde{e}_\varphi \in \mathbb{Z}[\Delta]$ and $\tilde{e}_{\psi_n} \in \mathbb{Z}[\Gamma_n]$ congruent to $e_\varphi$ and $e_{\psi_n}$ modulo $\ell$, respectively. For $n \geq 0$, let $K_n = \mathbb{Q}(\zeta_m, \zeta_{p^{n+1}})$, and $K_n^+$ its maximal real subfield. We have $F_n \subseteq K_n^+$ because the conductor of $F_n$ is $mp^{n+1}$ when $n \geq 1$ and it is $m$ or $mp$ when $n = 0$. We put $t = 1 + p^n$ and

$$c_n = \zeta_{p^{n+1}}^{(t-1)/2} \frac{\zeta_m \zeta_{p^{n+1}} - 1}{\zeta_m \zeta_{p^{n+1}}^t - 1}.$$

The element $c_n$ is a cyclotomic unit of $K_n^+$. We define a cyclotomic unit $\epsilon_n$ of $F_n$ by

$$\epsilon_n = N_{K_n^+/F_n}(c_n).$$

The Galois group $\mathrm{Gal}(K_n/K_{n-1}) = \mathrm{Gal}(K_n^+/K_{n-1}^+)$ is generated by the automorphism sending $\zeta_{p^{n+1}}$ to $\zeta_{p^{n+1}}^t$. Hence, we see that

$$N_{n,n-1}(\epsilon_n) = 1 \tag{5}$$

where $N_{n,n-1}$ is the norm map from $F_n$ to $F_{n-1}$. We put

$$\eta_n = \epsilon_n^{\tilde{e}_\varphi \tilde{e}_{\psi_n}}.$$

We denote by $\mathcal{F}$ the Frobenius automorphism of $F_n$ at $\ell$.

Lemma 2. *Assume that $n \geq n_0 + \mathrm{ord}_p(d)$. If $\lambda_\chi > 0$, then $\eta_n^{\mathcal{F}} \equiv \eta_n^\ell \bmod \ell^2$.*

*Proof.* Let $\mathcal{U}_n$ be the group of semi-local units of $F_n$ at $\ell$. Let $C_n$ be the group of cyclotomic units of $F_n$ defined in Gillard [4, §2.3], and let $\mathcal{C}_n$ be the topological closure of $C_n \cap \mathcal{U}_n$ in $\mathcal{U}_n$. Let

$$\eta_n' = \epsilon_n^{e_\varphi e_{\psi_n}} \in \mathcal{C}_n(\chi).$$

For a $\bar{\mathbb{Q}}_\ell$-valued character $\theta$ of $\mathrm{Gal}(F_n/\mathbb{Q})$, the structure of the $\theta$-component $\mathcal{C}_n(\theta)$ is slightly complicated when $\theta(\ell) = 1$ or $\theta\omega_{\tilde{\ell}}^{-1}(\ell) = 1$. However, $\chi(\ell) = \varphi(\ell)\psi_n(\ell) \neq 1$ because $\psi_n(\ell)$ is a primitive $p^{n+1-n_0}$th root of unity and $n + 1 - n_0 > \mathrm{ord}_p(d)$ by assumption. Further, $\chi\omega_{\tilde{\ell}}^{-1}(\ell) = 0$ as $\ell \nmid f_\chi$. The $\chi$-part $\mathcal{U}_n(\chi)$ is a free $\mathcal{O}_\chi$-module of rank 1. By the theorem of Gillard [5, Theorem 2] on semi-local units modulo cyclotomic units, we see that $(\mathcal{U}_n/\mathcal{C}_n)(\chi)$ is isomorphic to $\mathcal{O}_\chi/g_\chi(c_\chi)$ as $\mathcal{O}_\chi$-modules, where $g_\chi$ is the power series defined by (1). Since the order $dp^{n+1}$ of $\chi = \varphi\psi_n$ is relatively prime to $\ell$, the extension $\Omega_\chi/\mathbb{Q}_\ell$ is unramified. It follows that the ideal $g_\chi(c_\chi)\mathcal{O}_\chi$ equals $\ell^e\mathcal{O}_\chi$ for some nonnegative integer $e$. Assume that $\lambda_\chi > 0$. Then, as $g_\chi$ is not a unit, it follows that $g_\chi(c_\chi)\mathcal{O}_\chi \subseteq \ell\mathcal{O}_\chi$. Therefore, $\eta_n'$ is an $\ell$th power in $\mathcal{U}_n$, and hence $\eta_n \equiv v^\ell \bmod \ell^2$ for some $v \in F_n$. As $F_n/\mathbb{Q}$ is unramified at $\ell$, $v^{\mathcal{F}} \equiv v^\ell \bmod \ell$. Therefore, we see that

$$\eta_n^{\mathcal{F}} \equiv (v^{\mathcal{F}})^\ell \equiv v^{\ell^2} \equiv \eta_n^\ell \bmod \ell^2. \ \blacksquare$$

The following key lemma is shown in Section 5.

Lemma 3. *If $p^{n+1-n_0} > N_\varphi$, then $\eta_n^{\mathcal{F}} \not\equiv \eta_n^\ell \bmod \ell^2$.*

*Proof of Theorem 2.* As $d$ is a divisor of $\phi(mp)$, the condition $p^{n+1-n_0} > N_\varphi$ implies $n \geq n_0 + \mathrm{ord}_p(d)$. Hence, we obtain Theorem 2 immediately from Lemmas 2 and 3. ∎

## 4. Lemmas

**4.1. Lemmas.** In this section, we prepare several lemmas which are necessary to prove Lemma 3.

LEMMA 4. *Let $q_i$ $(1 \leq i \leq s)$ be distinct prime numbers with $q_i \neq \ell$. Let $k = \prod_i q_i^{e_i}$ and $k_0 = \prod_i q_i^{f_i}$ with $e_i > f_i \geq 1$. Let $N$ be a number field unramified at each $q_i$. Let $A$ be a finite subset of $\mathbb{Z}$, and for $u \in \mathbb{Z}$, let $A_u$ consist of integers $a \in A$ with $a \equiv u \bmod k_0$. Let $\kappa : A \to \mathcal{O}_N$ be an arbitrary map where $\mathcal{O}_N$ is the ring of integers of $N$. Then the condition $\sum_{a\in A} \kappa(a)\zeta_k^a \equiv 0 \bmod \ell$ implies $\sum_{a\in A_u} \kappa(a)\zeta_k^a \equiv 0 \bmod \ell$.*

*Proof.* Let $L = N(\zeta_k)$ and $L_0 = N(\zeta_{k/k_0})$. As $N$ is unramified at each $q_i$, the degree $[L : L_0]$ equals $k_0$, and hence it is not divisible by $\ell$. Further, for a $k$th root $\zeta$ of unity, $\mathrm{Tr}_{L/L_0}(\zeta) = [L : L_0]\zeta$ or $0$ according as $\zeta^{k/k_0} = 1$ or not. Assume that $X = \sum_{a\in A} \kappa(a)\zeta_k^a \equiv 0 \bmod \ell$. Then, taking the trace of $\zeta_k^{-u}X$ to $L_0$, we see from the above remark that

$$[L : L_0] \cdot \sum_{a\in A_u} \kappa(a)\zeta_k^{a-u} \equiv 0 \bmod \ell.$$

The assertion follows since $\ell \nmid [L : L_0]$. ∎

As in Horie [9, 10], we choose a complete set $\mathcal{V}$ of representatives of the quotient $\mu_{p-1}/\{\pm1\}$ as follows, where $\mu_{p-1}$ is the group of $(p-1)$st roots of unity in the complex number field $\mathbb{C}$. Write $(p-1)/2 = m_1 \cdots m_s$ where $m_i$ is a power of a prime number with $(m_i, m_j) = 1$ for $i \neq j$. We put

$$\mathcal{V} = \left\{ \exp\left( \left( \frac{c_1}{m_1} + \cdots + \frac{c_s}{m_s} \right) \pi\sqrt{-1} \right) \;\middle|\; 0 \leq c_i \leq m_i - 1 \ (1 \leq i \leq s) \right\}.$$

The following assertion was shown in [9, Lemma 7].

LEMMA 5. *Let $z : \mathcal{V} \to \mathbb{Z}$ be a map such that $z(\nu) \geq 0$ for all $\nu \in \mathcal{V}\backslash\{1\}$. If $\sum_{\nu\in\mathcal{V}} z(\nu)\nu = 0$, then $z(\nu) = 0$ for all $\nu \in \mathcal{V}$.*

We fix an integer $n \geq 2n_0 - 1$ and a prime ideal $\wp$ of $\mathbb{Q}(\mu_{p-1})$ over $p$. Let $\mathcal{I}$ be the set of integers $u$ with $1 \leq u \leq p^{n+1} - 1$ satisfying $u^{p-1} \equiv 1 \bmod p^{n+1}$ and $u \equiv \nu \bmod \wp^{n+1}$ for some $\nu \in \mathcal{V}$. Then we have a bijection

$$\omega_\wp : \mathcal{I} \to \mathcal{V}$$

sending $u \in \mathcal{I}$ to $\nu \in \mathcal{V}$ with $\nu \equiv u \bmod \wp^{n+1}$.

In the following, we rewrite the expression $\eta_n = \epsilon_n^{\tilde{e}_\varphi \tilde{e}_{\psi_n}}$ into a more convenient form and show some lemmas which are necessary to prove the key lemma. We abbreviate

$$\zeta_0 = \zeta_m \quad \text{and} \quad \zeta = \zeta_{p^{n+1}}$$

in this subsection (and Section 5). We naturally identify $\Gamma_n$ with $\mathrm{Gal}(K_n/K_0) = \mathrm{Gal}(K_n^+/K_0^+)$.

By (5), we can replace $\tilde{e}_{\psi_n}$ with $\tilde{e}'_{\psi_n} = \tilde{e}_{\psi_n} - \alpha N_{n,n-1}$ for any $\alpha \in \mathbb{Z}[\Gamma_n]$. The integer $n_0 = \mathrm{ord}_p(\ell^{p-1} - 1)$ is the largest integer such that $\mathbb{Q}_\ell(\zeta_p) = \mathbb{Q}_\ell(\zeta_{p^{n_0}})$. For $\gamma \in \Gamma_n$, the trace of $\psi_n(\gamma)^{-1}$ to $\mathbb{Q}_\ell(\zeta_p)$ equals $p^{n-n_0}\psi_n(\gamma)^{-1}$ or 0 according as $\gamma^{p^{n_0}} = 1$ or not. For $a \in \mathbb{Z}$ with $a \equiv 1 \bmod p$, let $\gamma_a$ be the automorphism in $\Gamma_n$ such that $\zeta^{\gamma_a} = \zeta^a$ (and $\zeta_0^{\gamma_a} = \zeta_0$). For an integer $j$, we put

$$s_j = 1 + jp^{n+1-n_0}.$$

From the definition of $e_{\psi_n}$ and the above remark, we can write

$$e_{\psi_n} = \frac{1}{p^{n_0}} \sum_{j=0}^{p^{n_0}-1} \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_p)/\mathbb{Q}_\ell}(\psi_n(s_j)^{-1})\gamma_{s_j} \in \mathbb{Z}_\ell[\Gamma_n^{p^{n-n_0}}].$$

As in [13], we fix $\alpha \in \mathbb{Z}[\Gamma_n^{p^{n-n_0}}]$ so that the number of non-zero terms of $e_{\psi_n} - \alpha N_{n,n-1} \bmod \ell$ is minimal. Let $J_{\psi_n}$ be the set of integers $j$ with $0 \le j \le p^{n_0} - 1$ such that the coefficient $a_j$ of $\gamma_{s_j}$ in $e_{\psi_n} - \alpha N_{n,n-1} \bmod \ell$ is non-zero. Then

$$e_{\psi_n} - \alpha N_{n,n-1} \equiv \sum_{j \in J_{\psi_n}} a_j \gamma_{s_j} \bmod \ell \tag{6}$$

and we obtain the following

Lemma 6. *Under the above notation, we have*

$$\epsilon_n^{\tilde{e}_{\psi_n}} = \epsilon^\ell \prod_{j \in J_{\psi_n}} \epsilon_n^{a_j \gamma_{s_j}}$$

*for some unit $\epsilon$ of $K_n$.*

For the cardinality $|J_{\psi_n}|$, we showed in [13, Lemma 8] that

$$|J_{\psi_n}| \le \varpi_{p,\ell}. \tag{7}$$

Let $\zeta_{p^{n_0}} = \psi_n(1 + p^{n+1-n_0})$ be a primitive $p^{n_0}$th root of unity in $\bar{\mathbb{Q}}_\ell$. Using the congruence (6), we showed the following in [13, Lemma 9].

Lemma 7. *Under the above notation, we have*

$$\sum_{j \in J_{\psi_n}} a_j \zeta_{p^{n_0}}^j \in \mathbb{Z}_\ell[\zeta_{p^{n_0}}]^\times$$

*when $n \ge 2n_0 - 1$.*

Denote by $\mathbb{B}_n$ the subfield of $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_{p^{n+1}})$ with $[\mathbb{B}_n : \mathbb{Q}] = p^n$. In other words, $\mathbb{B}_n$ is the real abelian field associated to $\psi_n$. Let $D =$

$\mathrm{Gal}(K_n^+/\mathbb{B}_n)$, $D_1 = \mathrm{Gal}(K_n^+/\mathbb{B}_n(\zeta)^+)$ and $\tilde{D} = \mathrm{Gal}(K_n/\mathbb{B}_n)$. We can naturally regard $\Delta = \mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(F_n/\mathbb{B}_n)$ as a quotient of $D$, and hence $\varphi$ as a character of $D$. The operator $e_\varphi N_{K_n^+/F_n}$ in $\mathbb{Z}_\ell[D]$ can be written in the form

$$e_\varphi N_{K_n^+/F_n} \equiv \sum_{\delta \in D} b_\delta \delta \bmod \ell$$

for some integers $b_\delta \in \mathbb{Z}$ satisfying

$$b_\delta \equiv \frac{1}{d} \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi(\delta)^{-1}) \bmod \ell.$$

For each $\delta \in D$, there exists a unique $\tilde{\delta} \in \tilde{D}$ such that $\tilde{\delta}_{|K_n^+} = \delta$ and $\zeta^{\tilde{\delta}} = \zeta^{u'_\delta}$ for some $u'_\delta \in \mathcal{I}$. Let $u''_\delta$ be an integer (defined modulo $m$) such that $\zeta_0^{\tilde{\delta}} = \zeta_0^{u''_\delta}$. We denote by $u_\delta$ the unique integer with $1 \le u_\delta < mp^{n+1}$ satisfying $u_\delta \equiv u'_\delta \bmod p^{n+1}$ and $u_\delta \equiv u''_\delta \bmod m$. We put

$$I = I_\varphi = \{u_\delta \mid \delta \in D\} \quad \text{and} \quad I_1 = \{u \in I \mid u \equiv 1 \bmod p^{n+1}\}.$$

There is a natural bijection between $I$ (resp. $I_1$) and $D$ (resp. $D_1$). For an integer $v$ with $(v, mp) = 1$ and $v^{p-1} \equiv 1 \bmod p^{n+1}$, there exists a unique $u = u_\delta \in I$ such that $v \equiv \pm u \bmod mp^{n+1}$. We put $b_v = b_\delta$. Let $\delta_0$ be an arbitrary element of $D$, and $u_0 = u_{\delta_0}$. We easily see that

$$\delta_0^{-1} e_\varphi N_{K_n^+/F_n} \equiv \sum_{\delta \in D} b_{\delta\delta_0} \delta \bmod \ell.$$

Hence, under the above notation, we see from Lemma 6 that

$$\eta_n^{\delta_0^{-1}} = \epsilon_1 \epsilon_2^\ell \cdot \xi_{n,u_0}$$

with

$$\xi_{n,u_0} = \prod_{j \in J_{\psi_n}} \prod_{\delta \in D} \left( \frac{\zeta_0^{\tilde{\delta}} \zeta^{\tilde{\delta} s_j} - 1}{\zeta_0^{\tilde{\delta}} \zeta^{\tilde{\delta} t s_j} - 1} \right)^{a_j b_{\delta_0 \delta}} = \prod_{j \in J_{\psi_n}} \prod_{u \in I_\varphi} \left( \frac{\zeta_0^u \zeta^{u s_j} - 1}{\zeta_0^u \zeta^{t u s_j} - 1} \right)^{a_j b_{u_0 u}}.$$

Here, $\epsilon_1$ is a $p$th root of unity and $\epsilon_2$ is a unit of $K_n$. For brevity, we put

$$\xi_n = \xi_{n,1}.$$

Then we see that Lemma 3 (the key lemma) is equivalent to the following assertion because $\epsilon_1^{\mathcal{F}} = \epsilon_1^\ell$ and $(\epsilon_2^\ell)^{\mathcal{F}} \equiv \epsilon_2^{\ell^2} \bmod \ell^2$ where $\mathcal{F}$ is the Frobenius automorphism of $K_n$ over $\ell$.

Lemma 8. *Under the above notation, $\xi_n^{\mathcal{F}} \not\equiv \xi_n^\ell \bmod \ell^2$ when $p^{n+1-n_0} > N_\varphi$.*

Remark 4. The condition $\xi_n^{\mathcal{F}} \not\equiv \xi_n^\ell \bmod \ell^2$ in Lemma 8 is invariant under the Galois action. Hence, it is equivalent to $\xi_{n,u_0}^{\mathcal{F}} \not\equiv \xi_{n,u_0}^\ell \bmod \ell^2$ for any $u_0 \in I$.

Lemma 7 and the following lemma play an important role in the proof of Lemma 8.

LEMMA 9. *For some integer $u_0 \in I$, we have*

$$\sum_{u \in I_1} b_{u_0 u} \zeta_0^u \not\equiv 0 \bmod \ell$$

*in* $\mathbb{Q}(\zeta_0)$.

The assertion of Lemma 9 is equivalent to saying that the conclusion in Lemma 9 holds for some $u_0$ and some primitive $m$th root $\zeta_0$ of unity in the $\ell$-adic field $\mathbb{Q}_\ell(\zeta_0)$. So, in what follows, we mainly work $\ell$-adically.

For integers $k \geq 1$ and $u$, we denote by $[u] = [u]_k$ the class in $\mathbb{Z}/k = \mathbb{Z}/k\mathbb{Z}$ containing $u$. We can naturally identify the Galois group $D$ with $(\mathbb{Z}/mp)^\times/\langle J \rangle$ where $J = [-1]$. Under this identification, we have

$$D_1 = \{[u]_{mp} \mid u \equiv 1 \bmod p\}\langle J \rangle/\langle J \rangle.$$

Though the sets $I$ and $I_1$ defined above depend on $n$, we see that the maps

$$I \to D = (\mathbb{Z}/mp)^\times/\langle J \rangle \quad \text{and} \quad I_1 \to D_1$$

sending an integer $u$ to the class $\bar{u} = [u]_{mp} \bmod \langle J \rangle$ are bijective. Since the value $b_u$ depends only on the class $\bar{u}$, Lemma 9 can be rewritten in the following form:

LEMMA 10. *Let $m$ be an integer with $(m, p\ell) = 1$. Let $\varphi$ be an even Dirichlet character defined modulo $mp$. Assume that the non-$p$-part of the conductor of $\varphi$ equals $m$, and the order $d$ of $\varphi$ is relatively prime to $\ell$. Then*

$$\sum_{u \in D_1} \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi(u_0 u)^{-1})\zeta_m^u \not\equiv 0 \bmod \ell$$

*for some integer $u_0$ with $(u_0, mp) = 1$ and some primitive $m$th root $\zeta_m$ of unity. Here, $u$ runs over the integers with $1 \leq u \leq mp-1$ and $u \equiv 1 \bmod p$.*

**4.2. Proof of Lemma 10.** We begin with the following simple lemma. For an integer $k \geq 2$, let $\mu_k$ be the group of $k$th roots of unity in $\bar{\mathbb{Q}}_\ell$.

LEMMA 11. *Let $m$ be an integer and $X$ a subset of $\mathbb{Z}/m$. Let $d_1$ and $d_2$ be integers with $\ell \nmid d_2$, and $d$ the least common multiple of $d_1$ and $d_2$. Let $X \to \mu_{d_1}$, $[x] \mapsto \epsilon_x$, be an arbitrary map. Let $\zeta_m$ be a fixed primitive $m$th root of unity in $\bar{\mathbb{Q}}_\ell$. Assume that for every $\epsilon \in \mu_{d_2}$,*

$$\sum_{x \in X} \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\epsilon\epsilon_x)\zeta_m^x \equiv 0 \bmod \ell$$

*where $x$ runs over the integers with $0 \leq x \leq m-1$ and $[x] \in X$. Then*

$$\sum_{x \in X} \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_{d_1})/\mathbb{Q}_\ell}(\epsilon_x)\zeta_m^x \equiv 0 \bmod \ell.$$

*Proof.* Let $\Omega' = \mathbb{Q}_\ell(\zeta_d)$ and $\Omega = \mathbb{Q}_\ell(\zeta_{d_1})$. As $d$ is the least common multiple, we see that $\Omega' = \Omega(\zeta_{d_2})$. Let $\Omega_0' = \mathbb{Q}_\ell(\zeta_{d_2})$ and $\Omega_0 = \Omega_0' \cap \Omega$. As $\ell \nmid d_2$, the extension $\Omega_0'/\Omega_0$ is tame and hence $\mathrm{Tr}_{\Omega_0'/\Omega_0}(\mathcal{O}_{\Omega_0'}) = \mathcal{O}_{\Omega_0}$ where

$\mathcal{O}_{\Omega_0'}$ and $\mathcal{O}_{\Omega_0}$ are the rings of integers of $\Omega_0'$ and $\Omega_0$, respectively. Then, since $\mathcal{O}_{\Omega_0'} = \mathbb{Z}_\ell[\zeta_{d_2}]$, there exists an element

$$\alpha = \sum_{\epsilon \in \mu_{d_2}} a_\epsilon \epsilon \in \mathcal{O}_{\Omega_0'}$$

with $a_\epsilon \in \mathbb{Z}_\ell$ such that $\mathrm{Tr}_{\Omega_0'/\Omega_0}(\alpha) = \mathrm{Tr}_{\Omega'/\Omega}(\alpha) = 1$. Therefore, we see that

$$\mathrm{Tr}_{\Omega/\mathbb{Q}_\ell}(\epsilon_x) = \mathrm{Tr}_{\Omega/\mathbb{Q}_\ell}(\epsilon_x \,\mathrm{Tr}_{\Omega'/\Omega}(\alpha)) = \sum_{\epsilon \in \mu_{d_2}} a_\epsilon \,\mathrm{Tr}_{\Omega'/\mathbb{Q}_\ell}(\epsilon \epsilon_x).$$

From this, we obtain the assertion. ∎

Let $m$, $\varphi$ and $d$ be as in Lemma 10. Choose an integer $p^*$ such that $pp^* \equiv 1 \bmod m$. For an integer $v$ with $(v, m) = 1$, we put $v' = 1 + pp^*(v-1)$. Then we have an isomorphism $\iota : (\mathbb{Z}/m\mathbb{Z})^\times \to D_1$ by sending the class $[v]_m$ to $[v']_{mp} \bmod \langle J \rangle \in D_1$. Let $\varphi_1 = \varphi \circ \iota$. We easily see that the conductor of the Dirichlet character $\varphi_1$ equals $m$ from the assumption on the conductor of $\varphi$. Clearly, the order $d_1$ of $\varphi_1$ divides $d$.

To show Lemma 10, assume to the contrary that

$$\sum_{u \in D_1} b_{u_0 u} \zeta_m^u = \sum_v b_{u_0 v'} \zeta_m^{v'} \equiv 0 \bmod \ell$$

for all $u_0$ and all $\zeta_m$. Here, in the second sum, $v$ runs over the integers with $1 \le v \le m-1$ and $(v, m) = 1$. For each $[v] \in (\mathbb{Z}/m\mathbb{Z})^\times$, we have

$$b_{u_0 v'} = \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi_1(v)^{-1} \varphi(u_0)^{-1}),$$

and

$$\zeta_m^{v'} = \zeta_m^{1+pp^*(v-1)} = \zeta_m^v$$

as $pp^* \equiv 1 \bmod m$. As $u_0$ varies, the value $\varphi(u_0)^{-1}$ runs over all $d$th roots of unity. Hence, we see by Lemma 11 (with $d_2 = d$) that

$$\sum_v b_v \zeta_m^v \equiv 0 \bmod \ell \quad \text{with} \quad b_v = \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_{d_1})/\mathbb{Q}_\ell}(\varphi_1(v)^{-1})$$

where $v$ runs over the integers with $1 \le v \le m-1$ and $(v, m) = 1$.

From the above observation, we see that to show Lemma 10, it suffices to prove the following lemma. In the rest of this subsection, we change the notation a little. Let $m$ be an integer with $(m, p\ell) = 1$, and let $\varphi$ be a Dirichlet character of conductor $m$ and order $d$ with $(d, \ell) = 1$.

LEMMA 12. *Under the above setting, we have*

$$\sum_u \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi(u)^{-1}) \zeta_m^u \not\equiv 0 \bmod \ell$$

*for some primitive $m$th root $\zeta_m$ of unity in $\bar{\mathbb{Q}}_\ell$, where $u$ runs over the integers with $1 \le u \le m-1$ and $(u, m) = 1$.*

*Proof.* First, let $m = q_1^{e_1} \cdots q_r^{e_r}$ where $q_1, \ldots, q_r$ are distinct prime numbers and $e_i \geq 2$ $(1 \leq i \leq r)$. Let $m_0 = q_1 \cdots q_r$ and $m' = m/m_0$. As the conductor of $\varphi$ is $m$, we have $m_0 \mid d$. Assume that the following congruence holds for all $\zeta_m$:

$$X = \sum_u \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi(u)^{-1})\zeta_m^u \equiv 0 \bmod \ell. \tag{8}$$

Let $a$ be an integer with $(a, m) = 1$. By Lemma 4, we have

$$\sum_{u \equiv a} \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi(u)^{-1})\zeta_m^u \equiv 0 \bmod \ell$$

where $u$ runs over the integers with $1 \leq u \leq m-1$ and $u \equiv a \bmod m'$. For an integer $u$ with $u \equiv a \bmod m'$, we can write $u \equiv a(1 + bm') \bmod m$ for some $b$ with $0 \leq b \leq m_0 - 1$. Therefore,

$$\sum_{b=0}^{m_0-1} \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi(a)^{-1}\varphi(1+bm')^{-1})\zeta_{m_0}^b \equiv 0 \bmod \ell.$$

Here, $\zeta_{m_0} = \zeta_m^{am'}$. We see that $\varphi(1 + m')$ is a primitive $m_0$th root of unity and $\varphi(1+bm') = \varphi(1+m')^b$ since $\varphi$ is of conductor $m$ and $e_i \geq 2$ $(1 \leq i \leq r)$. As $\varphi(a)$ runs over all $d$th roots of unity, we obtain from Lemma 11 (with $d_1 = m_0$ and $d_2 = d$)

$$Y = \sum_{b=0}^{m_0-1} \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_{m_0})/\mathbb{Q}_\ell}(\varphi(1+bm')^{-1})\zeta_{m_0}^b \equiv 0 \bmod \ell.$$

This congruence holds for any primitive $m_0$th root $\zeta_{m_0}$ of unity because (8) holds for all $\zeta_m$. We choose $\zeta_{m_0} = \varphi(1 + m')$. Then, since the mapping $[b]_m \mapsto \varphi(1 + bm')$ is a character of the additive group $\mathbb{Z}/m_0$, we see that $Y = m_0$ by orthogonality of characters. As $\ell \nmid m$, this is impossible.

Next, write $m = m_1 m_2$ with $(m_1, m_2) = 1$ and assume that $m_2$ is square free and that $m_1 = 1$ or $m_1 = q_1^{e_1} \cdots q_r^{e_r}$ where $q_1, \ldots, q_r$ are distinct prime numbers and $e_i \geq 2$ $(1 \leq i \leq r)$. Let $m_2^*$ (resp. $m_1^*$) be an integer satisfying $m_2 m_2^* \equiv 1 \bmod m_1$ (resp. $m_1 m_1^* \equiv 1 \bmod m_2$). For integers $x$ and $y$, we put

$$x' = 1 + m_2 m_2^*(x-1) \quad \text{and} \quad y'' = 1 + m_1 m_1^*(y-1).$$

Then the mappings

$$\iota_1 : (\mathbb{Z}/m_1)^\times \to (\mathbb{Z}/m)^\times, \qquad [x]_{m_1} \mapsto [x']_m,$$

and

$$\iota_2 : (\mathbb{Z}/m_2)^\times \to (\mathbb{Z}/m)^\times, \qquad [y]_{m_2} \mapsto [y'']_m,$$

are injective, and $(\mathbb{Z}/m)^\times$ is the direct product of the images of $\iota_1$ and $\iota_2$. Let $\varphi_i = \varphi \circ \iota_i$ and $d_i$ be the order of $\varphi_i$ with $i = 1, 2$. Then the order $d$ of $\varphi$ equals the least common multiple of $d_1$ and $d_2$. Writing $\zeta_m = \zeta_{m_1}\zeta_{m_2}$ for some primitive $m_i$th root $\zeta_{m_i}$ of unity $(i = 1, 2)$, we easily see that

$\zeta_m^{x'y''} = \zeta_{m_1}^x \zeta_{m_2}^y$. Now assume that the congruence (8) holds for all $\zeta_m$ under this setting. Then, since the elements of $(\mathbb{Z}/m)^\times$ are written in the form $[x'y'']_m$, we obtain the following congruence for all $\zeta_{m_1}$ and $\zeta_{m_2}$:

$$\sum_y \Big( \sum_x \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi_1(x)^{-1}\varphi_2(y)^{-1})\zeta_{m_1}^x \Big) \zeta_{m_2}^y \equiv 0 \bmod \ell.$$

Here, $x$ (resp. $y$) runs over the integers with $1 \le x \le m_1 - 1$ (resp. $1 \le y \le m_2 - 1$) relatively prime to $m_1$ (resp. $m_2$). Choose $a_{x,y} \in \mathbb{Z}$ congruent to $\mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi_1(x)^{-1}\varphi_2(y)^{-1})$ modulo $\ell$. Since the above congruence holds for all $\zeta_{m_1}$ and $\zeta_{m_2}$, we obtain a congruence

$$\sum_y \Big( \sum_x a_{x,y} \zeta_{m_1}^x \Big) \zeta_{m_2}^y \equiv 0 \bmod \ell$$

in the global field $\mathbb{Q}(\zeta_m)$. Let $N = \mathbb{Q}(\zeta_{m_1})$ and $N' = N(\zeta_{m_2})$. Since $m_2$ is square free and $(m_1, m_2) = 1$, we see that the Galois extension $N'/N$ has a normal integral basis (NIB) and that $\zeta_{m_2}$ is a generator of NIB. As $\ell$ is unramified at $N$, it follows that

$$\sum_x a_{x,y} \zeta_{m_1}^x \equiv 0 \bmod \ell$$

for all $y$. Hence, in the $\ell$-adic field $\mathbb{Q}_\ell(\zeta_{m_1})$, we obtain

$$\sum_x \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_d)/\mathbb{Q}_\ell}(\varphi_1(x)^{-1}\varphi_2(y)^{-1})\zeta_{m_1}^x \equiv 0 \bmod \ell$$

for all $y$ and all $\zeta_{m_1}$. As $\varphi_2(y)$ runs over all $d_2$th roots of unity, Lemma 11 yields

$$\sum_x \mathrm{Tr}_{\mathbb{Q}_\ell(\zeta_{d_1})/\mathbb{Q}_\ell}(\varphi_1(x)^{-1})\zeta_{m_1}^x \equiv 0 \bmod \ell.$$

When $m_1 = 1$, this is clearly impossible. When $m_1 > 1$, we have already shown that this congruence does not hold. ∎

**5. Proof of Lemma 8.** We use the same notation as in the previous sections. In particular, $n \ge 1$ is a fixed integer, and $\zeta_0$ (resp. $\zeta$) is a primitive $m$th (resp. $p^{n+1}$st) root of unity. We write $I = I_\varphi$ and $J = J_{\psi_n}$ for brevity. Let $\varPhi$ be the set of maps $z$ from $\mathcal{V}$ to $\{0, 1, \ldots, 2\ell\phi(m)|J|\}$. We put

$$M_\chi = \max_{z \in \varPhi} \Big\{ \Big| N\Big( \sum_{\nu \in \mathcal{V}} z(\nu)\nu - 1 \Big) \Big| \Big\}$$

where $N$ is the norm map from $\mathbb{Q}(\zeta_{p-1})$ to $\mathbb{Q}$. We see from (7) that $M_\chi \le N_\varphi$ because

$$\Big| \sum_{\nu \in \mathcal{V}} z(\nu)\nu - 1 \Big| \le 2\ell\phi(m)|J| \cdot |\mathcal{V}| = \ell\phi(m)(p-1)|J|$$

for each embedding $\mathbb{Q}(\zeta_{p-1}) \hookrightarrow \mathbb{C}$.

We easily see that $N_\varphi > p^{n_0}$. Hence, the condition $n \geq 2n_0 - 1$ in Lemma 7 is satisfied when $p^{n+1-n_0} > N_\varphi$. Therefore, as $N_\varphi > M_\chi$, it suffices to derive a contradiction assuming that $p^{n+1-n_0} > M_\chi$, $n \geq 2n_0 - 1$ and $\xi_n^{\mathcal{F}} \equiv \xi_n^{\ell} \bmod \ell^2$. We prove Lemma 8 using an argument in [10, 11, 13]. We fix an arbitrary integer $u_0 \in I$. By Remark 4, the assumption $\xi_n^{\mathcal{F}} \equiv \xi_n^{\ell} \bmod \ell^2$ is equivalent to $\xi_{n,u_0}^{\mathcal{F}} \equiv \xi_{n,u_0}^{\ell} \bmod \ell^2$. For $j \in J$ and $u \in I$, let $c_{j,u}$ be the integer such that $0 \leq c_{j,u} \leq \ell - 1$ and $c_{j,u} \equiv a_j b_{uu_0} \bmod \ell$. We put

$$G(T) = \frac{1}{\ell}((T-1)^\ell - (T^\ell - 1)) \in \mathbb{Z}[T].$$

Then we easily see that

$$\begin{aligned} (T-1)^{b\ell} &= ((T-1)^\ell)^b = (T^\ell - 1 + \ell G(T))^b \\ &\equiv (T^\ell - 1)^{b-1}(T^\ell - 1 + \ell b G(T)) \bmod \ell^2. \end{aligned} \tag{9}$$

From the assumption $\xi_{n,u_0}^{\mathcal{F}} \equiv \xi_{n,u_0}^{\ell} \bmod \ell^2$, it follows that

$$\prod_{j\in J}\prod_{u\in I}\left(\frac{\zeta_0^{\ell u}\zeta^{\ell s_j u} - 1}{\zeta_0^{\ell u}\zeta^{\ell t s_j u} - 1}\right)^{c_{j,u}} \equiv \prod_{j\in J}\prod_{u\in I}\left(\frac{\zeta_0^{u}\zeta^{s_j u} - 1}{\zeta_0^{u}\zeta^{t s_j u} - 1}\right)^{\ell c_{j,u}} \bmod \ell^2.$$

Using (9), we see that

$$\begin{aligned} &\prod_j\prod_u(\zeta_0^{\ell u}\zeta^{\ell s_j u} - 1)(\zeta_0^{\ell u}\zeta^{\ell t s_j u} - 1 + \ell c_{j,u} G(\zeta_0^{u}\zeta^{t s_j u})) \\ &\qquad \equiv \prod_j\prod_u(\zeta_0^{\ell u}\zeta^{\ell t s_j u} - 1)(\zeta_0^{\ell u}\zeta^{\ell s_j u} - 1 + \ell c_{j,u} G(\zeta_0^{u}\zeta^{s_j u})) \end{aligned} \tag{10}$$

modulo $\ell^2$. For each $r \in J$ and $w \in I$, we put

$$\Pi_{r,w} = \prod_{(j,u)\neq(r,w)}(\zeta_0^{\ell u}\zeta^{\ell t s_j u} - 1) \quad \text{and} \quad \Pi'_{r,w} = \prod_{(j,u)\neq(r,w)}(\zeta_0^{\ell u}\zeta^{\ell s_j u} - 1)$$

where $(j,u)$ runs over $J \times I$ with $(j,u) \neq (r,w)$. Then we see from (10) that

$$\Big(\prod_j\prod_u(\zeta_0^{\ell u}\zeta^{\ell s_j u} - 1)\Big)\cdot\Big(\sum_r\sum_w c_{r,w} G(\zeta_0^{w}\zeta^{t s_r w})\Pi_{r,w}\Big) \tag{11}$$

$$\equiv \Big(\prod_j\prod_u(\zeta_0^{\ell u}\zeta^{\ell t s_j u} - 1)\Big)\cdot\Big(\sum_r\sum_w c_{r,w} G(\zeta_0^{w}\zeta^{s_r w})\Pi'_{r,w}\Big) \tag{12}$$

modulo $\ell$. We expand (11) and (12) as polynomials on $\zeta$. Let $\Psi$ be the set of maps from $J \times I$ to $\{0,1\}$, and $\Psi_{r,w}$ the set of maps from $J \times I \setminus \{(r,w)\}$ to $\{0,1\}$. For maps $\kappa \in \Psi$ and $\kappa' \in \Psi_{r,w}$, we put

$$A(\kappa) = \sum_{j,u}\ell s_j u \kappa(j,u), \qquad A_0(\kappa) = \sum_{j,u}\ell u \kappa(j,u)$$

and

$$B(\kappa') = \sum_{(j,u)\neq(r,w)} \ell s_j u \kappa'(j,u), \qquad B_0(\kappa') = \sum_{(j,u)\neq(r,w)} \ell u \kappa'(j,u).$$

Further, we put

$$K(\kappa,\kappa') = \kappa(r,w) + \sum_{(j,u)\neq(r,w)} (\kappa(j,u) + \kappa'(j,u)).$$

Then we see that (11) and (12) equal

$$-\sum_{r}\sum_{w}\sum_{\kappa}\sum_{\kappa'} (-1)^{K(\kappa,\kappa')} c_{r,w} G(\zeta_0^w \zeta^{ts_r w}) \zeta_0^{A_0(\kappa)+B_0(\kappa')} \zeta^{A(\kappa)+tB(\kappa')} \tag{13}$$

and

$$-\sum_{r}\sum_{w}\sum_{\kappa}\sum_{\kappa'} (-1)^{K(\kappa,\kappa')} c_{r,w} G(\zeta_0^w \zeta^{s_r w}) \zeta_0^{A_0(\kappa)+B_0(\kappa')} \zeta^{tA(\kappa)+B(\kappa')}, \tag{14}$$

respectively. Let $\tau$ be an integer with $1 \le \tau \le \ell - 1$ (resp. $0 \le \tau \le 1$) when $\ell \ge 3$ (resp. $\ell = 2$). Then the terms $\zeta^{ts_r w\tau}$ and $\zeta^{s_r w\tau}$ appear in (13) and (14) from the factor $G(\zeta_0^w \zeta^{ts_r w})$ and $G(\zeta_0^w \zeta^{s_r w})$, respectively.

We extract terms of the form $\zeta^*$ with

$$* \equiv \sum_{j,u} 2\ell u - 1 \quad \Big(= |J| \sum_{u} 2\ell u - 1\Big)$$

modulo $p^{n+1-n_0}$ from (13) and (14), and apply Lemma 4. For this purpose, we consider the following conditions for each $r \in J$:

$$ts_r w\tau + A(\kappa) + tB(\kappa') \equiv \sum_{j,u} 2\ell u - 1 \bmod p^{n+1-n_0}, \tag{15}$$

$$s_r w\tau + tA(\kappa) + B(\kappa') \equiv \sum_{j,u} 2\ell u - 1 \bmod p^{n+1-n_0}. \tag{16}$$

As $t = 1 + p^n$, the two conditions are equivalent. Let us show the following:

Claim. *For each $r \in J$, the conditions* (15) *and* (16) *are satisfied if and only if $w \equiv 1 \bmod p^{n+1}$, $\tau = \ell - 1$, $\kappa(j,u) = 1$ for all $(j,u) \in J \times I$ and $\kappa'(j,u) = 1$ for all $(j,u) \in J \times I$ with $(j,u) \neq (r,w)$.*

*Proof.* We easily obtain the "if" part of the assertion from the definitions of $A(\kappa)$ and $B(\kappa')$. Let us show the "only if" part. Put

$$x_u = \begin{cases} \ell\Big(\sum_{j}(2 - \kappa(j,u) - \kappa'(j,u))\Big) & \text{if } u \neq w, \\ \ell\Big(2 - \kappa(r,w) + \sum_{j\neq r}(2 - \kappa(j,w) - \kappa'(j,w))\Big) - \tau & \text{if } u = w. \end{cases}$$

As $s_j \equiv 1 \bmod p^{n+1-n_0}$, we see that the conditions (15) and (16) are equivalent to

$$\sum_{u \in I} x_u u - 1 \equiv 0 \bmod p^{n+1-n_0}. \tag{17}$$

Further, we see that

$$0 \leq x_u \leq 2\ell|J|$$

and that

$$x_u \equiv 0 \text{ or } -\tau \tag{18}$$

modulo $\ell$ according as $u \neq w$ or $u = w$. The reduction map $(\mathbb{Z}/mp^{n+1})^\times \to (\mathbb{Z}/p^{n+1})^\times$ induces a surjection $I \to \mathcal{I}$ (sending $u_\delta$ to $u'_\delta$ in the notation of Subsection 4.1). We easily see that the map $I \to \mathcal{I}$ is $\phi(m)$-to-1. Let $i_0$ be the image of $w$ under this map. For each $i \in \mathcal{I}$, we put

$$y_i = \sum_{u \equiv i} x_u$$

where $u$ runs over the elements of $I$ with $u \equiv i \bmod p^{n+1}$. Then the condition (17) is equivalent to

$$\sum_{i \in \mathcal{I}} y_i i - 1 \equiv 0 \bmod p^{n+1-n_0}. \tag{19}$$

Further, we have

$$0 \leq y_i \leq 2\ell\phi(m)|J| \tag{20}$$

and

$$y_i \equiv 0 \text{ or } -\tau \tag{21}$$

modulo $\ell$ according as $i \neq i_0$ or $i = i_0$. Let $\nu = \omega_\wp(i) \in \mathcal{V}$ and $g(\nu) = y_i$. Then $\nu \equiv i \bmod \wp^{n+1}$. From (19), we obtain

$$X = \sum_{\nu \in \mathcal{V}} g(\nu)\nu - 1 \equiv 0 \bmod \wp^{n+1-n_0}.$$

It follows that

$$N(X) \equiv 0 \bmod p^{n+1-n_0},$$

where $N$ is the norm map from $\mathbb{Q}(\zeta_{p-1})$ to $\mathbb{Q}$. Now, from (20) and the assumption $p^{n+1-n_0} > M_\chi$, we obtain $X = 0$. Therefore, by Lemma 5, we see that $g(\nu) = 0$ or 1 according as $\nu \neq 1$ or $= 1$. It follows from (21) that $i_0 = 1$ (i.e., $w \equiv 1 \bmod p^{n+1}$) and $\tau = \ell - 1$. Further, $y_i = 0$ or 1 according as $i \neq i_0 = 1$ or $i = 1$. Hence, we obtain $x_u = 0$ or 1 according as $u \neq w$ or $u = w$, considering the congruence (18) for $u \equiv 1 \bmod p^{n+1}$. Now, we see that $\kappa(j, u) = 1$ for all $(j, u) \in J \times I$ and $\kappa'(j, u) = 1$ for all $(j, u) \in J \times I$ with $(j, u) \neq (r, w)$. ∎

In view of the Claim, we put

$$A = A(\kappa) = \sum_{j,u} \ell s_j u \quad \text{and} \quad A_0 = A_0(\kappa) = \sum_{j,u} \ell u.$$

Further, for each $r \in J$ and $w \in I$ with $w \equiv 1 \bmod p^{n+1}$, we put

$$B(r,w) = B(\kappa') = \sum_{(j,u)\neq(r,w)} \ell s_j u = A - \ell s_r w,$$
$$B_0(w) = B_0(\kappa') = \sum_{(j,u)\neq(r,w)} \ell u = A_0 - \ell w.$$

From the congruence (11) $\equiv$ (12) mod $\ell$, we see by the Claim and Lemma 4 (with $k = p^{n+1}$ and $k_0 = p^{n+1-n_0}$) that

$$\sum_r {\sum_w}' c_{r,w} \zeta_0^{w(\ell-1)} \zeta^{ts_r w(\ell-1)} \zeta_0^{A_0+B_0(w)} \zeta^{A+tB(r,w)} \equiv \sum_r {\sum_w}' c_{r,w} \zeta_0^{w(\ell-1)} \zeta^{s_r w(\ell-1)} \zeta_0^{A_0+B_0(w)} \zeta^{tA+B(r,w)} \bmod \ell$$

where in $\sum_w'$, $w$ runs over the subset $I_1$ of $I$. Using $\zeta^w = \zeta$, we see that

$$\sum_r {\sum_w}' c_{r,w} \zeta_0^{-w} \zeta^{ts_r(\ell-1)+(1+t)A-\ell s_r t} \equiv \sum_r {\sum_w}' c_{r,w} \zeta_0^{-w} \zeta^{s_r(\ell-1)+(1+t)A-\ell s_r} \bmod \ell.$$

Taking the complex conjugation of both sides and multiplying by $\zeta^{(1+t)A}$, we obtain

$$\sum_r {\sum_w}' c_{r,w} \zeta_0^{w} \zeta^{ts_r} \equiv \sum_r {\sum_w}' c_{r,w} \zeta_0^{w} \zeta^{s_r} \bmod \ell.$$

Letting $\zeta_{p^{n_0}} = \zeta^{p^{n+1-n_0}}$ and $\zeta_p = \zeta^{p^n}$, we have $\zeta^{s_r} = \zeta\zeta_{p^{n_0}}^r$ and $\zeta^{ts_r} = \zeta\zeta_p\zeta_{p^{n_0}}^r$. Now, noting that $c_{r,w} \equiv a_r b_{wu_0} \bmod \ell$, we see from the above congruence that

$$\zeta(\zeta_p - 1) \cdot {\sum_w}' b_{wu_0} \zeta_0^w \cdot \sum_r a_r \zeta_{p^{n_0}}^r \equiv 0 \bmod \ell.$$

As $\zeta(\zeta_p - 1)$ is relatively prime to $\ell$, it follows that

$${\sum_w}' b_{wu_0} \zeta_0^w \cdot \sum_r a_r \zeta_{p^{n_0}}^r \equiv 0 \bmod \ell.$$

Taking the Galois conjugate over $\mathbb{Q}$ shows that this congruence holds for any primitive $m$th (resp. $p^{n_0}$th) root $\zeta_0$ (resp. $\zeta_{p^{n_0}}$) of unity. We fix an arbitrary $\zeta_{p^{n_0}}$. We see from Lemma 7 that there exists some prime ideal $\mathcal{L}$

of $\mathbb{Q}(\zeta_{p^{n_0}})$ over $\ell$ such that $\sum_r a_r \zeta_{p^{n_0}}^r \not\equiv 0 \bmod \mathcal{L}$. Hence,

$$\sum_w{}' b_{wu_0} \zeta_0^w \equiv 0 \bmod \tilde{\mathcal{L}}$$

for any prime ideal $\tilde{\mathcal{L}}$ of $K_{n_0-1} = \mathbb{Q}(\zeta_0, \zeta_{p^{n_0}})$ over $\mathcal{L}$. We see that this congruence holds for any primitive $m$th root $\zeta_0$ of unity since $\mathbb{Q}(\zeta_0)$ and $\mathbb{Q}(\zeta_{p^{n_0}})$ are linearly disjoint over $\mathbb{Q}$. Therefore,

$$\sum_w{}' b_{wu_0} \zeta_0^w \equiv 0 \bmod \ell$$

for all $u_0 \in I$, which contradicts Lemma 9. Now, we have completed the proof of Lemma 8.

**Acknowledgements.** The author thanks K. Horie for informing him of the papers [11, 12]. The author was partially supported by Grant-in-Aid for Scientific Research (C), (No. 19540005), Japan Society for the Promotion of Science.

## References

[1] B. Ferrero and L. C. Washington, *The Iwasawa invariant $\mu_p$ vanishes for abelian number fields*, Ann. of Math. 109 (1979), 377–395.

[2] E. Friedman, *Ideal class groups in basic $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s}$-extensions of abelian number fields*, Invent. Math. 65 (1982), 425–440.

[3] E. Friedman and J. W. Sands, *On the $\ell$-adic Iwasawa $\lambda$-invariant in a $p$-extension* (with an appendix by L. C. Washington), Math. Comp. 64 (1995), 1659–1674.

[4] R. Gillard, *Remarques sur les unités cyclotomiques et unités elliptiques*, J. Number Theory 11 (1979), 21–48.

[5] —, *Unités cyclotomiques, unités semi-locales et $\mathbb{Z}_\ell$-extensions, II*, Ann. Inst. Fourier (Grenoble) 29 (1979), no. 4, 1–15.

[6] R. Greenberg, *On p-adic L-functions and cyclotomic fields, II*, Nagoya Math. J. 67 (1977), 139–158.

[7] —, *On 2-adic L-functions and cyclotomic invariants*, Math. Z. 159 (1978), 37–45.

[8] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, reprint of the first edition, Springer, Berlin, 1985.

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

[10] —, *The ideal class group of the basic $\mathbb{Z}_p$-extension over an imaginary quadratic field*, Tohoku Math. J. 57 (2005), 375–394.

[11] —, *Triviality in ideal class groups of Iwasawa-theoretical abelian number fields*, J. Math. Soc. Japan 57 (2005), 827–857.

[12] —, *Primary components of the ideal class group of an Iwasawa-theoretical abelian number field*, ibid. 59 (2007), 811–824.

[13] H. Ichimura and S. Nakajima, *On the 2-part of the class numbers of cyclotomic fields of prime power conductors*, ibid., to appear.

[14] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. of Math. 98 (1973), 246–326.

[15] H. W. Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. Deutsch. Akad. Wiss. Berlin, Akademie-Verlag, Berlin, 1954.
[16] B. Mazur and A. Wiles, *Class fields of abelian extensions over* $\mathbb{Q}$, Invent. Math. 76 (1984), 179–330.
[17] T. Tsuji, *Semi-local units modulo cyclotomic units*, J. Number Theory 78 (1999), 1–26.
[18] L. C. Washington, *The non-p-part of the class numbers in a cyclotomic* $\mathbb{Z}_p$*-extension*, Invent. Math. 49 (1978), 87–97.
[19] —, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, New York, 1997.
[20] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. 131 (1990), 493–540.

Humio Ichimura
Faculty of Science
Ibaraki University
Bunkyo 2-1-1, Mito, 310-8512, Japan
E-mail: hichimur@mx.ibaraki.ac.jp

*Received on 12.11.2010*
*and in revised form on 26.2.2011* (6545)