©2012 The Mathematical Society of Japan
J. Math. Soc. Japan
Vol. 64, No. 1 (2012) pp. 317–342
doi: 10.2969/jmsj/06410317

On the 2-part of the class numbers of cyclotomic fields of prime power conductors

By Humio Ichimura and Shoichi Nakajima

(Received Aug. 17, 2010)

Abstract. Let p be an odd prime number and ℓ a prime number with $\ell \neq p$. Let $K_n = \boldsymbol{Q}(\zeta_{p^{n+1}})$ be the p^{n+1}-st cyclotomic field. Let h_n and h_n^- be the class number and the relative class number of K_n, respectively. When $\ell = 2$, we give an explicit bound $\boldsymbol{m}_p$ depending on p such that the ratio h_n^-/h_{n-1}^- is odd for all $n > \boldsymbol{m}_p$. When $\ell \geq 3$, we also give a corresponding result on the ℓ-part of the relative class number of $K_n^+(\zeta_\ell)$. As an application, we show that when $p \leq 509$, the ratio h_n/h_0 is odd for all $n \geq 1$.

1. Introduction.

Let p be a fixed prime number. Let F be a number field, and F_∞/F the cyclotomic $\boldsymbol{Z}_p$-extension with its n-th layer F_n $(n \geq 0)$. Let h_{F_n} be the class number of F_n. It is a well known theorem of Washington [**23**] that for a prime number $\ell \neq p$, the ratio $h_{F_n}/h_{F_{n-1}}$ is not divisible by ℓ for all sufficiently large n. In [**6**], [**7**], [**8**], [**9**], Horie gave an "explicit" version when the base field F is a *real* abelian field whose conductor and the degree over $\boldsymbol{Q}$ are not divisible by ℓ. Namely, he gave an explicit bound $m = m_{F,p,\ell}$ depending on F, p and ℓ such that $h_{F_n}/h_{F_{n-1}}$ is not divisible by ℓ for all $n \geq m$ ([**7**, Lemma 7], [**8**, Proposition 3]). In this paper, we give an explicit version for certain *relative* class numbers and give its numerical application.

We fix an odd prime number p and a prime number $\ell \neq p$. Let $K_n = \boldsymbol{Q}(\zeta_{p^{n+1}})$ be the p^{n+1}-st cyclotomic field, and K_n^+ its maximal real subfield. Here, for an integer $m \geq 2$, ζ_m denotes a primitive m-th root of unity. Let h_n and h_n^+ be the class numbers of K_n and K_n^+, respectively, and let $h_n^- = h_n/h_n^+$ be the relative class number. Let $n_0 = \mathrm{ord}_p(\ell^{p-1} - 1)$ be the p-adic valuation of $\ell^{p-1} - 1$. When $\ell = 2$, let $\boldsymbol{a}_p$ be the number of p-th roots ζ of unity such that $\mathrm{Tr}(\zeta) \equiv 0 \bmod 2$, and let $\boldsymbol{b}_p = p - \boldsymbol{a}_p$. Here, Tr is the trace map from $\boldsymbol{Q}_2(\zeta_p)$ to $\boldsymbol{Q}_2$, $\boldsymbol{Q}_2$ being the field of 2-adic rationals. We easily see that $1 \leq \min(\boldsymbol{a}_p, \boldsymbol{b}_p) \leq (p-1)/2$. We define an

---

2000 *Mathematics Subject Classification.* Primary 11R18, 11R23.

Key Words and Phrases. cyclotomic field, Z_p-extension, parity of class number.

The first author was partially supported by Grant-in-Aid for Scientific Research (C) (No. 19540005), Japan Society for the Promotion of Science.

integer $\varpi_{p,\ell} \geq 1$ as follows. We put $\varpi_{p,\ell} = 1$ when ℓ is a primitive root modulo p^2. Otherwise, we put

$$\varpi_{p,\ell} = \begin{cases} \left(p - 1 - \left[\dfrac{p}{\ell}\right]\right) p^{n_0 - 1}, & \text{if } \ell > 2 \text{ or } n_0 > 1 \\ \min(\boldsymbol{a}_p, \boldsymbol{b}_p), & \text{if } \ell = 2 \text{ and } n_0 = 1. \end{cases}$$

Here, $[x]$ is the largest integer $\leq x$. We define an integer $M_{p,\ell}$ by

$$M_{p,\ell} = \ell(p-1)\varpi_{p,\ell} - 1.$$

Theorem 1. *Under the above setting, assume that* $p^{n+1-n_0} > (M_{p,\ell})^{\phi(p-1)}$, *where* ϕ *is the Euler function. Then the following assertions hold.*

(I) *The ratio* h_n^+/h_{n-1}^+ *is relatively prime to* ℓ.
(II) *When* $\ell = 2$, h_n/h_{n-1} *is odd.*

It is known that h_n^+/h_{n-1}^+ is odd when h_n^-/h_{n-1}^- is odd (see Remarks 1(I)). Hence, the essential part of Theorem 1(II) is the assertion $2 \nmid h_n^-/h_{n-1}^-$. However, we need Theorem 1(I) to prove Theorem 1(II). When $\ell \geq 3$, we give a corresponding assertion (Theorem 3) at the end of Section 2 under an additional assumption on p and ℓ.

Using the analytic class number formula, we can check the parity of h_n^-/h_{n-1}^- with the help of computer. We checked the parity for $p \leq 509$ and n smaller than the bound given in Theorem 1, and obtained the following:

Theorem 2. *Let* p *be an odd prime number with* $p \leq 509$. *Then the ratio* h_n/h_0 *is odd for all* $n \geq 1$.

When $p = 3, 5, 7, 17, 257$, this assertion was already shown in [**11**], [**12**], [**13**], [**22**]. As for the plus part h_n^+, there is a heuristic argument in Buhler *et al* [**1**] which suggests not only that the ratio h_n^+/h_0^+ is odd, but also that it should be 1 for all $n \geq 1$, except for a finite number of primes p.

Theorem 1(I) is quite similar to an assertion obtained directly from [**8**, Proposition 3] which is given in a very general setting. (A correction to this proposition in [**8**] is given in page 823 of [**10**].) Horie proved [**8**, Proposition 3] using (a) some tools in Leopoldt [**16**], in particular, Leopoldt's algebraic interpretation of the analytic class number formula for a real abelian field and (b) his new idea and technique on very subtle treatment of cyclotomic units. We prove Theorem 1(I) using Horie's idea and technique and some tools in modern theory of cyclotomic fields, in particular, the Iwasawa main conjecture. By applying [**8**, Proposition 3] in our special setting, we can show that ℓ does not divide h_n^+/h_{n-1}^+ if $p^{n+1-n_0} > (M'_{p,\ell})^{\phi(p-1)}$ when we put $M'_{p,\ell} = \ell(p-1)^3 p^{n_0-1} - 1$. Our bound in Theorem 1(I) is sharper than this bound. To compare the two bounds, let $\ell = 2$. By the above bound, we see that when $p = 509$ (resp. $p = 503$), the ratio h_n^+/h_{n-1}^+ is odd for all $n \geq 785$ (resp. 778). On the other hand, by the bound in Theorem 1(I), we see that it is odd for all $n \geq 280$ (resp. 500). In view of the application to Theorem 2, it is desirable to choose the bound as small as possible.

This paper is organized as follows. In Section 2, we prove Theorems 1 and 3 postponing the proof of a key lemma (Lemma 4). We prove Lemma 4 in Section 3 using some lemmas and an argument in [**7**], [**8**]. In Section 4, we prove Theorem 2 using Theorem 1 and the analytic class number formula with the help of computer.

Remarks 1.

(I) It is well known that the condition $2 \nmid h_n^-$ implies $2 \nmid h_n^+$ (Hasse [**5**, Satz 45], Iwasawa [**14**, Theorem 6]). We can easily show that $2 \nmid h_n^-/h_{n-1}^-$ implies $2 \nmid h_n^+/h_{n-1}^+$ applying an argument in [**14**] after decomposing the 2-part of the class group of $\boldsymbol{Q}(\zeta_{p^{n+1}})$ by the action of $\mathrm{Gal}(K_n/K_0)$.

(II) By a table in Schoof [**19**] on the relative class number h_0^- for $p \leq 509$, we see that among the odd primes ≤ 509, h_0 is even for $p = 29$, 113, 163, 197, 239, 277, 311, 337, 349, 373, 397, 421, 463, 491.

(III) Let $p = 3$ and let k be an imaginary abelian field whose conductor is not divisible by 9. For each odd prime number $\ell \neq 3$, Friedman and Sands [**3**, Corollary 1.4] gave an explicit bound m_ℓ depending on k and ℓ such that $\ell \nmid h_{k_n}^-/h_{k_{n-1}}^-$ for all $n \geq m_\ell$. Here, $h_{k_n}^-$ is the relative class number of k_n. Their method depends on the fact that the group of roots of unity in the ring $\boldsymbol{Z}_3$ of 3-adic integers is $\{\pm 1\}$, and it is completely different from that of Horie and this paper.

2. Proof of Theorem 1.

We use the same notation as in Section 1. In particular, p is a fixed odd prime number and ℓ is a prime number with $\ell \neq p$. Let $\mathscr{A}_n^+$ be the ℓ-part of the ideal class group of K_n^+. As the natural map $\mathscr{A}_{n-1}^+ \to \mathscr{A}_n^+$ is injective, we often regard $\mathscr{A}_{n-1}^+$ as a subgroup of $\mathscr{A}_n^+$. Denote by $\boldsymbol{B}_n$ the n-th layer of the cyclotomic $\boldsymbol{Z}_p$-extension over $\boldsymbol{Q}$ with $\boldsymbol{B}_0 = \boldsymbol{Q}$. Let $\Delta = \mathrm{Gal}(K_0^+/\boldsymbol{B}_0) = \mathrm{Gal}(K_n^+/\boldsymbol{B}_n)$. Denote by Δ_ℓ and Δ_0 the ℓ-part and the non-ℓ-part of Δ, respectively. Let $\Gamma_n = \mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q}) = \mathrm{Gal}(K_n/K_0)$. We regard the group $\mathscr{A}_n^+$ as a module over the group ring $\boldsymbol{Z}_\ell[\Delta_0 \times \Gamma_n]$. Let X be a module over $\boldsymbol{Z}_\ell[\Delta_0 \times \Gamma_n]$, and let φ (resp. ψ) be a $\bar{\boldsymbol{Q}}_\ell$-valued character of Δ_0 (resp. Γ_n). Here, $\boldsymbol{Z}_\ell$ is the ring of ℓ-adic integers, $\boldsymbol{Q}_\ell$ the field of ℓ-adic rationals, and $\bar{\boldsymbol{Q}}_\ell$ an algebraic closure of $\boldsymbol{Q}_\ell$. Regarding

$\varphi\psi = \varphi \times \psi$ as a character of $\Delta_0 \times \Gamma_n$, we denote by $X(\varphi\psi)$ the $\varphi\psi$-part of X. (For the definition of $\varphi\psi$-part and some of its properties, see Tsuji [**21**, Section 2].) We have a canonical decomposition

$$\frac{\mathscr{A}_n^+}{\mathscr{A}_{n-1}^+} = \bigoplus_{\varphi,\psi} \mathscr{A}_n^+(\varphi\psi)$$

where φ runs over a complete set of representatives of the $\boldsymbol{Q}_\ell$-equivalent classes of $\bar{\boldsymbol{Q}}_\ell$-valued characters of Δ_0 and ψ runs over that of $\bar{\boldsymbol{Q}}_\ell$-valued characters of Γ_n of order p^n. Because of this decomposition, we work componentwise in the following. We fix a character φ (resp. ψ) of Δ_0 (resp. of Γ_n of order p^n), and we put

$$\chi = \varphi\psi$$

for brevity. Let $\boldsymbol{Q}_\ell(\chi)$ be the subfield of $\bar{\boldsymbol{Q}}_\ell$ generated by the values of χ over $\boldsymbol{Q}_\ell$, and $\boldsymbol{Z}_\ell[\chi]$ the ring of integers of $\boldsymbol{Q}_\ell(\chi)$. Then, for a $\boldsymbol{Z}_\ell[\Delta_0 \times \Gamma_n]$-module X, the χ-part $X(\chi)$ is naturally regarded as a module over $\boldsymbol{Z}_\ell[\chi]$. Denote by F_n the intermediate field of $K_n^+/\boldsymbol{B}_n$ fixed by Δ_ℓ, so that we have $\mathrm{Gal}(F_n/\boldsymbol{B}_n) = \Delta_0$ and $\mathrm{Gal}(K_n^+/F_n) = \Delta_\ell$. Let A_n be the ℓ-part of the ideal class group of F_n. Since exactly one prime of F_n ramifies in the ℓ-extension K_n^+/F_n, we obtain the following lemma using a classical argument in [**24**, pp. 186–187].

Lemma 1. *Under the above setting, we have* $\mathscr{A}_n^+(\chi) = \{0\}$ *if and only if* $A_n(\chi) = \{0\}$.

Because of this lemma, it suffices to work on the class group A_n of F_n.

Let E_n be the group of units of F_n. We *fix* a primitive p^{n+1}-st root

$$\zeta = \zeta_{p^{n+1}}$$

of unity in all what follows. Let D_n be the subgroup of $K_n^\times$ generated by $-\zeta$ and $(1-\zeta)^\sigma$ for all $\sigma \in \mathrm{Gal}(K_n/\boldsymbol{Q})$, and let

$$C_n = E_n \cap D_n$$

be a group of cyclotomic units of F_n. Let $\bar{E}_n$ and $\bar{C}_n$ be the pro-ℓ-completions of E_n and C_n, respectively. We see that the χ-part $\bar{E}_n(\chi)$ is free of rank one over $\boldsymbol{Z}_\ell[\chi]$ by a theorem of Minkowski on units of Galois extension over $\boldsymbol{Q}$ (cf. Narkiewicz [**18**, Theorem 3.26]). A formula for the class number of F_n is given by Theorems 4.1 and 5.1 of Sinnott [**20**]. A "refined version" of this formula, which is a consequence of the Iwasawa main conjecture, was obtained in Greenberg [**4**, Proposition 9], Kuz'min [**15**, Theorem 9.2] and Cornacchia and Greither [**2**, Proposition 10] as follows:

$$|A_n(\chi)| = \left[\bar{E}_n(\chi) : \bar{C}_n(\chi)\right]. \tag{1}$$

Let e_ψ and e_φ be the idempotents of $\boldsymbol{Z}_\ell[\Gamma_n]$ and $\boldsymbol{Z}_\ell[\Delta_0]$ corresponding to ψ and φ, respectively:

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

$$e_\varphi = \frac{1}{|\Delta_0|} \sum_{\delta \in \Delta_0} \mathrm{Tr}_{\boldsymbol{Q}_\ell(\zeta_d)/\boldsymbol{Q}_\ell}(\varphi(\delta)^{-1})\delta.$$

Here, d is the order of φ. Let $\tilde{e}_\psi$ (resp. $\tilde{e}_\varphi$) be an element of $\boldsymbol{Z}[\Gamma_n]$ (resp. $\boldsymbol{Z}[\Delta_0]$) such that

$$\tilde{e}_\psi \equiv e_\psi \bmod \ell \quad \text{and} \quad \tilde{e}_\varphi \equiv e_\varphi \bmod \ell.$$

Let $t = 1 + p^n$ and let

$$\epsilon_n = N_{K_n^+/F_n}\left(\frac{\zeta - \zeta^{-1}}{\zeta^t - \zeta^{-t}}\right) \in C_n.$$

The Galois group $\mathrm{Gal}(K_n/K_{n-1}) = \mathrm{Gal}(F_n/F_{n-1})$ is generated by the automorphism sending ζ to ζ^t. Hence, it follows that

$$N_{n,n-1}(\epsilon_n) = 1, \tag{2}$$

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

$$\eta_n = \epsilon_n^{\tilde{e}_\psi \tilde{e}_\varphi} \in C_n.$$

From the definition of C_n, we see that the class containing the unit η_n generates $(C_n/C_n^\ell)(\chi)$ over $\boldsymbol{Z}_\ell[\chi]$. The following lemma is an immediate consequence of (1). It corresponds to [**6**, Lemma 2], [**7**, Lemma 2] and [**8**, Proposition 1].

Lemma 2. *If $A_n(\chi)$ is nontrivial, then $\eta_n \in (K_n^\times)^\ell$.*

Lemma 3. *Let λ be the Frobenius automorphism of ℓ for $K_n/\boldsymbol{Q}$. For an element $\eta \in K_n^\times$ with $(\eta, \ell) = 1$, assume that the cyclic extension $K_n(\zeta_\ell)(\eta^{1/\ell})$ over $K_n(\zeta_\ell)$ is unramified at the primes over ℓ. Then $\eta^\lambda \equiv \eta^\ell \bmod \ell^2$.*

Remark 2. When $\eta \in (K_n^\times)^\ell$, the assumption of Lemma 3 is clearly satisfied. In this case, the assertion of Lemma 3 was shown in [**6**, Lemma 5].

Proof of Lemma 3. Assume that $K_n(\zeta_\ell)(\eta^{1/\ell})/K_n(\zeta_\ell)$ is unramified at the primes over ℓ. Then we have $\eta \equiv u^\ell \bmod \pi_\ell^\ell$ for some $u \in K_n(\zeta_\ell)^\times$ by Exercises 9.2 and 9.3 of [**24**]. Here, $\pi_\ell = \zeta_\ell - 1$. Taking the norm to K_n, we obtain $\eta \equiv v^\ell \bmod \ell^2$ for some $v \in K_n^\times$ because $K_n/\boldsymbol{Q}$ is unramified at ℓ. Since $v^\lambda \equiv v^\ell \bmod \ell$, it follows that

$$\eta^\lambda \equiv (v^\lambda)^\ell \equiv v^{\ell^2} \equiv \eta^\ell \bmod \ell^2. \qquad \square$$

The following key lemma is proved in Section 3.

Lemma 4. *If $p^{n+1-n_0} > (M_{p,\ell})^{\phi(p-1)}$, then $\eta_n^\lambda \not\equiv \eta_n^\ell \bmod \ell^2$.*

Proof of Theorem 1. From Lemmas 1-4, we immediately see that $\ell \nmid h_n^+/h_{n-1}^+$ (including the case $\ell = 2$).

Let $\ell = 2$. To prove that $2 \nmid h_n/h_{n-1}$, it suffices to show $2 \nmid h_n^-/h_{n-1}^-$. We show this using the fact $2 \nmid h_n^+/h_{n-1}^+$ and the classical "Spiegelung" argument. Let $\mathscr{A}_n$ be the 2-part of the ideal class group of K_n. It is known that the natural map $\mathscr{A}_n^+ \to \mathscr{A}_n$ is injective ([**24**, Theorem 4.14]). We define the minus part $\mathscr{A}_n^-$ to be the cokernel of the injection:

$$\mathscr{A}_n^- = \frac{\mathscr{A}_n}{\mathscr{A}_n^+}.$$

As $\ell = 2$, the non-ℓ-part Δ_0 of $\Delta = \mathrm{Gal}(K_n^+/\boldsymbol{B}_n)$ is naturally regarded as a subgroup of $\mathrm{Gal}(K_n/\boldsymbol{B}_n)$. Hence, we can view $\mathscr{A}_n^-$ as a module over $\boldsymbol{Z}_\ell[\Delta_0 \times \Gamma_n]$. It suffices to show that $\mathscr{A}_n^-(\chi) = \{0\}$ for each $\chi = \varphi\psi$. Assume that $\mathscr{A}_n^-(\chi)$ is nontrivial. Let Ω/K_n be the class field corresponding to $\mathscr{A}_n^-(\chi) = (\mathscr{A}_n/\mathscr{A}_n^+)(\chi)$. Namely, Ω/K_n is an unramified abelian extension and $\mathrm{Gal}(\Omega/K_n)$ is isomorphic to $\mathscr{A}_n^-(\chi)$ via the reciprocity law map. As $\mathscr{A}_n^-(\chi)$ is stable under the action of $\mathrm{Gal}(K_n/\boldsymbol{Q})$, Ω is Galois over $\boldsymbol{Q}$. The 2-extension K_n/F_n is ramified only at the unique prime over p and the infinite prime divisors. Therefore, using a classical argument in [**24**, pp. 186–187], we see that there exists a quadratic extension H'/F_n unramified at all finite primes satisfying $H'K_n \subseteq \Omega$. Let H be the Galois closure of H' over $\boldsymbol{Q}$, and $\mathscr{G} = \mathrm{Gal}(H/F_n)$. As Ω is Galois over $\boldsymbol{Q}$, we have $HK_n \subseteq \Omega$. It follows that

$$\mathscr{G} = \mathscr{G}(\chi) \cong \boldsymbol{F}_2[\chi] \tag{3}$$

where $\boldsymbol{F}_2 = \boldsymbol{Z}/2\boldsymbol{Z}$ is the finite field of 2 elements and $\boldsymbol{F}_2[\chi] = \boldsymbol{Z}_2[\chi]/2\boldsymbol{Z}_2[\chi]$ is the residue field of $\boldsymbol{Q}_2(\chi)$. Let V be the subgroup of $F_n^\times/(F_n^\times)^2$ such that

$$H = F_n(v^{1/2} \mid [v] \in V).$$

The Kummer pairing

$$V \times \mathscr{G} \to \{\pm 1\}, \quad ([v], g) \to \langle v, g\rangle = (v^{1/2})^{g-1}$$

is nondegenerate and satisfies the relation $\langle v^\rho, g^\rho\rangle = \langle v, g\rangle$ for $\rho \in \Delta_0 \times \Gamma_n$. Therefore, by (3), it follows that

$$V = V(\chi^{-1}) \cong \boldsymbol{F}_2[\chi^{-1}] = \boldsymbol{F}_2[\chi]. \tag{4}$$

For an element $[v] \in V$, we have $v\mathscr{O}_{F_n} = \mathfrak{A}^2$ for some ideal $\mathfrak{A}$ of F_n, where $\mathscr{O}_{F_n}$ is the ring of integers of F_n. Consider the homomorphism f from V to A_n sending $[v] \in V$ to the ideal class containing $\mathfrak{A}$. Then we have a Kummer sequence

$$\{0\} \to V \cap \left(\frac{E_n(F_n^\times)^2}{(F_n^\times)^2}\right) \to V = V(\chi^{-1}) \xrightarrow{f} A_n.$$

The image of f is contained in $A_n(\chi^{-1})$ as f commutes with the Galois action. However, we see that $A_n(\chi^{-1})$ is trivial by $2 \nmid h_n^+/h_{n-1}^+$ and Lemma 1. Hence, by the Kummer sequence, we can regard V as a submodule of $(E_n/E_n^2)(\chi^{-1})$. On the other hand, we have $(E_n/E_n^2)(\chi^{-1}) \cong \boldsymbol{F}_2[\chi^{-1}]$ by [**18**, Theorem 3.26]. By (4), this implies that $V = (E_n/E_n^2)(\chi^{-1})$. By $A_n(\chi^{-1}) = \{0\}$ and (1), it follows that $V = (C_n/C_n^2)(\chi^{-1})$. Therefore, since $(C_n/C_n^2)(\chi^{-1})$ is generated by the class containing the unit η_n (with respect to the character χ^{-1}), the extension $F_n(\eta_n^{1/2})$ is unramified at all finite primes. This contradicts Lemmas 3 and 4. □

In the rest of this section, let $\ell \geq 3$. We put $L_n = K_n^+(\zeta_\ell)$ and $W_\ell = \mathrm{Gal}(L_n/K_n^+)$. Denote by A_{L_n} the ℓ-part of the ideal class group of L_n. We naturally regard $A_{L_{n-1}}$ as a subgroup of A_{L_n}, and put $B_{L_n} = A_{L_n}/A_{L_{n-1}}$. Let ω_ℓ be the $\boldsymbol{Q}_\ell$-valued character of W_ℓ representing the Galois action on ζ_ℓ. (Namely, $\zeta_\ell^\sigma = \zeta_\ell^{\omega_\ell(\sigma)}$ for $\sigma \in W_\ell$.) Denote by $B_{L_n}(\omega_\ell)$ the ω_ℓ-part of the $\boldsymbol{Z}_\ell[W_\ell]$-module B_{L_n}.

Theorem 3. *Assume that $p^{n+1-n_0} > (M_{p,\ell})^{\phi(p-1)}$, and that p is a primitive root modulo ℓ. Then the class group $B_{L_n}(\omega_\ell)$ is trivial.*

Proof of Theorem 3. Let $\chi = \varphi\psi$ be as before, and $\tilde{\chi} = \omega_\ell \times \chi$ be the character of $\Theta = W_\ell \times \Delta_0 \times \Gamma_n$. Regarding A_{L_n} as a module over $\boldsymbol{Z}_\ell[\Theta]$, it suffices to show that the $\tilde{\chi}$-part $A_{L_n}(\tilde{\chi})$ is trivial for each χ. Assume that $A_{L_n}(\tilde{\chi}) \neq \{0\}$. By the second assumption of the assertion, there is a unique prime ideal $\wp$ of $F_n(\zeta_\ell)$ ($\subseteq L_n$) over p. Further, the ℓ-extension $L_n/F_n(\zeta_\ell)$ is ramified only at $\wp$. Therefore, from the assumption $A_{L_n}(\tilde{\chi}) \neq \{0\}$, we can show, similarly to the case $\ell = 2$, that there is a nontrivial unramified abelian extension $H/F_n(\zeta_\ell)$ of exponent ℓ such that (i) H is Galois over $\boldsymbol{Q}$ and (ii) the Galois group $\mathscr{G} = \mathrm{Gal}(H/F_n(\zeta_\ell))$ satisfies

$$\mathscr{G} = \mathscr{G}(\tilde{\chi}) \cong \boldsymbol{F}_\ell[\tilde{\chi}] = \boldsymbol{F}_\ell[\chi].$$

Let V be the subgroup of $F_n(\zeta_\ell)^\times/(F_n(\zeta_\ell)^\times)^\ell$ such that

$$H = F_n(\zeta_\ell)(v^{1/\ell} \mid [v] \in V).$$

Denote by $\mu_\ell = \langle \zeta_\ell \rangle$ the group of ℓ-th roots of unity. The Kummer pairing

$$V \times \mathscr{G} \to \mu_\ell, \quad ([v], g) \to \langle v, g \rangle = (v^{1/\ell})^{g-1}$$

is nondegenerate and satisfies

$$\langle v^\rho, g^\rho \rangle = \langle v, g \rangle^\rho = \langle v, g \rangle^{\omega_\ell(\rho)}$$

for $\rho \in \Theta$. Here, we are regarding ω_ℓ as a character of Θ via the natural surjection $\Theta \to W_\ell$. It follows from $\mathscr{G} = \mathscr{G}(\tilde{\chi})$ that $V = V(\omega_0 \times \chi^{-1})$ where ω_0 is the trivial character of W_ℓ. This implies that $V \subseteq (F_n^\times/(F_n^\times)^\ell)(\chi^{-1})$. Now, we can derive a contradiction using Theorem 1(I) and Lemmas 1, 3 and 4 similarly to the case $\ell = 2$. □

3. Proof of Lemma 4.

3.1. Preliminaries.

We use the same notation as in the previous sections. In particular, $\zeta = \zeta_{p^{n+1}}$ is a fixed primitive p^{n+1}-st root of unity. We recall some lemmas from [**6**], [**7**].

Lemma 5 ([**7**, Lemma 5]). *Let $Y \subset \boldsymbol{Z}$ be a finite set, and $u \in \boldsymbol{Z}$ an* *integer. Let $m \le n$ be an integer, and Y_u the subset of Y consisting of $y \in Y$ with $y \equiv u \bmod p^m$. Let $\kappa : Y \to \boldsymbol{Z}$ be an arbitrary map. If $\sum_{y \in Y} \kappa(y)\zeta^y \equiv 0 \bmod \ell$, then $\sum_{y \in Y_u} \kappa(y)\zeta^y \equiv 0 \bmod \ell$.*

As in [**6**], [**7**], we choose a complete set $\mathscr{V}$ of representatives of the quotient $\mu_{p-1}/\{\pm 1\}$ as follows, where μ_{p-1} is the group of $(p-1)$-st roots of unity in the complex number field $\boldsymbol{C}$. Write $(p-1)/2 = q_1 q_2 \cdots q_r$ with q_i a power of a prime number and $(q_i, q_j) = 1$ for $i \ne j$. We put

$$\mathscr{V} = \left\{ \exp\left(\left(\frac{c_1}{q_1} + \cdots + \frac{c_r}{q_r} \right) \pi \sqrt{-1} \right) \,\middle|\, 0 \le c_i \le q_i - 1 \ (1 \le i \le r) \right\}$$

where $\exp(*)$ is the exponential function.

Lemma 6 ([**6**, Lemma 7]). *Let $z : \mathscr{V} \to \boldsymbol{Z}$ be a map such that $z(\nu) \ge 0$ for all $\nu \in \mathscr{V} \setminus \{1\}$. If $\sum_{\nu \in \mathscr{V}} z(\nu)\nu = 0$, then $z(\nu) = 0$ for all $\nu \in \mathscr{V}$.*

We fix an integer $n \ge 1$ and a prime ideal $\wp$ of $\boldsymbol{Q}(\mu_{p-1})$ over p. Let $\mathscr{I}$ be the set of integers u with $1 \le u \le p^{n+1} - 1$ such that $u^{p-1} \equiv 1 \bmod p^{n+1}$ and $u \equiv \nu \bmod \wp^{n+1}$ for some $\nu \in \mathscr{V}$. Then we have a bijection

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

sending $u \in \mathscr{I}$ to $\nu \in \mathscr{V}$ with $\nu \equiv u \bmod \wp^{n+1}$. For a subset Δ' of $\Delta = \mathrm{Gal}(K_n^+/\boldsymbol{B}_n)$, we put

$$I_{\Delta'} = \left\{ u \in \mathscr{I} \mid \sigma_{u|K_n^+} \in \Delta' \right\} \quad \text{and} \quad V_{\Delta'} = \omega_\wp(I_{\Delta'}), \tag{5}$$

where σ_u is the automorphism of K_n sending ζ to ζ^u.

Let φ be a $\bar{\boldsymbol{Q}}_\ell$-valued character of Δ_0, and ψ that of Γ_n of order p^n. For the expression $\eta_n = \epsilon_n^{\tilde{e}_\psi \tilde{e}_\varphi}$ in Section 2, we can replace $\tilde{e}_\psi$ with $\tilde{e}'_\psi = \tilde{e}_\psi - \alpha N_{n,n-1}$ for any $\alpha \in \boldsymbol{Z}[\Gamma_n]$ because of the relation (2). Here, $N_{n,n-1}$ is the norm map from F_n to F_{n-1}. We choose $\tilde{e}'_\psi$ as follows. We see that $n_0 = \mathrm{ord}_p(\ell^{p-1} - 1)$ is the largest integer satisfying $\boldsymbol{Q}_\ell(\zeta_p) = \boldsymbol{Q}_\ell(\zeta_{p^{n_0}})$. If an element $\gamma \in \Gamma_n$ satisfies $\gamma^{p^{n_0}} \ne 1$, then the trace of $\psi(\gamma)$ to $\boldsymbol{Q}_\ell(\zeta_p) = \boldsymbol{Q}_\ell(\zeta_{p^{n_0}})$ equals 0. For $a \equiv 1 \bmod p$, let $\gamma_a \in \Gamma_n$ be the automorphism of K_n sending ζ to ζ^a. For an integer j, put

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

From the definition of e_ψ and the above remark, we can write

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

When ℓ is a primitive root modulo p^2, we see that

$$e_\psi = 1 - \frac{1}{p} N_{n,n-1}$$

since $\mathrm{Tr}_{\boldsymbol{Q}_\ell(\zeta_p)/\boldsymbol{Q}_\ell}(\psi(s_j)^{-1}) = -1$ for $1 \le j \le p-1$. In view of this, we choose $\tilde{e}'_\psi = 1$ in this case. Further, we put $J_\psi = \{0\}$ and $a_0 = 1$. Assume that ℓ is not a primitive root modulo p^2. We choose and fix an element $\alpha \in \boldsymbol{Z}[\Gamma_n^{p^{n-n_0}}]$ so that the number of non-zero terms of $e_\psi - \alpha N_{n,n-1} \bmod \ell$ is minimal. Let J_ψ be the set of integers j with $0 \le j \le p^{n_0} - 1$ for which the coefficient a'_j of γ_{s_j} in $e_\psi - \alpha N_{n,n-1} \bmod \ell$ is nonzero. Letting a_j be the integer with $a_j \equiv a'_j \bmod \ell$ and $1 \le a_j \le \ell - 1$, we put

$$\tilde{e}'_\psi = \sum_{j \in J_\psi} a_j \gamma_{s_j} \quad (\equiv e_\psi - \alpha N_{n,n-1} \bmod \ell). \tag{6}$$

From the above, we obtain

Lemma 7. *Under the above setting and notation, the unit* $\epsilon_n^{\tilde{e}_\psi}$ *equals*

$$\prod_{j \in J_\psi} \epsilon_n^{a_j \gamma_{s_j}}$$

times an ℓ*-th power of a unit of* K_n.

As for the cardinality $|J_\psi|$, we show

Lemma 8. $|J_\psi| \le \varpi_{p,\ell}$.

Proof. When ℓ is a primitive root modulo p^2, the assertion is obvious as $J_\psi = \{0\}$ and $\varpi_{p,\ell} = 1$. So, we deal with the case where ℓ is not a primitive root. Let $X = \Gamma_n^{p^{n-n_0}}$ and $Y = \Gamma_n^{p^{n-1}}$. Let ρ_j $(1 \le j \le p^{n_0-1})$ be a complete set of representatives of the quotient X/Y. We can write

$$e_\psi = \sum_{j=1}^{p^{n_0-1}} \Big(\sum_{\gamma \in Y} x_{n,j,\gamma}\gamma \Big) \rho_j$$

with

$$x_{n,j,\gamma} = \frac{1}{p^{n_0}} \operatorname{Tr}_{\boldsymbol{Q}_\ell(\zeta_p)/\boldsymbol{Q}_\ell} \left(\psi(\gamma^{-1})\psi(\rho_j^{-1})\right).$$

First, assume that $\ell > 2$ or $n_0 > 1$. For each j, we see that among the p quantities $x_{n,j,\gamma} \bmod \ell$ with $\gamma \in Y$, at least $[p/\ell]+1$ ones have the same value, say c_j. Letting $\beta = \sum_j c_j \rho_j$, we see that the number of nonzero terms of $e_\psi - \beta N_{n,n-1} \bmod \ell$ is less than or equal to $\varpi_{p,\ell}$. Next, assume that $\ell = 2$ and $n_0 = 1$. Then among the p quantities $x_{n,1,\gamma} \bmod 2$, $\boldsymbol{a}_p$ ones equal 0, and $\boldsymbol{b}_p = p - \boldsymbol{a}_p$ ones equal 1. Hence, letting $\delta_p = 0$ or 1 according to whether or not $\boldsymbol{a}_p > \boldsymbol{b}_p$, we see that the number of nonzero terms of $e_\psi - \delta_p N_{n,n-1} \bmod 2$ equals $\varpi_{p,2}$. □

The following lemma plays an important role in the proof of Lemma 4.

LEMMA 9. *Let $\zeta_{p^{n_0}} = \psi(1 + p^{n+1-n_0})$ be a primitive p^{n_0}-th root of unity. When $n \geq 2n_0 - 1$, we have*

$$\sum_{j \in J_\psi} a_j \zeta_{p^{n_0}}^j \in \boldsymbol{Z}_\ell[\zeta_{p^{n_0}}]^\times.$$

PROOF. When ℓ is a primitive root modulo p^2, the assertion is obvious as $J_\psi = \{0\}$ and $a_0 = 1$. Let us deal with the case where ℓ is not a primitive root. We regard the character ψ as a homomorphism from $\boldsymbol{Z}_\ell[\Gamma_n]$ to $\bar{\boldsymbol{Q}}_\ell$ by linearity. We have $\psi(N_{n,n-1}) = 0$ as ψ is of order p^n. Therefore, we see from the congruence (6) that $\sum_j a_j \psi(\gamma_{s_j})$ is an ℓ-adic unit since e_ψ is a unit of the ring $\boldsymbol{Z}_\ell[\Gamma_n]e_\psi$. Since $n \geq 2n_0 - 1$, we see that $s_j \equiv (1 + p^{n+1-n_0})^j \bmod p^{n+1}$, and hence $\psi(\gamma_{s_j}) = \zeta_{p^{n_0}}^j$. Thus, we obtain the assertion. □

REMARK 3. We easily see that the condition $n \geq 2n_0 - 1$ is satisfied when the condition $p^{n+1-n_0} > (M_{p,\ell})^{\phi(p-1)}$ in Theorem 1 is satisfied.

Finally, we rewrite the expression $\eta_n = \epsilon_n^{\tilde{e}_\psi \tilde{e}_\varphi}$. We can naturally regard the operator $e_\varphi N_{K_n^+/F_n}$ as an element of $\boldsymbol{Z}_\ell[\Delta]$. Let Δ_φ be the subset of $\Delta = \operatorname{Gal}(K_n^+/\boldsymbol{B}_n)$ consisting of elements $\delta \in \Delta$ for which the coefficient of δ in $e_\varphi N_{K_n^+/F_n}$ ($\in \boldsymbol{Z}_\ell[\Delta]$) modulo ℓ is nonzero. Regarding φ as a homomorphism $\boldsymbol{Z}_\ell[\Delta_0] \to \bar{\boldsymbol{Q}}_\ell$ by linearity, we have $\varphi(e_\varphi) = 1$. From this, we see that the set Δ_φ is non-empty. Clearly, we have

$$|\Delta_\varphi| \leq \frac{p-1}{2}. \tag{7}$$

We write

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

for some integer b_δ with

$$1 \leq b_\delta \leq \ell - 1.$$

Let

$$I_\varphi = I_{\Delta_\varphi} \quad \text{and} \quad V_\varphi = V_{\Delta_\varphi}$$

be the subset of $\mathscr{I}$ and $\mathscr{V}$ defined by (5). For $u \in I_\varphi$, we write $b_u = b_\delta$ with $\delta = \sigma_{u|K_n^+} \in \Delta_\varphi$ (see (5)). Now, from Lemma 7, we see that the unit η_n in Lemma 4 equals the unit

$$\xi'_n = \prod_{j\in J_\psi}\prod_{u\in I_\varphi}\left(\frac{\zeta^{s_j u} - \zeta^{-s_j u}}{\zeta^{t s_j u} - \zeta^{-t s_j u}}\right)^{a_j b_u}$$

times an ℓ-th power of a unit of K_n. We see that the unit ξ'_n is Galois conjugate to the unit

$$\xi_n = \prod_{j\in J_\psi}\prod_{u\in I_\varphi}\left(\frac{\zeta^{s_j u} - 1}{\zeta^{t s_j u} - 1}\right)^{a_j b_u}$$

times ζ^c for some $c \in \boldsymbol{Z}$. Hence, we can write $\eta_n = \zeta^c \epsilon^\ell \xi_n^\sigma$ for some unit ϵ of K_n and some $\sigma \in \mathrm{Gal}(K_n/\boldsymbol{Q})$. Since $\zeta^\lambda = \zeta^\ell$ and $(\epsilon^\ell)^\lambda \equiv \epsilon^{\ell^2} \bmod \ell^2$, we see that Lemma 4 is equivalent to the following assertion.

Lemma 10. *If $p^{n+1-n_0} > (M_{p,\ell})^{\phi(p-1)}$, then we have $\xi_n^\lambda \not\equiv \xi_n^\ell \bmod \ell^2$.*

Remark 4. The conclusion of Lemma 10 is invariant under the Galois action of Δ. Therefore, replacing Δ_φ with $\delta^{-1}\Delta_\varphi$ for any $\delta \in \Delta_\varphi$, we may as well assume that $1 \in I_\varphi$ and $1 \in V_\varphi$.

3.2. Proof of Lemma 10.

We use the notation as in the previous sections. We fix an integer n and write $\chi = \varphi\psi$. For brevity, we put $I = I_\varphi$, $V = V_\varphi$ and $J = J_\psi$. As we have noted in Remark 4, we may as well assume that $1 \in V$ and $1 \in I$. Let Φ_ℓ be the set of all maps z from V to $\{0, 1, \ldots, 2\ell|J|\}$. Let

$$M_\chi = \max_{z \in \Phi_\ell} \left\{ \left| N\left(\sum_{\nu \in V} z(\nu)\nu - 1 \right) \right| \right\},$$

where N is the norm map from $\boldsymbol{Q}(\zeta_{p-1})$ to $\boldsymbol{Q}$. We see that

$$M_\chi \leq (M_{p,\ell})^{\phi(p-1)} \tag{8}$$

by Lemma 8, (7) and

$$\left| \sum_{\nu \in V} z(\nu)\nu - 1 \right| \leq |z(1) - 1| + \sum_{\nu \neq 1} |z(\nu)| \leq 2\ell|J| \times |I| - 1$$

for each embedding of $\boldsymbol{Q}(\zeta_{p-1})$ into the complex numbers $\boldsymbol{C}$.

We derive a contradiction assuming that $p^{n+1-n_0} > M_\chi$, $n \geq 2n_0 - 1$ and $\xi_n^\lambda \equiv \xi_n^\ell \bmod \ell^2$ following Horie's argument in [**7**], [**8**]. Then, from (8) and Remark 3, we obtain Lemma 10. For integers $j \in J$ and $u \in I$, let $c_{j,u}$ be the integer such that

$$1 \leq c_{j,u} \leq \ell - 1 \quad \text{and} \quad c_{j,u} \equiv a_j b_u \bmod \ell.$$

By the congruence $\xi_n^\lambda \equiv \xi_n^\ell \bmod \ell^2$, we have

$$\prod_{j \in J} \prod_{u \in I} \left(\frac{\zeta^{\ell s_j u} - 1}{\zeta^{\ell t s_j u} - 1} \right)^{c_{j,u}} \equiv \prod_{j \in J} \prod_{u \in I} \left(\frac{\zeta^{s_j u} - 1}{\zeta^{t s_j u} - 1} \right)^{\ell c_{j,u}} \bmod \ell^2. \tag{9}$$

Define a polynomial $G(T) \in \boldsymbol{Z}[T]$ by

$$G(T) = \frac{1}{\ell}((T-1)^\ell - (T^\ell - 1)) = \sum_{k=1}^{\ell-1} \frac{(-1)^{k-1}}{\ell} {}_\ell C_k T^k$$

or

$$G(T) = -T + 1$$

according as $\ell > 2$ or $\ell = 2$. Here, ${}_\ell C_k$ is the binomial coefficient. Then we have

$$(T-1)^{\ell} = T^{\ell} - 1 + \ell G(T)$$

and

$$(T^c-1)^{b\ell} = ((T^c-1)^{\ell})^b \equiv (T^{\ell c}-1)^{b-1} \times (T^{\ell c} - 1 + b\ell G(T^c)) \bmod \ell^2.$$

Using this, we see from (9) that

$$\begin{aligned}\prod_j \prod_u (\zeta^{\ell s_j u} - 1)\big(\zeta^{\ell t s_j u} - 1 + \ell c_{j,u} G(\zeta^{t s_j u})\big) \\ \equiv \prod_j \prod_u (\zeta^{\ell t s_j u} - 1)\big(\zeta^{\ell s_j u} - 1 + \ell c_{j,u} G(\zeta^{s_j u})\big) \bmod \ell^2. \qquad (10)\end{aligned}$$

For $m \in J$ and $w \in I$, we put

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

where (j,u) runs over $J \times I$ with $(j,u) \neq (m,w)$. It follows from (10) that

$$\begin{aligned}\Big(\prod_j \prod_u (\zeta^{\ell s_j u} - 1)\Big) \times \Big(\sum_{m\in J} \sum_{w \in I} c_{m,w} G(\zeta^{t s_m w}) \Pi_{m,w}\Big) \qquad (11) \\ \equiv \Big(\prod_j \prod_u (\zeta^{\ell t s_j u} - 1)\Big) \times \Big(\sum_m \sum_w c_{m,w} G(\zeta^{s_m w}) \Pi'_{m,w}\Big) \bmod \ell. \qquad (12)\end{aligned}$$

We expand the both hand sides of this congruence. Let Ψ (resp. $\Psi_{m,w}$) be the set of maps from $J \times I$ (resp. $J \times I \setminus \{(m,w)\}$) to $\{0,1\}$. For maps $\kappa \in \Psi$ and $\kappa' \in \Psi_{m,w}$, we put

$$A(\kappa) = \sum_{j,u} \ell s_j u \kappa(j,u), \quad B(\kappa') = \sum_{(j,u)\neq(m,w)} \ell s_j u \kappa'(j,u)$$

and

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

Then (11) and (12) equal

$$-\sum_m \sum_w \sum_{\kappa\in\Psi} \sum_{\kappa'\in\Psi_{m,w}} (-1)^{K(\kappa,\kappa')} c_{m,w} G(\zeta^{ts_m w}) \zeta^{A(\kappa)+tB(\kappa')} \tag{13}$$

and

$$-\sum_m \sum_w \sum_{\kappa\in\Psi} \sum_{\kappa'\in\Psi_{m,w}} (-1)^{K(\kappa,\kappa')} c_{m,w} G(\zeta^{s_m w}) \zeta^{tA(\kappa)+B(\kappa')}, \tag{14}$$

respectively. Let D be the set of integers d with $1 \le d \le \ell - 1$ when $\ell > 2$ and let $D = \{0, 1\}$ when $\ell = 2$. Then, the terms $\zeta^{ts_m wd}$ (resp. $\zeta^{s_m wd}$) with $d \in D$ appear in (13) (resp. (14)), from the factor $G(\zeta^{ts_m w})$ (resp. $G(\zeta^{s_m w})$).

Now we extract terms of the form ζ^* with $* \equiv \sum_{j,u} 2\ell u - 1 \bmod p^{n+1-n_0}$ from (13) and (14), and apply Lemma 5. For this purpose, we consider the following conditions for each $m \in J$:

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

and

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

Both conditions are equivalent as $t = 1 + p^n$. We show the following:

Claim. *For each $m \in J$, the conditions* (15) *and* (16) *are satisfied if and only if $w = 1$, $d = \ell - 1$, $\kappa(j, u) = 1$ for all $(j, u) \in J \times I$ and $\kappa'(j, u) = 1$ for all $(j, u) \in J \times I$ with $(j, u) \neq (m, 1)$.*

Proof. From the definitions of $A(\kappa)$ and $B(\kappa')$, we easily obtain the "if"-part of the assertion. Let us show the "only if"-part. We put

$$x_u = \begin{cases} \ell\left(\displaystyle\sum_j (2 - \kappa(j,u) - \kappa'(j,u))\right) & \text{or} \\ \ell\left(2 - \kappa(m,w) + \displaystyle\sum_{j\neq m} (2 - \kappa(j,w) - \kappa'(j,w))\right) - d \end{cases}$$

according as $u \neq w$ or $u = w$. From $s_j \equiv 1 \bmod p^{n+1-n_0}$ and the definitions of $A(\kappa)$ and $B(\kappa')$, 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

$$0 \le x_u \le 2\ell |J|,$$

and that

$$x_u \equiv 0 \quad \text{or} \quad -d \bmod \ell \tag{18}$$

according as $u \neq w$ or $u = w$. For each $\nu \in V$, letting $u = \omega_{\wp}^{-1}(\nu) \in I$, we put $g(\nu) = x_u$. We have $u \equiv \nu \bmod \wp^{n+1}$ by the definition of $\omega_{\wp}$. Hence, we obtain from (17),

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

It follows that

$$X = N\left(\sum_{\nu \in V} g(\nu)\nu - 1\right) \equiv 0 \bmod p^{n+1-n_0}$$

where N is the norm map from $\boldsymbol{Q}(\zeta_{p-1})$ to $\boldsymbol{Q}$. However, since $p^{n+1-n_0} > M_\chi$, we must have $X = 0$. Hence, we see from Lemma 6 that $g(\nu) = 1$ or 0 according as $\nu = 1$ or $\nu \neq 1$. (Here, we are assuming that $1 \in V$ and $1 \in I$ as we have noted in Remark 4.) Therefore, it follows from (18) that $w = 1$ and $d = \ell - 1$. Further, from the definition of x_u, we see that $\kappa(j,u) = 1$ and $\kappa'(j,u) = 1$ for all $(j,u) \in J \times I$ and $(j,u) \in J \times I$ with $(j,u) \neq (m,1)$. $\square$

In view of Claim, we put

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

and

$$B_m = B(\kappa') = \sum_{(j,u) \neq (m,1)} \ell s_j u = A - \ell s_m$$

for each $m \in J$. We see from (13) $\equiv$ (14) $\bmod \ell$, Lemma 5 and Claim that

$$\sum_{m \in J} c_{m,1} \zeta^{ts_m(\ell-1)} \zeta^{A+tB_m} \equiv \sum_{m \in J} c_{m,1} \zeta^{s_m(\ell-1)} \zeta^{tA+B_m} \bmod \ell.$$

Since

$$ts_m(\ell-1) + A + tB_m = -ts_m + (1+t)A$$

and

$$s_m(\ell-1) + tA + B_m = -s_m + (1+t)A,$$

we obtain

$$\sum_m c_{m,1} \zeta^{ts_m} \equiv \sum_m c_{m,1} \zeta^{s_m} \bmod \ell.$$

Letting $\zeta_p = \zeta^{p^n}$ and $\zeta_{p^{n_0}} = \zeta^{p^{n+1-n_0}}$, we see from the above that

$$(\zeta_p - 1) \sum_m c_{m,1} \zeta_{p^{n_0}}^m \equiv 0 \bmod \ell.$$

As $\zeta_p - 1$ is relatively prime to ℓ and $c_{m,1} \equiv a_m b_1 \bmod \ell$, it follows that

$$\sum_{m \in J} a_m \zeta_{p^{n_0}}^m \equiv 0 \bmod \ell.$$

However, this congruence is impossible by Lemma 9. Now, we have completed the proof of Lemma 10.

Remark 5. We can show that the value $|J| = |J_\psi|$ depends only on p and ℓ and that $|\Delta_\varphi|$ depends only on the order d of φ. If we obtain estimates for $|J_\psi|$ and $|\Delta_\varphi|$ better than Lemma 8 and (7), we can show a result sharper than Theorem 1 by the above argument.

4. Proof of Theorem 2.

In this section, we prove Theorem 2 by combining Theorem 1 and computer calculation.

4.1. Application of the class number formula.

To prove $2 \nmid h_n/h_{n-1}$, it suffices to show $2 \nmid h_n^-/h_{n-1}^-$ (cf. Remarks 1(I)). We note that $n_0 = 1$ for $p \le 509$ because, as is well known, the minimal prime p satisfying $2^{p-1} \equiv 1 \bmod p^2$ is 1093. As $n_0 = 1$, we have

$$M_{p,2} = 2p-3 \quad \text{or} \quad 2(p-1)\min(\boldsymbol{a}_p, \boldsymbol{b}_p) - 1$$

according as 2 is a primitive root modulo p^2 or not. Putting

$$\boldsymbol{m}_p = \left[\frac{\phi(p-1)\log M_{p,2}}{\log p} \right],$$

we know that h_n^-/h_{n-1}^- is odd for $n > \boldsymbol{m}_p$, by virtue of Theorem 1. So, it remains to show that h_n^-/h_{n-1}^- is odd for $1 \le n \le \boldsymbol{m}_p$. For that purpose, we make use of the analytic class number formula (cf. [**24**, Theorem 4.17]). Because the unit index equals 1 in this case ([**24**, Corollary 4.13]), the formula gives

$$\frac{h_n^-}{h_{n-1}^-} = p \prod_{\chi} \left(-\frac{1}{2} B_{1,\chi} \right), \tag{19}$$

where χ runs over all odd Dirichlet characters of conductor p^{n+1} and

$$B_{1,\chi} = \frac{1}{p^{n+1}} \sum_{a=1}^{p^{n+1}} a\chi(a).$$

Throughout this section, we put

$$p - 1 = 2^t q \quad (t \ge 1,\ q : \text{odd})$$

and express an odd character χ of conductor p^{n+1} as a product $\chi = \delta\varphi\psi$ of characters δ, φ, ψ satisfying

character	δ	φ	ψ
conductor	p	p	p^{n+1}
order	2^t	d	p^n
parity	odd	even	even

where d is a divisor of q. For this χ, the generalized Bernoulli number $B_{1,\chi}$ belongs to $\boldsymbol{Q}(\zeta_{2^t dp^n})$. We denote by Tr the trace map from $\boldsymbol{Q}(\zeta_{2^t dp^n})$ to $\boldsymbol{Q}(\zeta_{2^t dp})$.

LEMMA 11. *Assume $n_0 = 1$ and that for any odd character $\chi = \delta\varphi\psi$ of conductor p^{n+1} and any prime ideal $\tilde{\mathscr{L}}$ of $\boldsymbol{Q}(\zeta_{2^t dp})$ lying above 2, there is an integer α which is prime to p and satisfies*

$$\mathrm{Tr}\left(\frac{1}{2}\chi(\alpha)^{-1}B_{1,\chi}\right) \not\equiv 0 \bmod \tilde{\mathscr{L}}. \tag{20}$$

Then the quotient h_n^-/h_{n-1}^- is odd.

PROOF. If h_n^-/h_{n-1}^- is even, then, by the formula (19), there exist an odd character χ and a prime ideal $\hat{\mathscr{L}}$ of $\boldsymbol{Q}(\zeta_{2^t dp^n})$ lying above 2 which satisfy

$$\frac{1}{2}B_{1,\chi} \equiv 0 \bmod \hat{\mathscr{L}}.$$

Because of the assumption $n_0 = 1$, $\hat{\mathscr{L}}$ is inert in the extension $\boldsymbol{Q}(\zeta_{2^t dp^n})/\boldsymbol{Q}(\zeta_{2^t dp})$. Hence, for the prime ideal $\tilde{\mathscr{L}}$ of $\boldsymbol{Q}(\zeta_{2^t dp})$ lying below $\hat{\mathscr{L}}$, the congruence

$$\mathrm{Tr}\left(\frac{1}{2}\chi(\alpha)^{-1}B_{1,\chi}\right) \equiv 0 \bmod \tilde{\mathscr{L}}$$

must hold for any integer α relatively prime to p. This proves Lemma 11. □

For further computation, we introduce some notation. For an integer a, $s_n(a)$ denotes the integer satisfying

$$s_n(a) \equiv a \bmod p^{n+1} \quad \text{and} \quad 0 \leq s_n(a) < p^{n+1}.$$

Here we note that

$$s_n(-a) = p^{n+1} - s_n(a) \tag{21}$$

holds when $a \not\equiv 0 \bmod p^{n+1}$. We take a primitive root g modulo p^2, which is a primitive root modulo p^{n+1} for $n \geq 1$. Then, for any integer i_0, we have

$$\begin{aligned}\frac{1}{2}\chi(g^{i_0})^{-1}B_{1,\chi} &= \frac{1}{2p^{n+1}} \sum_{i \bmod (p-1)p^n} s_n(g^i)\chi(g^{i-i_0}) \\ &= \frac{1}{2p^{n+1}} \sum_{i \bmod (p-1)p^n} s_n(g^{i_0+i})\chi(g^i),\end{aligned}$$

where i moves over $\boldsymbol{Z}/(p-1)p^n\boldsymbol{Z}$ in the sum. Since, for a $2^t dp^n$-th root ξ of unity, $\mathrm{Tr}(\xi)$ equals $p^{n-1}\xi$ or 0 according as ξ lies in $\boldsymbol{Q}(\zeta_{2^t dp})$ or not, we have

$$\mathrm{Tr}(\chi(g^i)) = p^{n-1}\chi(g^i) \quad \text{or} \quad 0$$

according as i is divisible by p^{n-1} or not. Hence, by writing $i = p^{n-1}i'$ when i is divisible by p^{n-1}, we obtain

$$\mathrm{Tr}\left(\frac{1}{2}\chi(g^{i_0})^{-1}B_{1,\chi}\right) = \frac{1}{2p^2}\sum_{i' \bmod (p-1)p} s_n\bigl(g^{i_0+p^{n-1}i'}\bigr)\chi\bigl(g^{p^{n-1}i'}\bigr). \tag{22}$$

For making use of Lemma 11, we give two congruences.

Lemma 12. *Assume $n_0 = 1$. Then, with the above notation, the following congruences hold for any integer i_0 and any prime ideal $\tilde{\mathscr{L}}$ of $\boldsymbol{Q}(\zeta_{2^t dp})$ lying above 2.*

(I) *Put $\rho = \varphi(g^{2^t})\psi(g^{2^t p^{n-1}})$. Then ρ is a primitive dp-th root of unity, and a congruence*

$$\begin{aligned}&\mathrm{Tr}\left(\frac{1}{2}\chi(g^{i_0})^{-1}B_{1,\chi}\right)\\ &\quad\equiv \sum_{v=0}^{dp-1}\left(\sum_{u=0}^{d'-1}\sum_{l=0}^{2^{t-1}-1} s_n\bigl(g^{i_0+2^t p^{n-1}v+2^t dp^n u+qp^n l}\bigr)\right)\rho^v\end{aligned} \tag{23}$$

modulo $\tilde{\mathscr{L}}$ holds with $d' = q/d$.

(II) *Put $\eta = \varphi(g)\psi(g^{p^{n-1}})$. Then η is a primitive dp-th root of unity, and a congruence*

$$(1-\eta)\,\mathrm{Tr}\left(\frac{1}{2}\chi(g^{i_0})^{-1}B_{1,\chi}\right) \equiv (1-\eta)\left(\sum_{j=0}^{2^{t-1}qp-1} s_n\bigl(g^{i_0+p^{n-1}j}\bigr)\eta^j\right) + 1 \tag{24}$$

modulo $\tilde{\mathscr{L}}$ holds.

Proof. Because $\chi = \delta\varphi\psi$ has order $2^t dp^n$, we easily see that ρ and η are primitive dp-th roots of unity.

First we prove (I). In (22) we put $i' = 2^t k + qpl$, where k and l move over integers modulo qp and 2^t, respectively. Decomposing $\chi = \delta\varphi\psi$, we have $\delta(g^{2^t}) =$

$\varphi(g^{qp^n}) = \psi(g^{qp^n}) = 1$ and $\varphi(g^{p^{n-1}}) = \varphi(g)$ (note that $p-1$ is divisible by d). Hence $\varphi(g^{2^t p^{n-1}})\psi(g^{2^t p^{n-1}}) = \rho$, and the right hand side of (22) becomes

$$\frac{1}{2p^2} \sum_{k \bmod qp} \Bigl(\sum_{l \bmod 2^t} s_n\bigl(g^{i_0+2^t p^{n-1}k+qp^n l}\bigr)\delta\bigl(g^{qp^n l}\bigr) \Bigr) \rho^k. \tag{25}$$

In the sum for l in (25), we combine terms for l and $l+2^{t-1}$ $(0 \le l < 2^{t-1})$. Then, since $g^{2^{t-1}qp^n} \equiv -1 \bmod p^{n+1}$, we obtain

$$\begin{aligned} &s_n\bigl(g^{i_0+2^t p^{n-1}k+qp^n l}\bigr)\delta\bigl(g^{qp^n l}\bigr) + s_n\bigl(g^{i_0+2^t p^{n-1}k+qp^n (l+2^{t-1})}\bigr)\delta\bigl(g^{qp^n (l+2^{t-1})}\bigr) \\ &\quad = \bigl(2s_n\bigl(g^{i_0+2^t p^{n-1}k+qp^n l}\bigr) - p^{n+1}\bigr) \times \delta\bigl(g^{qp^n l}\bigr) \end{aligned} \tag{26}$$

in view of (21). Then (22) and (25) show

$$\begin{aligned} \mathrm{Tr}\left(\frac{1}{2}\chi(g^{i_0})^{-1}B_{1,\chi}\right) &= \frac{1}{p^2}\sum_{k=0}^{qp-1}\Bigl(\sum_{l=0}^{2^{t-1}-1} s_n\bigl(g^{i_0+2^t p^{n-1}k+qp^n l}\bigr)\delta\bigl(g^{qp^n l}\bigr)\Bigr)\rho^k \\ &\quad - \frac{p^{n-1}}{2}\Bigl(\sum_{k=0}^{qp-1}\rho^k\Bigr)\Bigl(\sum_{l=0}^{2^{t-1}-1}\delta(g^{qp^n l})\Bigr) \\ &= \frac{1}{p^2}\sum_{k=0}^{qp-1}\Bigl(\sum_{l=0}^{2^{t-1}-1} s_n\bigl(g^{i_0+2^t p^{n-1}k+qp^n l}\bigr)\delta\bigl(g^{qp^n l}\bigr)\Bigr)\rho^k \end{aligned} \tag{27}$$

because ρ is a qp-th root of unity different from 1. Since $\delta(g)$ is a 2^t-th root of unity and the prime ideal $\tilde{\mathscr{L}}$ divides 2, we have congruences $\delta(g) \equiv 1 \bmod \tilde{\mathscr{L}}$ and $p \equiv 1 \bmod \tilde{\mathscr{L}}$. Moreover, putting

$$d' = \frac{q}{d} \quad \text{and} \quad k = dpu + v \quad (0 \le u < d',\ 0 \le v < dp),$$

we have $\rho^k = \rho^v$ because ρ is a dp-th root of unity. Therefore, we obtain (23) easily from (27).

Next we prove (II). Putting $m = (p-1)p/2$, we have $g^{p^{n-1}m} \equiv -1 \bmod p^{n+1}$. Hence, we see that for an integer j,

$$\begin{aligned} &s_n\bigl(g^{i_0+p^{n-1}j}\bigr)\chi\bigl(g^{p^{n-1}j}\bigr) + s_n\bigl(g^{i_0+p^{n-1}(j+m)}\bigr)\chi\bigl(g^{p^{n-1}(j+m)}\bigr) \\ &\quad = 2s_n\bigl(g^{i_0+p^{n-1}j}\bigr)\chi\bigl(g^{p^{n-1}j}\bigr) - p^{n+1}\chi\bigl(g^{p^{n-1}j}\bigr) \end{aligned}$$

similarly to (26). Hence, combining the terms for $i' = j$ and $i' = j + m$, the right hand side of (22) becomes

$$\frac{1}{p^2}\sum_{j=0}^{m-1} s_n\big(g^{i_0+p^{n-1}j}\big)\chi\big(g^{p^{n-1}j}\big) - \frac{p^{n-1}}{2}\sum_{j=0}^{m-1}\chi\big(g^{p^{n-1}j}\big). \tag{28}$$

The sum in the second term of (28) equals

$$\frac{1-\chi(g^{p^{n-1}m})}{1-\chi(g^{p^{n-1}})} = \frac{2}{1-\chi(g^{p^{n-1}})}$$

because $\chi(g^{p^{n-1}m}) = \chi(-1) = -1$. From (22) and (28), we obtain

$$\mathrm{Tr}\left(\frac{1}{2}\chi(g^{i_0})^{-1}B_{1,\chi}\right) = \frac{1}{p^2}\sum_{j=0}^{m-1} s_n\big(g^{i_0+p^{n-1}j}\big)\chi\big(g^{p^{n-1}j}\big) - \frac{p^{n-1}}{1-\chi(g^{p^{n-1}})}.$$

We easily see that

$$\chi\big(g^{p^{n-1}}\big) = \delta\big(g^{p^{n-1}}\big)\varphi\big(g^{p^{n-1}}\big)\psi\big(g^{p^{n-1}}\big) \equiv \eta \bmod \tilde{\mathscr{L}}$$

as $\delta(g) \equiv 1 \bmod \tilde{\mathscr{L}}$ and $\varphi(g^{p^{n-1}}) = \varphi(g)$. Hence, we obtain (24) from the above equality. $\square$

4.2. Methods of computation.

When p and n are given, Lemma 12 supplies two methods of computation for showing that h_n^-/h_{n-1}^- is odd. Both methods are based on calculation of greatest common divisor for polynomials (of variable T) with coefficients in $\boldsymbol{F}_2$, the field with 2 elements. In applying Lemma 12, we take $i_0 = (p-1)r = 2^t qr$ with a non-negative integer r.

Method 1: For a divisor d of q and an integer $r \geq 0$, define a polynomial $F_{d,r}(T) \in \boldsymbol{F}_2[T]$ by

$$F_{d,r}(T) = \sum_{v=0}^{dp-1}\left(\sum_{u=0}^{d'-1}\sum_{l=0}^{2^{t-1}-1} s_n\big(g^{2^t qr + 2^t p^{n-1}v + 2^t dp^n u + qp^n l}\big)\right)T^v \bmod 2.$$

Here, the symbol "mod 2" indicates the reduction modulo 2 of an integral polynomial in T. If, for each divisor d of q, we can find an $r \geq 0$ for which

$$\gcd\left(F_{d,r}(T), \overline{\Phi}_{dp}(T)\right) = 1 \tag{29}$$

holds, then h_n^-/h_{n-1}^- is odd. Here, $\Phi_{dp}(T)$ is the dp-th cyclotomic polynomial and $\overline{\Phi}_{dp}(T) = \Phi_{dp}(T) \bmod 2$.

Method 2: For an integer $r \geq 0$, define a polynomial $G_r(T) \in \boldsymbol{F}_2[T]$ by

$$G_r(T) = (1-T)\left(\sum_{j=0}^{2^{t-1}qp-1} s_n\left(g^{2^t qr + p^{n-1}j}\right)T^j\right) + 1 \bmod 2.$$

If we can find an $r \geq 0$ for which

$$\gcd\left(G_r(T), \frac{T^{qp}-1}{T^q-1} \bmod 2\right) = 1 \tag{30}$$

holds, then h_n^-/h_{n-1}^- is odd.

Both methods are direct consequences of Lemmas 11 and 12. We denote by $\mathscr{L}$ the prime ideal of $\boldsymbol{Q}(\zeta_{dp})$ lying below $\tilde{\mathscr{L}}$. Noting that the right hand sides of (23) and (24) belong to $\boldsymbol{Q}(\zeta_{dp})$, we see that if either of them is prime to $\mathscr{L}$, then $\mathrm{Tr}((1/2)\chi(g^{2^t qr})^{-1}B_{1,\chi})$ is prime to $\tilde{\mathscr{L}}$ (recall that $1-\eta$ is prime to $\tilde{\mathscr{L}}$). By general theory of cyclotomic fields, the prime ideal $\mathscr{L}$ corresponds to an irreducible factor of $\overline{\Phi}_{dp}(T)$. Hence, if (29) holds for some r, then $\mathrm{Tr}((1/2)\chi(g^{2^t qr})^{-1}B_{1,\chi})$ is prime to $\tilde{\mathscr{L}}$. This proves validity of Method 1, in view of Lemma 11. For Method 2, the situation is the same except that the right hand side of (24) (and hence $G_r(T)$) does not depend on d. So, instead of checking that $G_r(T)$ is prime to $\overline{\Phi}_{dp}(T)$ for each d, we should verify that $G_r(T)$ is prime to their product

$$\prod_{d|q} \overline{\Phi}_{dp}(T) = \frac{T^{qp}-1}{T^q-1} \bmod 2,$$

where, in the product on the left hand side, d runs over all divisors of q.

4.3. Data of computation.

As stated at the beginning of this section, we verified that h_n^-/h_{n-1}^- is odd for $p \leq 509$ and $1 \leq n \leq \boldsymbol{m}_p$. We applied both Methods 1 and 2, for cross checking. The computation was done by using Maple 13 (cf. [**17**]) on Apple's Mac Pro computer with dual Quad-Core Intel Xeon CPU of 2.8 GHz. Total time of computation was about 18 hours for Method 1 and about 21 hours for Method 2. Compared to Method 1, Method 2 has a merit of treating all d at one time, but, at the same time, has a demerit that the degrees of the polynomials to be treated are higher. As its consequence, Method 2 works faster than Method 1 for small p, but becomes slower as p grows. Moreover, in Method 2 we must find a value of r which is valid for all d, though, in Method 1, it suffices to find an r for each d. For these reasons, we describe, in the following, the data of computation for Method 1.

The number $\boldsymbol{m}_p$, which gives the upper limit of our verification, is smaller when 2 is a primitive root modulo p^2. Among 96 odd primes p under 509, 2 is a primitive root for 39 primes. Table 1 (resp. Table 2) is a list of all pairs $(p, \boldsymbol{m}_p)$ with $p \leq 509$ for which $\boldsymbol{m}_p > 180$ (resp. $\boldsymbol{m}_p > 300$) and 2 is (resp. is not) a primitive root modulo p^2.

Table 1. Large $\boldsymbol{m}_p$: 2 is a primitive root.

p	347	389	419	443	461	467	491	509
$\boldsymbol{m}_p$	192	214	200	213	195	258	186	279

Table 2. Large $\boldsymbol{m}_p$: 2 is not a primitive root.

p	359	383	401	431	449	479	487	499	503
$\boldsymbol{m}_p$	355	379	319	335	383	475	323	317	499

When p, n, d are given, we first tried to verify (29) for $r = 0$, and if (29) did not hold for $r = 0$, we increased $r = 1, 2, \cdots$ successively until (29) comes to be true. The computation showed, to our surprise, that in almost all cases the first candidate (i.e. $r = 0$) was valid for the verification. All the exceptional cases in which we must take $r > 0$ are given in Table 3.

Table 3. Choice of positive r.

p	7	31	127								
$\boldsymbol{m}_p$	3	15	71								
n	2	8	12	23	25	26	43	45	48	63	66
d	1	1	1	1	1	1	1	1	1	1	1
r	2	2	2	1	1	1	1	1	1	1	2

Looking at Table 3, we notice that positive r is needed only when $d = 1$. This might seem to suggest a possibility that the condition (29) always holds for $r = 0$ as long as $d > 1$. For investigating this point, we continued checking if (29) holds for $r = 0$ when n is larger than our bound $\boldsymbol{m}_p$. As its result, we found examples of $d > 1$ and n for which (29) does not hold for $r = 0$. Such examples were likely to be found when the multiplicative order of 2 modulo p is rather small. One example is the case of $p = 31$, for which the order of 2 is 5. We applied Method 1 for $p = 31$ and $n \leq 5000$ (cf. $\boldsymbol{m}_{31} = 15$), and we found that for $d = 3$ and the values

$$\begin{aligned} n = {} & 121, 148, 212, 296, 360, 505, 511, 518, 521, 524, 695, 725, 742, 827, \\ & 1114, 1275, 1467, 2176, 2335, 2528, 2543, 2632, 2742, 2747, 2848, \\ & 2926, 3178, 3500, 3598, 3845, 3960, 4048, 4828, \end{aligned}$$

(29) is not true for $r = 0$ (in all cases, (29) holds with $r = 1$). This result seems to indicate that, for very large n, (29) does not necessarily hold for $r = 0$, even when $d > 1$. In this respect, our upper bound $\boldsymbol{m}_p$ might be said to be rather "small".

Acknowledgements. The authors thank Kuniaki Horie for informing them of the papers [**8**], [**10**].

References

[1] J. Buhler, C. Pomerance and L. Robertson, Heuristics for class numbers of prime-power real cyclotomic fields, Fields Inst. Commun., **41** (1994), 149–157.

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

[3] E. Friedman and J. W. Sands, On the ℓ-adic Iwasawa λ-invariant in a p-extension, (With an appendix by Lawrence C. Washington), Math. Comp., **64** (1995), 1659–1674.

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

[5] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Springer-Verlag, Berlin, 1985.

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

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

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

[9] K. Horie, Certain primary components of the ideal class group of the $\boldsymbol{Z}_p$-extension over the rationals, Tohoku Math. J., **59** (2007), 259–291.

[10] K. Horie, Primary components of the ideal class group of an Iwasawa-theoretical abelian number field, J. Math. Soc. Japan, **59** (2007), 811–824.

[11] K. Horie and M. Horie, The narrow class groups of the $\boldsymbol{Z}_{17}$- and $\boldsymbol{Z}_{19}$-extensions over the rational field, Abh. Math. Sem. Univ. Hamburg, **80** (2010), 47–57.

[12] H. Ichimura, On the parity of the class number of the 7^nth cyclotomic field, Math. Slovaca, **59** (2009), 357–364.

[13] H. Ichimura and S. Nakajima, On the 2-part of the ideal class group of the cyclotomic $\boldsymbol{Z}_p$-extension over the rationals, Abh. Math. Sem. Univ. Hamburg, **80** (2010), 175–182.

[14] K. Iwasawa, A note on ideal class groups, Nagoya Math. J., **27** (1966), 239–247.

[15] L. V. Kuz'min, A formula for the class number of real abelian fields, Izv. Math., **60** (1996), 695–761.

[16] H. W. Leopoldt, Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper, Abh. Deutsch. Acad. Wiss. Berlin Kl. Math. Nat., 1953, **2**, Academie-Verlag, Berlin, 1954.

[17] Maplesoft, http://www.maplesoft.com/products/maple/index.aspx.

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

[19] R. Schoof, Minus class groups of the field of ℓth roots of unity, Math. Comp., **67** (1998), 1225–1245.

[20] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math., **62** (1980), 181–234.

[21] T. Tsuji, Semi-local units modulo cyclotomic units, J. Number Theory, **78** (1999), 1–26.

[22] L. C. Washington, Class numbers and $\boldsymbol{Z}_p$-extensions, Math. Ann., **214** (1975), 177–193.

[23] L. C. Washington, The non-p-part of the class number in a cyclotomic $\boldsymbol{Z}_p$-extension, Invent. Math., **49** (1978), 87–97.

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

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

Shoichi Nakajima
Department of Mathematics
Gakushuin University
Mejiro 1-5-1, Toshima-ku
Tokyo 171-8588, Japan
E-mail: shoichi.nakajima@gakushuin.ac.jp