

Kummer's Lemma for Some Cyclotomic Fields

Tsutomu SHIMADA

Kanagawa Prefectural Shōyō High-School

(Communicated by N. Sasakura)

Introduction.

Let p be a prime number and $\zeta_n = \exp(2\pi i/n)$ for each natural number n . Kummer's lemma proved in [2] says that "for regular p , a unit of $\mathbf{Q}(\zeta_p)$ congruent to a rational integer modulo p is a p th power in $\mathbf{Q}(\zeta_p)$ ". L. C. Washington generalized this theorem as follows:

THEOREM ([3]). *Let $M = \text{Max}\{v_p(L_p(1, \omega^i))\}; i = 2, 4, \dots, p-3\}$ and let ε be a unit of $\mathbf{Z}[\zeta_p]$. If ε is congruent to a rational integer modulo p^{M+1} , then ε is a p th power of a unit of $\mathbf{Z}[\zeta_p]$.*

And further,

THEOREM ([4]). *Let $M = \text{Max}_\chi v_{\pi_n}(\tau(\chi^{-1})L_p(1, \chi))$, where χ runs through the even nontrivial Dirichlet characters of conductor dividing p^n . Here $\tau(\chi)$ is a Gauss sum. If ε is a unit of $\mathbf{Z}[\zeta_{p^n}]$ such that $\varepsilon \equiv 1 \pmod{p^n \pi_n^{M-1}}$, then ε is a p th power in $\mathbf{Z}[\zeta_{p^n}]$.*

In the present paper, following the beautiful method of Washington, we give a proof of a generalization of Kummer's lemma for some other cyclotomic fields. In the following, p denotes an odd prime number. Let m be a natural number such that p does not divide $m\varphi(m)$ and p is congruent to 1 modulo the exponent of the galois group of $\mathbf{Q}(\zeta_m)$ over \mathbf{Q} , where φ denotes the Euler function. Let $K = \mathbf{Q}(\zeta_{mp})$, E be the group of units of K , K^+ the maximal real subfield of K and E^+ its group of units. Let G be the galois group of K over \mathbf{Q} , \hat{G} its character group and $L_p(s, \chi)$ the p -adic L -function. Let \mathbf{C}_p be the completion of the algebraic closure of the p -adic rational field \mathbf{Q}_p . Throughout the paper, we fix an embedding of K in \mathbf{C}_p , that is, fix a prime \wp of K over p .

Our main result is the following:

THEOREM. *Let p and m be as above. Let M_\wp be the least natural number such that*

$$M_{\wp}(p-1) > \text{Max} \left\{ v_{\wp} \left(\frac{p}{\tau(\chi)} L_p(1, \chi) \right) ; \hat{G} \ni \chi \neq 1, \text{ even} \right\},$$

where v_{\wp} denotes the \wp -adic additive valuation normalized by $v_{\wp}(1 - \zeta_p) = 1$. If $u \in E$ is congruent to a rational integer modulo $p^{M_{\wp}}$, then u is a p th power in E .

This is also a generalization of a result of Washington [3] (corollary to Theorem 2, cf. Theorem 8.22 of [4]) because $v_{\wp}(\tau(\omega^i)) = p - 1 - i$ ($i = 2, \dots, p-3$, even). The proof is based on the non-vanishing of the p -adic regulator of K proved by Brumer [1].

1. Structure of $E \otimes_{\mathbf{Z}} \mathbf{Z}_p$.

Let Δ be the Galois group of K over $\mathbf{Q}(\zeta_m)$, which is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^{\times}$, and M the Galois group of K over $\mathbf{Q}(\zeta_p)$, which is isomorphic to $(\mathbf{Z}/m\mathbf{Z})^{\times}$. Of course we have $G = \Delta \times M$. Let ω be the Teichmüller character which generates $\hat{\Delta}$. By our assumption on p and m stated in the Introduction, the values of all $\chi \in \hat{G}$ belong to the ring of p -adic integers \mathbf{Z}_p in which $|G|$, the order of G , is invertible. We define the homomorphism ψ from E to $E \otimes_{\mathbf{Z}} \mathbf{Z}_p$ by $\psi : u \mapsto u \otimes 1$ and the logarithm from $E \otimes_{\mathbf{Z}} \mathbf{Z}_p$ to \mathbf{C}_p by

$$\log_p \left(\sum_i (u_i \otimes \alpha_i) \right) = \sum_i \alpha_i \log_p u_i.$$

We may consider $E \otimes_{\mathbf{Z}} \mathbf{Z}_p$ as a $\mathbf{Z}_p[G]$ -module and the logarithm is a \mathbf{Z}_p -homomorphism.

LEMMA 1. For any unit $u \in E$, $u \in E^p$ if and only if $\psi(u) \in E \otimes_{\mathbf{Z}} p\mathbf{Z}_p$.

PROOF. Clearly, $u \in E^p$ implies $\psi(u) \in E \otimes_{\mathbf{Z}} p\mathbf{Z}_p$. For a subset S of $E \otimes_{\mathbf{Z}} \mathbf{Z}_p$, we denote by $\langle S \rangle$ the subgroup generated by S over \mathbf{Z}_p . Now assume $\psi(u) \in E \otimes_{\mathbf{Z}} p\mathbf{Z}_p$ and $u \notin E^p$, then we can choose $\varepsilon_1, \dots, \varepsilon_{r-1}$ such that the subgroup of E generated by $\{\varepsilon_1, \dots, \varepsilon_{r-1}, u, \zeta_p\}$, say E' , has the index in E which is prime to p , where r is the \mathbf{Z} -rank of E . So we have $E \otimes_{\mathbf{Z}} \mathbf{Z}_p = \langle \psi(E) \rangle = \langle \psi(E') \rangle$. It holds that

$$\dim_{\mathbf{F}_p}(E \otimes_{\mathbf{Z}} \mathbf{Z}_p / E \otimes_{\mathbf{Z}} p\mathbf{Z}_p) = r + 1.$$

But from our assumption that $\psi(u) \in E \otimes_{\mathbf{Z}} p\mathbf{Z}_p$, we have

$$\dim_{\mathbf{F}_p}(E \otimes_{\mathbf{Z}} \mathbf{Z}_p / E \otimes_{\mathbf{Z}} p\mathbf{Z}_p) \leq r.$$

That is a contradiction and the lemma is proved.

Next, we study the $\mathbf{Z}_p[G]$ -module structure of $E \otimes_{\mathbf{Z}} \mathbf{Z}_p$. Define

$$e_{\chi} = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma) \sigma^{-1} \in \mathbf{Z}_p[G].$$

The e_{χ} 's are orthogonal idempotents of $\mathbf{Z}_p[G]$.

LEMMA 2. *Let p and m be the same as before. Then we have:*

$$E \otimes_{\mathbf{Z}} \mathbf{Z}_p \simeq \left(\bigoplus_{1 \neq \chi: \text{even}} e_{\chi}(E \otimes_{\mathbf{Z}} \mathbf{Z}_p) \right) \oplus e_{\omega}(E \otimes_{\mathbf{Z}} \mathbf{Z}_p),$$

$$e_{\omega}(E \otimes_{\mathbf{Z}} \mathbf{Z}_p) \simeq \langle \zeta_p \otimes 1 \rangle \simeq \mathbf{Z}/p\mathbf{Z}.$$

PROOF. Let W_K be the group of roots of unity in K . Then since p does not divide $[E : E^+ W_K]$, we have

$$E \otimes_{\mathbf{Z}} \mathbf{Z}_p = E^+ W_K \otimes_{\mathbf{Z}} \mathbf{Z}_p = E^+ \langle \zeta_p \rangle \otimes_{\mathbf{Z}} \mathbf{Z}_p.$$

Now we have

$$|G|e_{\chi} = \sum'_{1 \leq a \leq mp} \chi(\sigma_a)\sigma_a^{-1} = \sum'_{1 \leq a \leq mp/2} \{\chi(\sigma_a)\sigma_a^{-1} + \chi(\sigma_{-a})\sigma_{-a}^{-1}\},$$

here \sum' denotes the sum over all a which are prime to mp and σ_a denotes the automorphism sending ζ_{mp} to ζ_{mp}^a . And we have $\sigma_{-a} = \sigma_{-1}\sigma_a$, $\sigma_{-a}^{-1} = (\sigma_{-1}\sigma_a)^{-1} = \sigma_{-1}\sigma_a^{-1}$. Therefore, for each $u \in E^+$,

$$\begin{aligned} (\chi(\sigma_a)\sigma_a^{-1} + \chi(\sigma_{-a})\sigma_{-a}^{-1})(u \otimes 1) &= (\chi(\sigma_a)\sigma_a^{-1} + \chi(\sigma_{-1})\chi(\sigma_a)\sigma_{-1}\sigma_a^{-1})(u \otimes 1) \\ &= (\chi(\sigma_a)\sigma_a^{-1} + \chi(\sigma_{-1})\chi(\sigma_a)\sigma_a^{-1})(u \otimes 1). \end{aligned}$$

Consequently, if χ is odd, we have $(\chi(\sigma_a)\sigma_a^{-1} + \chi(\sigma_{-a})\sigma_{-a}^{-1})(u \otimes 1) = 0$. Since $\{u \otimes 1; u \in E^+\}$ generates $E^+ \otimes_{\mathbf{Z}} \mathbf{Z}_p$,

$$e_{\chi}(E^+ \otimes_{\mathbf{Z}} \mathbf{Z}_p) = 0 \quad \text{for all odd } \chi.$$

Corresponding to the decomposition $G \simeq M \times \Delta$ we may write any character $\chi \in \hat{G}$ as $\chi = \psi\omega^i$ ($0 \leq i \leq p-2$, $\psi \in \hat{M}$).

$$\begin{aligned} |G|e_{\chi} &= \sum_{\tau \in M} \sum_{\sigma \in \Delta} \psi(\tau\sigma)\omega^i(\tau\sigma)\tau^{-1}\sigma^{-1} = \sum_{\tau \in M} \sum_{\sigma \in \Delta} \psi(\tau)\omega^i(\sigma)\tau^{-1}\sigma^{-1} \\ &= \left(\sum_{\tau \in M} \psi(\tau)\tau^{-1} \right) \left(\sum_{\sigma \in \Delta} \omega^i(\sigma)\sigma^{-1} \right). \end{aligned}$$

Now we have

$$\left(\sum_{\tau \in M} \psi(\tau)\tau^{-1} \right) (\zeta_p \otimes 1) = \left(\sum_{\tau \in M} \psi(\tau) \right) (\zeta_p \otimes 1) = 0$$

for $\psi \neq 1_M$ (the principal character of \hat{M}) and $(\sum_{\tau \in M} 1_M(\tau)\tau^{-1})(\zeta_p \otimes 1) = \zeta_p^{|\hat{M}|} \otimes 1$. Therefore,

$$\left\langle \left(\sum_{\tau \in M} \psi(\tau)\tau^{-1} \right) (\zeta_p \otimes 1) \right\rangle \simeq \begin{cases} 0 & \text{if } \psi \neq 1_M, \\ \langle \zeta_p \otimes 1 \rangle & \text{if } \psi = 1_M. \end{cases}$$

On the other hand, from the fact that $(\sum_{\sigma \in \Delta} \omega^i(\sigma)\sigma^{-1})\zeta_p = (\sum_{a=1}^{p-1} a^{i-1})\zeta_p$, we have

$$\left\langle \left(\sum_{\sigma \in \Delta} \omega^i(\sigma)\sigma^{-1} \right) (\zeta_p \otimes 1) \right\rangle \simeq \begin{cases} 0 & \text{if } i \neq 1. \\ \langle \zeta_p \otimes 1 \rangle & \text{if } i = 1. \end{cases}$$

Therefore, we have $e_\chi(E \otimes_{\mathbf{Z}} \mathbf{Z}_p) = 0$ for all odd $\chi \neq \omega$ and $e_\omega(E \otimes_{\mathbf{Z}} \mathbf{Z}_p) \simeq \langle \zeta_p \otimes 1 \rangle$. In addition, when $\chi = 1$, $|G|e_\chi$ is the norm map from K to \mathbf{Q} , so $e_\chi(E \otimes_{\mathbf{Z}} \mathbf{Z}_p) = 0$. This completes the proof of our lemma.

Let f be the order of p modulo m . In the following, we shall regard every unit in E as its image by ψ .

LEMMA 3. *Let $\chi \in \hat{G}$ be an even nontrivial character of conductor f_χ which is not a prime power. Let*

$$U(\chi) = (1 - \zeta_{f_\chi})^{(p^f - 1)e_\chi}.$$

Then, we have

$$\log_p U(\chi) = (p^f - 1) \frac{1}{\varphi(f_\chi)} \frac{p}{\chi(p) - p} \frac{f_\chi}{\tau(\chi)} L_p(1, \chi).$$

PROOF. Let H be the subgroup of G corresponding to $\mathbf{Q}(\zeta_{f_\chi})$ and G_1 a subset of G representing G/H . Since χ has conductor f_χ , $\chi(H) = 1$.

$$\begin{aligned} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} &= \sum_{\sigma \in G_1} \sum_{\tau \in H} \chi(\sigma\tau)\sigma^{-1}\tau^{-1} = \sum_{\sigma \in G_1} \sum_{\tau \in H} \chi(\sigma\tau)\sigma^{-1}\tau^{-1} \\ &= \sum_{\sigma \in G_1} \sum_{\tau \in H} \chi(\sigma)\sigma^{-1}\tau^{-1} = \left(\sum_{\sigma \in G_1} \chi(\sigma)\sigma^{-1} \right) \left(\sum_{\tau \in H} \tau^{-1} \right). \end{aligned}$$

Consequently, it holds that

$$\begin{aligned} U(\chi) &= (1 - \zeta_{f_\chi})^{(p^f - 1) \frac{1}{|G|} (\sum_{\sigma \in G_1} \chi(\sigma)\sigma^{-1}) (\sum_{\tau \in H} \tau^{-1})} \\ &= (1 - \zeta_{f_\chi})^{(p^f - 1) \frac{1}{\varphi(f_\chi)} \sum_{\sigma \in G_1} \chi(\sigma)\sigma^{-1}}. \end{aligned}$$

So, we have

$$\log_p U(\chi) = (p^f - 1) \frac{1}{\varphi(f_\chi)} \sum_{\sigma \in G_1} \chi(\sigma) \log_p (1 - \zeta_{f_\chi}^{\sigma^{-1}}).$$

Our lemma is now clear from the well known fact:

$$L_p(1, \chi) = - \left(1 - \frac{\chi(p)}{p} \right) \frac{\tau(\chi)}{f} \sum_{l=1}^f \chi^{-1}(l) \log_p (1 - \zeta_f^l),$$

where χ is an even nontrivial Dirichlet character of conductor f .

By means of a discussion similar to the above, we have the following:

LEMMA 4. Let $\chi \in \hat{G}$ be an even nontrivial character of conductor f_χ which is a prime power and α a primitive root modulo f_χ . Let

$$V(\chi) = \left(\frac{1 - \zeta_{f_\chi}^\alpha}{1 - \zeta_{f_\chi}} \right)^{(p^f - 1)e(\chi)}$$

Then we have:

$$\log_p V(\chi) = (p^f - 1) \frac{1}{\varphi(f_\chi)} (\chi(\sigma_\alpha) - 1) \frac{p}{\chi(p) - p} \frac{f_\chi}{\tau(\chi)} L_p(1, \chi).$$

Note that $\chi(\sigma_\alpha)$ is a $(p-1)$ -st root of unity and different from 1. So, we have $\chi(\sigma_\alpha) - 1 \not\equiv 0 \pmod{p}$.

PROPOSITION 5. Let $\chi \in \hat{G}$ be an even nontrivial character of conductor f_χ . Let $U(\chi)$ and $V(\chi)$ be the same as before. Then we have

$$v_\wp \left(\frac{p}{\tau(\chi)} L_p(1, \chi) \right) = \begin{cases} v_\wp(\log_p U(\chi)) & \text{if } f_\chi \text{ is not a prime power,} \\ v_\wp(\log_p V(\chi)) & \text{if } f_\chi \text{ is a prime power.} \end{cases}$$

PROOF. If p does not divide f_χ ,

$$v_\wp \left(\frac{p}{\chi(p) - p} \frac{f_\chi}{\tau(\chi)} L_p(1, \chi) \right) = v_\wp \left(\frac{p}{\tau(\chi)} L_p(1, \chi) \right).$$

If p divides f_χ , as p is the exact power of f_χ and $\chi(p) = 0$, we have

$$v_\wp \left(\frac{p}{\chi(p) - p} \frac{f_\chi}{\tau(\chi)} L_p(1, \chi) \right) = v_\wp \left(\frac{p}{-p} \frac{f_\chi}{\tau(\chi)} L_p(1, \chi) \right) = v_\wp \left(\frac{p}{\tau(\chi)} L_p(1, \chi) \right).$$

The proof is now completed by Lemmas 3 and 4.

PROPOSITION 6. Let p, m, G and E be as before. Then we have

$$e_\chi(E \otimes_{\mathbf{Z}} \mathbf{Z}_p) \simeq \mathbf{Z}_p \quad \text{for all even nontrivial } \chi \in \hat{G}.$$

PROOF. From the definition of $U(\chi)$ and $V(\chi)$,

$$U(\chi) \in e_\chi(E \otimes_{\mathbf{Z}} \mathbf{Z}_p) \quad \text{or} \quad V(\chi) \in e_\chi(E \otimes_{\mathbf{Z}} \mathbf{Z}_p).$$

By the theorem of A. Brumer [1], we have $L_p(1, \chi) \neq 0$. So, from Proposition 5, $e_\chi(E \otimes_{\mathbf{Z}} \mathbf{Z}_p)$ is not trivial and $\text{rank}_{\mathbf{Z}_p} e_\chi(E \otimes_{\mathbf{Z}} \mathbf{Z}_p) \geq 1$. From Lemma 2, $\text{rank}_{\mathbf{Z}_p} e_\omega(E \otimes_{\mathbf{Z}} \mathbf{Z}_p) = 0$ and

$$\text{rank}_{\mathbf{Z}_p} (E \otimes_{\mathbf{Z}} \mathbf{Z}_p) \leq r = \#\{\chi ; \chi \text{ is even nontrivial character}\}.$$

Therefore, $\text{rank}_{\mathbf{Z}_p} e_\chi(E \otimes_{\mathbf{Z}} \mathbf{Z}_p) = 1$ for all even nontrivial characters χ . Our proposition is proved.

LEMMA 7. Let p, m, G and E be as above. Let $\chi \in \hat{G}$ be any even nontrivial character. Then we have

$$v_{\wp}(\log_p \eta_{\chi}) \leq v_{\wp} \left(\frac{p}{\tau(\chi)} L_p(1, \chi) \right),$$

for any generator η_{χ} of $e_{\chi}(E \otimes_{\mathbf{Z}} \mathbf{Z}_p)$.

PROOF. From Proposition 6, $U(\chi) = \alpha \eta_{\chi}$ or $V(\chi) = \alpha \eta_{\chi}$ in $E \otimes_{\mathbf{Z}} \mathbf{Z}_p$, for some $\alpha \in \mathbf{Z}_p$. Then, it holds that

$$\log_p U(\chi) = \alpha \log_p \eta_{\chi} \quad \text{or} \quad \log_p V(\chi) = \alpha \log_p \eta_{\chi}.$$

Therefore

$$v_{\wp}(\log_p U(\chi)) = v_{\wp}(\alpha) + v_{\wp}(\log_p \eta_{\chi}) \geq v_{\wp}(\log_p \eta_{\chi})$$

or

$$v_{\wp}(\log_p V(\chi)) = v_{\wp}(\alpha) + v_{\wp}(\log_p \eta_{\chi}) \geq v_{\wp}(\log_p \eta_{\chi}).$$

By means of Proposition 5, the lemma is proved.

2. Proof of the theorem.

By our assumption, there exists a rational integer a such that $u \equiv a \pmod{p^{M_{\nu}}}$. First, we treat the case $u \equiv 1 \pmod{\wp}$. Then we have $a \equiv 1 \pmod{p}$. For each even nontrivial character $\chi \in \hat{G}$, from Proposition 6, there exists a generator η_{χ} of $e_{\chi}(E \otimes_{\mathbf{Z}} \mathbf{Z}_p)$. Then, from Lemma 2 and Proposition 6, we have

$$u \otimes 1 = \sum_{1 \neq \chi: \text{even}} \delta_{\chi} \eta_{\chi} + \delta_{\omega} (\zeta_p \otimes 1)$$

for some $\delta_{\chi} \in \mathbf{Z}_p$ and $\delta_{\omega} \in \mathbf{Z}$.

From our assumption, it holds that $u = a + p^{M_{\nu}} x$ for some $x \in \mathbf{Z}[\zeta_{mp}]$. So, for any $\sigma \in G$, we have

$$\begin{aligned} (\chi(\sigma) \sigma^{-1})(u \otimes 1) &= u^{\sigma^{-1}} \otimes \chi(\sigma) = (a + p^{M_{\nu}} x^{\sigma^{-1}}) \otimes \chi(\sigma) \\ &= a \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_{\nu}} \right) \otimes \chi(\sigma) = a \otimes \chi(\sigma) + \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_{\nu}} \right) \otimes \chi(\sigma). \end{aligned}$$

Then, we have

$$\begin{aligned} \left(\sum_{1 \neq \chi: \text{even}} \chi(\sigma) \sigma^{-1} \right) (u \otimes 1) &= \sum_{1 \neq \chi: \text{even}} (a \otimes \chi(\sigma)) + \sum_{1 \neq \chi: \text{even}} \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_{\nu}} \right) \otimes \chi(\sigma) \\ &= \sum_{1 \neq \chi: \text{even}} \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_{\nu}} \right) \otimes \chi(\sigma). \end{aligned}$$

We define $\chi(\sigma)_{M_\varphi}$ to be a natural number such that $\chi(\sigma)_{M_\varphi} \equiv \chi(\sigma) \pmod{p^{M_\varphi+1}}$ and $\chi(\sigma)'_{M_\varphi}$ the element of $p^{M_\varphi+1}\mathbf{Z}_p$ such that $\chi(\sigma) = \chi(\sigma)_{M_\varphi} + \chi(\sigma)'_{M_\varphi}$. Then, from above, it holds that

$$\begin{aligned} \left(\sum_{1 \neq \chi: \text{even}} \chi(\sigma)\sigma^{-1} \right) (u \otimes 1) &= \sum_{1 \neq \chi: \text{even}} \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_\varphi} \right) \otimes (\chi(\sigma)_{M_\varphi} + \chi(\sigma)'_{M_\varphi}) \\ &= \sum_{1 \neq \chi: \text{even}} \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_\varphi} \right) \otimes \chi(\sigma)_{M_\varphi} + \sum_{1 \neq \chi: \text{even}} \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_\varphi} \right) \otimes \chi(\sigma)'_{M_\varphi}. \end{aligned}$$

Consequently,

$$\begin{aligned} \log_p \left(\left(\sum_{1 \neq \chi: \text{even}} \chi(\sigma)\sigma^{-1} \right) (u \otimes 1) \right) &= \sum_{1 \neq \chi: \text{even}} \chi(\sigma)_{M_\varphi} \log_p \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_\varphi} \right) \\ &\quad + \sum_{1 \neq \chi: \text{even}} \chi(\sigma)'_{M_\varphi} \log_p \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_\varphi} \right) \\ &\equiv \sum_{1 \neq \chi: \text{even}} \chi(\sigma)_{M_\varphi} \log_p \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_\varphi} \right) \pmod{p^{M_\varphi+1}}. \end{aligned}$$

Because

$$v_\varphi \left(\log_p \left(1 + \frac{x^{\sigma^{-1}}}{a} p^{M_\varphi} \right) \right) = v_\varphi \left(\frac{x^{\sigma^{-1}}}{a} p^{M_\varphi} \right) \geq M_\varphi(p-1),$$

we see that $v_\varphi(\log_p(e_\chi(u \otimes 1))) \geq M_\varphi(p-1)$.

On the other hand, since $e_\chi(u \otimes 1) = \delta_\chi \eta_\chi$, we have, from Lemma 7,

$$\begin{aligned} v_\varphi(\log_p(e_\chi(u \otimes 1))) &= v_\varphi(\delta_\chi) + v_\varphi(\log_p \eta_\chi) \leq v_\varphi(\delta_\chi) + v_\varphi \left(\frac{p}{\tau(\chi)} L_p(1, \chi) \right) \\ &< v_\varphi(\delta_\chi) + M_\varphi(p-1). \end{aligned}$$

So, we have

$$M_\varphi(p-1) < v_\varphi(\delta_\chi) + M_\varphi(p-1).$$

Therefore, $v_\varphi(\delta_\chi) > 0$, so that $\delta_\chi \equiv 0 \pmod{p}$. Now we have proved that

$$E \otimes_{\mathbf{Z}} p\mathbf{Z}_p \ni u \otimes 1 - \delta_\omega(\zeta_p \otimes 1) = u\zeta_p^{-\delta_\omega} \otimes 1 = \psi(u\zeta_p^{-\delta_\omega}).$$

Lemma 1 means that $u\zeta_p^{-\delta_\omega} \in E^p$. Let v be a unit such that $u\zeta_p^{-\delta_\omega} = v^p$ and

$$v = z_0 + z_1(\zeta_p - 1) + \cdots + z_{p-2}(\zeta_p - 1)^{p-2} \quad \text{and} \quad z_0 \not\equiv 0 \pmod{\varphi},$$

where $z_i \in \mathbf{Z}[\zeta_m]$ ($0 \leq i \leq p-2$). Then, $a \equiv u \equiv \zeta_p^{\delta_\omega} v^p \equiv \zeta_p^{\delta_\omega} z_0^p \pmod{p}$. Since $\zeta_p^{\delta_\omega} \equiv a/z_0^p \pmod{p}$ is Δ -invariant, we have $\delta_\omega \equiv 0 \pmod{p}$. As a result, $u \in E^p$ is proved.

Next, we assume $u \not\equiv 1 \pmod{\varphi}$. Then, clearly, $u^{p^f-1} \equiv 1 \pmod{\varphi}$ and further $u^{p^f-1} \equiv a^{p^f-1} \pmod{p^{M_\varphi}}$. From the same discussion as above, u^{p^f-1} is a p th power, and

so is u . The proof of the theorem is completed.

References

- [1] A. BRUMER, On the units of algebraic number fields, *Mathematika* **14** (1967), 121–124.
- [2] E. E. KUMMER, Zwei besondere Untersuchungen über die Classen-Anzahl und über die Einheiten der aus λ ten Wurzeln der Einheit gebildeten complexen Zahlen, *J. Reine Angew. Math.* **40** (1850), 117–129.
- [3] L. C. WASHINGTON, Units of irregular cyclotomic fields, *Illinois J. Math.* **23** (1979), 635–647.
- [4] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, Springer (1982).
- [5] L. C. WASHINGTON, Kummer's lemma for prime power cyclotomic fields, *J. Number Theory* **40** (1992), 165–173.

Present Address:

KANAGAWA PREFECTURAL YAMATO-HIGASHI HIGH-SCHOOL,
1760 FUKAMI, YAMATO, KANAGAWA, 242 JAPAN.