Ichimura, H.
Osaka J. Math.
57 (2020), 949–959

RELATIVE CLASS NUMBERS INSIDE THE pTH CYCLOTOMIC FIELD

HUMIO ICHIMURA

(Received February 7, 2019, revised August 9, 2019)

Abstract

For a prime number $p \equiv 3 \bmod 4$, we write $p = 2n\ell^f + 1$ for some power ℓ^f of an odd prime number ℓ and an odd integer n with $\ell \nmid n$. For $0 \le t \le f$, let K_t be the imaginary subfield of $\mathbb{Q}(\zeta_p)$ of degree $2\ell^t$ and let h_t^- be the relative class number of K_t. We show that for $n = 1$ (resp. $n \ge 3$), a prime number r does not divide the ratio h_t^-/h_{t-1}^- when r is a primitive root modulo ℓ^2 and $r \ge \ell^{f-t} - 1$ (resp. $r \ge (n-2)\ell^{f-t} + 1$). In particular, for $n = 1$ or 3, the ratio h_f^-/h_{f-1}^- at the top is not divisible by r whenever r is a primitive root modulo ℓ^2. Further, we show that the ℓ-part of h_t^-/h_{t-1}^- stabilizes for "large" t under some assumption.

1. Introduction

Let $p \ge 7$ be a prime number with $p \equiv 3 \bmod 4$. Then we can write $p = 2n\ell^f + 1$ for some power ℓ^f of an odd prime number ℓ and an odd integer n with $\ell \nmid n$. (Of course, this expression or the pair (n, ℓ^f) is not uniquely determined for a given p.) As $p \equiv 3 \bmod 4$, the imaginary quadratic field $K_0 = \mathbb{Q}(\sqrt{-p})$ is a subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$. Here, for an integer m, ζ_m denotes a primitive mth root of unity. For each $1 \le t \le f$, let K_t/K_0 be the cyclic extension of degree ℓ^t contained in $\mathbb{Q}(\zeta_p)$. Let h_t^- denote the relative class number of K_t. It is known and easy to see that h_{t-1}^- divides h_t^- (see Hasse [8, Satz 32]). When $f = 1$ and $n = 1$ (resp. $n > 1$), it is shown in Metsänkylä [18, Theorem 1] (resp. [11, Theorem 2]) that h_1^-/h_0^- is not divisible by a prime number r if r is a primitive root modulo ℓ and $r \ge n - 1$. Further, when $f \ge 2$ and $n = 1$, we have shown in [5, Theorem] that the ratio h_f^-/h_{f-1}^- at the top is not divisible by a prime number r whenever r is a primitive root modulo ℓ^2. We generalize these results as follows.

Theorem 1. *Under the above setting, let $p = 2n\ell^f + 1$ be a prime number where ℓ is an odd prime number, $f \ge 1$ and n is an odd integer with $\ell \nmid n$. Let t be an integer with $1 \le t \le f$. Then a prime number r does not divide the ratio h_t^-/h_{t-1}^- under the following two conditions on r.*

(i) *r is a primitive root modulo ℓ^2.*

(ii) *r satisfies the inequality*

$$r \ge \begin{cases} \ell^{f-t} - 1, & \text{if } n = 1, \\ (n-2)\ell^{f-t} + 1, & \text{if } n \ge 3. \end{cases}$$

The following theorem for the case $t = f$ is an immediate consequence of Theorem 1.

2010 Mathematics Subject Classification. Primary 11R29; Secondary 11R18.

Theorem 2. *Under the above setting, the following assertions hold on the ratio* h_f^-/h_{f-1}^- *at the top .*

(I) *A prime number* r *does not divide* h_f^-/h_{f-1}^- *when it satisfies the condition* (i) *in* Theorem 1 *and* $r \geq n-1$.

(II) *For* $n = 1$ *or* 3*, a prime number* r *does not divide* h_f^-/h_{f-1}^- *when it satisfies the condition* (i) *in* Theorem 1.

Let p be a prime number of the special form $p = 2\cdot 3^f + 1$ with $f \geq 2$. When $2 \leq f \leq 325$, it is known that $p = 2\cdot 3^f + 1$ is a prime number for $f = 2, 4, 5, 6, 9, 16, 17, 30, 54, 57, 60, 65, 132, 180, 320$ by Williams and Zarnke [26]. Further, it is a prime number for $f = 1175232$ by Grau, Oller-Marcén and Sadornil [7, page 511]. For such a prime number, the following assertion is also an immediate consequence of Theorem 1.

Proposition 1. *Let* $p = 2\cdot 3^f + 1$ *with* $f \geq 2$*. Then, a prime number* r *does not divide the ratio* h_f^-/h_{f-2}^- *when* $r \equiv 2, 5 \bmod 9$.

As for the ℓ-part of the class numbers h_t^-, we observe that there are several cases where they enjoy Iwasawa type class number "formula" in Example of Lehmer [16, page 607] and in Schoof [21, Appendix]. Such examples are found also in an unpublished table of Ken Yamamura on relative class numbers of imaginary abelian fields of prime power conductors $< 10^4$. For instance, let $(p, \ell, f) = (379, 3, 3)$ or $(751, 5, 3)$, where a triple (p, ℓ, f) means a prime number $p = 2n\ell^f + 1$ with $n = (p-1)/2\ell^f$ and $\ell \nmid n$. Then, accordingly, we have $3^{t+1} \| h_t^-$ or $5^{t+1} \| h_t^-$ for $0 \leq t \leq 3$. We define an integer e_t by $\ell^{e_t} \| h_t^-$ for each $0 \leq t \leq f$. As h_{t-1}^- divides h_t^-, we have $e_t \geq e_{t-1}$. On the integers e_t, the following assertion holds.

Theorem 3. *Under the above setting, let* $f \geq 2$ *and assume that* $e_s - e_{s-1} < \phi(\ell^s)$ *for some* $1 \leq s \leq f-1$*, where* $\phi(*)$ *is the Euler function. Then* $e_t - e_{t-1} = e_s - e_{s-1}$ *for every* t *with* $s \leq t \leq f$.

Under the assumption that the ℓ-part of the ideal class group of K_0 is cyclic, Theorem 3 for the case $s = 1$ is an immediate consequence of [21, Proposition 2.4]. The above two examples satisfy the assumption of Theorem 3 for $s = 1$. Further examples are given at the end of §3 after showing Theorem 3.

Remark 1. (I) The assumption (i) in Theorem 1 is necessary only to assure that the prime number r remains prime in $\mathbb{Q}(\zeta_{\ell^t})$. Therefore, when $t = 1$, we can replace the assumption (i) with the weaker one that

(i') r is a primitive root modulo ℓ.

See Proof of Theorem 1; *the case* $t = 1$ in §3.

(II) Let $n = 1$, and let us fix an odd prime number ℓ such that 2 is a primitive root modulo ℓ^2. Then, for a prime number p of the form $p = 2\ell^f + 1$ with $f \geq 2$, we showed in [12, Propositions 2, 3] that h_{f-1}^-/h_{f-2}^- is odd if p is larger than $(2\ell(\ell-1))^{\ell(\ell-1)}$, and that it is always odd when $\ell = 3$ using some computational data obtained in [5]. In [12], we showed this fact for $\ell = 3$ (namely, Proposition 1 for the case $r = 2$) with a method completely different from the one in this paper.

(III) When $f = 1$, several other results are known on indivisibility of the class number of K_1 or the maximal real subfield K_1^+ such as [3, 4, 6, 13, 15, 19, 22].

REMARK 2. Let ℓ be an odd prime number with $\ell \equiv 3 \bmod 4$. Let Ω_∞ be the cyclotomic $\mathbb{Z}_\ell$-extension over the imaginary quadratic field $\Omega_0 = \mathbb{Q}(\sqrt{-\ell})$. We denote by h_n^* the relative class number of the nth layer Ω_n of Ω_∞/Ω_0. It is a well known theorem of Washington [24] that a prime number $r \neq \ell$ does not divide the ratio h_n^*/h_{n-1}^* for sufficiently large n. Explicit versions of the theorem are given in Horie [9, Theorem 2] and [10, Proposition 2], [14, Proposition 1]. For instance, a prime number r does not divide h_n^* for all $n \geq 0$ when r is a primitive root modulo ℓ^2 and $r \geq (\ell-1)/2 - 2d_\ell$ where d_ℓ is the maximal proper divisor of $(\ell-1)/2$ ([10, Proposition 2]). Our Theorem 1 for the finite tower K_f/K_0 is, in a sense, analogous to these results for the $\mathbb{Z}_\ell$-tower Ω_∞/Ω_0.

For the class numbers in Ω_∞/Ω_0, it is shown in [14, Proposition 2] with the help of computer that r does not divide h_n^*/h_{n-1}^* for all $\ell < 10000$ and all $1 \leq n \leq 100$ whenever r is a primitive root modulo ℓ^2. At present, we have no example of a triple (ℓ, n, r) for which r divides h_n^*/h_{n-1}^* and r is a primitive root modulo ℓ^2. However, in our setting inside the pth cyclotomic field, there do exist some exceptional cases where r divides h_1^-/h_0^- and r is a primitive root modulo ℓ^2. As an example, when $p = 163 = 2 \cdot 3^4 + 1$ and $r = 2$, the ratio h_1^-/h_0^- is even and h_t^-/h_{t-1}^- is odd for $2 \leq t \leq 4$ by a table in [21, Appendix]. As another example, let $p = 2 \cdot 3^{30} + 1$, which is known to be a prime number (see [26]). We have shown in [5, §4] with the help of computer that h_1^-/h_0^- is even but h_t^-/h_{t-1}^- is odd for every $2 \leq t \leq 30$. Even in such exceptional cases, Theorem 2 says that r never divides the ratio at the top when r is a primitive root modulo ℓ^2 (and $r \geq n-1$).

2. Bernoulli numbers

For an odd Dirichlet character χ of conductor d, we denote by

$$\beta_\chi = \frac{1}{2} B_{1,\chi} = \frac{1}{2d} \sum_{a=1}^{d-1} a\chi(a)$$

the *half* of the generalized Bernoulli number. We let $p = 2n\ell^f + 1$ be as in §1, and we use the same notation as in §1. We denote by δ the quadratic character associated to the imaginary quadratic field $K_0 = \mathbb{Q}(\sqrt{-p})$. For each $1 \leq t \leq f$, we have

$$(1) \qquad h_t^-/h_{t-1}^- = p^\alpha \prod_{\varphi_t} (-\beta_{\delta\varphi_t})$$

by the analytic class number formula (Washington [25, Theorem 4.17]) where φ_t runs over the even Dirichlet characters of conductor p and order ℓ^t and $\alpha = 1$ or 0 according as $(n, t) = (1, f)$ or not. Here, we have used the fact that the unit index of an imaginary abelian field of conductor p is 1 ([8, Satz 23]). The proofs of our assertions are based on the class number formula (1).

We fix a primitive root g modulo p. We easily see that the set $\pm g^{2(\ell^f w + nv)}$ with $0 \leq w \leq n-1$ and $0 \leq v \leq \ell^f - 1$ is a complete set of representatives of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. For an integer $x \in \mathbb{Z}$, let $s_p(x)$ denote the unique integer such that $s_p(x) \equiv x \bmod p$ and $0 \leq s_p(x) \leq p-1$. We see that

$$(2) \qquad s_p(-x) = p - s_p(x)$$

for x with $p \nmid x$. In all what follows, we put

$$\zeta_{\ell^t} = \varphi_t(g^{2n}), \tag{3}$$

which is a primitive ℓ^tth root of unity. Then, noting that the quadratic character δ is odd and using (2), we observe that

$$\begin{aligned}\beta_{\delta\varphi_t} &= \frac{1}{2p}\sum_{w=0}^{n-1}\sum_{v=0}^{\ell^f-1}\left(s_p(g^{2(\ell^f w+nv)}) - s_p(-g^{2(\ell^f w+nv)})\right)\zeta_{\ell^t}^v \\ &= \frac{1}{2p}\sum_{w=0}^{n-1}\sum_{v=0}^{\ell^f-1}\left(2s_p(g^{2(\ell^f w+nv)}) - p\right)\zeta_{\ell^t}^v \\ &= \frac{1}{p}\sum_{v=0}^{\ell^f-1}\sum_{w=0}^{n-1} s_p(g^{2(\ell^f w+nv)})\zeta_{\ell^t}^v - \frac{n}{2}\sum_{v=0}^{\ell^f-1}\zeta_{\ell^t}^v.\end{aligned}$$

We see that the last sum vanishes as $t \geq 1$, and hence we obtain

$$\beta_{\delta\varphi_t} = \frac{1}{p}\sum_{v=0}^{\ell^f-1}\left(\sum_{w=0}^{n-1} s_p(g^{2\ell^f w+2nv})\right)\zeta_{\ell^t}^v. \tag{4}$$

3. Proofs of Theorems 1 and 3

In this section, we first prove Theorem 1 after showing some preliminary lemmas, and give a related proposition. The proof of Theorem 3 is given at the end of the section.

Let $p = 2n\ell^f + 1$ be as in §1, and we use the same notation as in the previous sections. To prove Theorem 1, we may as well assume that $f \geq 2$ because, as we mentioned in §1, Theorem 1 for the case $f = 1$ is already settled in [11, 18]. Further, we may as well assume that $n > 1$ or $f - t \geq 1$, or equivalently that

$$n\ell^{f-t} > 1 \tag{5}$$

because Theorem 1 for the case $n = 1$ and $t = f$ (≥ 2) is already shown in [5, Theorem]. For $1 \leq t \leq f$, let $E_t = \mathbb{Q}(\zeta_{\ell^t})$ so that $\beta_{\delta\varphi_t} \in E_t$. The condition $n\ell^{f-t} > 1$ implies that the order of the character $\delta\varphi_t$ does not equal $p - 1 = 2n\ell^f$. Hence, $\beta_{\delta\varphi_t}$ is an algebraic integer of E_t by [8, Satz 32]. Let $\zeta_{\ell^t} = \varphi_t(g^{2n})$ be as in (3). Let $\mathcal{O}_t$ be the ring of algebraic integers of E_t.

First, we show Theorem 1 for the case $t \geq 2$. Since $\beta_{\delta\varphi_t} \in \mathcal{O}_t$ and the set $\zeta_{\ell^t}^j$ with $0 \leq j \leq \ell^{t-1} - 1$ constitutes a free basis of $\mathcal{O}_t$ over $\mathcal{O}_1$, we can uniquely write

$$\beta_{\delta\varphi_t} = \sum_{j=0}^{\ell^{t-1}-1} a_j\zeta_{\ell^t}^j \tag{6}$$

for some $a_j \in \mathcal{O}_1$. For u and j_0 with $0 \leq u \leq \ell - 1$ and $0 \leq j_0 \leq \ell^{t-1} - 1$, we put

$$x_u^{(j_0)} = \frac{1}{p}\sum_{v=0}^{\ell^{f-t}-1}\sum_{w=0}^{n-1} s_p\left(g^{2\ell^f w+2n(\ell^t v+\ell^{t-1}u+j_0)}\right), \tag{7}$$

and

$$y_u^{(j_0)} = \begin{cases} x_u^{(j_0)} - 1, & \text{if } n = 1, \\ x_u^{(j_0)} - \ell^{f-t}, & \text{if } n \geq 3. \end{cases}$$

Lemma 1. *The rational $y_u^{(j_0)}$ is an integer and satisfies the inequality:*

$$0 \leq y_u^{(j_0)} \leq \begin{cases} \ell^{f-t} - 2, & \text{if } n = 1, \\ (n-2)\ell^{f-t}, & \text{if } n \geq 3. \end{cases}$$

Proof. We see that $x_u^{(j_0)} \in \mathbb{Z}$ because $n\ell^{f-t} > 1$ by the assumption (5) and the elements $g^{2\ell^f w + 2n\ell^t v}$ mod p in the sum (7) are all the $n\ell^{f-t}$th roots of unity in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. It follows that

$$1 \leq x_u^{(j_0)} \leq n\ell^{f-t} - 1$$

and hence, in particular, the assertion for the case $n = 1$ is settled. Let us deal with the case $n \geq 3$. In this case, we observe from (7) that

$$x_u^{(j_0)} = \sum_{v=0}^{\ell^{f-t}-1} x_{u,j_0,v} \quad \text{with} \quad x_{u,j_0,v} = \frac{1}{p}\sum_{w=0}^{n-1} s_p\left(g^{2\ell^f w + 2n(\ell^t v + \ell^{t-1}u + j_0)}\right).$$

In the last sum, since the elements $g^{2\ell^f w}$ mod p with $0 \leq w \leq n-1$ run over the nth roots of unity in $(\mathbb{Z}/p\mathbb{Z})^\times$, we see that $x_{u,j_0,v} \in \mathbb{Z}$. It follows that

$$1 \leq x_{u,j_0,v} \leq n-1 \quad \text{and hence} \quad \ell^{f-t} \leq x_u^{(j_0)} \leq (n-1)\ell^{f-t}.$$

From this, we obtain the assertion for the case $n \geq 3$. □

For integers t and j_0 with $2 \leq t \leq f$ and $0 \leq j_0 \leq \ell^{t-1} - 1$, we define polynomials G_{t,j_0} and F_{t,j_0} in $\mathbb{Z}[T]$ by

$$G_{t,j_0} = G_{t,j_0}(T) = \sum_{u=0}^{\ell-1} x_u^{(j_0)} T^u \quad \text{and} \quad F_{t,j_0} = F_{t,j_0}(T) = \sum_{u=0}^{\ell-1} y_u^{(j_0)} T^u,$$

respectively. We put $\zeta_\ell = \zeta_{\ell^t}^{\ell^{t-1}} = \varphi_t(g^{2n\ell^{t-1}})$.

Lemma 2. *Under the above setting and notation, we have*

$$a_{j_0} = G_{t,j_0}(\zeta_\ell) = F_{t,j_0}(\zeta_\ell).$$

Proof. Let j_0 be an integer with $0 \leq j_0 \leq \ell^{t-1} - 1$. We see from (4) and (6) that

$$\zeta_{\ell^t}^{-j_0}\beta_{\delta\varphi_t} = \sum_{j=0}^{\ell^{t-1}-1} a_j \zeta_{\ell^t}^{j-j_0} = \frac{1}{p}\sum_{v=0}^{\ell^f-1}\left(\sum_{w=0}^{n-1} s_p\left(g^{2\ell^f w + 2nv}\right)\right)\zeta_{\ell^t}^{v-j_0}. \tag{8}$$

For an ℓ^tth root ζ of unity, we have $\mathrm{Tr}_{E_t/E_1}(\zeta) = \ell^{t-1}\zeta$ or 0 according as $\zeta^\ell = 1$ or not, where Tr denotes the trace map. Hence, it follows from the first equality of (8) that

$$\ell^{t-1}a_{j_0} = \mathrm{Tr}_{E_t/E_1}\left(\zeta_{\ell^t}^{-j_0}\beta_{\delta\varphi_t}\right) \tag{9}$$

because $-(\ell^{t-1} - 1) \leq j - j_0 \leq \ell^{t-1} - 1$. In the third term of (8), $\zeta_{\ell^t}^{v-j_0}$ is an ℓth root of unity if and only if $v - j_0$ is a multiple of ℓ^{t-1}. Hence, writing $v - j_0 = \ell^{t-1}\mu$ with $0 \leq \mu \leq \ell^{f-t+1} - 1$ for such v, we observe that

$$\mathrm{Tr}_{E_t/E_1}(\zeta_{\ell^t}^{-j_0}\beta_{\delta\varphi_t}) = \frac{\ell^{t-1}}{p}\sum_{\mu=0}^{\ell^{f-t+1}-1}\left(\sum_{w=0}^{n-1}s_p\left(g^{2\ell^f w+2n(\ell^{t-1}\mu+j_0)}\right)\right)\zeta_\ell^\mu.$$

Finally, writing $\mu = \ell v + u$ with $0 \le v \le \ell^{f-t}-1$ and $0 \le u \le \ell-1$, we obtain

$$\begin{aligned}(10)\qquad \mathrm{Tr}_{E_t/E_1}(\zeta_{\ell^t}^{-j_0}\beta_{\delta\varphi_t}) &= \frac{\ell^{t-1}}{p}\sum_{u=0}^{\ell-1}\left(\sum_{v=0}^{\ell^{f-t}-1}\sum_{w=0}^{n-1}s_p\left(g^{2\ell^f w+2n(\ell^t v+\ell^{t-1}u+j_0)}\right)\right)\zeta_\ell^u \\ &= \ell^{t-1}G_{t,j_0}(\zeta_\ell) = \ell^{t-1}F_{t,j_0}(\zeta_\ell).\end{aligned}$$

The assertion follows from (9) and (10). □

We denote by $\Phi_\ell = \Phi_\ell(T)$ the ℓth cyclotomic polynomial. For a prime number r and a polynomial $G(T) \in \mathbb{Z}[T]$, let $\tilde{G}(T) = G(T) \bmod r \in \mathbb{F}_r[T]$ where $\mathbb{F}_r$ is the finite field with r elements.

Lemma 3. *Under the above setting, let r be a prime number satisfying the condition* (ii) *in* Theorem 1. *Then, there exists some j_0 such that $\tilde{F}_{t,j_0}(T)$ is not a multiple of $\tilde{\Phi}_\ell(T)$ in $\mathbb{F}_r[T]$.*

Proof. It is well known that $\beta_{\delta\varphi_t} \ne 0$ (see [25, page 38]). This implies that in the formula (6), $a_{j_0} \ne 0$ for some j_0. For this j_0, we see from Lemma 2 that $y_0^{(j_0)} \ne y_u^{(j_0)}$ for some $1 \le u \le \ell-1$. For this pair (j_0, u), it follows from Lemma 1 that

$$1 \le |y_0^{(j_0)} - y_u^{(j_0)}| \le \begin{cases} \ell^{f-t}-2, & \text{if } n = 1, \\ (n-2)\ell^{f-t}, & \text{if } n \ge 3. \end{cases}$$

If $F_{t,j_0} \equiv c\Phi_\ell \bmod r$ for some constant c, then $y_0^{(j_0)} - y_u^{(j_0)}$ is a multiple of r. Hence, it follows from the above inequality that $r \le \ell^{f-t}-2$ or $r \le (n-2)\ell^{f-t}$ according as $n = 1$ or $n \ge 3$. Thus we obtain the assertion. □

Proof of Theorem 1; the case $t \ge 2$. Let r be a prime number satisfying the conditions (i) and (ii) of Theorem 1. Assume that r divides h_t^-/h_{t-1}^-. Then it follows from (1) that

$$\beta_{\delta\varphi_t} \equiv 0 \bmod r\mathcal{O}_t$$

because r remains prime in E_t by the condition (i). Hence, by (6), we have $a_{j_0} \equiv 0 \bmod r\mathcal{O}_1$ for all j_0. On the other hand, $\tilde{\Phi}_\ell(T)$ is irreducible over $\mathbb{F}_r$ as r is a primitive root modulo ℓ. Therefore, we observe from Lemma 2 that $\tilde{F}_{t,j_0}(T)$ is a multiple of $\tilde{\Phi}_\ell(T)$ for all j_0, which contradicts Lemma 3. □

Next, let us show Theorem 1 for the case $t = 1$. In (4), rewriting v with $\ell v + u$ with $0 \le v \le \ell^{f-1}-1$ and $0 \le u \le \ell-1$, we see that

$$(11)\qquad \beta_{\delta\varphi_1} = \frac{1}{p}\sum_{u=0}^{\ell-1}\left(\sum_{v=0}^{\ell^{f-1}-1}\sum_{w=0}^{n-1}s_p\left(g^{2\ell^f w+2n\ell v+2nu}\right)\right)\zeta_\ell^u \in E_1.$$

For each $0 \le u \le \ell-1$, we put

(12) $$x_u = \frac{1}{p} \sum_{v=0}^{\ell^{f-1}-1} \sum_{w=0}^{n-1} s_p\left(g^{2\ell^f w + 2n\ell v + 2nu}\right)$$

and

$$y_u = \begin{cases} x_u - 1, & \text{if } n = 1, \\ x_u - \ell^{f-1}, & \text{if } n \geq 3. \end{cases}$$

Similarly to Lemma 1, we can show the following assertion using the assumption (5) with $t = 1$.

Lemma 4. *Under the above setting, the rational y_u is an integer and satisfies*

$$0 \leq y_u \leq \begin{cases} \ell^{f-1} - 2, & \text{if } n = 1, \\ (n-2)\ell^{f-1}, & \text{if } n \geq 3. \end{cases}$$

We define polynomials G_1 and F_1 in $\mathbb{Z}[T]$ by

$$G_1 = G_1(T) = \sum_{u=0}^{\ell-1} x_u T^u \quad \text{and} \quad F_1 = F_1(T) = \sum_{u=0}^{\ell-1} y_u T^u,$$

respectively. Then, by (11) and (12), we have

(13) $$\beta_{\delta\varphi_1} = G_1(\zeta_\ell) = F_1(\zeta_\ell).$$

Similarly to Lemma 3, we can show the following assertion using Lemma 4 and the fact $\beta_{\delta\varphi_1} \neq 0$.

Lemma 5. *Under the above setting, let r be a prime number satisfying the condition* (ii) *in* Theorem 1 *with $t = 1$. Then, $\tilde{F}_1(T)$ is not a multiple of $\tilde{\Phi}_\ell(T)$ in $\mathbb{F}_r[T]$.*

Proof of Theorem 1; the case $t = 1$. Let r be a prime number satisfying the condition (i') in Remark 1(I) and the condition (ii) in Theorem 1 with $t = 1$. Assume that r divides h_1^-/h_0^-. Then, it follows from (1) that $\beta_{\delta\varphi_1} \equiv 0 \bmod r\mathcal{O}_1$ because r remains prime in E_1 by (i'). By (13), this implies that $\tilde{F}_1(T)$ is a multiple of $\tilde{\Phi}_\ell(T)$ because $\tilde{\Phi}_\ell$ is irreducible over $\mathbb{F}_r$ by (i'). Thus we obtain the assertion from Lemma 5. □

Denote by h_t^+ the class number of the maximal real subfield K_t^+ of K_t in the usual sense. Similarly to the relative class numbers, we see that h_{t-1}^+ divides h_t^+. It is known that h_t^+/h_{t-1}^+ is odd if h_t^-/h_{t-1}^- is odd ([12, Lemma 1]). Hence, for $n = 1$ or 3, it follows from Theorem 2 that h_f^+/h_{f-1}^+ is odd when 2 is a primitive root modulo ℓ^2. We can slightly relax the assumption of this assertion as follows.

Proposition 2. *Let $n = 1$ or 3. Let ℓ be an odd prime number with $\ell \equiv 3 \bmod 4$, and assume that the order of the class 2 modulo ℓ^2 in the multiplicative group $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$ is $(\ell-1)\ell/2$. Then h_f^+/h_{f-1}^+ is odd.*

Proof. When $n = 1$, we already showed the assertion in [12, Proposition 1] effectively using the fact that $\tilde{G}_{f,j_0}$ is not a multiple of $\tilde{\Phi}_\ell$ in $\mathbb{F}_2[T]$ for some j_0 ([12, Lemma 3]) and a theorem of Cornacchia [2, Theorem 1] on class number parity of the cyclotomic fields of prime conductor. When $n = 3$, we can show the assertion exactly in the same way using Lemma 3. □

Proof of Theorem 3. In view of (4), we put

$$g(T) = \sum_{v=0}^{\ell^f-1}\left(\sum_{w=0}^{n-1} s_p(g^{2\ell^f w+2nv})\right)(1+T)^v \tag{14}$$

$$= c_0 + c_1T + \cdots + c_{\ell^f-1}T^{\ell^f-1} \in \mathbb{Z}[T].$$

By (4), we have

$$\beta_{\delta\varphi_t} = \frac{1}{2}B_{1,\delta\varphi_t} = \frac{1}{p}\, g(\zeta_{\ell^t}-1) \quad \text{with} \quad \zeta_{\ell^t} = \varphi_t(g^{2n}). \tag{15}$$

If c_0 is not divisible by ℓ, we see from (1), (14) and (15) that $\ell \nmid h_t^-/h_{t-1}^-$ for every t, and we have nothing to do. Therefore, we let $\ell|c_0$. We put $m_t = e_t - e_{t-1}$ for brevity, so that we have $\ell^{m_t}||h_t^-/h_{t-1}^-$. Assume that $m_s < \phi(\ell^s)$ for some $1 \le s \le f-1$. If c_i were divisible by ℓ for all $0 \le i \le \phi(\ell^s)-1$, then it would follow that $\beta_{\delta\varphi_s} \equiv 0 \bmod \ell$ from (14) and (15), and hence $m_s \ge \phi(\ell^s)$ by (1). Therefore, we see that there exists some $1 \le k \le \phi(\ell^s)-1$ for which $\ell|c_i$ for all $0 \le i \le k-1$ and $\ell \nmid c_k$. Then we observe from (14) and (15) that for every t with $s \le t \le f$, $\beta_{1,\varphi_t} = (\zeta_{\ell^t}-1)^k \times x_t$ with some ℓ-adic unit x_t. By (1), this implies that $m_t = k$ for $s \le t \le f$. □

Example 1. When $(p,\ell,f) = (81163, 3, 5)$, we find that $h_0^- = 39$ in the table of Wada and Saito [23] on the class number of imaginary quadratic fields $\mathbb{Q}(\sqrt{-m})$ for $m < 10^5$. As h_0^- is divisible by 3, so is h_1^-/h_0^- by [16, Theorem 5]. Shoich Fujima kindly computed the values x_u defined in (12) at the request of the author. The values are 6571, 6740 and 6780 for $u = 0$, 1 and 2, respectively, with a primitive root $g = 2$. It follows from (11) that $\beta_{\delta\varphi_1} \equiv 1-\zeta_3 \bmod 3$. Hence, $3||h_1^-/h_0^-$ by (1). Therefore, we see from Theorem 3 with $s = 1$ that $3||h_t^-/h_{t-1}^-$ for all $1 \le t \le 5$.

The referee kindly supplied us with the following examples. When $(p,\ell,f) = (131707, 3, 5)$, $(e_0,e_1,e_2,e_3,e_4,e_5)$ equals $(1,3,8,13,18,23)$ and the assumption of Theorem 3 is satisfied with $s = 2$. Further, for $(p,\ell,f) = (1051639, 7, 4)$, $(365251, 5, 3)$ and $(7860079, 3, 8)$, e_i's are equal to

$$(1,4,7,10,13), \quad (1,5,9,13), \quad \text{and} \quad (3,7,17,25,33,41,49,57,65)$$

and the assumption is satisfied with $s = 1$, $s = 2$ and $s = 3$, respectively. These examples are obtained by using PARI/GP [27].

4. Several related results

In this section, we give some other results on the ratio h_t^-/h_{t-1}^- using the following assertion of Ramaré [20, Corollary 1] on Bernoulli numbers. We put

$$\varpi_p = \frac{\log p + \kappa}{4\pi}\sqrt{p} \quad \text{with} \quad \kappa = 5 - 2\log 6 = 1.416481\cdots$$

for each odd prime number p.

Lemma 6 (Ramaré)**.** *The inequality $|\beta_\chi| \le \varpi_p$ holds for an odd prime number p and every odd Dirichlet character χ of conductor p.*

A result quite similar to Lemma 6 is also given in Louboutin [17, Theorem 1].

Let $p = 2n\ell^f + 1$ be as in §1, and we use the same notation as in the previous sections. The following assertion is sharper (resp. weaker) than Theorem 1, roughly speaking when $t < f/2$ (resp. $t > f/2$).

Proposition 3. *Under the above setting, a prime number r does not divide the ratio h_t^-/h_{t-1}^- for all t with $1 \leq t \leq f$ when r satisfies the condition* (i) *in* Theorem 1 *and the inequality $r > \varpi_p$.*

Proof of Proposition 3. Assume that r divides h_t^-/h_{t-1}^- for some t with $1 \leq t \leq f$. Then, since r remains prime in $E_t = \mathbb{Q}(\zeta_{\ell^t})$, we observe from (1) that $r^{\phi(\ell^t)}$ divides h_t^-/h_{t-1}^-, where $\phi(*)$ denotes the Euler function. On the other hand, we see from Lemma 6 and (1) that the r-part of h_t^-/h_{t-1}^- is smaller than or equals to $\varpi_p^{\phi(\ell^t)}$. Therefore, we obtain the assertion. □

The following assertion is an immediate consequence of Lemma 6 and the class number formula for the imaginary quadratic field $K_0 = \mathbb{Q}(\sqrt{-p})$ ([25, Theorem 4.17]).

Lemma 7. *Under the above setting, a prime number r does not divide h_0^- when $r > 2\varpi_p$.*

When $n > 1$, Proposition 3 is an assertion on the relative class number of a proper subfield of $\mathbb{Q}(\zeta_p)$. However, in a special setting where $n = r^e$ is a power of an odd prime number r, we can derive assertions on h_p^- as follows.

Proposition 4. *Let $p = 2r^e\ell^f + 1$ be a prime number where r and ℓ are different odd prime numbers and $e, f \geq 1$. Then r does not divide h_p^- when r satisfies the condition* (i) *in* Theorem 1 *and the inequality $r > 2\varpi_p$.*

Proposition 5. *Let $p = 2r\ell + 1$ be a prime number where r and ℓ are different odd prime numbers, and assume that r is a primitive root modulo ℓ (the condition* (i') *in Remark 1(I)). Then r divides h_p^- if and only if it divides h_0^-.*

Proof of Proposition 4. We see from Proposition 3 and Lemma 7 that r does not divide the relative class number h_f^- of K_f. As $[\mathbb{Q}(\zeta_p) : K_f] = r^e$, the condition $r \nmid h_f^-$ is equivalent to $r \nmid h_p^-$ by [16, Theorem 5]. Hence, we obtain the assertion. □

Proof of Proposition 5. We see that r does not divide h_1^-/h_0^- from Theorem 2 (I) noting that $r \geq r - 1 = n - 1$ under the notation in Theorem 2. Thus, the relative class number h_1^- is divisible by r if and only if so is h_0^-. As $[\mathbb{Q}(\zeta_p) : K_1] = r$, we obtain the assertion by [16, Theorem 5]. □

In [1, Proposition 3.2], Agoh showed that $r \nmid h_p^-$ for any prime number p of the form $p = 4r + 1$ where r is a prime number with $r \equiv 3 \bmod 4$. We can give similar type of assertions using Lemma 7 and Proposition 5 as follows.

Example 2. (I) Let $p = 6r + 1$; the case $\ell = 3$ in Proposition 5. Let r be an odd prime number such that $r \equiv 2 \bmod 3$ and $p = 6r + 1$ is a prime number; $r = 5, 11, 17, 23, 47, \cdots$. By Lemma 7, we have $r \nmid h_0^-$ when

$$r = \frac{p-1}{6} > 2\varpi_p = \frac{\log p + \kappa}{2\pi}\sqrt{p}. \tag{16}$$

Then it follows from Proposition 5 that $r \nmid h_p^-$. We can show that (16) is satisfied when $p = 6r + 1 > 25$ in an elementary way. The minimal case where $r = 5$ and $p = 31$ satisfies the last inequality. Hence, we see that $r \nmid h_p^-$ for $p = 6r + 1$ whenever $r \equiv 2 \bmod 3$.

(II) Let $p = 10r + 1$; the case $\ell = 5$ in Proposition 5. The prime numbers r with $r \equiv 2, 3 \bmod 5$ for which $p = 10r + 1$ is a prime number are $r = 3, 7, 13, 43, 97, \cdots$. Using Lemma 7 and Proposition 5 for this type of p, we see that among such r, $r \nmid h_0^-$ and hence $r \nmid h_p^-$ for $r \geq 13$ in a way similar to (I). For $r = 3$ or 7, we have $h_0^- = r$ (and $h_1^-/h_0^- = 1$) from the table [21, Appendix].

(III) Let $p = 14r + 1$; the case $\ell = 7$ in Proposition 5. The prime numbers r with $r \equiv 3, 5 \bmod 7$ for which $p = 14r + 1$ is a prime number are $3, 5, 17, 47, 59, \cdots$. Again using Lemma 7 and Proposition 5, we see that among such r, $r \nmid h_0^-$ and hence $r \nmid h_p^-$ for $r \geq 47$. For $r = 3, 5$ or 17, we see that $r \nmid h_0^-$ from [21, Appendix], and hence that $r \nmid h_p^-$ by Proposition 5. Therefore, $r \nmid h_p^-$ for $p = 14r + 1$ when r satisfies $r \equiv 3, 5 \bmod 7$.

Acknowledgements. The author is grateful to S. Fujima for computing the values of x_u in Example 1. In the first version of the paper, Theorem 3 is given only for the case $s = 1$. The author thanks to the anonymous referee for suggesting him to include the case $s > 1$ in Theorem 3 and for supplying him with several impressive examples for Theorem 3.

References

[1] T. Agoh: *On the relative class number of special cyclotomic fields*, Math. Appl. **1** (2012), 1–12.

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

[3] D. Davis: *Computing the number of totally positive circular units which are squares*, J. Number Theory **10** (1978), 1–9.

[4] D.R. Estes: *On the parity of the class number of the field of qth roots of unity*, Rocky Mountain J. Math. **19** (1989), 675–682.

[5] S. Fujima and H. Ichimura: *Note on the class number of the pth cyclotomic field*, Funct. Approx. Comment. Math. **52** (2015), 299–309.

[6] S. Fujima and H. Ichimura: *Note on the class number of the pth cyclotomic field, II*, Exp. Math. **27** (2018), 111–118.

[7] J.M. Grau, A.M. Oller-Marcén and D. Sadornil: *A primarity test for $Kp^n + 1$ numbers*, Math. Comp. **84** (2015), 505–512.

[8] H. Hasse: Über die Klassenzahl abelscher Zahlkörper, Akademia Verlag, Berlin, 1952. Reprinted with an introduction by J. Martine, Springer, Berlin, 1985.

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

[10] H. Ichimura: *A note on the relative class number of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\sqrt{-p})$, II*, Proc. Japan Acad. Ser. A **89** (2013), 21–23.

[11] H. Ichimura: *Note on Bernoulli numbers associated to some Dirichlet character of prime conductor*, Arch. Math. (Basel) **107** (2016), 595–601.

[12] H. Ichimura: *Note on the class number of the pth cyclotomic field, III*, Funct. Approx. Comment. Math. **57** (2017), 93–103.

[13] H. Ichimura: *Triviality of Iwasawa module associated to some abelian fields of prime conductors*, Abh. Math. Semin. Univ. Hambg. **88** (2018), 51–66.

[14] H. Ichimura and S. Nakajima: *A note on the relative class number of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\sqrt{-p})$*, Proc. Japan Acad. Ser. A **88** (2012), 16–20.

[15] S. Jakubec, M. Pasteka and A. Schinzel: *Class number of real Abelian fields*, J. Number Theory **148** (2015), 365–371.
[16] D.H. Lehmer: *Prime factors of cyclotomic class numbers*, Math. Comp. **31** (1977), 599–607.
[17] S.R. Louboutin: *Lower bounds for relative class numbers of imaginary abelian number fields and CM fields*, Acta Arith. **121** (2006), 199–220.
[18] T. Metsänkylä: *Some divisibility results for the cyclotomic class number*, Tatra Mt. Math. Publ. **11** (1997), 59–68.
[19] T. Metsänkylä: *An application of the p-adic class number formula*, Manuscripta Math. **93** (1997), 481–498.
[20] O. Ramaré: *Approximate formulae for* $L(1,\chi)$, Acta Arith. **100** (2001), 245–266.
[21] R. Schoof: *Minus class groups of the fields of the* ℓ*th roots of unity*, Math. Comp. **67** (1998), 1225–1245.
[22] P. Stevenhagen: *Class number parity for the pth cyclotomic field*, Math. Comp. **63** (1994), 773–784.
[23] H. Wada and M. Saito: A Table of Ideal Class Groups of Imaginary Quadratic Fields, Sophia Kokyuroku in Mathematics **28**, Sophia Univ., Tokyo, 1988.
[24] L.C. Washington: *The non-p-part of the class number in a cyclotomic* $\mathbb{Z}_p$*-extension*, Invent. Math. **49** (1978), 87–97.
[25] L.C. Washington: Introduction to Cyclotomic Fields, second edition, Springer, New York, 1997.
[26] H.C. Williams and C.R. Zarnke: *Some prime numbers of the forms* $2A3^n + 1$ *and* $2A3^n - 1$, Math. Comp. **26** (1972), 995–998.
[27] The PARI Group, PARI/GP version 2.12.0, Bordeaux, 2019, http://pari.math-u.bordeaux.fr/.

Faculty of Science
Ibaraki University
Bunkyo 2–1–1, Mito, 310–8512
Japan
e-mail: humio.ichimura.sci@vc.ibaraki.ac.jp