Functiones et Approximatio
52.2 (2015), 299–309
doi: 10.7169/facm/2015.52.2.8

NOTE ON THE CLASS NUMBER OF THE pTH CYCLOTOMIC FIELD

Shoichi Fujima, Humio Ichimura

Abstract: Let p be a prime number of the form $p = 2\ell^f + 1$ with an odd prime number ℓ, and h_p^- the relative class number of the pth cyclotomic field $K = \mathbb{Q}(\zeta_p)$. When $f = 1$, it is conjectured that h_p^- is odd, and there are several results related to this conjecture. In this paper, we deal with the case $f \geqslant 2$. For $0 \leqslant t \leqslant f$, let $h_{p,t}^-$ denote the relative class number of the imaginary subfield K_t of K of degree $2\ell^t$ over $\mathbb{Q}$. We show that the ratio $h_{p,f}^-/h_{p,f-1}^-$ is not divisible by a prime number r if r is a primitive root modulo ℓ^2. Further, when $r \leqslant 47$, we give some computational results on the ratio $h_{p,t}^-/h_{p,t-1}^-$ for $1 \leqslant t \leqslant f$. In the range of our computation, we find that the ratio is divisible by r only in some exceptional cases.

Keywords: relative class number, cyclotomic field, computation.

1. Introduction

Let p be an odd prime number. Let $K = \mathbb{Q}(\zeta_p)$ be the pth cyclotomic field, and h_p^- the relative class number of K. Here, for an integer $m \geqslant 2$, ζ_m denotes a primitive mth root of unity. Consider for a while, a prime number of the form $p = 2\ell + 1$ with ℓ an odd prime number. Then it is conjectured that h_p^- is odd with many numerical examples and it is known that h_p^- is odd if 2 is a primitive root modulo ℓ. For these, see the papers of Davis [3], Estes [4] and Stevenhagen [11]. Further, Metsänkylä [9, Theorem 1] proved more generally that for a prime number r, the ratio $h_p^-/h_{\mathbb{Q}(\sqrt{-p})}$ is not divisible by r if r is a primitive root modulo ℓ, where $h_{\mathbb{Q}(\sqrt{-p})}$ is the class number of $\mathbb{Q}(\sqrt{-p})$. (This contains the result for the case $r = 2$ since $h_{\mathbb{Q}(\sqrt{-p})}$ is odd.)

In this paper, we deal with a prime number p of the form $p = 2\ell^f + 1$ for $f \geqslant 2$ with an odd prime number ℓ. For each odd f, it is conjectured that there exist infinitely many prime numbers p of this form. For this, see Bateman and Horn [1]. When f is even, we easily see that $p = 2\ell^f + 1$ can be a prime number only for the case $\ell = 3$. For instance, it is known that h_p^- is even when $p = 163 = 2 \cdot 3^4 + 1$. Thus an exact analogue of the classical conjecture for the case $f = 1$ ($p = 2\ell + 1$)

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

does not hold in general. For $0 \leqslant t \leqslant f$, denote by K_t the imaginary subfield of K of degree $2\ell^t$ over $\mathbb{Q}$, and by $h^-_{p,t}$ the relative class number of K_t. Thus we have $K_f = K$, $K_0 = \mathbb{Q}(\sqrt{-p})$ and $h^-_{p,f} = h^-_p$. We can easily show that $h^-_{p,t-1}$ divides $h^-_{p,t}$ using class field theory or the analytic class number formula (see the formula (4) in Section 2). In this paper, we study the ratio $h^-_{p,t}/h^-_{p,t-1}$ (and not the whole class number h^-_p). When $p = 163 = 2 \cdot 3^4 + 1$, the ratio $h^-_{p,1}/h^-_{p,0}$ is even but $h^-_{p,t}/h^-_{p,t-1}$ is odd for $2 \leqslant t \leqslant 4$. For this, see for instance, the table of Yamamura [14] on the relative class number of $\mathbb{Q}(\zeta_{p^{n+1}})$ for $p^{n+1} < 10000$. First, we show the following analogue of the above mentioned theorem of Metsänkylä.

Theorem. *Let $f \geqslant 2$ be an integer, and r a prime number. Let $p = 2\ell^f + 1$ be a prime number with an odd prime number $\ell \neq r$. Then r does not divide the ratio $h^-_{p,f}/h^-_{p,f-1}$ if r is a primitive root modulo ℓ^2.*

To show this theorem, we give a necessary and sufficient condition for $r \nmid h^-_{p,t}/h^-_{p,t-1}$ $(1 \leqslant t \leqslant f)$. The condition is given in terms of some polynomials related to a trace of Bernoulli numbers. It is of classical nature dating back to the paper of Washington [12] on the non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension, and is quite analogous to the ones given in [5, Lemma 12] and [6, Lemma 4]. Using the condition, we checked whether or not the ratio $h^-_{p,t}/h^-_{p,t-1}$ is divisible by r for several couples (f, ℓ) and prime numbers r with $r \leqslant 47$ and $r \neq \ell$. The computational results are summarized in Section 4. In the range of our computation, we found (i) that $r \nmid h^-_{p,f}/h^-_{p,f-1}$ even when r is not a primitive root modulo ℓ^2 and (ii) that $h^-_{p,t}/h^-_{p,t-1}$ is divisible by r only in some exceptional cases. The above theorem and the computation are quite analogous to the results for the classical situation where $r = 2$ and $f = 1$ $(p = 2\ell + 1)$.

Remark 1. Several results are obtained on the divisibility of the class number of a subfield of the real abelian field $\mathbb{Q}(\zeta_p)^+$. See for instance, Jakubec [8], Metsänkylä [10] and Yoshino [15].

2. Analytic class number formula

We fix an integer $f \geqslant 2$ and a prime number r. Let $p = 2\ell^f + 1$ be a prime number with an odd prime number $\ell \neq r$. In all what follows, we assume that $p \neq r$. (For this, see Remark 3 at the end of this section.) We put $t_0 = \mathrm{ord}_\ell(r^{\ell-1} - 1)$. For an integer $x \in \mathbb{Z}$, denote by $s_p(x)$ the unique integer satisfying $s_p(x) \equiv x \bmod p$ and $0 \leqslant s_p(x) < p$. We have

$$s_p(-x) = p - s_p(x) \tag{1}$$

when $p \nmid x$. We choose and fix a primitive root g modulo p. For each integer t with $1 \leqslant t \leqslant f$, we define a polynomial G_{t,j_0} or H_t in $\mathbb{Z}[T]$ as follows. When $t_0 < f$ and $t_0 + 1 \leqslant t \leqslant f$, we put

$$G_{t,j_0} = G_{t,j_0}(T) = \sum_{v=0}^{\ell^{t_0}-1} \left(\sum_{u=0}^{\ell^{f-t}-1} s_p(g^{2(\ell^t u + \ell^{t-t_0} v + j_0)}) \right) T^v \tag{2}$$

with an integer $j_0 \geqslant 0$. When $1 \leqslant t \leqslant \min(t_0,\ f)$, we put

$$H_t = H_t(T) = \sum_{v=0}^{\ell^t-1} \left(\sum_{u=0}^{\ell^{f-t}-1} s_p(g^{2(\ell^t u+v)}) \right) T^v. \tag{3}$$

Further, we denote by $\Phi_{\ell^t}(T)$ the ℓ^tth cyclotomic polynomial. For a polynomial $F = F(T)$ in $\mathbb{Z}[T]$, let $\tilde{F} = F \bmod r \in \mathbb{F}_r[T]$, where $\mathbb{F}_r$ is the finite field with r elements. For each t with $1 \leqslant t \leqslant f$, we put

$$D_t = \begin{cases} \mathrm{GCD}(\tilde{G}_{t,j_0},\ \tilde{\Phi}_{\ell^{t_0}} \mid 0 \leqslant j_0 \leqslant \ell^{t-t_0}-1), & \text{when } \ t_0+1 \leqslant t \leqslant f \\ \mathrm{GCD}(\tilde{H}_t,\ \tilde{\Phi}_{\ell^t}), & \text{when } \ 1 \leqslant t \leqslant \min(t_0, f). \end{cases}$$

Here, $\mathrm{GCD}(*)$ denotes the greatest common divisor of polynomials in $\mathbb{F}_r[T]$.

Remark 2. We can easily show that

$$TG_{t,j_0+\ell^{t-t_0}}(T) \equiv G_{t,j_0}(T) \bmod (T^{\ell^{t_0}}-1)$$

from the definition of G_{t,j_0}. From this, it follows that when $t_0+1 \leqslant t \leqslant f$, the polynomial D_t equals the greatest common divisor of $\tilde{\Phi}_{\ell^{t_0}}$ and the set of $\tilde{G}_{t,j_0}$ for *all* integers $j_0 \geqslant 0$.

Proposition 1. *For an integer t with $1 \leqslant t \leqslant f$, we have $r \nmid h^-_{p,t}/h^-_{p,t-1}$ if and only if $D_t = 1$.*

For an odd Dirichlet character ψ of conductor m, let

$$B_{1,\psi} = \frac{1}{m} \sum_{a=1}^{m-1} a\psi(a)$$

be the generalized Bernoulli number. Denote by δ the quadratic character of conductor p, which is an odd character as $p \equiv 3 \bmod 4$. It follows from Conner and Hurrelbrink [2, Lemma 13.5] that the unit index of each imaginary abelian field K_t equals 1. Therefore, by the analytic class number formula (cf. Washington [13, Theorem 4.17]), we have

$$h^-_{p,t}/h^-_{p,t-1} = \prod_{\varphi_t} \left(-\frac{1}{2} B_{1,\delta\varphi_t} \right) \tag{4}$$

where φ_t runs over the even Dirichlet characters of conductor p and order ℓ^t. We put $E_t = \mathbb{Q}(\zeta_{\ell^t})$, the field of ℓ^tth roots of unity. We easily see that $\dfrac{1}{2}B_{1,\delta\varphi_t}$ is an algebraic integer of E_t. Since the class in $(\mathbb{Z}/p\mathbb{Z})^\times$ containing g^2 is of order $\ell^f = (p-1)/2$, any integer $1 \leqslant a \leqslant p-1$ satisfies $a \equiv \pm g^{2j} \bmod p$ for some j with

$0 \leqslant j \leqslant \ell^f - 1$. Then noting that δ (resp. φ_t) is odd (resp. even) and using (1), we observe that

$$\begin{aligned}\frac{1}{2}B_{1,\delta\varphi_t} &= \frac{1}{2p}\sum_{a=1}^{p-1} a\delta(a)\varphi_t(a) \\ &= \frac{1}{2p}\sum_{j=0}^{\ell^f-1}\left(s_p(g^{2j})\varphi_t(g^{2j}) - s_p(-g^{2j})\varphi_t(g^{2j})\right) \\ &= \frac{1}{p}\sum_{j=0}^{\ell^f-1} s_p(g^{2j})\varphi_t(g^{2j}) = \frac{1}{p}\sum_{j=0}^{\ell^f-1} s_p(g^{2j})\zeta_{\ell^t}^j \ (\in E_t) \end{aligned} \tag{5}$$

where $\zeta_{\ell^t} = \varphi_t(g^2)$ is a primitive ℓ^tth root of unity.

Proof of Proposition 1 for the case $t_0 + 1 \leqslant t \leqslant f$. Let t be an integer with $t_0 + 1 \leqslant t \leqslant f$. Let φ_t be an arbitrary Dirichlet character of conductor p and order ℓ^t, and $\zeta_{\ell^t} = \varphi_t(g^2)$. We easily see that the system $\zeta_{\ell^t}^j$ with $0 \leqslant j \leqslant \ell^{t-t_0} - 1$ constitutes an integral basis of E_t/E_{t_0}. Hence, we can uniquely write

$$\frac{1}{2}B_{1,\delta\varphi_t} = \sum_{j=0}^{\ell^{t-t_0}-1} a_j\zeta_{\ell^t}^j$$

for some integer a_j of E_{t_0}. Let Tr denote the trace map from E_t to E_{t_0}. We see that for integers j_0 and j with $0 \leqslant j_0,\ j \leqslant \ell^{t-t_0} - 1$, $\zeta_{\ell^t}^{j-j_0}$ is contained in E_{t_0} if and only if $j = j_0$. Hence, it follows that

$$\ell^{t-t_0}a_{j_0} = \mathrm{Tr}\left(\frac{1}{2}\zeta_{\ell^t}^{-j_0}B_{1,\delta\varphi_t}\right). \tag{6}$$

Let $\mathfrak{P}_t$ be an arbitrary prime ideal of E_t over r, and set $\wp = \mathfrak{P}_t \cap E_{t_0}$. As $t_0 + 1 \leqslant t \leqslant f$, $\wp$ remains prime in E_t. First, we show that the congruence

$$\frac{1}{2}B_{1,\delta\varphi_t} \equiv 0 \mod \mathfrak{P}_t \tag{7}$$

holds if and only if $a_{j_0} \equiv 0 \bmod \wp$ for all j_0 with $0 \leqslant j_0 \leqslant \ell^{t-t_0} - 1$. The "if" part is obvious. Assume that (7) holds. Then, as $\wp$ remains prime in E_t, it follows that

$$\mathrm{Tr}\left(\frac{1}{2}\zeta_{\ell^t}^{-j_0}B_{1,\delta\varphi_t}\right) \equiv 0 \mod \wp$$

for all j_0. Hence, we see from (6) that $a_{j_0} \equiv 0 \bmod \wp$ for all j_0.

Next, we show that

$$a_{j_0} = \frac{1}{p}G_{t,j_0}(\zeta_{\ell^{t_0}}). \tag{8}$$

Here, $\zeta_{\ell^t} = \varphi_t(g^2)$ and $\zeta_{\ell^{t_0}} = \zeta_{\ell^t}^{\ell^{t-t_0}} = \varphi_t(g^{2\ell^{t-t_0}})$. Using (8) and the above assertion on the congruence (7), we obtain Proposition 1 for the case $t_0+1 \leqslant t \leqslant f$ from the class number formula (4).

From (5), we see that

$$\frac{1}{2}\varphi_t(g^{-2j_0})B_{1,\delta\varphi_t} = \frac{1}{p}\sum_{j=0}^{\ell^f-1} s_p(g^{2j})\varphi_t(g^{2(j-j_0)}) = \frac{1}{p}\sum_{j=0}^{\ell^f-1} s_p(g^{2(j+j_0)})\zeta_{\ell^t}^j$$

replacing $j-j_0$ with j. We have $\mathrm{Tr}(\zeta_{\ell^t}^j) = \ell^{t-t_0}\zeta_{\ell^t}^j$ or 0 according as ℓ^{t-t_0} divides j or not. For those j divisible by ℓ^{t-t_0}, we put $j = \ell^{t-t_0}k$ with $0 \leqslant k \leqslant \ell^{f-t+t_0}-1$. Then it follows from the above that

$$\mathrm{Tr}\left(\frac{1}{2}\varphi_t(g^{-2j_0})B_{1,\delta\varphi_t}\right) = \frac{\ell^{t-t_0}}{p} \times \sum_{k=0}^{\ell^{f-t+t_0}-1} s_p(g^{2(\ell^{t-t_0}k+j_0)})\zeta_{\ell^{t_0}}^k.$$

Writing $k = \ell^{t_0}u + v$, we obtain

$$\begin{aligned}\mathrm{Tr}\left(\frac{1}{2}\varphi_t(g^{-2j_0})B_{1,\delta\varphi_t}\right) &= \frac{\ell^{t-t_0}}{p} \times \sum_{v=0}^{\ell^{t_0}-1}\left(\sum_{u=0}^{\ell^{f-t}-1} s_p(g^{2(\ell^t u+\ell^{t-t_0}v+j_0)})\right)\zeta_{\ell^{t_0}}^v \\ &= \frac{\ell^{t-t_0}}{p} \times G_{t,j_0}(\zeta_{\ell^{t_0}}).\end{aligned}$$

The formula (8) follows from this and (6). ■

Proof of Proposition 1 for the case $1 \leqslant t \leqslant \min(t_0, f)$**.** Writing $j = \ell^t u + v$, we can rewrite the formula (5) as

$$\frac{1}{2}B_{1,\delta\varphi_t} = \frac{1}{p}\sum_{v=0}^{\ell^t-1}\left(\sum_{u=0}^{\ell^{f-t}-1} s_p(g^{2(\ell^t u+v)})\right)\zeta_{\ell^t}^v = \frac{1}{p}H_t(\zeta_{\ell^t}). \tag{9}$$

We can show the assertion from this and the class number formula (4). ■

Remark 3. If $r = p\ (= 2\ell^f+1)$, we have $t_0 = f$. We imposed the condition $p \neq r$ because of the denominator p in (9).

3. Proof of Theorem

We begin with the following elementary lemma.

Lemma. *Let p be an arbitrary prime number and $r \geqslant 2$ an integer with $p \nmid r$. For integers x and y with $1 \leqslant x < y \leqslant p-1$, we have $s_p(r^n x) \not\equiv s_p(r^n y) \bmod r$ for some $n \geqslant 0$.*

Proof. Assume to the contrary that

$$s_p(r^n x) \equiv s_p(r^n y) \mod r \tag{10}$$

for all $n \geqslant 0$. We show by induction on n that

$$\frac{a}{r^n}p < x < y < \frac{(a+1)}{r^n}p \tag{11}$$

holds for some a with $0 \leqslant a \leqslant r^n - 1$. When $n = 0$, the assertion holds with $a = 0$. Assume that (11) holds for an integer $n \geqslant 0$ with some a. Then it follows that

$$arp < r^{n+1}x < r^{n+1}y < (a+1)rp = arp + rp. \tag{12}$$

For an integer z with $p \nmid z$ and $arp < r^{n+1}z < arp + rp$, there uniquely exists an integer k_z with $0 \leqslant k_z \leqslant r - 1$ satisfying

$$arp + k_z p < r^{n+1}z < arp + (k_z + 1)p.$$

Then we see that

$$s_p(r^{n+1}z) = r^{n+1}z - arp - k_z p \equiv -k_z p \mod r,$$

and hence the integer k_z is uniquely determined by the value $s_p(r^{n+1}z) \bmod r$ because p and r are relatively prime. Therefore, from the congruence (10) for $n + 1$ and (12), we observe that

$$arp + kp < r^{n+1}x < r^{n+1}y < arp + (k+1)p$$

for some k with $0 \leqslant k \leqslant r - 1$. It follows that

$$\frac{ar + k}{r^{n+1}}p < x < y < \frac{ar + k + 1}{r^{n+1}}p$$

and hence the assertion (11) holds for $n + 1$. Thus (11) holds for all n. However, the inequality (11) is impossible when $r^n \geqslant p$. Therefore, the congruence (10) does not hold for some n. ∎

Proof of Theorem. We work under the setting and notation of Section 2. In particular, $p = 2\ell^f + 1$ with an odd prime number ℓ, and r is a prime number with $r \neq \ell$. Assume that r is a primitive root modulo ℓ^2. Then, we have $r \neq p$ and $t_0 = 1$. We put $x_v = s_p(g^{2\ell^{f-1}v})$ for $0 \leqslant v \leqslant \ell - 1$. As g is a primitive root modulo p, these ℓ integers are different from each other. As $t_0 = 1$, we have

$$G_{j_0} = G_{f,j_0}(T) = \sum_{v=0}^{\ell-1} s_p(g^{2(\ell^{f-1}v + j_0)})T^v = \sum_{v=0}^{\ell-1} s_p(g^{2j_0}x_v)T^v.$$

Assume that r divides the ratio $h^-_{p,f}/h^-_{p,f-1}$. Then it follows from Proposition 1 and Remark 2 that

$$\mathrm{GCD}(\tilde{G}_{j_0}, \tilde{\Phi}_\ell) \neq 1$$

for all j_0. As r is a primitive root modulo ℓ, the polynomial $\tilde{\Phi}_\ell(T)$ is irreducible over $\mathbb{F}_r$. Therefore, we see that $\tilde{G}_{j_0} = c\tilde{\Phi}_\ell$ for some constant $c \in \mathbb{F}_r$. Hence, it follows that the congruence

$$s_p(g^{2j_0}x_0) \equiv s_p(g^{2j_0}x_1) \equiv \cdots \equiv s_p(g^{2j_0}x_{\ell-1}) \mod r$$

holds for all j_0. For each $n \geqslant 0$, we have $r^n \equiv g^{2j_0}$ or $-g^{2j_0}$ modulo p for some j_0 since $p \equiv 3 \bmod 4$ and g is a primitive root modulo p. Hence, we see from the above congruence and (1) that

$$s_p(r^n x_0) \equiv s_p(r^n x_1) \equiv \cdots \equiv s_p(r^n x_{\ell-1}) \mod r$$

for all integers $n \geqslant 0$. However, this is impossible by Lemma. ■

4. Numerical results

For each prime number $p = 2\ell^f + 1$ with $p < 2^{56}$ and each prime number r with $2 \leqslant r \leqslant 47$ and $r \neq \ell$, we computed the polynomial D_t in §2 mainly for t with $t_0 + 1 \leqslant t \leqslant f$. If $D_t = 1$, then we obtain $r \nmid h^-_{p,t}/h^-_{p,t-1}$ by Proposition 1. There are 1500 pairs (f, ℓ) of an integer $f \geqslant 2$ and an odd prime ℓ for which $p = 2\ell^f + 1$ is a prime number with $p < 2^{56}$. When f is even (and $\ell = 3$), the condition is satisfied for $f = 2$, 4, 6, 16 and 30. When $f = 3$ (resp. 5, 7, 9), there are 1468 (resp. 21, 2, 2) primes ℓ satisfying the condition. When $f = 13$ or 17, there is just one such ℓ. For the other f, there are no such ℓ. For these, see Table 3. Summing up, there are $5 + 1468 + 21 + 2 + 2 + 1 + 1 = 1500$ pairs (f, ℓ). For these (f, ℓ), we always have $p \neq r$ $(\leqslant 47)$. For these ℓ and r with $2 \leqslant r \leqslant 47$, we found that $t_0 = 1$ or 2. In Table 4, we give a list of r, ℓ and f for which $t_0 = 2$ (and $p = 2\ell^f + 1$ is a prime). We have $t_0 = 2$ only for relatively small ℓ, except for the case where $\ell = 48947$, $f = 3$ and $r = 17$. For the exceptional case, see a comment in a paragraph on the computation complexity near the end of this section.

Table 3: Pairs (f, ℓ) for odd f

f	ℓ $(p < 2^{56})$
3	5, 11, 29, 59, 71, 107, 149, 191, 197, 227, 269, 431, 479, 491, 857, ..., 328421, 329267, 329627, 329687, 329729 (1468 pairs)
5	3, 23, 29, 53, 149, 251, 389, 401, 443, 839, 953, 983, 1061, 1103, 1319, 1361, 1409, 1451, 1481, 1613, 1733 (21 pairs)
7	29, 179
9	3, 11
13	5
17	3

Proposition 2. *For each of the* 1500 *pairs* (f, ℓ) *and each prime number* r *with* $2 \leqslant r \leqslant 47$ *and* $r \neq \ell$, *we have* $D_t = 1$ *and hence* $r \nmid h^-_{p,t}/h^-_{p,t-1}$ *for any* t *with* $t_0 + 1 \leqslant t \leqslant f$ *except for the case where* $(f, \ell) = (3, 48947)$ *and* $r = 17$, $t = 3$.

Table 4: List of (r, ℓ, f) with $t_0 = 2$

r	ℓ	f
3	11	3, 9
7	5	3, 13
11	71	3
17	3	2, 4, 5, 6, 9, 16, 17, 30
17	48947	3
19	3	2, 4, 5, 6, 9, 16, 17, 30
37	3	2, 4, 5, 6, 9, 16, 17, 30
41	29	3, 5, 7
43	5	3, 13

As for those t with $1 \leqslant t \leqslant \min(t_0, f)$, we obtained results for each of 294 pairs (f, ℓ) in Table 5. We give in Table 6 a list of ten quadruplets (f, ℓ, t, r) and the polynomial D_t for which we found that $\deg D_t \geqslant 1$ and hence r divides $h^-_{p,t}/h^-_{p,t-1}$.

Table 5: 294 pairs (f, ℓ) for the case $1 \leqslant t \leqslant \min(t_0, f)$

f	ℓ	Number of pairs
2,4,6,16,30	3	5
3	5, 11, 29, 59, 71, ..., 39749, 39761, 39839	274
5	3, 23, 29, 53, 149, 251, 389, 401, 443, 839	10
7	29	1
9	3, 11	2
13	5	1
17	3	1

Proposition 3. *For each of the* 294 *pairs* (f, ℓ) *in Table 3 and each prime number* r *with* $2 \leqslant r \leqslant 47$ *and* $r \neq \ell$, *we have* $D_t = 1$ *and hence* $r \nmid h^-_{p,t}/h^-_{p,t-1}$ *for any* t *with* $1 \leqslant t \leqslant \min(t_0, f)$ *except for those given in Table 6.*

Remark 4. From these computational results with $r \leqslant 47$, we might expect that the ratio $h^-_{p,t}/h^-_{p,t-1}$ is not divisible by r for any triple (f, ℓ, t) and a relatively small prime number r when $p = 2\ell^f + 1$ is a prime and $t_0 + 1 \leqslant t \leqslant f$. We already know that $r \nmid h^-_{p,f}/h^-_{p,f-1}$ when r is a primitive root modulo ℓ^2 (Theorem).

Table 6: Quadruplets (f, ℓ, t, r) and the polynomial D_t with $\deg D_t \geqslant 1$

(f, ℓ)	t	r	D_t
(3,5)	1	11	$2 + T$
(4,3)	1	2	$1 + T + T^2 \quad (H_t \bmod 2 = 0)$
(5,3)	1	7	$3 + T$
(5,3)	2	37	$26 + 21T + T^2$
(5,23)	1	47	$44 + 43T + 30T^2 + T^3$
(6,3)	1	31	$6 + T$
(16,3)	1	13	$4 + T$
(17,3)	1	13	$10 + T$
(17,3)	2	37	$21 + T$
(30,3)	1	2	$1 + T + T^2$

To show Proposition 2 ($t_0 + 1 \leqslant t \leqslant f$), our calculation for each triple (f, ℓ, t) was carried out as follows. For each r and $j_0 \geqslant 0$, we put

$$\mathrm{GCD}_{j_0} = \mathrm{GCD}(G_{t,j} \bmod r, \Phi_{\ell^{t_0}} \bmod r \;\big|\; 0 \leqslant j \leqslant j_0)$$

for brevity. If we can compute $\mathrm{GCD}_{j_0} = 1$ for some j_0, then we obtain $D_t = 1$. We denote by $n\sharp$ the primorial of n, the product of prime numbers less than or equal to n. Since $47\sharp < 2^{63}$, a coefficient of a polynomial mod $47\sharp$ can be stored in one word (4 bytes). The calculation for the triple is organized as follows.

(I) For each prime r with $2 \leqslant r \leqslant 47$ and $r \neq \ell$, we proceed as follows:

(II-i) Compute the actual value of $t_0 = \mathrm{ord}_\ell(r^{\ell-1} - 1)$.

(II-ii) If $t \leqslant \min(t_0, f)$, we skip the r and go back to (I).

(III) Compute GCD_{j_0} one by one for $j_0 = 0, 1, \cdots$, until we obtain $D_t = 1$ as follows:

(III-i) Compute the coefficients of $G_{t,j_0}(T)$ mod $47\sharp$ (which depends on t_0), if we have not yet computed it.

(III-ii) Calculate $G_{t,j_0}(T)$ mod r.

(III-iii) Compute the polynomial GCD_{j_0}:

$$\mathrm{GCD}_{j_0} = \begin{cases} \mathrm{GCD}(G_{t,j_0}(T) \bmod r, \Phi_{\ell^{t_0}} \bmod r) & (j_0 = 0) \\ \mathrm{GCD}(G_{t,j_0}(T) \bmod r, \mathrm{GCD}_{j_0-1}) & (j_0 \geqslant 1) \end{cases}$$

by Euclidean algorithm.

Except for the single case mentioned in Proposition 2, we were able to find that $D_t = 1$ with $j_0 \leqslant 3$. It is noteworthy that, in almost all cases, the value $j_0 = 0$ worked for showing $D_t = 1$. Table 7 is a list of the number of triples (f, ℓ, t) for which we needed $j_0 = 1$, 2 or 3.

Table 7: Number of triplets (f, ℓ, t) for which we needed $j_0 \geqslant 1$.

r	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$j_0 = 1$	17	1	1	8	5	8	0	14	4	1	11	7	5	3	2
2	3			3	1	1		2							
3	1					1									

On the other hand, for Proposition 3 ($1 \leqslant t \leqslant \min(t_0, f)$), steps (II-ii)-(III-iii) in the above process are replaced by the following.

(II-ii) If $t > \min(t_0, f)$, we skip the r and go back to (I).
(III-i) Compute the coefficients of $H_t(T)$ mod 47♯, if we have not yet computed it.
(III-ii) Calculate $H_t(T)$ mod r.
(III-iii) Compute $D_t = \mathrm{GCD}(H_t(T) \bmod r, \Phi_{\ell^t} \bmod r)$ by Euclidean algorithm.

Remark 5. For an odd prime number p, let h_n^* denote the relative class number of the p^{n+1}st cyclotomic field $\mathbb{Q}(\zeta_{p^{n+1}})$. In [5], we gave a condition for $2 \nmid h_n^*/h_{n-1}^*$ similar to Proposition 1, and showed that when $p \leqslant 509$, the ratio h_n^*/h_{n-1}^* is odd for *all* $n \geqslant 1$ with the help of computer. Similarly to the above, "$j_0 = 0$" was enough for showing $2 \nmid h_n^*/h_{n-1}^*$ in almost all cases (see [5, §4.3]). Similar phenomenon also appeared in [7] where we dealt with the 3-part of class numbers.

Let us comment on the computation complexity. The complexity of computing $G = G_{t,j_0}$ (resp. $H = H_t$) modulo #47 is measured by the number of terms $s_p(*)$ in the formula (2) (resp. (3)). Therefore, the order of the complexity for G (resp. H) is $O(\ell^{f-(t-t_0)})$ (resp. $O(\ell^f)$). Thus, the computation of G (resp. H) is very hard when $f - (t - t_0)$ (resp. f) is large. In the range of our computation, it was hardest when $(f, \ell) = (30, 3)$ and $(5, 839)$ with small t. When $(f, \ell) = (30, 3)$, we encountered four polynomials G_{t,j_0} with $(t, j_0, t_0) = (2, 0, 1)$, $(2, 1, 1)$, $(3, 0, 2)$, $(3, 1, 2)$, which have 3^{29} ($\sim 7 \times 10^{13}$) terms $s_p(*)$. Each needed computation time of 35-50 days. Further, two polynomials H_t with $t = 1$, 2 have 3^{30} ($\sim 2 \times 10^{14}$) terms. Each needed computation time of 3.5 months. When $(f, \ell) = (5, 839)$, H_1 modulo #47 is

$$318301740960876433 + \cdots + 628720698341741017^{838},$$

which has 839^5 ($\sim 4 \times 10^{14}$) terms $s_p(*)$ in the formula (3). It needed computation time of 9.5 months.

For computing the GCD by Euclidean algorithm, the complexity is measured by the product of the degrees of the related two polynomials. Hence, the order is $O(\ell^{2t_0})$ (resp. $O(\ell^{2t})$) for G (resp. H). GCD computation of the exceptional case in Proposition 2 has $\ell^{2t_0} = 48947^4$ ($\sim 6 \times 10^{18}$) steps, so that its computation time is estimated to be greater than many years.

The computations in Propositions 2 and 3 were done in parallel by assignment of each triplet (f, ℓ, t) to a thread of personal computer(s) one by one. They started at 21 Feb., 2013 and finished at 20 July, 2014, in a personal computer with

8 threads, Intel Core i7-3840QM CPU and 32GB RAM. Temporarily, additional 40 threads of 11 PCs with Intel i7, i5 or Core 2 CPU were used for 37 days in Sep.-Oct., 2013. Java program language was used.

Acknowledgements. The authors are gratefull to Shoichi Nakajima and the anonymous referee for several valuable comments and suggestions which improved the presentation of the whole paper.

References

[1] P.T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers,* Math. Comp. **16** (1962), 363–367.
[2] P.E. Conner and J. Hurrelbrink, *Class Number Parity,* World Scientific, Singapore, 1988.
[3] D. Davis, *Computing the number of totally positive circular units which are square,* J. Number Theory **10** (1978), 1–9.
[4] D.R. Estes, *On the parity of the class number of the field of q-th roots of unity,* Rocky Mountain J. Math. **19** (1989), 675–682.
[5] H. Ichimura and S. Nakajima, *On the* 2*-part of the class numbers of cyclotomic fields of prime power conductors,* J. Math. Soc. Japan **64** (2012), 317–342.
[6] 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. **88A** (2012), 16–20.
[7] H. Ichimura, S. Nakajima and H. Sumida-Takahashi, *On the Iwasawa lambda invariant of an imaginary abelian field of conductor $3p^{n+1}$,* J. Number Theory **133** (2013), 787–801.
[8] S. Jakubec, *On the class number of some real abelian fields of prime conductors,* Acta Arith. **145** (2010), 315–318.
[9] T. Metsänkylä, *Some divisibility results for the cyclotomic class number,* Tatra Mt. Math. Publ. **11** (1997), 59-68.
[10] T. Metsänkylä, *An application of the p-adic class number formula,* Manuscripta Math. **93** (1997), 481–498.
[11] P. Stevenhagen, *Class number parity of the pth cyclotomic field,* Math. Comp. **63** (1994), 773–784.
[12] L.C. Washington, *The non-p-part of the class number in cyclotomic $\mathbb{Z}_p$-extension,* Invent. Math. **49** (1979), 87–97.
[13] L.C. Washington, *Introduction to Cyclotomic Fields (2nd ed.),* Springer, New York, 1997.
[14] K. Yamamura, `http://tnt.math.se.tmu.ac.jp/pub/CDROM/rcn/`.
[15] K. Yoshino, *A condition for divisibility of the class number of real pth cyclotomic field by an odd prime number distinct from p,* Abh. Math. Semin. Hamburg **69** (1999), 37–57.

Address: Shoichi Fujima, Humio Ichimura: Faculty of Science, Ibaraki University, Bunkyo 2-1-1, Mito, 310-8512, Japan.
E-mail: fujima@mx.ibaraki.ac.jp, hichimur@mx.ibaraki.ac.jp
Received: 28 May 2014; **revised:** 24 July 2014