A note on the relative class number of the cyclotomic $\boldsymbol{Z}_p$-extension of $\boldsymbol{Q}(\sqrt{-p})$

By Humio ICHIMURA*) and Shoichi NAKAJIMA**)

(Communicated by Shigefumi MORI, M.J.A., Dec. 12, 2011)

Abstract: Let p be a prime number with $p \equiv 3 \bmod 4$ and $q = (p-1)/2$. Let $k = \boldsymbol{Q}(\sqrt{-p})$ and k_∞/k be the cyclotomic $\boldsymbol{Z}_p$-extension. Denote by h_n^- the relative class number of the n-th layer k_n. Let ℓ be a prime number with $\ell \neq p$. We show that, for any $n \geq 1$, ℓ does not divide h_n^-/h_{n-1}^- (resp. h_1^-/h_0^-) if ℓ is a primitive root modulo p^2 (resp. p) and $\ell \geq q-2$ (resp. $\ell \geq q-6$). Further, we show with the help of computer that when $p < 10000$ and $n \leq 100$, ℓ does not divide h_n^-/h_{n-1}^- (resp. h_1^-/h_0^-) for any prime ℓ which is a primitive root modulo p^2 (resp. p).

Key words: Class number; quadratic field; cyclotomic $\boldsymbol{Z}_p$-extension; non-p part.

1. Introduction. Let p be a prime number with $p \equiv 3 \bmod 4$. Let $k = \boldsymbol{Q}(\sqrt{-p})$, and k_∞/k be the cyclotomic $\boldsymbol{Z}_p$-extension. Let k_n be the n-th layer of k_∞/k with $k_0 = k$. Denote by h_n^- the relative class number of k_n. Let ℓ be a prime number with $\ell \neq p$. By a well known theorem of Washington [7], ℓ does not divide the ratio h_n^-/h_{n-1}^- for sufficiently large n. By Horie [4, Theorem 2], $\ell \nmid h_n^-/h_{n-1}^-$ for all $n \geq 1$ if ℓ is a primitive root modulo p^2 and ℓ is larger than an explicit but complicated constant depending on p. In this note, we show the following assertion. We put $q = (p-1)/2$.

Proposition 1. *The setting is the same as above.*

(I) *If $\ell \geq q-2$ and ℓ is a primitive root modulo p^2, then $\ell \nmid h_n^-/h_{n-1}^-$ for all $n \geq 1$.*

(II) *If $\ell \geq q-6$ and ℓ is a primitive root modulo p, then $\ell \nmid h_1^-/h_0^-$.*

Proposition 1(I) generalizes [6, Proposition 2] which treats the case $\ell \geq q-1$. Our method for proof of Proposition 1 is a modification of the argument in [6] and effective use of the classical class number formula for $k = \boldsymbol{Q}(\sqrt{-p})$. When $p = 3$, the assertion of Proposition 1(I) is contained in Horie [3, Proposition 3].

When p and ℓ are small and ℓ is a primitive root modulo p^2 (or p when $n = 1$), we can effectively decide, by using Lemma 4 in §3, whether h_n^-/h_{n-1}^- is divisible by ℓ. With the help of computer, we show the following result.

Proposition 2. *Let $p < 10000$ be a prime number with $p \equiv 3 \bmod 4$ and ℓ a prime number. Then ℓ does not divide h_n^-/h_{n-1}^- for any $n \leq 100$ if ℓ is a primitive root modulo p^2. Further, ℓ does not divide h_1^-/h_0^- if ℓ is a primitive root modulo p.*

2. Preliminaries. In this section we define integers $x_{n,b,\alpha}$, $y_{n,b,\alpha}$ and give some properties of them. They will be used in the following sections for proving Propositions 1 and 2.

Let p, q, k_n and h_n^- be as in §1. Let μ_q be the group of q-th roots of unity in the ring $\boldsymbol{Z}_p$ of p-adic integers. For each integer b with $0 \leq b \leq p-1$ and each p-adic integer $\alpha \in \boldsymbol{Z}_p$ with $\alpha \equiv 1 \bmod p$, we put

$$x_{n,b,\alpha} = \sum_{\epsilon \in \mu_q} s_n(\epsilon\alpha(1+bp^n)),$$

where $s_n(x)$ is the unique integer satisfying $s_n(x) \equiv x \bmod p^{n+1}$ and $0 \leq s_n(x) < p^{n+1}$. When $p = 3$, we easily have

$$x_{n,b,1} = 1 + b3^n \tag{1}$$

for any $n \geq 1$ and b. When $p \geq 7$, we have $q > 1$ and hence $\sum_{\epsilon \in \mu_q} \epsilon = 0$ holds. Therefore, we easily see that $x_{n,b,\alpha}$ is a multiple of p^{n+1} when $p \geq 7$. So, when $p \geq 7$, we put

$$y_{n,b,\alpha} = \frac{1}{p^{n+1}} x_{n,b,\alpha}. \tag{2}$$

When $\alpha = 1$, we simply write

$$x_{n,b} = x_{n,b,1} \quad \text{and} \quad y_{n,b} = y_{n,b,1}.$$

2000 Mathematics Subject Classification. Primary 11R18.

*) Faculty of Science, Ibaraki University, 2-1-1 Bunkyo, Mito, Ibaraki 310-8512, Japan.

**) Department of Mathematics, Gakushuin University, 1-5-1 Mejiro, Toshima-ku, Tokyo 171-8588, Japan.

doi: 10.3792/pjaa.88.16

Since $0 < s_n(\epsilon\alpha(1+bp^n)) < p^{n+1}$, inequalities

$$1 \le y_{n,b,\alpha} \le q-1 \tag{3}$$

hold for any n, b, α.

The following two results are important for our purpose.

Lemma 1. *Assume $p \ge 7$. For any α and $n \ge 1$, we have*

$$\sum_{b=0}^{p-1} y_{n,b,\alpha} = y_{n-1,0,\alpha} + q^2.$$

Proof. For $\epsilon \in \mu_q$, let

$$\epsilon\alpha = a_0 + a_1 p + \cdots + a_n p^n + \cdots$$

be the p-adic expansion of $\epsilon\alpha$ where a_i is an integer with $0 \le a_i \le p-1$. We see that

$$s_n(\epsilon\alpha(1+bp^n)) = s_{n-1}(\epsilon\alpha) + s_0(a_n + a_0 b)p^n.$$

Further, since $p \nmid a_0$, we have

$$\{s_0(a_n + a_0 b) \mid 0 \le b \le p-1\} = \{0, 1, \cdots, p-1\}.$$

Therefore, it follows that

$$\sum_{b=0}^{p-1} s_n(\epsilon\alpha(1+bp^n)) = ps_{n-1}(\epsilon\alpha) + qp^{n+1}.$$

Hence, we see that

$$\begin{aligned}\sum_{b=0}^{p-1} x_{n,b,\alpha} &= \sum_{\epsilon\in\mu_q}\left(\sum_{b=0}^{p-1} s_n(\epsilon\alpha(1+bp^n))\right)\\ &= p\sum_{\epsilon\in\mu_q} s_{n-1}(\epsilon\alpha) + q^2p^{n+1}\\ &= px_{n-1,0,\alpha} + q^2p^{n+1},\end{aligned}$$

from which the assertion follows immediately. □

Lemma 2. *Assume $p \ge 7$. For any $n \ge 1$ and α, we have $y_{n,b,\alpha} \ne y_{n,0,\alpha}$ for some b.*

Proof. Assume that the values $y_{n,b,\alpha}$ are the same for all $b = 0, \cdots, p-1$. Then, Lemma 1 shows $y_{n-1,0,\alpha} \equiv -q^2 \bmod p$. This implies $y_{n-1,0,\alpha} \equiv (3q+1)/2 \bmod p$, since $-q^2 = -p(q+1)/2 + (3q+1)/2$ (note that q is an odd integer). But this contradicts (3) because $q-1 < (3q+1)/2 < p = 2q+1$. □

3. Proof of Proposition 1. We are going to prove Proposition 1, making use of the analytic class number formula. Throughout the section, δ denotes the odd character of conductor p and order 2, and for $n \ge 0$, ψ_n denotes a character of conductor p^{n+1} and order p^n. Note that, when $n = 0$, ψ_0 is the trivial character.

For these characters δ and ψ_n, let

$$B_{1,\delta\psi_n} = \frac{1}{p^{n+1}}\sum_{a=1}^{p^{n+1}-1} a\cdot\delta\psi_n(a)$$

be the generalized Bernoulli number. Then, $B_{1,\delta\psi_n}$ belongs to the field $F_n = \boldsymbol{Q}(\zeta_{p^n})$. When $\alpha \in \boldsymbol{Z}_p$ with $\alpha \equiv 1 \bmod p$ is given, we define

$$X = \mathrm{Tr}_{n,1}\left(\frac{1}{2}\psi(\alpha^{-1})B_{1,\delta\psi_n}\right), \tag{4}$$

where $\mathrm{Tr}_{n,1}$ denotes the trace map from F_n to F_1 ($n \ge 1$). We can express X in terms of $x_{n,b,\alpha}$ defined in §2.

Lemma 3. *Put $\zeta_p = \psi_n(1+p^n)$, which is a primitive p-th root of unity. Then, for $n \ge 1$, we have*

$$X = \frac{1}{p^2}\sum_{b=0}^{p-1} x_{n,b,\alpha}\zeta_p^b. \tag{5}$$

Proof. Let μ_{p-1} be the group of $(p-1)$-st roots of unity in $\boldsymbol{Z}_p$. Replacing $\alpha^{-1}a$ with a, we have

$$\begin{aligned}\psi(\alpha^{-1})B_{1,\delta\psi_n} &= \frac{1}{p^{n+1}}\sum_{a=1}^{p^{n+1}-1} s_n(a\alpha)\cdot\delta\psi_n(a)\\ &= \frac{1}{p^{n+1}}\sum_{\epsilon\in\mu_{p-1}}\sum_{b=0}^{p^n-1} s_n(\epsilon\alpha(1+bp))\delta(\epsilon)\psi_n(1+bp).\end{aligned}$$

Since $p \equiv 3 \bmod 4$, we have $\mu_{p-1} = \mu_q \cup (-\mu_q)$. Further, $\delta(\epsilon) = 1, \delta(-\epsilon) = -1$ and $s_n(-\epsilon) = p^{n+1} - s_n(\epsilon)$ hold for any $\epsilon \in \mu_q$. Hence we obtain

$$\begin{aligned}&\frac{1}{2}\psi(\alpha^{-1})B_{1,\delta\psi_n}\\ &\quad= \frac{1}{p^{n+1}}\sum_{\epsilon\in\mu_q}\sum_{b=0}^{p^n-1} s_n(\epsilon\alpha(1+bp))\psi_n(1+bp).\end{aligned}$$

For a p^n-th root ζ of unity, we have $\mathrm{Tr}_{n,1}(\zeta) = p^{n-1}\zeta$ or 0 according as $\zeta^p = 1$ or not. This fact and $\psi_n(1+bp^n) = \zeta_p^b$ give

$$\begin{aligned}X &= \frac{1}{p^2}\sum_{\epsilon\in\mu_q}\sum_{b=0}^{p-1} s_n(\epsilon\alpha(1+bp^n))\zeta_p^b\\ &= \frac{1}{p^2}\sum_{b=0}^{p-1} x_{n,b,\alpha}\zeta_p^b,\end{aligned}$$

which proves (5). □

Here we apply the analytic class number formula (cf. Washington [8, Theorem 4.17]) to the field k_n. First, for $n \ge 1$, the class number formula implies

(6) $$h_n^-/h_{n-1}^- = p\prod_{\psi_n}\left(-\frac{1}{2}B_{1,\delta\psi_n}\right),$$

where ψ_n runs over the Dirichlet characters of conductor p^{n+1} and order p^n. (Note that the unit index of k_n equals 1; see e.g. Conner and Hurrelbrink [1, Lemma 13.5].) Next, for $n = 0$ and $p \geq 7$, we obtain

$$h_0^- = 2\times\left(-\frac{1}{2}B_{1,\delta}\right) = -B_{1,\delta},$$

and an easy calculation using $\delta(\pm\epsilon) = \pm 1$ gives

(7) $$h_0^- = -2y_{0,0} + q.$$

The following is our key lemma.

Lemma 4. *Assume that ℓ divides h_n^-/h_{n-1}^- and that ℓ is a primitive root modulo p^2 (resp. modulo p) when $n \geq 2$ (resp. $n = 1$). Further, assume that an element $\alpha \in \boldsymbol{Z}_p$ with $\alpha \equiv 1 \bmod p$ is given. Then we have*

(8) $$x_{n,b,\alpha} \equiv x_{n,0,\alpha} \bmod \ell$$

for all $b = 0, 1, \cdots, p-1$, and when $p \geq 7$ we have

(9) $$y_{n,b,\alpha} \equiv y_{n,0,\alpha} \bmod \ell$$

for all $b = 0, 1, \cdots, p-1$.

Proof. Put $F_n = \boldsymbol{Q}(\zeta_{p^n})$ as before. Then, the assumption of Lemma 4 means that the prime ℓ does not decompose in F_n. Namely, there is a unique prime ideal $\mathcal{L}$ of F_n lying over ℓ. If ℓ divides h_n^-/h_{n-1}^-, then, by (6), there exists a character ψ_n satisfying

(10) $$\frac{1}{2}B_{1,\delta\psi_n} \equiv 0 \bmod \mathcal{L}.$$

Multiplying $\psi(\alpha^{-1})$ to (10) and taking trace from F_n to F_1, we obtain

$$X \equiv 0 \bmod \mathcal{L}_1,$$

where X is defined by (4) and $\mathcal{L}_1 = \mathcal{L} \cap F_1$ which is the unique prime ideal of F_1 over ℓ. (In this argument, we rely on the fact that $\mathcal{L}$ is the only prime ideal over ℓ.) Therefore, we have from (5)

(11) $$\sum_{b=0}^{p-1} x_{n,b,\alpha}\zeta_p^b \equiv 0 \bmod \mathcal{L}_1,$$

noting that p is prime to ℓ. Since ℓ is a primitive root modulo p, the only linear relation among ζ_p^b's over $\boldsymbol{F}_\ell$ is $\sum_{b=0}^{p-1}\zeta_p^b = 0$, where $\boldsymbol{F}_\ell$ is the finite field with ℓ elements. Therefore, from (11) we see that (8) must hold for all b. Finally, (9) is derived directly from (8) when $p \geq 7$ (cf. (2)). □

Proof of Proposition 1. When $p = 3$, (1) shows $x_{n,1,1} - x_{n,0,1} = 3^n$, which implies that (8) does not hold for any $\ell \neq 3$. Hence, by Lemma 4, Proposition 1 holds for $p = 3$. Hereafter we assume $p \geq 7$.

First, we consider the case $\ell \geq q - 1$. If ℓ divides h_n^-/h_{n-1}^-, then, by Lemma 4, (9) holds for all b. (Here we fix an arbitrary α, e.g. $\alpha = 1$.) Then, we obtain $y_{n,b,\alpha} = y_{n,0,\alpha}$ from (9), thanks to (3). This contradicts Lemma 2, which proves Proposition 1 in this case. (This argument is the same as in [6, Proposition 2].)

In dealing with the case $\ell \leq q - 2$, we need the result of Gut [2] which asserts

(12) $$h_0^- \leq \frac{p-3}{4}$$

in our situation. Now assume $\ell = q - 2$. Then it follows from (3)

(13) $$1 \leq y_{n,b,\alpha} \leq \ell + 1.$$

If ℓ divides h_n^-/h_{n-1}^-, then we see from Lemma 2 that, for any b, $y_{n,b,\alpha}$ must be equal to 1 or $\ell + 1$, because both (9) and (13) hold. Hence,

(14) $$y_{n,b,\alpha} \equiv 1 \bmod \ell$$

for all α and b. Then, from Lemma 1 we obtain

$$y_{n-1,0,\alpha} \equiv p - q^2 \equiv 2\ell + 5 - (\ell+2)^2 \equiv 1 \bmod \ell$$

for any α. This congruence and an easily verified equation

$$y_{n-1,0,\alpha(1+bp^{n-1})} = y_{n-1,b,\alpha}$$

show that

(15) $$y_{n-1,b,\alpha} \equiv 1 \bmod \ell$$

holds for any α and b. Thus we derived (15) from (14). Repeating this process, we finally reach the congruence $y_{0,0} \equiv 1 \bmod \ell$, which gives

(16) $$h_0^- \equiv -2 + \ell + 2 \equiv 0 \bmod \ell$$

by virtue of (7). But (16) contradicts (12) because we have $(p-3)/4 = (\ell+1)/2 < \ell$. This completes the proof of Proposition 1 (I) and the case $\ell \geq q - 2$ of Proposition 1 (II).

In the rest of this section, we deal with the case $n = 1, q - 6 \leq \ell \leq q - 3$. Since q is odd, $\ell = q - 3$, $q - 5$ occurs only when $\ell = 2$. In the case $2 = q - 3$, we have $p = 11$, and an easy computation shows $y_{1,1} - y_{1,0} = 1$. Hence, in this case, h_1^-/h_0^- is not divisible by $\ell = 2$ by Lemma 4. The case $2 = q - 5$ does not occur because $p = 2q + 1 = 15$ is not prime.

Next, assume $\ell = q - 4$, namely $q = \ell + 4$, $p = 2\ell + 9$. All possible values of $\ell < 41$ and p for which ℓ is a primitive root modulo p are listed in Table I. In each case of Table I, we can find a b for which $y_{1,b} - y_{1,0}$ is prime to ℓ, which shows that $\ell \nmid h_1^-/h_0^-$ by Lemma 4. Our choice of b is shown in Table I. So we assume $\ell \geq 41$ in the following argument. If ℓ divides h_1^-/h_0^-, then Lemma 4, Lemma 2 and (3) show that, for some $i = 1, 2, 3$,

$$y_{1,b} \equiv i \bmod \ell \quad (b = 0, 1, \cdots, p-1) \tag{17}$$

holds (note that $q - 1 = \ell + 3$ in this case). Then Lemma 1 gives

$$y_{0,0} \equiv ip - q^2 \equiv 9i - 16 \bmod \ell,$$

which implies

$$\begin{aligned} h_0^- &\equiv -2(9i - 16) + 4 \equiv 36 - 18i \\ &\equiv 18, \ell, \ell - 18 \bmod \ell \end{aligned} \tag{18}$$

by (7). The estimate (12) is $h_0^- \leq (\ell + 3)/2$ in this case, and $(\ell + 3)/2 < \ell - 18$ for $\ell \geq 41$. Hence the second and third congruences in (18) are impossible. The first congruence in (18) implies $h_0^- = 18$ for $\ell \geq 41$. But this is also impossible, because, as is well known, h_0^- is odd (this fact is also derived from (7)). Thus all possibilities have been excluded, showing $\ell \nmid h_1^-/h_0^-$ in this case.

Finally, we assume $\ell = q - 6$, for which $q = \ell + 6, p = 2\ell + 13$. Our argument proceeds in a way similar to the case $\ell = q - 4$. First, we settle the cases when $\ell < 113$ and ℓ is a primitive root modulo p, which are listed in Table II. In all these cases, we found that $y_{1,1} - y_{1,0}$ is prime to ℓ, as shown in Table II. Hence $\ell \nmid h_1^-/h_0^-$ holds by Lemma 4. Next we assume $\ell \geq 113$. If ℓ divides h_1^-/h_0^-, then the same argument as above shows that, for some i with $1 \leq i \leq 5$, $y_{1,b} \equiv i \bmod \ell$ for all b. Then $y_{0,0} \equiv 13i - 36$ by Lemma 1, and hence

$$h_0^- \equiv 52, 26, \ell, \ell - 26, \ell - 52 \bmod \ell \tag{19}$$

by (7). The estimate (12) is $h_0^- \leq (\ell + 5)/2$ in this case, and hence the last three congruences in (19) are impossible, because $\ell - 52 > (\ell + 5)/2$ for $\ell \geq 113$. The other cases $h_0^- = 26, 52$ are also impossible because h_0^- is odd. Thus we have $\ell \nmid h_1^-/h_0^-$ in this case, too.

Table I. $\ell = q - 4 < 41$

ℓ	7	11	19	31
p	23	31	47	71
b	1	1	1	2
$y_{1,b} - y_{1,0}$	-3	-1	2	-2

Table II. $\ell = q - 6 < 113$

ℓ	3	5	23	89	107
p	19	23	59	191	227
$y_{1,1} - y_{1,0}$	2	-3	-1	1	1

This completes the proof of Proposition 1. $\square$

Remark. In the process of our proof dealing with the case $\ell = q - 2$, it is essential that, if ℓ divides h_n^-/h_{n-1}^-, the values $y_{n,b,\alpha}$ modulo ℓ would be independent of b and α (cf. (14)). This independence is no longer true for $\ell \leq q - 4$. For example, if $\ell = q - 4$ and ℓ divides h_n^-/h_{n-1}^-, then, for a given α, $y_{n,b,\alpha}$ can be i or $i + \ell$ for all b with $i = 1$, 2 or 3. Because of these three possibilities, the argument for the case $\ell = q - 2$ does not work for $\ell = q - 4$.

Exceptionally, we can cope with this difficulty when $n = 1$, as shown in the proof of Proposition 1(II) for $\ell = q - 4$ and $\ell = q - 6$. It would be possible to obtain an assertion similar to Proposition 1(II) for smaller ℓ with a similar method.

4. Proof of Proposition 2.

In this section we explain how we verified Proposition 2 with a computer. We adopt the notation of previous sections and assume $p \geq 7$ because the case $p = 3$ is already settled in Proposition 1. Lemma 4 is the basic tool for proving Proposition 2. Namely, for a given p, n and ℓ, if we can find some b and α which do not satisfy the congruence (9), then we can conclude that ℓ does not divide h_n^-/h_{n-1}^-. As a result of our search for appropriate b and α, it turned out that the value $\alpha = 1$ is sufficient for our purpose. So, we always take $\alpha = 1$ in this section. To sum up, our task is finding a b for which $y_{n,b} - y_{n,0}$ is prime to ℓ.

What we actually did is as follows. When a prime number p with $p \equiv 3 \bmod 4$ and $n \geq 1$ are given, we put

$$d(B) = \gcd\{y_{n,b} - y_{n,0} \mid 1 \leq b \leq B\}$$

for a natural number $B \leq p - 1$. We run a program which computes $d(B)$ for $B = 1, 2, \cdots$ until $d(B) = 1$

is attained. Our computation was carried out by using Maple 15 (cf. [5]) on Apple's Mac Pro computer with two 2.4 GHz quad-core Intel Xeon processor and 16GB memory. As a result, we could find a B with $d(B) = 1$ for all p and n treated in Proposition 2. If $d(B) = 1$ holds for some B, then, for any prime ℓ, the congruence (9) in Lemma 4 can not be satisfied for all b. Therefore, our computation certainly verifies Proposition 2.

We observe that the first value of B with $d(B) = 1$, say B_0, is not so large. The largest B_0 in the range of our computation is 17 attained when $p = 6043, n = 19$. For reference, we prepared Table III which shows a state of distribution of B_0. In Table III, N is the number of pairs (p, n) in the range of Proposition 2 for which the first value of B with $d(B) = 1$ is $B = B_0$, and "ratio" is $(N/61800) \times 100$, where 61800 is the total number of pairs (p, n) we treated.

Table III. Distribution of B_0

B_0	1	2	3	4	≥ 5
N	3671	34298	13627	5539	4665
ratio (%)	5.9	55.5	22.0	9.0	7.6

References

[1] P. E. Conner and J. Hurrelbrink, *Class number parity*, Series in Pure Mathematics, 8, World Sci. Publishing, Singapore, 1988.

[2] M. Gut, Abschätzungen für die Klassenzahlen der quadratischen Körper, Acta Arith. **8** (1962/1963), 113–122.

[3] K. Horie, Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field, J. London Math. Soc. (2) **66** (2002), no. 2, 257–275.

[4] K. Horie, The ideal class group of the basic $\boldsymbol{Z}_p$-extension over an imaginary quadratic field, Tohoku Math. J. (2) **57** (2005), no. 3, 375–394.

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

[6] 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. Semin. Univ. Hambg. **80** (2010), no. 2, 175–182.

[7] L. C. Washington, The non-p-part of the class number in a cyclotomic $\boldsymbol{Z}_p$-extension, Invent. Math. **49** (1978), no. 1, 87–97.

[8] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, 83, Springer, New York, 1997.