A note on the relative class number of the cyclotomic Z_p-extension of $Q(\sqrt{-p})$, II

By Humio Ichimura

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

(Communicated by Shigefumi Mori, M.J.A., Jan. 15, 2013)

Abstract: Let p be a prime number with $p \equiv 3 \bmod 4$, and let $k = \boldsymbol{Q}(\sqrt{-p})$. Denote by h_n^- the relative class number of the nth layer of the cyclotomic $\boldsymbol{Z}_p$-extension over k. Let $q = (p-1)/2$ and d_p be the largest divisor of q with $d_p < q$. Let ℓ be a prime number with $\ell \neq p$. We show that $\ell \nmid h_n^-$ for all $n \geq 0$ if $\ell \geq q - 2d_p$ and ℓ is a primitive root modulo p^2.

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

1. Introduction. Let p be an odd prime number with $p \equiv 3 \bmod 4$. Let $k = \boldsymbol{Q}(\sqrt{-p})$ and k_∞/k be the cyclotomic $\boldsymbol{Z}_p$-extension. For an integer $n \geq 0$, we denote by k_n the nth layer of k_∞/k with $k_0 = k$. Let h_n^- be 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, Theorem 16.12], the ℓ-part of h_n^- is stable for sufficiently large n. Horie [2, Theorem 2] showed that $\ell \nmid h_n^-/h_{n-1}^-$ 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. Let $q = (p-1)/2$. In the previous paper [4, Proposition 1(I)], we obtained the following simple result. (See Remark 1.)

Proposition 1. *If $\ell \geq q - 2$ and ℓ is a primitive root modulo p^2, then $\ell \nmid h_n^-$ for all $n \geq 0$.*

In this paper, we show the following stronger version (when q is a composite). In what follows, we assume that $p \geq 7$, so that $q > 1$. We denote by d_p the largest divisor of q with $d_p < q$. Clearly, $d_p > 1$ if and only if q is a composite.

Proposition 2. *If $\ell \geq q - 2d_p$ and ℓ is a primitive root modulo p^2, then $\ell \nmid h_n^-$ for all $n \geq 0$.*

When $p = 3$, it is shown in Horie [1, Proposition 3] that $\ell \nmid h_n^-$ for all n if ℓ is a primitive root modulo p^2. For $p = 7, 11, 19$, we obtain the following assertion using Proposition 2.

Proposition 3. *When $p = 7$, 11 or 19, ℓ does not divide h_n^- for all $n \geq 0$ if ℓ is a primitive root modulo p^2.*

Remark 1. The statement of [4, Proposition 1(I)] is that "If $\ell \geq q - 2$ and ℓ is a primitive root modulo p^2, then $\ell \nmid h_n^-/h_{n-1}^-$ for all $n \geq 1$". Since $\ell \nmid h_0^-$ when $\ell \geq q - 2$ (see Lemma 5), this implies that $\ell \nmid h_n^-$ for all n.

Remark 2. In the previous paper [3, Theorem 2], it is shown that when $p \leq 509$, h_n^-/h_{n-1}^- is odd for all $n \geq 1$.

2. Lemmas. Let p and q be as in Section 1. We write $d = d_p$ for brevity. As q is odd (and $q > 1$), we have

$$d \leq \frac{q}{3}. \tag{1}$$

Let μ_q be the group of qth roots of unity in the ring $\boldsymbol{Z}_p$ of p-adic integers. For a p-adic integer $x \in \boldsymbol{Z}_p$, denote by $s_n(x) \in \boldsymbol{Z}$ the unique integer such that $s_n(x) \equiv x \bmod p^{n+1}$ and $0 \leq s_n(x) < p^{n+1}$. For each integer b with $0 \leq b \leq p-1$ and $\alpha \in \boldsymbol{Z}_p$ with $\alpha \equiv 1 \bmod p$, we put

$$y_{n,b,\alpha} = \frac{1}{p^{n+1}} \sum_{\epsilon \in \mu_q} s_n(\epsilon\alpha(1 + p^n b)),$$

where ϵ runs over the qth roots of unity. As $q > 1$, we see that $y_{n,b,\alpha}$ is an integer.

Lemma 1. *We have $d \leq y_{n,b,\alpha} \leq q - d$.*

Proof. Let $r = q/d$. As $d < q$, we have $r > 1$. Let μ_r be the group of rth roots of unity in $\boldsymbol{Z}_p$. We put

$$z_{n,b,\alpha} = \frac{1}{p^{n+1}} \sum_{\epsilon \in \mu_r} s_n(\epsilon\alpha(1 + p^n b)),$$

where ϵ runs over the rth roots of unity. As $r > 1$, $z_{n,b,\alpha}$ is an integer. Since $\epsilon\alpha(1 + p^n b)$ is a unit of $\boldsymbol{Z}_p$, we have $s_n(\epsilon\alpha(1 + p^n b)) > 0$. It follows that

2000 Mathematics Subject Classification. Primary 11R18.

doi: 10.3792/pjaa.89.21

$$1 \le z_{n,b,\alpha} \le r-1. \tag{2}$$

Let $\eta_1, \cdots, \eta_d$ be a complete set of representatives of the quotient μ_q/μ_r. Then we easily see that

$$y_{n,b,\alpha} = \sum_{i=1}^{d} z_{n,b,\eta_i\alpha}.$$

Hence, it follows from (2) that

$$d \le y_{n,b,\alpha} \le d(r-1) = q-d. \qquad \square$$

The following three lemmas are shown in [4].

Lemma 2 ([4, Lemma 1]). *For any $n \ge 1$ and α, we have*

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

Lemma 3 ([4, Lemma 2]). *For any $n \ge 1$ and α, $y_{n,b,\alpha} \ne y_{n,0,\alpha}$ for some b with $1 \le b \le p-1$.*

Lemma 4 ([4, Lemma 4]). *Assume that ℓ divides h_n^-/h_{n-1}^- and that ℓ is a primitive root modulo p^2. Then, for each $\alpha \in \boldsymbol{Z}_p$ with $\alpha \equiv 1 \bmod p$, we have*

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

for all b with $0 \le b \le p-1$.

Lemma 5. *Let p be a prime number with $p \equiv 3 \bmod 4$. Let ℓ be a prime number with $\ell \ge q-2d$. Then ℓ does not divide h_0^-.*

Proof. By Corollary to Narkiewicz [5, Theorem 4.10], we have

$$h_0^- \le \left(\frac{1}{\pi} + \frac{0.35}{\log p}\right)\sqrt{p}\log p.$$

As $\ell \ge q-2d$, it follows from (1) that $\ell \ge (p-1)/6$. When $p > 350$, we can show

$$\frac{p-1}{6} > 0.38\sqrt{p}\log p > \left(\frac{1}{\pi} + \frac{0.35}{\log 350}\right)\sqrt{p}\log p$$

in an elementary way. Hence, the assertion holds when $p > 350$. When $11 \le p < 350$, we see that $q - 2d > h_0^-$ from the table of Wada and Saito [6] on class groups of imaginary quadratic fields, and obtain the assertion in this case. When $p = 7$, the assertion is obvious as $h_0^- = 1$. $\square$

3. Proof of propositions.

Proof of Proposition 2. Let ℓ be a prime number with $\ell \ge q-2d$ which is a primitive root modulo p^2. By Lemma 5, it suffices to show that $\ell \nmid h_n^-/h_{n-1}^-$ for all $n \ge 1$. First, we deal with the case $\ell > q-2d$. As $d+\ell > q-d$, we have $d \le y_{n,b,\alpha} < d+\ell$ by Lemma 1. Hence, if ℓ divides h_n^-/h_{n-1}^-, then it follows from Lemma 4 that with any α, $y_{n,b,\alpha} = y_{n,0,\alpha}$ for all $0 \le b \le p-1$. However, this is impossible by Lemma 3.

Next, let $\ell = q-2d$. Then, by Lemma 1, we have $d \le y_{n,b,\alpha} \le d+\ell$. Assume that ℓ divides h_n^-/h_{n-1}^-. Then we see by Lemmas 3 and 4 that with any α, we have $y_{n,b,\alpha} \equiv d \bmod \ell$ for all b. From Lemma 2 and $q = \ell + 2d$, it follows that

$$y_{n-1,0,\alpha} = \sum_{b=0}^{p-1} y_{n,b,\alpha} - q^2 \equiv pd - q^2 \equiv d \bmod \ell.$$

Noting that $y_{n-1,0,(1+p^{n-1}b)\alpha} = y_{n-1,b,\alpha}$, we observe that $y_{n-1,b,\alpha} \equiv d \bmod \ell$ for any α and b. Repeating this process, we finally obtain $y_{0,0,1} \equiv d \bmod \ell$. By the class number formula for imaginary quadratic fields, we have

$$h_0^- = -2y_{0,0,1} + q.$$

(For this, see the formula (7) of [4].) Then we obtain $h_0^- \equiv 0 \bmod \ell$, which is impossible by Lemma 5. $\square$

Proof of Proposition 3. Because of Remark 2, we may as well assume that ℓ is odd as $h_0^- = 1$ for $p = 7, 11, 19$. For $p = 7$, we see that $q - 2d_p = 1$ and hence the assertion follows immediately from Proposition 2. For $p = 11$ (resp. 19), we see that $q - 2d_p = 3$ and that an odd prime number ℓ is a primitive root modulo p^2 when $\ell = 7, 13, \cdots$ (resp. $\ell = 3, 13, \cdots$). Thus, we obtain the assertion in this case. $\square$

Remark 3. Let $p = 23$ (resp. 31). Then $q - 2d_p = 9$ (resp. 5), and an odd prime number ℓ is a primitive root modulo p^2 when $\ell = 5, 7, 11, \cdots$ (resp. $\ell = 3, 11, \cdots$). Thus, we can not apply Proposition 2 for small ℓ.

Corrigenda. The previous paper [4] contains some quite minor missprints. Change ψ to ψ_n in the lines 6, 17 and 22 of the right column of page 17 and the line 26 of the left column of page 18. Change the right hand side of the formula (6) in page 18 as follows:

$$p\prod_{\psi_n}\left(-\frac{1}{2}B_{1,\delta\psi_n}\right) \Rightarrow \prod_{\psi_n}\left(-\frac{1}{2}B_{1,\delta\psi_n}\right).$$

References

[1] 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.

[2] 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.

[3] 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), no. 1, 317–342.

[4] H. Ichimura and S. Nakajima, A note on the relative class number of the cyclotomic $\boldsymbol{Z}_p$-extension of $\boldsymbol{Q}(\sqrt{-p})$, Proc. Japan Acad. Ser. A Math. Sci. **88** (2012), no. 1, 16–20.

[5] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 3rd ed., Springer Monographs in Mathematics, Springer, Berlin, 2004.

[6] H. Wada and M. Saito, *A table of the ideal class groups of imaginary quadratic fields*, Sophia Kokyuroku in Mathematics, vol. 28, Department of Mathematics, Sophia Univ., Tokyo, 1988.

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