Comm. Korean Math. Soc. **13** (1998), No. 2, pp. 233–242

ON THE $\mathbb{Z}_p$-EXTENSIONS OVER $\mathbb{Q}(\sqrt{m})$

JAE MOON KIM

ABSTRACT. Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field. In this paper, the following theorems on p-divisibility of the class number h of k are studied for each prime p.

THEOREM 1. *If the discriminant of k has at least three distinct prime divisors, then 2 divides h.*

THEOREM 2. *If an odd prime p divides h, then p divides $B_{1,\chi\omega^{-1}}$, where χ is the nontrivial character of k, and ω is the Teichmüller character for p.*

THEOREM 3. *Let h_n be the class number of k_n, the nth layer of the $\mathbb{Z}_p$-extension k_∞ of k. If p does not divide $B_{1,\chi\omega^{-1}}$, then $p \nmid h_n$ for all $n \geq 0$.*

1. Introduction

Fix a square free positive integer m and let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field of discriminant d. The history of the study of the class number of these real quadratic fields goes back to Gauss, who conjectured that there are infinitly many real quadratic fields of class number 1. Class numbers of these real quadratic fields have been studied in many different ways since then.

In this paper we study the class number of k by examining the p-divisibility of the class number for each odd prime p. When p=2, as we will see later in this section, a well known cohomological argument shows that if the discriminant d of k has at least three distinct prime divisors, then the class number is divisible by 2. The answer for p=3 is

Received May 15, 1997. Revised February 2, 1998.

1991 Mathematics Subject Classification: primary 11R11, 11R29, secondary 11R23.

Key words and phrases: class number, Kummer pairing, circular units.

This work was supported by research fund of Inha University, 1996 and was completed during the sabbatical year, 1996-1997

also known([2], [4]): if 3 divides the class number of k, then 3 divides the class number of $\mathbb{Q}(\sqrt{-3m})$. This can be proved either by applying the p-adic class number formula or by using the Kummer pairing as A. Scholz did([2]).

In this paper, we will generalize this to find and prove a similar statement for an arbitrary odd prime p. Let χ be the nontrivial character of k, and ω be the Teichmüller character for p. Let $B_{1,\chi\omega^{-1}}$ be the first generalized Bernoulli number for the character $\chi\omega^{-1}$. For instance, when $p = 3$, $\chi\omega^{-1}$ belongs to the field $\mathbb{Q}(\sqrt{-3m})$ and $-B_{1,\chi\omega^{-1}}$ is the class number of $\mathbb{Q}(\sqrt{-3m})$. And thus, the result for $p = 3$ can be stated as follows: if 3 divides the class number of k, then 3 divides $B_{1,\chi\omega^{-1}}$. We generalize this last statement to an arbitrary odd prime p.

THEOREM 2. *Let $k=\mathbb{Q}(\sqrt{m})$ and p be an odd prime. If p divides the class number of k, then p divides $B_{1,\chi\omega^{-1}}$.*

Theorem 2 can be generalized further. Let k_∞ be the $\mathbb{Z}_p$-extension of k and h_n be the class number of k_n, the nth layer of the $\mathbb{Z}_p$-extension. Then we have

THEOREM 3. *Let $k = \mathbb{Q}(\sqrt{m})$ and p be an odd prime. If p does not divide $B_{1,\chi\omega^{-1}}$, then $p \nmid h_n$ for all $n \geq 0$.*

The aim of this paper is to prove these two theorems. To prove theorem 2, one may use either the p-adic class number formula or the Kummer pairing or the main conjecture of Iwasawa theory as was done in [1]. Even though the proof using the p-adic class number formula or the main conjecture is much shorter, we will make use of the Kummer pairing for the proof since it gives some additional information on p-ranks of certain eigenspaces of the ideal class group.

When there is only one prime in k above p, it is well known that $p \nmid h_0$ if and only if $p \nmid h_n$ for all $n \geq 0$. So theorem 2 implies theorem 3 in this case. Thus, we will only consider when p splits in k. The proof of theorem 3 relies on some results developed in [1] on the circular units of abelian fields defined by W. Sinnott in [3]. We will review them in section 3.

We finish this section with a brief discussion on the p-divisibility of the class number when $p = 2$.

THEOREM 1. *Let $k = \mathbb{Q}(\sqrt{m})$. If the discriminant of k has at least three distinct prime divisors, then 2 divides the class number of k.*

PROOF. Let Δ_k be the Galois group $Gal(k/\mathbb{Q})$. Let I, P and C be the ideal group, its subgroup generated by principal ideals and the ideal class group of k respectively. From the short exact sequence

$$0 \to P \to I \to C \to 0,$$

we get a long exact sequence

$$0 \to P^{\Delta_k} \to I^{\Delta_k} \to C^{\Delta_k} \to .$$

Let E_k be the unit group of k. Then from the exact sequence

$$0 \to E_k \to k^\times \to P \to 0,$$

we have another long exact sequence

$$0 \to \{\pm 1\} \to \mathbb{Q}^\times \to P^{\Delta_k} \to H^1(\Delta_k, E_k) \to 0,$$

since $H^1(\Delta_k, k^\times) = 0$ by Hilbert theorem 90. By combining these two long exact sequences, we obtain a sequence

$$0 \to H^1(\Delta_k, E_k) \to (\mathbb{Z}/2\mathbb{Z})^e \to C^{\Delta_k} \to,$$

where e is the number of primes which ramify in k. By assumption, $e \geq 3$. But since the order of $H^1(\Delta_k, E_k)$ is at most 4, C^{Δ_k} is not trivial. Hence 2 divides the class number of k. □

2. Kummer pairing

Let p be an odd prime and $L = k(\zeta_p)$. We assume that $k \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ (for otherwise, $k = \mathbb{Q}(\sqrt{p})$ and $p \equiv 1 \bmod 4$, in which case p does not divide the class number of k). Let L' be the maximal unramified elementary abelian p-extension of L and let $H = Gal(L'/L)$. Then $L' = L(\sqrt[p]{B})$ for some subgroup B of $L^\times/(L^\times)^p$ and there is a nondegenerate

bilinear pairing $H \times B \to W = \{$ pth root of $1\}$ defined by $< h, b >= h(b^{\frac{1}{p}})/b^{\frac{1}{p}}$. Let A be the Sylow p-subgroup of the ideal class group of L. Let $R = Gal(k(\zeta_p)/k)$, $\Delta_k = Gal(k(\zeta_p)/\mathbb{Q}(\zeta_p))$ and $G = R \times \Delta_k = Gal(k(\zeta_p)/\mathbb{Q})$. We denote elements of R by σ_a, where $\sigma_a(\zeta_p) = \zeta_p^a$ and those of Δ_k by ρ^i for $i = 0, 1$. Then $H \simeq A/A^p$ as G-modules (G acts on H by conjugation) and $< h, b >^g =< h^g, b^g >$ for $g \in G$. For each character θ in G, let ϵ_θ be the idempotent of θ in $\mathbb{Z}_p[G]$,i.e.,

$$\epsilon_\theta = \frac{1}{2(p-1)} \sum_{\substack{0 \le i \le 1 \\ 1 \le a < p}} \theta(\sigma_a^{-1}\rho^i)\sigma_a\rho^i.$$

For any G-module M, we have a direct sum decomposition $M = \bigoplus_{\theta \in \hat{G}} \epsilon_\theta M$.

Let χ be the nontrivial character in $\hat{\Delta}_k$ and ω be the Teichmüller character in $\hat{R}$. We can think of χ and ω as elements of $\hat{G}$ in obvious ways. Since

$$\epsilon_\chi = \frac{1}{2(p-1)} \sum_{\substack{0 \le i \le 1 \\ 1 \le a < p}} \chi(\sigma_a^{-1}\rho^{-i})\sigma_a\rho^i = \frac{1}{2(p-1)}(1-\rho)N_{L/k},$$

we have $\epsilon_\chi A \subset A_k$, Sylow p-subgroup of the ideal class group of k. Conversely, if $a \in A_k$, then $(1+\rho)a = 0$ and $N_{L/k}(a) = (p-1)a$. Thus

$$a = \frac{1}{2}(1-\rho)a = \frac{1}{2(p-1)}(1-\rho)N_{L/k}(a) = \epsilon_\chi a.$$

Therefore, we have $A = \bigoplus_{\theta \in \hat{G}} \epsilon_\theta A$, with $\epsilon_\chi A = A_k$. By a p-rank of an abelian group M, we mean the p-rank of M/M^p.

THEOREM 2. *Let r and s be the p-ranks of A_k and $\epsilon_{\chi\omega}A$ respectively. Then $r \le s \le r+1$. In particular, if p divides the class number of k, then p divides $B_{1,\chi\omega^{-1}}$.*

PROOF. Note that the pairing $H \times B \to W$ induces nondegenerate pairings

$$\epsilon_\chi H \times \epsilon_{\chi\omega} B \to W \text{ and } \epsilon_{\chi\omega} H \times \epsilon_\chi B \to W.$$

We will check the first one only. For this, it is enough to show $< \epsilon_\chi H, \epsilon_\theta B >= 1$ unless $\theta = \chi\omega$. Suppose $h \in \epsilon_\chi H$. If $b \in \epsilon_{\omega^i} B$, then $h^\rho = h^{\chi(\rho)} = h^{-1}$ and $b^\rho = b^{\omega^i(\rho)} = b$. Thus

$$< h, b >^\rho = < h^\rho, b^\rho > = < h^{-1}, b > = < h, b >^{-1} .$$

Since $< h, b > \in \mathbb{Q}(\zeta_p)$ and since ρ fixes $\mathbb{Q}(\zeta_p)$, we have

$$< h, b > = < h, b >^\rho = < h, b >^{-1} .$$

Therefore $< h, b >= 1$, and so $< \epsilon_\chi H, \epsilon_{\omega^i} B >= 1$. If $b \in \epsilon_{\chi\omega^i} B$, then $h^{\sigma_a} = h^{\chi(\sigma_a)} = h$ and $b^{\sigma_a} = b^{\chi\omega^i(\sigma_a)} = b^{\omega^i(a)}$. Thus

$$< h, b >^{\sigma_a} = < h^{\sigma_a}, b^{\sigma_a} > = < h, b^{\omega^i(a)} > = < h, b >^{\omega^i(a)}$$

for every a, $1 \leq a \leq p-1$. If $i \neq 1$,then this is impossible unless $< h, b >= 1$. Therefore $< \epsilon_\chi H, \epsilon_{\chi\omega^i} B >= 1$ for $i \neq 1$.

Hence we have $\epsilon_\chi H \simeq \widehat{\epsilon_{\chi\omega} B} \simeq \epsilon_{\chi\omega} B$ and $\epsilon_{\chi\omega} H \simeq \widehat{\epsilon_\chi B} \simeq \epsilon_\chi B$. Note that we have a G-linear homomorphism

$$\phi : B \to A_p = \{x \in A | x^p = 1\}$$

with $Ker\phi \subset E/E^p$, where E is the group of units of L. This map ϕ induces

$$\phi : \epsilon_{\chi\omega} B \to \epsilon_{\chi\omega} A_p \text{ and } \phi : \epsilon_\chi B \to \epsilon_\chi A_p$$

whose kernels are contained in $\epsilon_{\chi\omega}(E/E^p)$ and $\epsilon_\chi(E/E^p)$ respectively. Since

$$\epsilon_\chi = \frac{1}{2(p-1)}(1-\rho)N_{L/k},$$

we have

$$\epsilon_\chi(E/E^p) = E_k/E_k^p \simeq \mathbb{Z}/p\mathbb{Z},$$

where E_k is the unit group of k. We claim that $\epsilon_{\chi\omega}(E/E^p) = \{1\}$. Note that

$$\begin{aligned} \epsilon_{\chi\omega} &= \frac{1}{2(p-1)} \sum_{1 \leq a < p, 0 \leq i \leq 1} \chi\omega(\sigma_a^{-1}\rho^i)\sigma_a\rho^i \\ &= \frac{1+\rho\sigma_{-1}}{2} \frac{1}{p-1} \sum_a \omega(\sigma_a^{-1})\sigma_a. \end{aligned}$$

Let M be the subfield of L fixed by $\{1, \rho\sigma_{-1}\}$. Then

$$\epsilon_{\chi\omega} = \frac{1}{2(p-1)}(\sum_a \omega(\sigma_a^{-1})\sigma_a)N_{L/M},$$

and so

$$\epsilon_{\chi\omega}(E/E^p) \subset \frac{1}{2(p-1)}(\sum_a \omega(\sigma_a^{-1})\sigma_a)(E_M/E_M^p),$$

where E_M is the unit group of M. Since M is a CM field, $[E_M : W_M E_M^+] = 1$ or 2, where W_M is the group of roots of 1 in M and E_M^+ is the unit group of the maximal real subfield of M, which is $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Since $W_M = \{\pm 1\}$,

$$E_M/E_M^p \simeq E_M^+/(E_M^+)^p.$$

For $\eta \in E_M^+$, $\eta^{\sigma_a} = \eta^{\sigma_{-a}}$ and thus

$$\eta^{\omega(\sigma_{-a})\sigma_{-a} + \omega(\sigma_a)\sigma_a} = 1.$$

Therefore

$$\epsilon_{\chi\omega}(E/E^p) \subset \frac{1}{2(p-1)}(\sum_a \omega(\sigma_a^{-1})\sigma_a)(E_M^+/(E_M^+)^p) = \{1\}.$$

By putting everything together with the additional information $\epsilon_\theta A \simeq \epsilon_\theta H$ for every θ, we get the desired inequality $r \leq s \leq r+1$.

To prove the second statement in the theorem, let η be the Stikelberger element for $k(\zeta_p)$, i.e.,

$$\eta = \frac{1}{f} \sum_{\substack{a \bmod f \\ (a,f)=1}} a\rho_a^{-1}|_L,$$

where f is the conductor of k and ρ_a is an element of $Gal(\mathbb{Q}(\zeta_f)/\mathbb{Q})$ such that $\rho_a(\zeta_f) = \zeta_f^a$. Notice that

$$\epsilon_{\chi\omega}\eta = (\frac{1}{f}\sum_a a\chi\omega(\rho_a^{-1}))\epsilon_{\chi\omega} = B_{1,\chi\omega^{-1}}\epsilon_{\chi\omega}.$$

By the Stickelberger theorem, $(a - \rho_a)\eta A = 0$ for all a, $(a, f) = 1$. Thus

$$\epsilon_{\chi\omega}(a - \rho_a)\eta A = (a - \chi\omega(\rho_a))B_{1,\chi\omega^{-1}}\epsilon_{\chi\omega}A = 0$$

for all a, $(a, f) = 1$. Take a such that $a - \chi\omega(\rho_a)$ is not divisible by p (for instance, choose i such that $\chi(\rho_{1+ip}) = -1$ and let $a = 1 + ip$). Hence if $A_k \neq 0$, then $\epsilon_{\chi\omega}A \neq 0$, and therefore $B_{1,\chi\omega^{-1}} \equiv 0 \ mod\ p$. □

3. $\mathbb{Z}_p$-extension of k

Let P_n be the multiplicative subgroup of $\mathbb{Q}(\zeta_n)^\times$ generated by $\{\pm 1\}$ and $\{1-\zeta_n^a \mid 0<a<n\}$. Then the group $C_{\mathbb{Q}(\zeta_n)}$ of cyclotomic units of $\mathbb{Q}(\zeta_n)$ is defined to be

$$C_{\mathbb{Q}(\zeta_n)} = E_{\mathbb{Q}(\zeta_n)} \cap P_n,$$

where $E_{\mathbb{Q}(\zeta_n)}$ is the group of units of $\mathbb{Q}(\zeta_n)$. In general, for an abelian field F, W. Sinnott defines the group of circular units of F as follows. For each $n>2$, let

$$F_n = F \cap \mathbb{Q}(\zeta_n) \text{ and } C_{F_n} = N_{\mathbb{Q}(\zeta_n)/F_n}(C_{\mathbb{Q}(\zeta_n)}),$$

where $C_{\mathbb{Q}(\zeta_n)}$ is the group of the cyclotomic units of $\mathbb{Q}(\zeta_n)$ as above. Then the group C_F of circular units of F is defined to be the multiplicative subgroup of $F^\times$ generated by C_{F_n} together with -1 (see [3]). Namely,

$$C_F =< -1,\ C_{F_n} > .$$

Note that if n is prime to the conducter of F, then $F_n = \mathbb{Q}$ and so $C_{F_n} = \{1\}$. Thus there are only finitely many n's to be considered in the definition of C_F. For example, when $F = k = \mathbb{Q}(\sqrt{m})$, $C_k =< N_{\mathbb{Q}(\zeta_d)/k}(C_{\mathbb{Q}(\zeta_d)}), -1 >$, where d is the conductor of k (d will always mean the conductor of k). To see this, first observe that $k \cap \mathbb{Q}(\zeta_n)$ is either $\mathbb{Q}$ or k. If $k \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$, then $C_{k_n} = \{1\}$. Otherwise, $\mathbb{Q}(\zeta_n)$ contains $\mathbb{Q}(\zeta_d)$ as a subfield and thus $N_{\mathbb{Q}(\zeta_n)/k}(C_{\mathbb{Q}(\zeta_n)})$ is contained in $N_{\mathbb{Q}(\zeta_d)/k}(C_{\mathbb{Q}(\zeta_d)})$.

Fix an odd prime p with $(p,m)=1$, and let $k_\infty = \bigcup_{n\geq 0} k_n$ be the $\mathbb{Z}_p$-extension of $k = k_0 = \mathbb{Q}(\sqrt{m})$. Here, k_n means the nth layer of the $\mathbb{Z}_p$-extension, not $k \cap \mathbb{Q}(\zeta_n)$. For each $n \geq 0$, we denote the group of circular units of k_n by C_n. It is not hard to show that

$$C_n = C_{n-1}\left(N_{\mathbb{Q}(\zeta_{p^{n+1}d})/k_n}(C_{\mathbb{Q}(\zeta_{p^{n+1}d})})\right)\left(N_{\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}_n}(C_{\mathbb{Q}(\zeta_{p^{n+1}})})\right),$$

where $\mathbb{Q}_n$ is the subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ whose degree over $\mathbb{Q}$ is p^n. Thus the generators of C_n are given so explicitly that we can compute the cohomology groups of circular units in the $\mathbb{Z}_p$-extension. Another feature of the circular units is the following index theorem discovered by W. Sinnott([3]).

THEOREM. *Let E_n be the unit group of k_n and h_n be the class number of k_n. Then $[E_n : C_n] = 2^{c_n} h_n$ for some integer c_n.*

In order to describe the cohomology groups of circular units, we need some more notations. For each integer s, we choose a primitive sth root of 1 so that $\zeta_t^{\frac{t}{s}} = \zeta_s$ if $s|t$. Let $L = \mathbb{Q}(\zeta_{pd})$ and L_∞ be its basic $\mathbb{Z}_p$-extension. Let σ be the topological generator of the Galois group $\Gamma = Gal(L_\infty/L)$ which maps ζ_{p^n} to $\zeta_{p^n}^{1+p}$ for all $n \geq 1$. Restrictions of σ to various subfields are also denoted by σ. Let $\Delta = Gal(K/k)$ and $\Delta_k = Gal(k/\mathbb{Q})$. Let $R = \{\omega \mid \omega^{p-1} = 1\}$ be the set of roots of 1 in $\mathbb{Z}_p$. Then R can be regarded as the Galois group $Gal(F/\mathbb{Q})$, where $F = \mathbb{Q}(\zeta_p)$. For $m > n$, let $G_{m,n}$ be the Galois group $Gal(k_m/k_n)$ and we will abbreviate $G_{m,0}$ by G_m. In [1], the following results on the cohomology groups of circular units are proved.

THEOREM. *Suppose p splits in k. For $m > n \geq 0$, we have the followings.*

(1) $$C_m^{G_{m,n}} = C_n,$$

(2) $$\widehat{H}^0(G_{m,n}, C_m) \simeq \mathbb{Z}/p^{m-n}\mathbb{Z},$$

(3) $$\widehat{H}^{-1}(G_{m,n}, C_m) \simeq (\mathbb{Z}/p^{m-n}\mathbb{Z})^2.$$

In fact, the following generators of $\widehat{H}^{-1}(G_n, C_n)$ are given in [1]. Let p be an odd prime which splits in k and let

$$\delta_n = \prod_{\omega \in R, \tau \in \Delta} (\zeta_{p^{n+1}}^{\omega} - \zeta_d^{\tau}), \quad \pi_n = \prod_{\omega \in R} (\zeta_{p^{n+1}}^{\omega} - 1).$$

Then δ_n and $\pi_n^{\sigma-1}$ generate $\widehat{H}^{-1}(G_n, C_n)$. And theorem 3 of [1] says the following congruence.

THEOREM. *Let ρ be the nontrivial element in Δ_k and $\pi = \zeta_{p^2} - 1$. Then, in $\mathbb{Q}_p(\zeta_{p^2})$, we have*

$$\delta_1^{1-\rho} \equiv 1 + \sqrt{d} B_{1,\chi\omega^{-1}} \pi^{p-1} \ mod\ (\zeta_p - 1).$$

Before we prove our main theorem 3, we need a lemma.

LEMMA. *Suppose p splits in k and $p \nmid B_{1,\chi\omega^{-1}}$. Then $\widehat{H}^{-1}(G_n, C_n) \to \widehat{H}^{-1}(G_n, E_n)$ is injective for all $n > 0$.*

PROOF. We prove this by induction on n. Suppose $\delta_1^a \pi_1^{(\sigma-1)b} = \eta_1^{\sigma-1}$ for some $\eta_1 \in E_1$. Since $\pi_1 \in \mathbb{Q}_1$, $\pi_1^{\rho} = \pi_1$. Thus

$$\delta_1^{a(1-\rho)} = \eta_1^{(1-\rho)(\sigma-1)}.$$

Read this equation modulo $(\zeta_p - 1)$ in $\mathbb{Q}_p(\zeta_{p^2})$. Then we have

$$\delta_1^{a(1-\rho)} \equiv 1 + a\sqrt{d}B_{1,\chi\omega^{-1}}\pi^{p-1} \ mod\ (\zeta_p - 1)$$

and

$$\eta_1^{(1-\rho)(\sigma-1)} \equiv 1 \ mod\ (\zeta_p - 1).$$

Therefore $a\sqrt{d}B_{1,\chi\omega^{-1}} \equiv 0 \ mod\ p$. Since $p \nmid B_{1,\chi\omega^{-1}}$, $a \equiv 0 \ mod\ p$, and thus $b \equiv 0 \ mod\ p$. This takes care of the case when $n = 1$. □

Now we assume the result for $n-1$ and let

$$\delta_n^a \pi_n^{(\sigma-1)b} = \eta_n^{\sigma-1}$$

for some $\eta_n \in E_n$. Then by taking norms of both sides from k_n to k_{n-1}, we have

$$\delta_{n-1}^a \pi_{n-1}^{(\sigma-1)b} = N_{k_n/k_{n-1}}(\eta_n)^{\sigma-1}.$$

Thus by the induction hypothesis, we get $a \equiv b \equiv 0 \ mod\ p^{n-1}$. Note that

$$\delta_n^{p^{n-1}} = \delta_1 \xi^{\sigma-1} \text{ and } \pi_n^{p^{n-1}} = \pi_1 \mu^{\sigma-1}$$

for some ξ, μ in C_n. Therefore

$$\delta_1^{a_1} \pi_1^{(\sigma-1)b_1} = u_n^{\sigma-1}$$

for some $u_n \in E_n$, where $a = a_1 p^{n-1}$ and $b = b_1 p^{n-1}$. Now consider the composition of the following maps:

$$H^1(G_1, C_1) \longrightarrow H^1(G_1, E_1) \longrightarrow H^1(G_n, E_n).$$

Since G_1 is cyclic, the injectivity of $\widehat{H}^{-1}(G_1, C_1) \to \widehat{H}^{-1}(G_1, E_1)$ implies the injectivity of $H^1(G_1, C_1) \to H^1(G_1, E_1)$. And since the inflation map on the first cohomology group is injective, $H^1(G_1, E_1) \to H^1(G_n, E_n)$ is also injective. Hence the composition is injective, from which we have

$$\delta_1^{a_1} \pi_1^{(\sigma-1)b_1} = \xi_1^{\sigma-1}$$

for some $\xi_1 \in C_1$. Therefore $a_1 \equiv b_1 \equiv 0 \ mod\ p$, and so $a \equiv b \equiv 0 \ mod\ p^n$.

THEOREM 3. *Let $k = \mathbb{Q}(\sqrt{m})$ and p be an odd prime. If $p \nmid B_{1,\chi\omega^{-1}}$, then $p \nmid h_n$ for all $n \geq 0$.*

PROOF. By theorem 2, $p \nmid h_0$. Thus by the index theorem of W. Sinnott, $p \nmid [E_0 : C_0]$. From the short exact sequence $0 \to C_n \to E_n \to E_n/C_n \to 0$, we get a long exact sequence

$$0 \to C_0 \to E_0 \to (E_n/C_n)^{G_n} \to H^1(G_n, C_n) \to H^1(G_n, E_n) \to .$$

Since $p \nmid B_{1,\chi\omega^{-1}}$, $\widehat{H}^{-1}(G_n, C_n) \to \widehat{H}^{-1}(G_n, E_n)$ is injective by the lemma. Since G_n is cyclic, $\widehat{H}^{-1}(G_n, *)$ is isomorphic to $H^1(G_n, *)$, and thus $H^1(G_n, C_n) \to H^1(G_n, E_n)$ is also injective. Hence $(E_n/C_n)^{G_n} \simeq E_0/C_0$. Therefore p does not divide $\#(E_n/C_n)^{G_n}$, and $p \nmid [E_n : C_n]$. So $p \nmid h_n$ by the index theorem again. □

References

[1] J. M. Kim, *Class numbers of real quadratic fields*, Bull. Austral. Math. Soc. **57** (1988), 261-274.

[2] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. reine angew. Math. **166** (1932), 201–203.

[3] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), 181–234.

[4] L. Washington, *Introduction to Cyclotomic Fields*, G. T. M. 83, Springer-Verlag, New York, 1980.

Department of Mathematics
Inha University
Inchon 402-751, Korea
E-mail: jmkim@math.inha.ac.kr