A note on integral bases of unramified cyclic extensions of prime degree, II

Humio Ichimura* and Hiroki Sumida†

October 30, 2000

Abstract

Let p be a prime number and K a number field containing a primitive p–th root of unity. It is known that an unramified cyclic extension L/K of degree p has a power integral basis if it has a normal integral basis. We show that for all p, the converse is not true in general.

1 Introduction

This is a sequel to the previous papers [10, 11, 12, 13]. For a finite extension L/K of a number field K, it has a power integral basis (PIB for short) when $O_L = O_K[\alpha]$ for some $\alpha \in O_L$. Here, O_L (resp. O_K) is the ring of integers of L (resp. K). If L/K is Galois, it has a normal integral basis (NIB for short) when O_L is free of rank one over the group ring $O_K[\mathrm{Gal}(L/K)]$. Let p be a prime number and K a number field containing a primitive p–th root ζ_p of unity. Then, it is known that an unramified cyclic extension L/K of degree p has a PIB if it has a NIB (cf. Childs [3], [11]). Here and in what follows,

[1]Department of Mathematics, Yokohama City University, 22–2, Seto, Kanazawa–ku, Yokohama, 236–0027, Japan. e-mail:ichimura@math.yokohama-cu.ac.jp
Partially supported by Grant–in–Aid for Scientific Research (C) (No.11640041), the Ministry of Education, Science, Sports and Culture of Japan.
[2]Faculty of Integrated Arts and Sciences, Hiroshima University, Kagamiyama, Higashi–Hiroshima, 739–8521, Japan. e-mail:sumida@mis.hiroshima-u.ac.jp
Partially supported by Grant–in–Aid for Encouragement of Young Scientists (No.11740020), the Ministry of Education, Science, Sports and Culture of Japan.
Mathematics Subject classification (1991):11R33, 11R23.

an extension of a number field is "unramified" when it is unramified at all finite prime divisors. On the other hand, we showed in [10, 12, 13] that when $p = 2,\ 3$, there exist infinitely many number fields K with $\zeta_p \in K^\times$ each of which has an unramified cyclic extension of degree p with PIB but no NIB. The main purpose of this note is to show that this assertion holds for all p. Namely, we prove the following:

Theorem 1. *Let p be an odd prime number, and N a multiple of $(p-1)p$. Then, there exist infinitely many number fields K of degree N each of which contains ζ_p and has an unramified cyclic extension of degree p with PIB but no NIB.*

In the next section, we give more precise statements after recalling some notation and related assertions.

2 Theorems

Let p be a fixed prime number, K a number field not necessarily containing ζ_p, and $E = E_K$ the group of units of K. Put $\pi = \zeta_p - 1$. An element $\alpha \in K^\times$ relatively prime to p is "singular primary" when $(\alpha) = \mathfrak{A}^p$ for some ideal $\mathfrak{A}$ of K and $\alpha \equiv u^p \bmod \pi^p$ for some $u \in O_K$. The class in $K^\times/(K^\times)^p$ represented by α is written in the form $[\alpha]$ or $[\alpha]_K$. We define subgroups $\mathcal{H}(K)$, $\mathcal{E}(K)$, $\mathcal{N}(K)$ of $K^\times/(K^\times)^p$ by

$$\begin{aligned} \mathcal{H}(K) &:= \{[\alpha] \in K^\times/(K^\times)^p \bigm| \alpha \text{ is singular primary}\}, \\ \mathcal{E}(K) &:= \mathcal{H}(K) \cap E(K^\times)^p/(K^\times)^p, \\ \mathcal{N}(K) &:= \{[\epsilon] \in E(K^\times)^p/(K^\times)^p \bigm| \epsilon \in E,\ \epsilon \equiv 1 \bmod \pi^p\}. \end{aligned}$$

Clearly, we have

$$\mathcal{N}(K) \subseteq \mathcal{E}(K) \subseteq \mathcal{H}(K).$$

We write $(\mathcal{E}/\mathcal{N})(K)$ for the quotient $\mathcal{E}(K)/\mathcal{N}(K)$. We often regard these groups as vector spaces over $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Let us assume that $\zeta_p \in K^\times$. Then, it is well known (cf. Washington [23, Exercises 9.2, 9.3]) that for $[\alpha] \in K^\times/(K^\times)^p$, the cyclic extension $K(\alpha^{1/p})/K$ is unramified if and only if $[\alpha] \in \mathcal{H}(K)$. In [3], Childs proved that for $[\alpha] \in \mathcal{H}(K)$, $K(\alpha^{1/p})/K$ has a NIB if and only if $[\alpha] \in \mathcal{N}(K)$. Further, F. Kawamoto, N. Suwa and the first author independently proved that for

$[\alpha] \in \mathcal{H}(K)$, $K(\alpha^{1/p})/K$ has a PIB if $[\alpha] \in \mathcal{E}(K)$, for which see [11]. From the above, our target is the quotient group $(\mathcal{E}/\mathcal{N})(K)$.

Assume further that K is a CM–field and that $p \geq 3$. Then, by the action of the complex conjugation, we can decompose each group defined above into the product of the even part and the odd part:

$$\mathcal{H}(K) = \mathcal{H}(K)^+ \oplus \mathcal{H}(K)^-, \quad \text{etc.}$$

Let $\mu(K) = \langle \zeta_{p^a} \rangle$ be the group of p–power roots of unity in K, where ζ_{p^a} is a primitive p^a–th root of unity. From the well known theorem on the units of CM–fields (cf. [23, Theorem 4.12]), it immediately follows that

$$\mathcal{E}(K)^- \subseteq \langle [\zeta_{p^a}] \rangle, \quad \text{and hence} \quad \dim \mathcal{E}(K)^- \leq 1, \tag{1}$$

where $\dim(*)$ denotes the dimension of a vector space over $\mathbf{F}_p$. It also follows from the above mentioned theorem that $\mathcal{N}(K)^- = \{0\}$, for which see also Brinkhuis [1]. Therefore, we can say that the odd part $(\mathcal{E}/\mathcal{N})(K)^- = \mathcal{E}(K)^-$ is a "tame" object. On the other hand, the even part $(\mathcal{E}/\mathcal{N})(K)^+$ is a "tough" object because, to deal with it, we have to fight with the group of units of the maximal real subfield of K. We prove the following theorems (Theorems 2, 3) on the odd part and the even part. Theorem 1 follows immediately from Theorem 2.

Theorem 2. *Let p be an odd prime number, and N a multiple of $(p-1)p$. Then, there exist infinitely many CM–fields K of degree N for which $\zeta_p \in K^\times$ and $(\mathcal{E}/\mathcal{N})(K)^- \neq \{0\}$.*

Theorem 3. *Let p be an odd prime number with $p < 100$, and N a proper multiple of $2(p-1)p$ with $N/(2(p-1))$ not a power of p. Then, there exist infinitely many CM–fields K of degree N for which $\zeta_p \in K^\times$ and $(\mathcal{E}/\mathcal{N})(K)^+ \neq \{0\}$.*

This note is organized as follows. In Section 3, we give some simple lemmas on $(\mathcal{E}/\mathcal{N})(K)$. In Section 4, we prove Theorem 2. In section 5, we give a sufficient condition for $(\mathcal{E}/\mathcal{N})(K)^+ \neq \{0\}$ using some results in cyclotomic Iwasawa theory. In Section 6, we prove Theorem 3.

3 Some lemmas

In this section, we give some simple lemmas on the quotient $(\mathcal{E}/\mathcal{N})(K)$. Unless otherwise stated, p is a prime number including $p = 2$, and K is an arbitrary number field. As before, we denote by $\mu(K)$ the group of p–power roots of unity in K.

Lemma 1. (I) *Let L/K be a finite extension with $p \nmid [L:K]$. Then, $(\mathcal{E}/\mathcal{N})(L) \neq \{0\}$ if $(\mathcal{E}/\mathcal{N})(K) \neq \{0\}$.* (II) *Let L/K be a finite extension with $p \nmid [L:K]$. Assume that $p \geq 3$ and that K, L are CM–fields. Then, $(\mathcal{E}/\mathcal{N})(L)^{\pm} \neq \{0\}$ if $(\mathcal{E}/\mathcal{N})(K)^{\pm} \neq \{0\}$.*

Proof. We prove only the first assertion. The second one is proved similarly. Let ϵ be a unit of K with $[\epsilon]_K \in \mathcal{E}(K)$. Assume that $[\epsilon]_L \in \mathcal{N}(L)$. Then, $\epsilon \equiv \eta^p \bmod \pi^p$ for some $\eta \in E_L$. Taking the norm from L to K, we obtain

$$\epsilon^n \equiv (N_{L/K}\,\eta)^p \bmod \pi^p \quad \text{with } n = [L:K].$$

This implies $[\epsilon]_K \in \mathcal{N}(K)$ since $p \nmid n$. Hence, we obtain the assertion (I). □

Lemma 2. *Let K be a number field. If the ramification index over $\mathbf{Q}$ of any prime ideal of K dividing p is smaller than p, then $(\mathcal{E}/\mathcal{N})(K) = \{0\}$. In particular, if $[K:\mathbf{Q}] < p$, then $(\mathcal{E}/\mathcal{N})(K) = \{0\}$.*

Proof. Let ϵ be a unit of K. Assume that $\epsilon \equiv u^p \bmod \pi^p$ for some $u \in O_K$. Replacing ϵ with ϵ^n for some n with $p \nmid n$, we may well assume that $u \equiv 1 \bmod \mathfrak{P}$ for all prime ideals $\mathfrak{P}$ of K over p. Then, we must have $u^p \equiv 1 \bmod \pi^p$ since the ramification index of $\mathfrak{P}$ is smaller than p for any $\mathfrak{P}$ with $\mathfrak{P}|p$. Thus, we obtain the assertion. □

Lemma 3. (I) *Let K be a number field with $\mu(K) = \langle \zeta_{p^a} \rangle$ and $a \geq 1$, and F the maximal abelian field contained in K. We have $[\zeta_{p^a}] \notin \mathcal{E}(K)$ if K/F is at most tamely ramified at a prime divisor of K over p.* (II) *Let $p \geq 3$, K a CM–field with $\zeta_p \in K^{\times}$, and F as above. We have $\mathcal{E}(K)^- = \{0\}$ if K/F is at most tamely ramified at a prime divisor of K over p.*

Proof. The first assertion holds since the extension $F(\zeta_{p^{a+1}})/F$ is of degree p and ramified at the primes over p. The second one follows from the first one and (1). □

Remark 1. In the statement of Theorem 2, the degree $N = [K:\mathbf{Q}]$ must be a multiple of p because of Lemma 3.

4 Proof of Theorem 2

Let p be an odd prime number, N a multiple of $(p-1)p$, and $n = N/p$. Choose and fix a CM–field k of degree n with $\mu(k) = \langle \zeta_p \rangle$. Let l be a prime number which splits completely in k, and $\mathfrak{L}$ a prime ideal of k over l. Take an element β of $k^\times$ satisfying (a) $\beta \equiv 1 \bmod \pi^p$ and (b) $\mathfrak{L} || \beta$ but $\mathfrak{L}^\rho \nmid \beta$. Here, ρ denotes the complex conjugation in k. Put $\alpha = \zeta_p \beta^{1-\rho}$, $\gamma = \alpha^{1/p}$ and $K = k(\gamma)$. By the condition (b), K/k is a cyclic extension of degree p in which $\mathfrak{L}$ is ramified. Let k^+ be the maximal subfield of k. Since $\alpha^\rho = \alpha^{-1}$, we see that there exists a cyclic extension K^+/k^+ of degree p such that $K = kK^+$ from the Kummer duality. Hence, K is a CM–field of degree $N = np$. By the condition (a), $\zeta_p \equiv \gamma^p \bmod \pi^p$. It is clear that $\mu(K) = \langle \zeta_p \rangle$. Therefore, the class $[\zeta_p] (\in K^\times/(K^\times)^p)$ is a nontrivial element of $\mathcal{E}(K)^-$. Thus, we obtain $(\mathcal{E}/\mathcal{N})(K)^- = \mathcal{E}(K)^- \neq 0$. Finally, by taking various prime numbers l, we complete the proof of Theorem 2.

5 A sufficient condition for $(\mathcal{E}/\mathcal{N})(K)^+ \neq \{0\}$

In this section, we give a sufficient condition for $(\mathcal{E}/\mathcal{N})(K)^+ \neq \{0\}$ using some results in cyclotomic Iwasawa theory. Let p be a fixed odd prime number, K an imaginary abelian field and $\Delta = \mathrm{Gal}(K/\mathbf{Q})$. We assume that K satisfies the condition

(C1) $\quad \zeta_p \in K^\times$ and the exponent of Δ equals $p-1$.

Let K_∞/K be the cyclotomic $\mathbf{Z}_p$–extension with its n–th layer K_n ($n \geq 0$). For brevity, we write $\mathcal{H}_n$, $\mathcal{E}_n$, $\mathcal{N}_n$ in place of $\mathcal{H}(K_n)$, $\mathcal{E}(K_n)$, $\mathcal{N}(K_n)$ respectively. Let A_n be the Sylow p-subgroup of the ideal class group of K_n, and let

$$X_\infty = \varprojlim A_n$$

be the projective limit with respect to the relative norms. These groups are naturally regarded as modules over the group ring $\mathbf{Z}_p[\Delta]$. By definition, for each $[\alpha] = [\alpha]_n = [\alpha]_{K_n} \in \mathcal{H}_n$, there exists an ideal $\mathfrak{A}$ of K_n such that $(\alpha) = \mathfrak{A}^p$. By mapping $[\alpha]$ to the ideal class $[\mathfrak{A}] \in A_n$, we obtain the following exact sequence of $\mathbf{Z}_p[\Delta]$–modules.

$$\{0\} \longrightarrow \mathcal{E}_n \longrightarrow \mathcal{H}_n \longrightarrow A_n. \tag{2}$$

For a $\mathbf{Z}_p[\Delta]$–module M and a ($\mathbf{Q}_p$–valued) character ψ of Δ, $M(\psi)$ denotes the ψ–component of M. Namely, $M(\psi)$ is the maximal submodule of M on which Δ acts via ψ. We denote by λ_ψ and μ_ψ the Iwasawa λ–invariant and the μ–invariant of the ideal class group $X_\infty(\psi)$, respectively. We have $\mu_\psi = 0$ by Ferrero and Washington [4]. Let χ be a *fixed* nontrivial *even* ($\mathbf{Q}_p$–valued) character of Δ, ω the character of Δ representing the Galois action on ζ_p, and $\chi^* = \omega \cdot \chi^{-1}$ the associated *odd* character. By the Iwasawa main conjecture (= the theorem of Mazur and Wiles [20]), we can calculate the invariant λ_{χ^*} using "Stickelberger elements". And there are several values of λ_{χ^*}, for which see Fukuda's table [5]. On the other hand, it is conjectured that $\lambda_\chi = 0$ by Greenberg [7]. Though this conjecture is far from being settled, a method to calculate λ_χ is established by Kraft and Schoof [18], Kurihara [19] and the authors [14, 15].

Under the above setting, we assume that K and χ satisfy the following two conditions.

(C2) $\quad \lambda_{\chi^*} = 1$ and $\lambda_\chi = 0$.

(C3) $\quad$ There is only one prime ideal of K over p.

As $\mu_{\chi^*} = 0$, it follows from $\lambda_{\chi^*} = 1$ and (C3) that

$$\mathcal{H}_n(\chi) \cong \mathbf{Z}/p\mathbf{Z} \quad \text{for all } n \geq 0 \tag{3}$$

using the Kummer duality. For this assertion, see for example, Section 5.1 of [9]. Let $[\alpha_0]_0$ be a generator of $\mathcal{H}_0(\chi)$ with $\alpha_0 \in K^\times$, and $\mathfrak{A}_0$ an ideal of K such that $(\alpha_0) = \mathfrak{A}_0^p$. Assume further that

(C4) $\quad \mathcal{E}_0(\chi) = \{0\}$.

Then, by (the χ–component of) the exact sequence (2) and (3) with $n = 0$, we see that $\mathfrak{A}_0$ is not a principal ideal of K (and hence, $A_0(\chi) \neq \{0\}$). Since $\lambda_\chi = 0$, the ideal $\mathfrak{A}_0$ is capitulated in K_n for some n by [7, Proposition 2]. Denote by m_0 the smallest such integer.

Theorem 4. *Under the above setting, assume that K and χ satisfy the four conditions* (C1),$\cdots$, (C4). *Then, $\mathcal{H}_n(\chi) = \mathcal{E}_n(\chi)$ for all $n \geq m_0$, and $\mathcal{N}_n(\chi) = \{0\}$ for all $n \geq 0$. In particular, $\mathcal{E}_n(\chi)/\mathcal{N}_n(\chi) \neq \{0\}$ for all $n \geq m_0$.*

Proof. By (3), $\mathcal{H}_n(\chi)$ is generated by the class $[\alpha_0]_n$. Then, since $\mathfrak{A}_0$ is a principal ideal in K_n for $n \geq m_0$, the first assertion follows from (the χ–component of) the exact sequence (2). By (C4), $\mathcal{N}_0(\chi) = \{0\}$. Because of the conditions (C1), (C2), (C3), this implies that $\mathcal{N}_n(\chi) = \{0\}$ for all $n \geq 0$ by virtue of [9, Proposition 1]. $\square$

6 Proof of Theorem 3

For proving Theorem 3, it suffices to show the following proposition because of Lemma 1 (II).

Proposition. *Let p be an odd prime number with $p < 100$, and $a\,(\geq 1)$ an integer. Then, there exists at least one imaginary abelian field K of degree $2(p-1)p^a$ for which $\zeta_p \in K^\times$ and $(\mathcal{E}/\mathcal{N})(K)^+ \neq \{0\}$.*

Let $k = \mathbf{Q}(\sqrt{f})$ be a real quadratic field with conductor f, χ the associated even Dirichlet character, and $K = k(\zeta_p)$. We regard χ as a character of $\Delta = \mathrm{Gal}(K/\mathbf{Q})$. Clearly, K satisfies (C1). In view of Theorem 4, it suffices, for showing Proposition 2, to give at least one numerical example of k for which K and χ satisfy the conditions (C2), (C3), (C4) and $m_0 = 1$. The examples are exhibited in the tables at the end of this note for $p < 100$. To check whether a given pair (K, χ) satisfies the above conditions, the hardest part is to verify $\lambda_\chi = 0$ and $m_0 = 1$. We briefly explain how to verify them following [15], after mentioning some simple remarks. Further, we explain how to look at the tables.

It is clear that (C4) is equivalent to $\mathcal{E}(k) = \{0\}$. Let ϵ be a fundamental unit of k. Then, the condition $\mathcal{E}(k) = \{0\}$ holds if and only if

$$\epsilon^{p^2-1} \not\equiv 1 \bmod p^2 \quad \text{or} \quad \epsilon^{p-1} \not\equiv 1 \bmod p(p, \sqrt{f})$$

according as $p \nmid f$ or $p | f$. This is shown by an argument similar to the proof of Lemma 2. Hence, the condition (C4) is quite easily checked. As we have mentioned in Section 5, we have

$$A_0(\chi) \neq \{0\} \tag{4}$$

when $\lambda_{\chi^*} = 1$ and (C3), (C4) hold.

Let q be the least common multiple of f and p. By Iwasawa [17], there exists a unique power series $g_\chi(T)$ in $\mathbf{Z}_p[[T]]$ related to the p–adic L–function $L_p(s,\,\chi)$ by

$$g_\chi((1+q)^{1-s}-1)=L_p(s,\,\chi),\quad \text{for all } s\in\mathbf{Z}_p.$$

When $\lambda_{\chi^*}=1$, $g_\chi(T)$ has a unique zero α ($\in p\mathbf{Z}_p$). We have $\alpha\neq 0$ because the Leopoldt conjecture holds for K by Brumer [2]. We can calculate the value $\alpha \bmod p^n$ using the approximation formula [17, Section 6] for $g_\chi(T)$.

For a while, we assume that the conditions (C3), (4) and $\lambda_{\chi^*}=1$ are satisfied. In [15], we introduced, for each $n\geq 0$, a condition (H_n) which is given in terms of an explicitly written cyclotomic unit of K_n and the value $\alpha \bmod p^{n+e}$, where $e=\mathrm{ord}_p\alpha$. The main theorem in [15] asserts that $\lambda_\chi=0$ if and only if (H_n) holds for some $n\geq 0$. Let f' be the non–p–part of f. For each prime number ℓ with $\ell\equiv 1 \bmod f'p^{n+e}$, we introduced a condition ($\mathrm{H}'_{n,\ell}$) which is a kind of "reduction modulo ℓ" of (H_n) and for which it is quite easy to check whether or not hold by computer calculation. We showed that (H_n) holds if and only if ($\mathrm{H}'_{n,\ell}$) holds for some ℓ ([15, Proposition 2]). Let n_0 be the smallest integer n for which k satisfies (H_n). We also showed that $m_0=1$ if $n_0=0$ and that $m_0=n_0$ otherwise. (For this, see [15, Proposition 1].) Further, it is known (that $|A_0(\chi)|\leq p^e$ and) that (H_0) does not hold if and only if

$$|A_0(\chi)|=p^e \tag{5}$$

holds by [15, Remark 4]. The last condition (or equivalently, the opposite of (H_0)) is equivalent to (C4) except when $p=3$ and p ramifies in k. For the exceptional case, (C4) implies (5). For these, see Section 5.3 of [9]. From the above, excluding the exceptional case, a real quadratic field $k=\mathbf{Q}(\sqrt{f})$ (or the associated pair (K,χ)) satisfies the conditions (C1),$\cdots$, (C4) and $m_0=1$ if it satisfies (C3), (4), $\lambda_{\chi^*}=1$ and $n_0=1$.

Our computer calculation was performed as follows. First, we check whether or not (H_0) is satisfied using (5). When (H_0) does not hold, we check, one by one, starting from $n=1$, whether or not ($\mathrm{H}'_{n,\ell}$) is satisfied for the first five prime numbers ℓ with $\ell\equiv 1 \bmod f'p^{n+e}$ until it is satisfied for some n and some such l. When (H_0) does not hold and ($\mathrm{H}'_{1,l}$) is satisfied for some such l, we can conclude that $n_0=1$. However, in general, the method is not efficient at calculating the exact value of n_0, and it gives an upper bound of n_0. This is because we deal only with relatively small primes l for each n.

Table I deals with prime numbers p with $p \geq 11$ and *all* real quadratic fields $k = \mathbf{Q}(\sqrt{f})$ with $f < 100,000$ satisfying (C3) and (4). For $p = 31$, 41 and $p > 47$, there are no such fields in the range $f < 100,000$. Corresponding tables for $p = 3$, 5, 7 are given in [15]. For each f in the row "$n_0 = i$" ($i = 0, 1, 2$), we have $\lambda_{\chi^*} = 1$. For each f in the row "$n_0 = 0$" (resp. "$n_0 = 1$"), we showed that $n_0 = 0$ (resp. $n_0 = 1$) by the above method. For each f in the row "$n_0 = 2$", we have $n_0 \leq 2$. For these f, we saw that $k = \mathbf{Q}(\sqrt{f})$ does not satisfy (H_0) nor ($\mathrm{H}'_{1,l}$) for the first five prime numbers l with $l \equiv 1 \bmod f'p^{1+e}$ but it satisfies ($\mathrm{H}'_{2,l}$) for some of the first five primes l with $l \equiv 1 \bmod f'p^{2+e}$. As we explained above, we can not exclude the possibility of $n_0 = 1$ for these f. (For this, see Remark 2.) For each f in the row "@", we have $\lambda_{\chi^*} > 1$ and we have verified $\lambda_\chi = 0$ by the method in [14]. Further, the $*$–mark after the value f means that p ramifies in k. For the other f, p remains prime in k.

For each prime number p with $3 \leq p < 100$, Table II gives a list of the smallest f for which $k = \mathbf{Q}(\sqrt{f})$ satisfies the conditions $\lambda^*_\chi = 1$, (C3), (C4), (4), and $m_0 = 1$. (We showed that for f_1 with $f_1 < f$, $k = \mathbf{Q}(\sqrt{f_1})$ does not satisfy (C4) when it satisfies (C3), (4) and $\lambda_{\chi^*} = 1$.) We also give, for each such f, the value of $\alpha \bmod p^2$ and the smallest prime ℓ with $\ell \equiv 1 \bmod f'p^{1+e}$ for which ($\mathrm{H}'_{1,\ell}$) holds.

Remark 2. Recently, in [21], the second author exploited a method to calculate the exact value of n_0 using not only cyclotomic units but also Gauss sums.

Remark 3. As we have mentioned in Section 2, the difficulty in proving $(\mathcal{E}/\mathcal{N})(K)^+ \neq \{0\}$ lies in that we need a knowledge on the p–adic behaviour of the full group E_K of all units. For abelian fields, we have a beautiful theorem of Iwasawa [16] and Gillard [6] on local units modulo cyclotomic units. Under some conditions, we can use this for obtaining some ample information on E_K for abelian fields K. Proposition 1 of [9] which is crucial in the proof of Theorem 4 was proved in this way. Greither [8] and, recently, Tsuji [22] gave some generalization of this important theorem of Iwasawa and Gillard.

TABLE I

$p = 11$

	f								
$n_0 = 0$	36709	51553	91585						
$n_0 = 1$	10401	14009	19021	19048	20369	22129	22501	24801	27473
	32236	33833	43753	49953	50937	51457	51985	53349	55281
	55336	55948	57409*	57713	65361	65797	67341	69209	69729*
	78889	83569	84685	86017	86869	91384	91913	92265	92408
	95477	97576							
$n_0 = 2$	37353	65353							
@	1297	12161	26617	74857	91769				

$p = 13$

	f								
$n_0 = 0$	13033								
$n_0 = 1$	8101	13457	14113	15377	18817	20977	21613	31241	33209
	33857	34588	35297	39193	39201	40669	55569	58661	60029
	61033	64313	68881	69009	77149	78028	79633	81785	83969
	85265	90040	90313	90329	92417*	97973			
$n_0 = 2$	24601	31193	40441	41801	45329	61989			
@	26241	82373	83377						

$p = 17$

	f								
$n_0 = 1$	11257	42937	47657	54541	55697	63505	65473	69697	79009

$p = 19$

	f								
$n_0 = 1$	31333	38569	44101	49393	54753	68281	70429	71689	97141
@	18229	39801							

$p = 23$

	f			
$n_0 = 1$	30977	56065	67409	91813

$p = 29$

	f			
$n_0 = 1$	49281	56857	90001	99401

$p = 37$

	f	
$n_0 = 1$	55561	94321

$p = 43$

	f
$n_0 = 0$	14401

$p = 47$

	f
$n_0 = 1$	78401

TABLE II

p	f	$\alpha \bmod p^2$	l
3	761	3	27397
5	1093	15	437201
7	577	35	113093
11	10401	33	7551127
13	8101	156	16428829
17	11257	170	39039277
19	31333	171	248846687
23	30977	230	196641997
29	49281	812	414453211
31	158649	372	2744310403
37	55561	740	3042520372
41	205753	943	1383483173
43	189229	817	41986130531
47	78401	2021	34637561811
53	312361	1643	10529064589
59	360697	2124	87891037991
61	586321	3233	61087612349
67	614657	67	38628733823
71	812449	3692	40955554091
73	444089	4745	255587430349
79	641521	3397	160149302441
83	1022869	4067	211396336231
89	614849	7031	68183065007
97	1106209	1164	603682587899

Acknowledgements. We are grateful to the referee for carefully reading the manuscript and for valuable comments. In Theorems 1 and 2 of the former version, we had imposed the stronger condition $p^2|N$ for a technical reason. The referee kindly informed us how to simplify the original proof of Theorem 2 replacing the condition $p^2|N$ with $p|N$.

References

[1] J. Brinkhuis, *On the Galois module structure over CM–fields*, Manuscripta Math. **75** (1992), 333–347.

[2] A. Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124.

[3] L. Childs, *The group of unramified Kummer extensions of prime degree*, Proc. London Math. Soc. **35** (1977), 89–111.

[4] B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.

[5] T. Fukuda, *Iwasawa λ-invariants of imaginary quadratic fields*, J. College Industrial Technology Nihon Univ. **27** (1994), 35–88.

[6] R. Gillard, *Unités cyclotomiques, unités semi locales et $\mathbf{Z}_l$-extensions II*, Ann. Inst. Fourier **29** (1979), 1–15.

[7] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.

[8] C. Greither, *Class groups of abelian fields, and the main conjecture*, Ann. Inst. Fourier **42** (1992), 449–499.

[9] H. Ichimura, *On a normal integral bases problem over cyclotomic $\mathbf{Z}_p$--extensions*, J. Math. Soc. Japan **48** (1996), 689–703.

[10] ———, *A note on unramified quadratic extensions of algebraic number fields*, Proc. Japan Acad. **76A** (2000), 78–81.

[11] ———, *On power integral basis of unramified cyclic extensions of prime degree*, to appear in Journal of Algebra (2000a).

[12] ______, *On a power integral bases problem over cyclotomic $\mathbf{Z}_p$-extensions*, to appear in Journal of Algebra (2000b).

[13] ______, *A note on integral bases of unramified cyclic extensions of prime degree*, to appear in Abh. Math. Sem. Univ. Hamburg (2000c).

[14] H. Ichimura and H. Sumida, *On the Iwasawa invariants of certain real abelian fields II*, Internat. J. Math. **7** (1996), 721–744.

[15] ______, *On the Iwasawa invariants of certain real abelian fields*, Tôhoku Math. J. **49** (1997), 203–215.

[16] K. Iwasawa, *On some modules in the theory of cyclotomic fields*, J. Math. Soc. Japan **16** (1964), 42–82.

[17] ______, *Lectures on p-adic L-functions*, Ann. of Math. Stud., vol. 74, Princeton Univ. Press: Princeton, N.J., 1972.

[18] J. S. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), 135–155.

[19] M. Kurihara, *The Iwasawa λ invariants of real abelian fields and the cyclotomic elements*, Tokyo J. Math. **22** (1999), 259–277.

[20] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.

[21] H. Sumida, *Cyclotomic units, Gauss sums, and Iwasawa invariants of certain real abelian fields*, preprint (2000).

[22] T. Tsuji, *Semi-local units modulo cyclotomic units*, J. Number Theory **78** (1999), 1–26.

[23] L. Washington, *Introduction to cyclotomic fields. second edition*, Graduate Texts in Math., vol. 83, Springer-Verlag: New York, 1997.