Functiones et Approximatio
54.1 (2016), 7–17
doi: 10.7169/facm/2016.54.1.1

ON THE IWASAWA λ-INVARIANT OF THE CYCLOTOMIC $\mathbb{Z}_2$-EXTENSION OF $\mathbb{Q}(\sqrt{p})$, III

Takashi Fukuda, Keiichi Komatsu, Manabu Ozaki, Takae Tsuji

Abstract: In the preceding papers, two of authors developed criteria for Greenberg conjecture of the cyclotomic $\mathbb{Z}_2$-extension of $k = \mathbb{Q}(\sqrt{p}\,)$ with prime number p. Criteria and numerical algorithm in [5], [3] and [6] enable us to show $\lambda_2(k) = 0$ for all p less than 10^5 except $p = 13841, 67073$. All the known criteria at present can not handle $p = 13841, 67073$. In this paper, we develop another criterion for $\lambda_2(k) = 0$ using cyclotomic units and Iwasawa polynomials, which is considered a slight modification of the method of Ichimura and Sumida. Our new criterion fits the numerical examination and quickly shows that $\lambda_2(\mathbb{Q}(\sqrt{p}\,)) = 0$ for $p = 13841, 67073$. So we announce here that $\lambda_2(\mathbb{Q}(\sqrt{p}\,)) = 0$ for all prime numbers p less that 10^5.

Keywords: Iwasawa invariant, cyclotomic unit, real quadratic field.

1. Introduction

Let $k = \mathbb{Q}(\sqrt{p}\,)$ be a real quadratic field with prime number p and k_∞ the cyclotomic $\mathbb{Z}_2$-extension of k. It is very important to study Greenberg conjecture for k_∞/k, namely to consider whether the Iwasawa λ-invariant $\lambda_2(k) = \lambda(k_\infty/k)$ is zero or not. First approach on this problem was made by Ozaki and Taya [14] in which they proved that $\lambda_2(k) = 0$ if p satisfies $p \not\equiv 1 \pmod{16}$ or $2^{(p-1)/4} \not\equiv 1 \pmod{p}$. After Ozaki and Taya, the authors developed criteria for $\lambda_2(k) = 0$ when p satisfies $p \equiv 1 \pmod{16}$ and $2^{(p-1)/4} \equiv 1 \pmod{p}$ (cf. [5], [3], [6]). Our criteria are described by units in k_n, which is the intermediate field of k_∞/k with $[k_n : k] = 2^n$, and numerical calculations in k_n $(0 \leqslant n \leqslant 8)$ show that $\lambda_2(k) = 0$ for all prime number p less than 10^5 except $p = 13841, 67073$. All the known criteria accompanied with calculation in k_8 failed to show $\lambda_2(k) = 0$ for $p = 13841, 67073$. It seems necessary to calculate at least in k_{13} in order to show $\lambda_2(k) = 0$ using those criteria. Such a calculation is far beyond the ability of current computer.

2010 Mathematics Subject Classification: primary: 11R23; secondary: 11Y40

In this paper, we develop one more criterion using cyclotomic units, which is considered a slight modification of the method of Ichimura and Sumida [10], and verify that $\lambda_2(k) = 0$ for $p = 13841, 67073$ by using cyclotomic units and Iwasawa polynomials in k_8. Namely, we prove the following theorem:

Theorem 1.1. *We have* $\lambda_2(\mathbb{Q}(\sqrt{p})) = 0$ *for all prime number* p *less than* 10^5.

2. Preliminaries

From now on, we assume that p is a prime number satisfying $p \equiv 1 \pmod{16}$ and $2^{(p-1)/4} \equiv 1 \pmod{p}$. Let k_n be the n-th layer of the cyclotomic $\mathbb{Z}_2$-extension k_∞ of k as above, $\mathcal{O}_{k_n}$ the integer ring of k_n, $E_n = \mathcal{O}_{k_n}^\times$ the unit group of k_n, A_n the 2-part of the ideal class group of k_n, $\mathfrak{l}_n$ a prime ideal of k_n lying above 2. We put $\mathbb{B}_n = \mathbb{Q}(\cos\frac{2\pi}{2^{n+2}})$ and $\mathbb{B}_\infty = \cup_{n=0}^\infty \mathbb{B}_n$. Then $k_n = k\mathbb{B}_n$ and $k_\infty = k\mathbb{B}_\infty$. Moreover, let $\Delta = G(k_\infty/\mathbb{B}_\infty)$ the Galois group of k_∞ over $\mathbb{B}_\infty$ with a generator τ and $\Gamma = G(k_\infty/k)$ the Galois group of k_∞ over k with a topological generator γ.

Then we have $2\mathcal{O}_{k_n} = (\mathfrak{l}_n\mathfrak{l}_n^\tau)^{2^n}$. Let $k_{n\,\mathfrak{l}_n}$ be the completion of k_n at $\mathfrak{l}_n$ and put $c_n = 1 + 2\cos\frac{2\pi}{2^{n+2}}$. Then we have $k_{n\,\mathfrak{l}_n} = \mathbb{Q}_2(c_n)$, where $\mathbb{Q}_2$ is the 2-adic field. Let I'_n be the group of fractional ideals in k_n generated by ideals which are prime to 2. We put $E'_n = \{\, \alpha \in k_n \mid (\alpha) \in I'_n \,\}$ and $U_n = \mathcal{O}_{k_n\,\mathfrak{l}_n}^\times \times \mathcal{O}_{k_n\,\mathfrak{l}_n}^\times$.

We embed E'_n in U_n by the injective homomorphism $\varphi : E'_n \ni \alpha \mapsto (\alpha, \alpha^\tau) \in U_n$. We put $(\alpha, \alpha^\tau)^{\tau^*} = (\alpha^\tau, \alpha)$ for $(\alpha, \alpha^\tau) \in \varphi(E'_n)$. Since the topological closure $\overline{\varphi(E'_n)}$ of $\varphi(E'_n)$ is U_n, we can extend the mapping τ^* to U_n continuously.

Now we develop a quadratic version of [15, Theorem 3.3] by following the arguments in [9, §2]. We put $\mathbb{U} = \varprojlim U_n$, where the projective limit is taken with respect to the relative norms. Let $u = (u_n)_{n=1}^\infty$ be an element in $\varprojlim \mathcal{O}_{k_n\mathfrak{l}_n}^\times$. Then there exists a unique power series $f_u(X) \in \mathbb{Z}_2[[X]]$ satisfying

$$f_u(1 - \zeta_{2^{n+2}}) = u_n,$$

where ζ_m means $\exp(2\pi\sqrt{-1}/m)$. Let $D = (1-X)\frac{d}{dX}$ be a derivative operator on $\mathbb{Z}_2[[X]]$. We put $\Lambda = \mathbb{Z}_2[[T]]$ and let $1+T$ act on $\mathbb{U}$ as $\gamma \in \Gamma$. Let s be a primitive root modulo p and put $\xi = \sum_{i=1}^{(p-1)/2}(\zeta_p^{s^{2i}} - \zeta_p^{s^{2i+1}})$, which we regard as the image of the embedding $\mathcal{O}_k \hookrightarrow \mathcal{O}_{k_\mathfrak{l}} = \mathbb{Z}_2$. Then there exists a unique element $G_u(T)$ of Λ such that

$$D^\nu(\log f_u(X) - \tfrac{1}{2}\log f_u(1-(1-X)^2))|_{X=0} = G_u((1+4p)^\nu - 1)\xi.$$

We note that the correspondence $\mathbb{U}^{1-\tau^*} \ni (u, u^{-1}) \mapsto \frac{1}{2}G_u(T) \in \Lambda$ defines a Λ-isomorphism $\Psi : \mathbb{U}^{1-\tau^*} \longrightarrow \Lambda$. Now, we put

$$\eta_n = \zeta_{2^{n+2}}^{(p-1)/4} \prod_{i=1}^{(p-1)/2} \left(\zeta_{2^{n+2}}^{-1} - \zeta_p^{s^{2i}}\right),$$

and $\eta = (\eta_n)_{n=1}^\infty$. A straightforward calculation, which was presented in [6] for instance, shows that

$$\eta_n^2 = N_{\mathbb{Q}(\zeta_{2^{n+2}p})/k_n}(1 - \zeta_{2^{n+2}}\zeta_p).$$

From now on, we specify the topological generator γ of Γ by the relation

$$(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1})^{\gamma} = \zeta_{2^{n+2}}^{1+4p} + \zeta_{2^{n+2}}^{-1-4p} \quad (n \geqslant 0)\,.$$

Then Iwasawa's construction of 2-adic L-function associated to k varies now into the following form.

Theorem 2.1. *Let χ be the non-trivial character modulo p associated to k and $\frac{1}{2}G(T)$ the image of the element $(\eta^{1-\tau}, \eta^{\tau-1})$ in $\mathbb{U}^{1-\tau^*}$ by the above isomorphism $\mathbb{U}^{1-\tau^*} \cong \Lambda$. Then we have*

$$G((1+4p)^{\nu} - 1) = -(1 - 2^{\nu-1})\frac{B_{\nu,\chi}}{\nu} \qquad \textit{for} \;\; \nu \equiv 0 \pmod 2.$$

Here $B_{\nu,\chi}$ is a generalized Bernoulli number.

Since the Iwasawa μ-invariant $\mu_2(k) = \mu(k_\infty/k)$ is known to be zero by Ferrero-Washington [2], there exist a unique unit element $u(T) \in \Lambda^{\times}$ and a unique distinguished polynomial $g(T) \in \mathbb{Z}_2[[T]]$ such that

$$G(T) = 2u(T)g(T). \tag{2.1}$$

The distinguished polynomial $g(T)$, which is called Iwasawa polynomial, plays essential role in our arguments. We fix the notation $g(T)$ throughout the paper.

3. Criterion

In this section, we work in abelian extensions of $\mathbb{Q}$. So Leopoldt conjecture is valid in our situation (cf. [1]). Let L_∞ is the maximal unramified abelian 2-extension of k_∞ and M_∞ the maximal abelian 2-extension of k_∞ unramified outside 2. Then the Galois groups $I_\infty = G(M_\infty/L_\infty)$, $\mathfrak{X}_\infty = G(M_\infty/k_\infty)$ and $X_\infty = G(L_\infty/k_\infty)$ are finitely generated Λ-modules (cf. [12]). For a finitely generated Λ-module X, $\mathrm{ch}(X)$ denotes the characteristic polynomial of X. Then we have the following:

Lemma 3.1. *The tensor product $\mathfrak{X}_\infty \otimes_{\mathbb{Z}_2[\Delta]} \mathbb{Z}_2$ is pseudo-isomorphic to $\mathfrak{X}_\infty^{1-\tau}$, where τ acts on $\mathbb{Z}_2$ by $\tau a = -a$ for $a \in \mathbb{Z}_2$.*

Proof. Let ψ be a Δ-homomorphism of $\mathfrak{X}_\infty \otimes_{\mathbb{Z}_2[\Delta]} \mathbb{Z}_2$ to $\mathfrak{X}_\infty^{1-\tau}$ defined by $\psi(x \otimes a) = (x^a)^{1-\tau}$. Then ψ is surjective. Now, we assume $\psi(x \otimes a) = 1$. Then we have $(x^a)^{1-\tau} = 1$, which means $(x^a)^{\tau} = x^a$. Hence $x \otimes a = x^a \otimes 1 = (x^a)^{\tau} \otimes 1 = x^a \otimes (-1) = (x^a \otimes 1)^{-1}$, which shows $(x \otimes a)^2 = 1$. Since $\mathfrak{X}_\infty \otimes_{\mathbb{Z}_2[\Delta]} \mathbb{Z}_2$ is finitely generated $\mathbb{Z}_2$-module, the kernel of ψ is finite. ■

Hence we have the following (cf. [18, Theorem 6.2]):

Lemma 3.2. *We have $ch(\mathfrak{X}_\infty^{1-\tau}) = g(T)$.*

Moreover, we have the following:

Lemma 3.3. *Λ-modules $\mathfrak{X}_\infty^{1-\tau} \cap I_\infty$ and $I_\infty^{1-\tau}$ are pseudo-isomorphic. Namely, $ch(\mathfrak{X}_\infty^{1-\tau} \cap I_\infty) = ch(I_\infty^{1-\tau})$.*

Proof. Let x be an element in $\mathfrak{X}_\infty^{1-\tau} \cap I_\infty$. Since $x^\tau = x^{-1}$, we have $x^2 = x^{1-\tau}$, which means $x^2 \in I_\infty^{1-\tau}$. Since $I_\infty^{1-\tau} \subset \mathfrak{X}_\infty^{1-\tau} \cap I_\infty$ and since $\mathfrak{X}_\infty^{1-\tau} \cap I_\infty$ is a finitely generated $\mathbb{Z}_2$-module, the index $(\mathfrak{X}_\infty^{1-\tau} \cap I_\infty : I_\infty^{1-\tau})$ is finite. ■

Since $X_\infty^{1-\tau} = \mathfrak{X}_\infty^{1-\tau} I_\infty / I_\infty$ is isomorphic to $\mathfrak{X}_\infty^{1-\tau} / \mathfrak{X}_\infty^{1-\tau} \cap I_\infty$, we have the following:

Lemma 3.4. *We have*

$$g(T) = ch(X_\infty^{1-\tau}) ch(\mathfrak{X}_\infty^{1-\tau} \cap I_\infty).$$

Now, we put $E_n = \mathcal{O}_{k_n}^\times$. Then $\varphi(E_n) = \{ (\varepsilon, \varepsilon^\tau) \mid \varepsilon \in E_n \}$. Moreover, we put $\mathcal{E}_n = \overline{\varphi(E_n)} \subset U_n$ and $\mathcal{E} = \varprojlim \mathcal{E}_n$. Then I_∞ is isomorphic to $\mathbb{U}/\mathcal{E}$ by class field theory, which shows $I_\infty^{1-\tau}$ is isomorphic to $\mathbb{U}^{1-\tau}\mathcal{E}/\mathcal{E}$. Let $P(T)$ be a monic irreducible polynomial in Λ which divides $g(T)$ and put

$$Q(T) = \frac{g(T)}{P(T)}.$$

Assume that $P(T)$ divides $\mathrm{ch}(X_\infty^{1-\tau})$. Then $\mathrm{ch}(I_\infty^{1-\tau})$ divides $Q(T)$, which shows $(\mathbb{U}^{1-\tau})^{Q(T)} \subset \mathcal{E}$, because $\mathfrak{X}_\infty$ has no finite Λ-submodule (cf. [8, Theorem 1]). Since $P(T)$ and $\omega_n(T) = (1+T)^{2^n} - 1$ are mutually prime in Λ, which is a consequence of Leopoldt conjecture, there exist elements $q_n(T)$, $r_n(T) \in \Lambda$ with

$$P(T)q_n(T) + r_n(T)\omega_n(T) = 2^{a_n},$$

where a_n is a non-negative integer. Hence we have

$$(\eta_n^{1-\tau}, \eta_n^{\tau-1})^{q_n(T)} = \Psi^{-1}(u(T))^{P(T)Q(T)q_n(T)} \in \mathcal{E}_n^{2^{a_n}}$$

with $u(T)$ define by (2.1). Now we follow the arguments in [4] and [16] noting that Leopoldt conjecture is valid in our situation to establish the following theorem.

Theorem 3.5. *Assume that for any monic irreducible polynomial $P(T)$ dividing $g(T)$, there exists $n \geqslant 1$ which satisfies*

$$\eta_n^{(1-\tau)q(\gamma-1)} \notin E_n^{2^a}. \tag{3.1}$$

Here $q(T)$ is a polynomial in Λ and a is a non-negative integer satisfying

$$P(T)q(T) \equiv 2^a \pmod{\omega_n(T)}.$$

Then we have $\lambda_2(k) = 0$.

The condition (3.1) in Theorem 3.5 guarantees $P(T) \not| \operatorname{ch}(X_\infty^{1-\tau})$, from which we deduce $\lambda_2(k) = 0$. In the practical computations, we are often aware of an upper bound d of λ-invariant. If $P(T)$ satisfies $\deg P(T) > d$, then we immediately conclude $P(T) \not| \operatorname{ch}(X_\infty^{1-\tau})$ because $\deg \operatorname{ch}(X_\infty) \leqslant d$. Hence we are able to transform Theorem 3.5 to the following effective form.

Corollary 3.6. *Assume that $\lambda_2(k) \leqslant d$ with positive integer d. Moreover, assume that for any monic irreducible polynomial $P(T)$ dividing $g(T)$ which satisfies $\deg P(T) \leqslant d$, there exists $n \geqslant 1$ which satisfies*

$$\eta_n^{(1-\tau)q(\gamma-1)} \notin E_n^{2^a}. \tag{3.2}$$

Here $q(T)$ is a polynomial in Λ and a is a non-negative integer satisfying

$$P(T)q(T) \equiv 2^a \pmod{\omega_n(T)}. \tag{3.3}$$

Then we have $\lambda_2(k) = 0$.

We note here that we verify the condition (3.2) by a congruence relation. Namely, let α be an integer in k_n and ℓ a prime number which satisfies $\chi(\ell) = 1$, $\ell \equiv 1 \pmod{2^{n+2}}$ and $\ell \equiv 1 \pmod{2^a}$. Then ℓ splits completely in $k_n/\mathbb{Q}$ and we find $x = x_{\mathfrak{l}} \in \mathbb{Z}$ satisfying $\alpha \equiv x \pmod{\mathfrak{l}}$ for each prime ideal $\mathfrak{l}$ of k_n lying above ℓ. If we find ℓ and $\mathfrak{l}$ such that

$$x^{\frac{\ell-1}{2^a}} \not\equiv 1 \pmod{\ell},$$

then we see that

$$\alpha \notin k_n^{2^a}.$$

4. Bound of Iwasawa invariants

In this section, we discuss an upper bound of Iwasawa invariants in a general situation. Let F be a finite algebraic extension of $\mathbb{Q}$, ℓ a prime number and K a $\mathbb{Z}_\ell$-extension of F. Let F_n be the intermediate field of K/F with $[F_n : F] = \ell^n$ and denote by ℓ^{e_n} the ℓ-part of the class number of F_n. Then there exist integers $\lambda(K/F) \geqslant 0$, $\mu(K/F) \geqslant 0$ and $\nu(K/F)$ which satisfy

$$e_n = \lambda(K/F)n + \mu(K/F)\ell^n + \nu(K/F)$$

for all sufficiently large n (cf. [12]).

In some situations, a few practical values of e_n estimate explicitly upper bounds of $\lambda(K/F)$ and $\mu(K/F)$ and enables us to apply Corollary 3.6 to $k = \mathbb{Q}(\sqrt{p})$. A similar estimate is also given in [11, Lemma 5].

Theorem 4.1. *Notations being as above, assume that all the ramified primes in K/F are totally ramified. Furthermore we assume that inequality $e_{n+1} - e_n < \ell^{n+1} - \ell^n$ holds for some $n \geqslant 0$. Then we have $\lambda(K/F) \leqslant e_{n+1} - e_n$ and $\mu(K/F) = 0$.*

Proof. Let A_n be the ℓ-part of the ideal class group of F_n. Then $|A_n| = \ell^{e_n}$. Put $e_{n+1} - e_n = b$. Let $X = G(L_\infty/K)$ and $Y = G(L_\infty/KL_0) \subseteq X$, where L_∞ and L_0 are the maximal unramified abelian ℓ-extensions of K and F, respectively. Then $\Gamma = G(K/F)$ acts on X by inner automorphism. If we fix a topological generator γ of Γ and associate γ with $1+T$, then we are able to regard X as a $\Lambda = \mathbb{Z}_\ell[[T]]$-module. We put

$$\nu_n = \frac{(1+T)^{\ell^n} - 1}{T}\ , \ \nu_{n+1,n} = \nu_{n+1}/\nu_n.$$

Then we have the isomorphism

$$A_n \simeq X/\nu_n Y \tag{4.1}$$

from our assumption on the ramification in K/F and [12, Theorem 6]. It follows from (4.1) and our assumption on the class numbers that

$$|\nu_n Y/\nu_{n+1} Y| = \ell^b$$

Hence if we put $M = \nu_n Y$, then we have

$$|M/\nu_{n+1,n} M| = \ell^b. \tag{4.2}$$

Here we note that $\lambda(K/F) = \operatorname{rank}_{\mathbb{Z}_\ell} X = \operatorname{rank}_{\mathbb{Z}_\ell} M$ because $X/\nu_n Y \simeq A_n$ is finite. Also, the triviality of the μ-invariant of the Λ-module M implies that of $\mu(K/F)$ by the same reason. Therefore it is enough to show that $\dim_{\mathbb{F}_\ell} M/\ell M \leqslant b$, because $\operatorname{rank}_{\mathbb{Z}_\ell} M \leqslant \dim_{\mathbb{F}_\ell} M/\ell M$ holds in general and the finiteness of $M/\ell M$ implies the vanishing of the μ-invariant of M by Nakayama's lemma. Since $\mathbb{F}_\ell[[T]]$ is a discrete valuation ring and $M/\ell M$ is a finitely generated $\mathbb{F}_\ell[[T]]$-module, we have

$$M/\ell M \simeq \mathbb{F}_\ell[[T]]^{\oplus r} \oplus \left(\bigoplus_{i=1}^{s} \mathbb{F}_\ell[[T]]/(T^{a_i}) \right) \tag{4.3}$$

for some integers $r \geqslant 0$ and $a_1 \geqslant \ldots \geqslant a_s \geqslant 0$. Then we get

$$\begin{aligned} M/(\ell, \nu_{n+1,n})M &= M/(\ell, T^{\ell^{n+1}-\ell^n})M \\ &\simeq \left(\mathbb{F}_\ell[[T]]/(T^{\ell^{n+1}-\ell^n})\right)^{\oplus r} \\ &\quad \oplus \left(\bigoplus_{i=1}^{s} \mathbb{F}_\ell[[T]]/(T^{\min\{a_i,\, \ell^{n+1}-\ell^n\}}) \right), \end{aligned} \tag{4.4}$$

because $\nu_{n+1,n} \equiv T^{\ell^{n+1}-\ell^n} \pmod{\ell}$. By using our assumption, (4.2) and (4.4), we derive

$$\begin{aligned} \ell^{n+1} - \ell^n > b &\geqslant \dim_{\mathbb{F}_\ell} (M/(\ell, \nu_{n+1,n})M) \\ &= r(\ell^{n+1} - \ell^n) + \sum_{i=1}^{s} \min\{a_i,\, \ell^{n+1} - \ell^n\}, \end{aligned} \tag{4.5}$$

from which we find immediately $r = 0$ and $a_i < \ell^{n+1} - \ell^n$ for all i. Therefore, we get inequality $\dim_{\mathbb{F}_\ell} M/\ell M = \sum_{i=1}^{s} a_i \leqslant b$ by (4.3) and (4.5), which implies the assertion of the theorem as mentioned above. ■

5. Calculation

In this section, we return to the case $\ell = 2$ and recall $\Lambda = \mathbb{Z}_2[[T]]$. Let $k = \mathbb{Q}(\sqrt{p})$ with prime number p satisfying $p \equiv 1 \pmod{16}$ and $2^{(p-1)/4} \equiv 1 \pmod{p}$. Let k_n be the intermediate field of the cyclotomic $\mathbb{Z}_2$-extension of k with $[k_n : k] = 2^n$ and A_n the 2-part of the ideal class group of k_n. We put $|A_n| = 2^{e_n}$.

First of all, we explain how to compute e_n. Straightforward calculation using several software packages developed for number theory handles e_1, e_2 and e_3. But it fails to compute e_4 because the degree $[k_n : k] = 2^n$ increases rapidly. So a custom algorithm specialized to k is needed. Thanks to [6, Proposition 3.5], the integer a_r in the table in [3], which is expected to be equal to e_r, is now actually equal to e_r. Hence we can calculate e_n $(1 \leqslant n \leqslant 8)$ by using the method in [5].

Let χ be the character of k and ω the Teichmüller character modulo 4. Then $\chi^* = \omega\chi^{-1}$ is the character of $\mathbb{Q}(\sqrt{-p})$. We define the integer s so that $p \equiv 1 \pmod{2^s}$ and $p \not\equiv 1 \pmod{2^{s+1}}$. Then the Stickelberger element ξ_n is defined by

$$\xi_n = \frac{1}{q_n} \sum_{\substack{a=1 \\ (a,q_n)=1}}^{q_n} a\chi^*(a)^{-1} \left(\frac{\mathbb{B}_n/\mathbb{Q}}{a}\right)^{-1} \in \mathbb{Z}_2[G(\mathbb{B}_n/\mathbb{Q})],$$

where $q_n = p2^{n+2}$ and $\left(\frac{\mathbb{B}_n/\mathbb{Q}}{a}\right)$ is the Artin symbol. It is known that $\frac{1}{2}\xi_n$ also has integral coefficients. So we associate $\left(\frac{\mathbb{B}_n/\mathbb{Q}}{1+q_0}\right)^{-1}$ with $\frac{1+T}{1+q_0}$ and construct the polynomial $G_n(T) \in \Lambda$ from $\frac{1}{2}\xi_n$. Weierstrass preparation theorem guarantees the decomposition

$$G_n(T) = u_n(T)g_n(T)$$

with the unit element $u_n(T) \in \Lambda$ and the distinguished polynomial $g_n(T) \in \Lambda$, where $g_n(T)$ is constructed explicitly by an algorithm in [17, Proposition 7.2]. Then we know the congruence relation

$$g(T) \equiv g_n(T) \pmod{2^{n-s+2}},$$

where $g(T)$ is the distinguished polynomial defined by (2.1).

Now we see

$$\begin{aligned}
\frac{1}{2}\xi_n &= \frac{1}{2^{n+3}p}\sum_{\substack{a=1\\(a,2p)=1}}^{2^{n+2}p} a\chi^*(a)^{-1}\left(\frac{\mathbb{B}_n/\mathbb{Q}}{a}\right)^{-1}\\
&= \frac{1}{2^{n+3}p}\sum_{\substack{j=0\\(j,2)=1}}^{2^{n+2}-1}\sum_{i=0}^{p-1}(2^{n+2}i+j)\chi^*(2^{n+2}i+j)\left(\frac{\mathbb{B}_n/\mathbb{Q}}{2^{n+2}i+j}\right)^{-1}\\
&= \frac{1}{2p}\sum_{\substack{j=0\\(j,2)=1}}^{2^{n+2}-1}\left(\frac{\mathbb{B}_n/\mathbb{Q}}{j}\right)^{-1}\sum_{i=0}^{p-1} i\chi^*(2^{n+2}i+j)\\
&\quad + \frac{1}{2^{n+3}p}\sum_{j=0}^{2^{n+2}-1} j\left(\frac{\mathbb{B}_n/\mathbb{Q}}{j}\right)^{-1}\sum_{i=0}^{p-1}\chi^*(2^{n+2}i+j)\\
&= \frac{1}{2p}\sum_{\substack{j=0\\(j,2)=1}}^{2^{n+2}-1}\left(\frac{\mathbb{B}_n/\mathbb{Q}}{j}\right)^{-1}\sum_{i=0}^{p-1} i\chi^*(2^{n+2}i+j),
\end{aligned}$$

because, for odd j, we have

$$\begin{aligned}
\sum_{i=0}^{p-1}\chi^*(2^{n+2}i+j) &= \sum_{i=0}^{p-1}(-1)^{2^{n+1}i}(-1)^{\frac{j-1}{2}}\left(\frac{2^{n+2}i+j}{p}\right)\\
&= (-1)^{\frac{j-1}{2}}\sum_{a=0}^{p-1}\left(\frac{a}{p}\right) = 0.
\end{aligned}$$

Put $G = (\mathbb{Z}/2^{n+2}\mathbb{Z})^\times$ and $H = \langle\, 1 + q_0 + 2^{n+2}\mathbb{Z}\,\rangle$. Then $G = H \cup (-H)$ and hence

$$\begin{aligned}
G_n(T) = \frac{1}{2p}\sum_{j=0}^{2^n-1}\left(\frac{1+T}{1+q_0}\right)^j\sum_{i=0}^{p-1} i\Big\{&\chi^*(2^{n+2}i + ((1+q_0)^j \bmod 2^{n+2}))\\
&+ \chi^*(2^{n+2}i + (-(1+q_0)^j \bmod 2^{n+2}))\Big\},
\end{aligned}$$

where $a \bmod 2^{n+2}$ means rational integer x satisfying

$$x \equiv a \pmod{2^{n+2}} \qquad \text{and} \qquad 0 \leqslant x < 2^{n+2}.$$

Now we show two examples, from which we derive Theorem 1.1. Let $p = 13841$. Then $s = 4$ and we see

$$\begin{aligned}
g(T) &\equiv 44128 + 126772T + 30644T^2 + T^3 \pmod{2^{17}}\\
&\equiv (2616 + T)(74772 + 28028T + T^2) \pmod{2^{17}} \qquad (5.1)
\end{aligned}$$

from ξ_{19}. Proposition 2 in [13, Chapter II] with the fact $g_{19}(-2616) \equiv 0 \pmod{2^{17}}$, $g'_{19}(-2616) \not\equiv 0 \pmod{2^3}$ implies that $g(T)$ has a factor $P_1(T) = \alpha + T$ ($\alpha \in \mathbb{Z}_2$) with $\alpha \equiv 2616 \pmod{2^{13}}$ and (5.1) implies that $g(T)/P_1(T)$ is irreducible modulo 2^{13}. Hence $g(T)/P_1(T)$ is irreducible in Λ and we see

$$g(T) = P_1(T)P_2(T)$$

with irreducible polynomial $P_2(T)$ of degree two.

Now we get e_n as follows:

n	1	2	3	4	5	6	7	8
e_n	2	4	5	6	7	8	9	10

Hence it follows that $\lambda_2(k) \leqslant 1$ by Theorem 4.1 and it suffices to verify the condition (3.2) only for $P(T) = P_1(T)$ in order to prove $\lambda_2(k) = 0$. When $n = 10$, we see that $a = 13$ in the expression (3.3) and the condition (3.2) holds. Hence we have $\lambda_2(k) = 0$.

Next we treat $p = 67073$. In this case, $s = 9$. We calculate ξ_{28} and find that

$$g(T) = P_1(T)P_2(T)P_3(T),$$

where $P_1(T)$, $P_2(T)$ and $P_3(T)$ are monic irreducible polynomials with degree 1,2 and 124 respectively by factoring $g_{28}(T)$ modulo 2^{21} and using Hensel's lemma. We also see

$$\begin{aligned} P_1(T) &\equiv 1000 + T \pmod{2^{11}}, \\ P_2(T) &\equiv 1392 + 796T + T^2 \pmod{2^{11}}, \end{aligned}$$

and

n	1	2	3	4	5	6	7	8
e_n	3	6	9	12	14	16	18	20

Hence it follows that $\lambda_2(k) \leqslant 2$ by Theorem 4.1 and it suffices to verify the condition (3.2) only for $P(T) = P_1(T)$ and $P(T) = P_2(T)$ in order to prove $\lambda_2(k) = 0$. Actually we verify the condition (3.2) for $P_1(T)$ with $n = 8$ and for $P_2(T)$ with $n = 3$. So we conclude $\lambda_2(k) = 0$.

6. Comparison of criteria

We would like to compare criteria of $\lambda_2(k) = 0$. Most fundamental criterion is Theorem 2.1 in [3]. The condition (C) was first verified in our all practical calculations. Theorems 2.1 and 2.2 in [6] are considered the improvement of that in special situations. At the present time, we are abel to check these criteria in k_n ($1 \leqslant n \leqslant 8$). On the other hand, Corollary 3.6 is a criterion of different type. We are abel to check this criterion for larger n.

In the following table, we show n where we verified $\lambda_2(k) = 0$ under the calculations in k_n. The sign $\times$ means that the criterion can not be applied for such p. The inequality $\geqslant 13$ or $\geqslant 12$ means that we need at least $n = 13$ or $n = 12$ to apply [3, Theorem 2.1]. For p where the sign ? is marked, we failed to factorize Iwasawa polynomial $g(T)$ which has degree 2047, 1022 or 16383. So all the criteria should be considered complementary to each other.

p	[3, Theorem 2.1]	[6, Theorem 2.1]	[6, Theorem 2.2]	Corollary 3.6
1201	2	$\times$	$\times$	10
3361	5	$\times$	$\times$	3
12161	4	2	$\times$	11
13121	4	$\times$	2	6
13841	$\geqslant 13$	$\times$	$\times$	10
67073	$\geqslant 12$	$\times$	$\times$	8
14929	5	$\times$	4	2
15217	3	$\times$	$\times$	3
20353	1	$\times$	4	7
61297	8	$\times$	7	2
40961	1	2	$\times$	?
61441	2	$\times$	$\times$	?
65537	7	$\times$	$\times$	?

References

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

[2] B. Ferrero and L.C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), no. 2, 377–395.

[3] T. Fukuda, *Greenberg conjecture for the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p})$*, Interdisciplinary Information Sciences, **16-1** (2010), 21–32.

[4] T. Fukuda and K. Komatsu, *Ichimura-Sumida criterion for Iwasawa λ-invariants*, Proc. Japan Acad. Ser. A Math. Sci. **76** (2000), 111-115.

[5] T. Fukuda and K. Komatsu, *On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p})$*, Math. Comp. **78** (2009), 1797–1808.

[6] T. Fukuda and K. Komatsu, *On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p})$ II*, Funct. Approx. Comment. Math. **51** (2014), no. 1, 167–179.

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

[8] R. Greenberg, *On the structure of certain Galois groups*, Inv. math. **47** (1978), 85–99.

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

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

[11] H. Ichimura, S. Nakajima and H. Sumida-Takahashi, *On the Iwasawa lambda invariants of an imaginary abelian field of conductor* $3p^{n+1}$, J. Number Theory **133** (2013), 787–801.

[12] K. Iwasawa, *On* $\mathbb{Z}_\ell$*-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[13] S. Lang, *Algebraic Number Theory*, Graduate Texts in Math. vol. 110, Springer, 1994.

[14] M. Ozaki and H. Taya, *On the Iwasawa* λ_2*-invariants of certain families of real quadratic fields*, Manuscripta Math. **94** (1997), no. 4, 437–444.

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

[16] T. Tsuji, *On the Iwasawa* λ*-invariants of real abelian fields*, Trans. Amer. Math. Soc. **355** (2003), 3699-3714.

[17] L.C. Washington, *Introduction to cyclotomic fields. Second edition*, Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997.

[18] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. Math. **131** (1990), 493–540.

Addresses: Takashi Fukuda: Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan;
Keiichi Komatsu and Manabu Ozaki: Department of Mathematical Science, School of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan;
Takae Tsuji: Department of Mathematics, Tokai University, 4-1-1 Kitakaname, Hiratsuka, Kanagawa, 259-1292, Japan.

E-mail: fukuda.takashi@nihon-u.ac.jp, kkomatsu@waseda.jp, ozaki@waseda.jp, tsuji@tokai-u.jp

Received: 7 November 2014; **revised:** 19 December 2015