ON THE IWASAWA λ-INVARIANT OF THE REAL p-CYCLOTOMIC FIELD

Humio Ichimura* and Hiroki Sumida**

Abstract For any totally real number field k and any prime number p, it is conjectured that the Iwasawa invariants $\lambda_p(k)$ and $\mu_p(k)$ are both zero. We give a new criterion for the conjecture to be true when k is the real p-cyclotomic field, introducing a new way to apply p-adic L-functions. In a sense, it is a natural "generalization" of the classical criterion for the Vandiver conjecture.

§1 Introduction

For a prime number p and a number field k, denote by $\lambda_p(k)$ and $\mu_p(k)$ the Iwasawa λ-invariant and the μ-invariant associated to the ideal class group of the cyclotomic $\mathbb{Z}_p$-extension k_∞/k, respectively. It is conjectured that these invariants are both zero for any p and any totally real number field k (cf. [Iw3, p. 316], [Gr]), which is often called Greenberg's conjecture. When k is abelian over $\mathbb{Q}$, we have $\mu_p(k) = 0$ for all p by [FW]. Several authors have given some sufficient conditions for the conjecture to be true when k is a real quadratic field (cf. [Ca], [FK1], [FK2], [FT], [Gr], [OT], [S], [T], etc). Using them, it is known that $\lambda_3(k) = 0$ for "many" of the real quadratic fields $k = \mathbb{Q}(\sqrt{m})$ with $1 < m < 10^4$ except, for example, $m = 254$, 473.

This paper is a continuation of our previous work [IS] on the conjecture. So, we first recall the content of [IS] briefly. Let k be a real abelian field with $\Delta = \mathrm{Gal}(k/\mathbb{Q})$. Assume that the exponent of Δ divides $(p-1)$. Let χ be a $\mathbb{Q}_p$-valued nontrivial (even) character of Δ and $\lambda_p(\chi)$ the "χ-component" of $\lambda_p(k)$. The "χ-component" of the conjecture asserts that $\lambda_p(\chi) = 0$. Denote by $\lambda_p^*(\chi)$ the λ-invariant of the power series $g_\chi(T)$ in $\mathbb{Z}_p[[T]]$ (see (1) in §1) associated to the p-adic L-function $L_p(s,\chi)$, where we are regarding χ as a primitive Dirichlet character. We have an upper bound $\lambda_p(\chi) \le \lambda_p^*(\chi)$ by the Iwasawa main conjecture proved by [MW]. Thus, $\lambda_p(\chi) = 0$ if $\lambda_p^*(\chi) = 0$. But, there are many examples with $\lambda_p^*(\chi) \ge 1$ (see e.g. [Gr, p. 266], [F]). In [IS], we have given a new criterion for $\lambda_p(\chi) = 0$ in the *simplest* case where $\lambda_p^*(\chi) = 1$

---

* Partly supported by the Grants-in-Aid for Scientific Research, The Ministry of Education, Science and Culture, Japan.

** Partly supported by JSPS Research Fellowships for Young Scientists.

1991 AMS Mathematics Classification 11R23

(and (p,χ) satisfies some additional conditions). In this case, $g_\chi(T)$ has a unique zero α ($\in \mathbb{Q}_p$). The criterion is given in terms of certain cyclotomic units and polynomials $X_{\alpha,n}(T)$ defined, in a simple way, for α and each integer n (≥ 0). Using the criterion, we have shown by some computation that $\lambda_p(\chi)=0$ for $p=3$ (resp. 5, 7) and all real quadratic characters χ corresponding to $k=\mathbb{Q}(\sqrt{m})$ for which $\lambda_p^*(\chi)=1$, $1<m<10^4$ and p does not split in $k(\sqrt{-3})$ (resp. k). These examples contain the case $p=3$ and $k=\mathbb{Q}(\sqrt{254})$, $\mathbb{Q}(\sqrt{473})$. These two are so notorious because, for these, $\lambda_3(\chi)=0$ had not been verified so far for about 20 years since the first attack of [Gr] and [Ca] in spite of efforts of several other authors.

In this paper, we concentrate on the special case where $k=\mathbb{Q}(\cos(2\pi/p))$, and give a criterion for $\lambda_p(\chi)=0$ *without* the assumption $\lambda_p^*(\chi)=1$, but under the assumption that all zeros of $g_\chi(T)$ are contained in $\mathbb{Q}_p$. It is given, in a style similar to the main theorem of [IS], in terms of cyclotomic units and polynomials $X_{\alpha,n}(T)$, α being zeros of $g_\chi(T)$. We obtain our result in a way and from a viewpoint both different from [IS]. Namely, we use in this paper some result related to the coefficients of Ihara's "Jacobi sum universal power series" constructed and studied in [Ih], [IKY], [A], [Col2], [IK], etc, while, in [IS], we effectively used the theorem of [Iw1] and [Gi] on local units modulo cyclotomic units. It is interesting that we have obtained criterions of similar style from thus different methods. Though the result in this paper is restricted to the case $k=\mathbb{Q}(\cos(2\pi/p))$, we believe that it serves as a nice model for obtaining a good criterion for the conjecture for general real abelian fields without the assumption $\lambda_p^*(\chi)=1$.

§2 Theorem

Let p be a fixed odd prime number, $K=\mathbb{Q}(\mu_p)$, and $K_\infty=\underset{n\geq 0}{\cup} K_n$ the cyclotomic $\mathbb{Z}_p$-extension of K with $K_n=\mathbb{Q}(\mu_{p^{n+1}})$ ($n\geq 0$). Let A_n be the Sylow p-subgroup of the ideal class group of K_n and $A_\infty=\varprojlim A_n$ the projective limit w.r.t. the relative norms. Put $\Delta=\mathrm{Gal}(K/\mathbb{Q})$, $\Gamma=\mathrm{Gal}(K_\infty/K)$ and $G_\infty=\mathrm{Gal}(K_\infty/\mathbb{Q})$. These groups act on A_∞ and A_n in a natural way. Let ψ be a $\mathbb{Q}_p$-valued character of Δ (of degree one) and

$$e_\psi=\frac{1}{\mid \Delta \mid}\sum_{\sigma\in\Delta}\psi(\sigma)\sigma^{-1}$$

the idempotent of $\mathbb{Z}_p[\Delta]$ corresponding to ψ. For a module M over $\mathbb{Z}_p[\Delta]$, we denote by $M(\psi)$ the ψ-component $e_\psi M$ (or M^{e_ψ}) of M. Let

$$\kappa: G_\infty\to\mathbb{Z}_p^\times$$

be the p-cyclotomic character. We choose and fix the topological generator $\gamma=\kappa^{-1}(1+p)$ of Γ. We identify, as usual, the completed group ring $\mathbb{Z}_p[[\Gamma]]$

with the power series ring $\Lambda = \mathbb{Z}_p[[T]]$ by $\gamma = 1+T$. Thus, for a module M over $\mathbb{Z}_p[[G_\infty]]$ (e.g. $M = A_\infty$), we may view $M(\psi)$ as a Λ-module. It is known that $A_\infty(\psi)$ is finitely generated and torsion over Λ (cf. [Iw3, Theorem 5]). For a finitely generated and torsion Λ-module M, denote by $\mathrm{char}(M)$ its characteristic polynomial. Denote by $\lambda_p(\psi)$ and $\mu_p(\psi)$ the λ-invariant and the μ-invariant of $\mathrm{char}(A_\infty(\psi))$, respectively.

Let χ be a *fixed* $\mathbb{Q}_p$-valued *even* character of Δ, which we also regard as a primitive Dirichlet character. The χ-component of Greenberg's conjecture for $\mathbb{Q}(\cos(2\pi/p))$ is stated as follows:

$$\mathrm{char}(A_\infty(\chi)) = 1, \text{namely, } \lambda_p(\chi) = \mu_p(\chi) = 0.$$

Since we already know that $\mu_p(k) = 0$ (cf. [FW]), the conjecture is equivalent to the assertion "$\lambda_p(\chi) = 0$". When $\chi = \chi_0$ is the trivial character, it is known that $A_n(\chi_0) = \{1\}$ for all $n \geq 0$ (cf. [W, Propositions 6.16, 13.22]. Hence, $\lambda_p(\chi_0) = \mu_p(\chi_0) = 0$. So, we may well assume that χ is nontrivial (and even) in what follows.

By [Iw2], there exists a unique power series $g_\chi(T)$ in $\mathbb{Z}_p[[T]]$ related to the p-adic L-function $L_p(s, \chi)$ by

$$g_\chi((1+p)^{1-s} - 1) = L_p(s, \chi). \tag{1}$$

By the p-adic Weierstrass preparation theorem, we can uniquely write

$$g_\chi(T) = p^\mu P_\chi(T) u_\chi(T)$$

for an integer $\mu = \mu_p^*(\chi)$ (≥ 0), a distinguished polynomial P_χ and a unit u_χ of Λ. We have $\mu_p^*(\chi) = 0$ by [FW]. Denote by $\lambda_p^*(\chi)$ the degree of P_χ. We have the following upper bound for $\mathrm{char}(A_\infty(\chi))$ and $\lambda_p(\chi)$ by the Iwasawa main conjecture proved by [MW]:

$$\mathrm{char}(A_\infty(\chi)) \mid P_\chi(T), \tag{2}$$

and hence

$$\lambda_p(\chi) \leq \lambda_p^*(\chi).$$

Assume that P_χ has a root α contained in $\mathbb{Q}_p$ (hence, in $p\mathbb{Z}_p$). For an integer n (≥ 0), put $\omega_n(T) = (1+T)^{p^n} - 1$. Define polynomials $X_{\alpha,n}(T)$ in $\mathbb{Z}_p[T]$ and $Y_{\alpha,n}(T)$ in $\mathbb{Z}[T]$ by

$$\begin{cases} X_{\alpha,n}(T) = (\omega_n(T) - \omega_n(\alpha))/(T-\alpha), \text{ and} \\ Y_{\alpha,n}(T) \equiv X_{\alpha,n}(T) \mod p^{n+1}. \end{cases} \tag{3}$$

These polynomials play an important role in [IS]. By the identification $\gamma = 1+T$, $Y_{\alpha,n}$ can act on any element of the multiplicative group $K_n^\times$. Let $e_{\chi,n}$ be an element of $\mathbb{Z}[\Delta]$ such that

$$e_{\chi,n} \equiv e_\chi \bmod p^{n+1}$$

and the sum of its coefficients is zero. *Fix* a primitive p^{n+1}-st root ζ_n of unity so that $\zeta_{n+1}^p = \zeta_n$ for all n (≥ 0). Define an element $c_{\chi,n}$ of K_n by

$$c_{\chi,n} = (1-\zeta_n)^{e_{\chi,n}}.$$

This is a unit (cyclotomic unit) since the sum of the coefficients of $e_{\chi,n}$ is zero.

Now, our result is stated as follows:

Theorem. *Let χ be a $\mathbb{Q}_p$-valued nontrivial even character of Δ. Assume that $P_\chi(T)$ has a root α contained in $\mathbb{Q}_p$. Then, we have $(T-\alpha) \nmid \mathrm{char}(A_\infty(\chi))$ if and only if the condition*

$$(\mathrm{H}_{\alpha,n}) \qquad (c_{\chi,n})^{Y_{\alpha,n}(T)} \notin (K_n^\times)^{p^{n+1}}$$

holds for some n (≥ 0).

We immediately obtain from Theorem and (2) the following:

Corollary 1. *Let χ be as above. Assume that all roots of $P_\chi(T)$ are contained in $\mathbb{Q}_p$. Then, $\lambda_p(\chi) = 0$ if and only if, for each root α of $P_\chi(T)$, the condition $(\mathrm{H}_{\alpha,n})$ holds for some n.*

From this and the Chebotarev density theorem, we obtain:

Corollary 2. *Under the assumption of Corollary 1, we have $\lambda_p(\chi) = 0$ if and only if, for each root α of $P_\chi(T)$, there exist some $n \geq 0$ and a prime ideal $\mathfrak{L}$ of K_n of degree one such that*

$$(c_{\chi,n})^{Y_{\alpha,n}(T)} \bmod \mathfrak{L} \notin ((\mathbb{Z}/l\mathbb{Z})^\times)^{p^{n+1}} \quad \textit{with } l = \mathfrak{L} \cap \mathbb{Q}.$$

This is quite analogous to the classical criterion(cf. [W, Corollary 8.19]) for the Vandiver conjecture ($p \nmid h(\mathbb{Q}(\cos(2\pi/p)))$).

We prove Theorem in §4 by using a "cyclotomic part" of the coefficient formula for the Jacobi sum universal power series, namely, a comparison formula between the "Soulé character" and the Coates-Wiles homomorphism. In §3, we recall the definition and some properties of the Soulé characters.

§3 Soulé characters χ_m

We use the same notation as in §2. For integers m (≥ 1) and n (≥ 0), define a cyclotomic p-unit $\varepsilon_n(m)$ of K_n by

$$\varepsilon_n(m) := \prod_a (1-\zeta_n^a)^{a^{m-1}}.$$

Here, a runs over all integers satisfying $0 < a < p^{n+1}$ and $p \nmid a$. The following lemma is easily proved.

Lemma 1. *The following congruences hold.*

(1) $\varepsilon_{n+1}(m) \equiv \varepsilon_n(m) \bmod (K_{n+1}^\times)^{p^{n+1}}$.

(2) *For all* $\sigma \in G_\infty$, $\varepsilon_n(m)^\sigma \equiv \varepsilon_n(m)^{\kappa(\sigma)^{1-m}} \bmod (K_n^\times)^{p^{n+1}}$.

Letting $\omega = \kappa_{|\Delta}$, denote by s the *odd* integer such that

$$\chi = \omega^{p-s}, \text{ and } 0 \leq s \leq p-2.$$

Then, from Lemma 1(2), we have

$$\varepsilon_n(m) \equiv \varepsilon_n(m)^{e_{\chi,n}} \bmod (K_n^\times)^{p^{n+1}} \tag{4}$$

for all m with $m \equiv s \bmod (p-1)$. Denoting by τ the canonical isomorphism $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \to \mathrm{Gal}(K_n/\mathbb{Q})$, we put $F = F_{m,n} = \sum_a a^{m-1}\tau_a$, where a runs over all integers with $0 < a < p^{n+1}$ and $p \nmid a$. Then, from the above, we get

$$\varepsilon_n(m) \equiv (1-\zeta_n)^{e_{\chi,n}F} \bmod (K_n^\times)^{p^{n+1}}, \qquad \text{for all } m \equiv s \bmod (p-1).$$

Since $\gamma = 1+T$, we easily see that

$$e_{\chi,n}F_{m,n} \equiv e_{\chi,n}e_\chi F_{m,n} \equiv (p-1)e_{\chi,n}f_{m,n}(T) \bmod (p^{n+1}, \omega_n)$$

with

$$f_{m,n}(T) = \sum_{0 \leq a < p^n} (1+p)^{(m-1)a}(1+T)^a \ (\in \mathbb{Z}[T]).$$

Therefore, we obtain

$$\varepsilon_n(m) \equiv (c_{\chi,n})^{(p-1)f_{m,n}(T)} \bmod (K_n^\times)^{p^{n+1}}, \qquad \text{for all } m \equiv s \bmod (p-1). \tag{5}$$

Let M/K_∞ be the maximal pro-p abelian extension unramified outside p and N its intermediate field defined by

$$N = \bigcup_{n \geq 0} K_\infty(\varepsilon^{1/p^n} \mid \varepsilon \in E'_\infty),$$

where E'_∞ is the group of p-units of K_∞. The Galois groups $\mathcal{G} = \mathrm{Gal}(M/K_\infty)$ and $\mathcal{H} = \mathrm{Gal}(N/K_\infty)$ can be viewed as modules over $\mathbb{Z}_p[[G_\infty]]$ in a natural way. From Lemma 1(1), we can define a Kummer character $\chi_m : \mathcal{G} \to \mathbb{Z}_p$, called the Soulé character, by the relations

$$(\varepsilon_n(m)^{1/p^{n+1}})^{(\rho-1)} = \zeta_n^{\chi_m(\rho)} \text{ for all } n \geq 0 \text{ and all } \rho \in \mathcal{G}.$$

Since $\varepsilon_n(m)$ is a p-unit, we may regard χ_m also as a character of $\mathcal{H}$. By Lemma 1(2), we see that χ_m is an element of $\mathrm{Hom}(\mathcal{H}, \mathbb{Z}_p(m))$. Here, for a module X over $\mathbb{Z}_p[[G_\infty]]$, $\mathrm{Hom}(X, \mathbb{Z}_p(m))$ denotes the abelian group consisting of homomorphisms $f : X \to \mathbb{Z}_p$ satisfying $f(x^\sigma) = \kappa(\sigma)^m f(x)$ for all $\sigma \in G_\infty$ and all $x \in X$. For an integer s' $(0 \leq s' \leq p-2)$ and m with $m \equiv s' \bmod (p-1)$, we easily see that $f \in \mathrm{Hom}(X, \mathbb{Z}_p(m))$ factors through the $\omega^{s'}$-component $X(\omega^{s'})$ and hence can be regarded as an element of $\mathrm{Hom}(X(\omega^{s'}), \mathbb{Z}_p(m))$. Let χ^* be the *odd* character of Δ defined by

$$\chi^* = \omega\chi^{-1} = \omega^s.$$

Then, from the above, we have $\chi_m \in \mathrm{Hom}(\mathcal{H}(\chi^*), \mathbb{Z}_p(m))$ for $m \equiv s \bmod (p-1)$.

Let L/K_∞ be the maximal unramified pro-p abelian extension. Then, we can identify $\mathrm{Gal}(L/K_\infty)$ with A_∞ by class field theory:

$$\mathrm{Gal}(L/K_\infty) = A_\infty.$$

Denote by $M(\chi^*)$ the intermediate field of M/K_∞ corresponding to $\prod_\psi \mathcal{G}(\psi)$ by Galois theory, where ψ runs over all characters of Δ with $\psi \neq \chi^*$. Define $N(\chi^*)$, $L(\chi^*)$ and $(N \cap L)(\chi^*)$ in a similar way. Then, we have

$$\mathrm{Gal}(M(\chi^*)/K_\infty) = \mathcal{G}(\chi^*), \quad \mathrm{Gal}(L(\chi^*)/K_\infty) = A_\infty(\chi^*), \text{ etc.}$$

These groups can be viewed as Λ-modules in a natural way. The following lemma is well known.

Lemma 2. (1) (cf. [IK, p. 328]) $N(\chi^*)L(\chi^*) = M(\chi^*)$.
(2) (cf. [Iw3, Theorem 16]) *The Λ-module* $\mathrm{Gal}(M(\chi^*)/N(\chi^*))$ *is isomorphic to* $\hat{A}_\infty = \mathrm{Hom}(\varinjlim A_n(\chi), \mu_{p^\infty})$. *Here, the inductive limit is induced from the inclusion $K_n \to K_{n+1}$, and γ acts on each element f of $\hat{A}_\infty$ by $f^\gamma(c) = (f(c^{\gamma^{-1}}))^\gamma$.*
(3) (cf. [Iw3, Theorem 15]) *The Λ-module $\mathcal{H}(\chi^*)$ is embedded into Λ with a finite cokernel.*

As for the torsion Λ-module $A_\infty(\chi^*)$, the following is known. Put

$$g_\chi^*(T) = g_\chi((1+p)(1+T)^{-1} - 1) \ (\in \mathbb{Z}_p[[T]]). \tag{6}$$

By the p-adic Weierstrass preparation theorem and $\mu_p^*(\chi) = 0$, we can write

$$g_\chi^*(T) = P_\chi^*(T) u_\chi^*(T)$$

for a distinguished polynomial P_χ^* and a unit u_χ^* of Λ. The Iwasawa main conjecture proved by [MW] asserts that

$$\mathrm{char}(A_\infty(\chi^*)) = P_\chi^*(T). \tag{7}$$

Therefore, we have

$$A_\infty(\chi^*)^{P_\chi^*} = \{1\} \tag{8}$$

since $A_\infty(\chi^*)$ has no nontrivial finite Λ-submodule (cf. [W, Proposition 13.28]).

Let $\mathcal{U}_n$ be the group of principal units of the local p-cyclotomic field $\mathbb{Q}_p(\mu_{p^{n+1}})$, and $\mathcal{U} = \varprojlim \mathcal{U}_n$ the projective limit w.r.t. the relative norms. By class field theory, the Λ-module $\mathcal{U}(\chi^*)$ is canonically isomorphic to the inertia group $\mathrm{Gal}(M/L)(\chi^*)$ (cf. [Coa, Theorem 1]). Hence, by Lemma 2(1), we may regard $\mathcal{U}(\chi^*)$ as a Λ-submodule of $\mathcal{H}(\chi^*) = \mathrm{Gal}(N(\chi^*)/K_\infty)$:

$$\mathcal{U}(\chi^*) = \mathrm{Gal}(N(\chi^*)/(N \cap L)(\chi^*))\ (\subseteq \mathcal{H}(\chi^*)).$$

Then, by (8), we get

$$\mathcal{H}(\chi^*)^{g_\chi^*} = \mathcal{H}(\chi^*)^{P_\chi^*} \subseteq \mathcal{U}(\chi^*). \tag{9}$$

For each $m \geq 1$, let φ_m ($\in \mathrm{Hom}(\mathcal{U}, \mathbb{Z}_p(m))$) denote the m-th Coates-Wiles homomorphism w.r.t. the system $(\zeta_n)_{n\geq 0}$ (see [W,§13-7]). When $m \equiv s \bmod (p-1)$, φ_m is regarded as an element of $\mathrm{Hom}(\mathcal{U}(\chi^*), \mathbb{Z}_p(m))$ as explained before. The homomorphisms χ_m and φ_m are related by the following formula.

Lemma 3. (cf. [Ih, p. 105], [Ich, Lemma 3]) *Assume $m \equiv s \bmod (p-1)$. Then, we have*

$$\chi_m(\rho) = (p^{m-1} - 1)\varphi_m(\rho^{g_\chi^*})$$

for all $\rho \in \mathcal{H}(\chi^*)$.

This is a "cyclotomic part" of the coefficient formula for Jacobi sum universal power series. Lemma 3 was proved by Coleman for $\rho \in \mathcal{U}(\chi^*)$ using some results in [Col1], and was generalized in [Ich].

§4 Proof of Theorem

Let α be a root of $P_\chi(T)$ contained in $\mathbb{Q}_p$. In view of (6), we put

$$\alpha^* = (1+p)(1+\alpha)^{-1} - 1. \tag{10}$$

Then, we can write

$$P_\chi(T) = (T-\alpha)^e Q(T) \text{ and } P_\chi^*(T) = (T-\alpha^*)^e Q^*(T)$$

for some integer e (≥ 1) and distinguished polynomials Q, Q^* with $Q(\alpha) \neq 0$, $Q^*(\alpha^*) \neq 0$.

The quotient Λ-module $\mathcal{U}(\chi^*)/\mathcal{H}(\chi^*)^{P_\chi^*}$ (see (9)) is finitely generated and torsion by $\mathcal{U}(\chi^*) \simeq \Lambda$ (cf. [W, Theorem 13.54]) and Lemma 2(3). First, let us show the following equivalence:

$$(T-\alpha) \mid \mathrm{char}(A_\infty(\chi)) \cdots \mathbf{1} \Leftrightarrow (T-\alpha^*) \mid \mathrm{char}(\mathcal{U}(\chi^*)/\mathcal{H}(\chi^*)^{P_\chi^*}) \cdots \mathbf{2}. \tag{11}$$

By Lemma 2(2), we see that $\mathrm{Gal}(M(\chi^*)/N(\chi^*))$ is finitely generated and torsion over Λ and that the condition **1** is equivalent to

$$(T-\alpha^*) \mid \mathrm{char}(\mathrm{Gal}(M(\chi^*)/N(\chi^*))).$$

Since $\mathrm{Gal}(M(\chi^*)/N(\chi^*))$ is isomorphic to $\mathrm{Gal}(L(\chi^*)/(N\cap L)(\chi^*))$ by Lemma 2(1), the latter condition holds if and only if $\mathrm{char}(\mathrm{Gal}((N\cap L)(\chi^*)/K_\infty))$ divides $P_\chi^*(T)/(T-\alpha^*)$ by (7). This last condition is equivalent to **2** by Lemma 2(3) (and (9)).

(I) *Proof of "if" part.* Assume that $(T-\alpha) \mid \mathrm{char}(A_\infty(\chi))$. Then, by (11) and $\mathcal{U}(\chi^*) \simeq \Lambda$, we easily see that

$$\mathcal{H}(\chi^*)^{P_\chi^*} \subseteq \mathcal{U}(\chi^*)^{T-\alpha^*}. \tag{12}$$

Let m (≥ 1) be any integer with $m \equiv s \bmod (p-1)$. Note that the Coates-Wiles homomorphism φ_m ($\in \mathrm{Hom}(\mathcal{U}(\chi^*), \mathbb{Z}_p(m))$) satisfies

$$\varphi_m(u^T) = \varphi_m(u^{\gamma-1}) = (\kappa(\gamma)^m - 1)\varphi_m(u) = ((1+p)^m - 1)\varphi_m(u) \tag{13}$$

for all $u \in \mathcal{U}(\chi^*)$. Then, by Lemma 3 and (12), we observe that, for any $\rho \in \mathcal{H}(\chi^*)$,

$$\chi_m(\rho) = (p^{m-1} - 1)\varphi_m(\rho^{g_\chi^*}) \in \varphi_m(\mathcal{U}(\chi^*)^{T-\alpha^*}) \subseteq ((1+p)^m - 1 - \alpha^*)\mathbb{Z}_p. \tag{14}$$

Now, fix an integer $n \geq 0$. Since the set $\{(1+p)^m - 1 \mid m \equiv s \bmod (p-1)\}$ is dense in $p\mathbb{Z}_p$, we can take an integer m with $m \equiv s \bmod (p-1)$ such that

$$(1+p)^m \equiv 1 + \alpha^* \bmod p^{n+1}. \tag{15}$$

Then, by (14), we have $\operatorname{Im}\chi_m \subseteq p^{n+1}\mathbb{Z}_p$. This implies

$$\varepsilon_n(m) \in (K_\infty^\times)^{p^{n+1}}$$

by the definition of χ_m. But, the extension $F = K_n(\varepsilon_n(m)^{1/p^{n+1}})$ is Galois over $\mathbb{Q}$ by Lemma 1(2), and Δ acts on $\mathrm{Gal}(F/K_n)$ through χ^* because of $m \equiv s \bmod (p-1)$ and (4). Therefore, since χ^* is not the trivial character, we obtain

$$\varepsilon_n(m) \in (K_n^\times)^{p^{n+1}}. \tag{16}$$

By (10) and (15), we have $(1+p)^{1-m} \equiv 1+\alpha \bmod p^{n+1}$. From this and the definition (3) of $Y_{\alpha,n}(T)$, we can transform the polynomial $f_{m,n}(T)$ as follows:

$$\begin{aligned} f_{m,n} &= \frac{(1+p)^{(m-1)p^n}\cdot(1+T)^{p^n}-1}{(1+p)^{m-1}\cdot(1+T)-1} = u\cdot\frac{(1+T)^{p^n}-(1+p)^{(1-m)p^n}}{(1+T)-(1+p)^{1-m}} \\ &\equiv u\cdot Y_{\alpha,n}(T) \bmod p^{n+1} \text{ (for some } u\in\mathbb{Z}_p^\times). \end{aligned}$$

Hence, by (5) and (16), we obtain $(c_{\chi,n})^{Y_{\alpha,n}} \in (K_n^\times)^{p^{n+1}}$ for all n as desired. □

(II) *Proof of "only if" part.* Assume that $(T-\alpha)\nmid \mathrm{char}(A_\infty(\chi))$. Then, by (11), the index

$$[\mathcal{U}(\chi^*)/\mathcal{H}(\chi^*)^{P_\chi^*} : (\mathcal{U}(\chi^*)/\mathcal{H}(\chi^*)^{P_\chi^*})^{T-\alpha^*}]$$

is finite. Hence, there is some $c\geq 0$ such that

$$\mathcal{U}(\chi^*)^{p^c} \subseteq \mathcal{U}(\chi^*)^{T-\alpha^*}\cdot\mathcal{H}(\chi^*)^{P_\chi^*}. \tag{17}$$

Fix an integer $n\geq c$ and take an integer m with $m\equiv s \bmod (p-1)$ satisfying (15). Then, by mapping the both sides of (17) into $\mathbb{Z}_p$ by φ_m, we obtain

$$p^c\mathbb{Z}_p \subseteq ((1+p)^m - 1-\alpha^*)\mathbb{Z}_p + \operatorname{Im}\chi_m \subseteq p^{n+1}\mathbb{Z}_p + \operatorname{Im}\chi_m$$

from (13), Lemma 3 and $\operatorname{Im}\varphi_m = \mathbb{Z}_p$ (cf. [W, Proposition 13.51]). But, since $n\geq c$, we must have $\operatorname{Im}\chi_m \not\subseteq p^{n+1}\mathbb{Z}_p$. Hence, by the definition of χ_m, we get $\varepsilon_n(m)\notin (K_n^\times)^{p^{n+1}}$ for $n\geq c$ and m satisfying (15). Now, by an argument similar to the end of (I), we see that $(\mathrm{H}_{\alpha,n})$ holds for all $n\geq c$. □

§5 Recent developments

During the preparation of this paper, Kraft and Schoof [KS] and Kurihara [K] obtained some effective criterions for the validity of the conjecture for certain classes of real abelian fields. [KS] deals with real quadratic fields k with $\left(\frac{k}{p}\right)\neq 1$ and without the assumption $\lambda_p^*(\chi)=1$, χ being the Dirichlet character associated to k. [K] works mainly under an assumption similar to that of our Corollaries. By some computations, they add new examples with $\lambda_p(k) = 0$. But, in [KS], there are some numerical mistakes such as data for $p = 3$ and $k = \mathbb{Q}(\sqrt{254})$, $\mathbb{Q}(\sqrt{473})$.

The criterions of [KS] and [K] and that of [IS] and this paper are different from each other. But, in practical computational applications, all these depend on some calculation of some cyclotomic units modulo several prime ideals. A feature of ours compared with [KS], [K] and other related works is that we have introduced a new way to apply p-adic L-functions to the conjecture. Namely, we have used effectively the polynomials $X_{\alpha,n}(T)$.

Recently, inspired by the results/ideas of [IS] and this paper, we have succeeded in obtaining an effective criterion for the conjecture for general real abelian fields k on which all we impose as an assumption is that the exponent of $\Delta = \mathrm{Gal}(k/\mathbb{Q})$ divides $(p-1)$. As its application, we have shown by some computation that $\lambda_3(k) = 0$ for all real quadratic fields $k = \mathbb{Q}(\sqrt{m})$ with $1 < m < 10^4$. We shall publish the general result, which is rather long and complicated, elsewhere.

References

[A] Anderson, G., *The hyperadelic gamma functions*, Invent. Math. **95** (1989), 63–131.

[Ca] Candiotti, A., *Computations of Iwasawa invariants and K_2*, Compositio Math. **29** (1974), 89–111.

[Coa] Coates, J., *p-adic L-functions and Iwasawa's theory*, Algebraic Number Fields(Durham Symposium; ed.by A. Fröhlich):Academic Press:London (1975), 269–353.

[Col1] Coleman, R., *The dilogarithm and the norm residue symbol*, Bull. Soc. Math. France **109** (1981), 373–402.

[Col2] Coleman, R., *Anderson-Ihara theory: Gauss sums and circular units*, Adv. Stud. Pure Math. **17** (1989), 55–72.

[F] Fukuda, T., *Iwasawa's λ-invariants of imaginary quadratic fields*, J. College. Industrial Technology Nihon Univ. (Corrigendum: to appear ibid) **27** (1994), 35–88.

[FK1] Fukuda, T. and K. Komatsu, *On $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Math.Soc.Japan **38** (1986), 95–102.

[FK2] Fukuda, T. and K. Komatsu, *A capitulation problem and Greenberg's conjecture of real quadratic fields*, Math. Comp. **65** (1996), 313–318.

[FT] Fukuda, T. and H. Taya, *The Iwasawa λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields*, Acta Arith. **69** (1995), 277–292.

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

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

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

[Ich] Ichimura, H., *On the coefficients of the universal power series for Jacobi sums*, J. Fac. Sci. Univ. Tokyo **36** (1989), 1–7.

[IK] Ichimura, H. and M. Kaneko, *On the universal power series for Jacobi sums and the Vandiver conjecture*, J. Number Theory **31** (1989), 312–334.

[IS] Ichimura, H. and H. Sumida, *On the Iwasawa invariants of certain real abelian fields*, to appear in Tohoku Math. J..

[Ih] Ihara, Y., *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. **123** (1986), 43–106.

[IKY] Ihara, Y., Kaneko, M. and A. Yukinari, *On some properties of the universal power series for Jacobi sums*, Adv. Stud. Pure Math. **12** (1987), 65–86.

[Iw1] Iwasawa, K., *On some modules in the theory of cyclotomic fields*, J. Math. Soc. Japan **16** (1964), 42–82.

[Iw2] Iwasawa, K., *Lectures on p-adic L-functions*, Ann. of Math. Stud. no. 74, Princeton Univ. Press: Princeton, N.J. (1972).

[Iw3] Iwasawa, K., *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[K] Kurihara, M., *The Iwasawa λ invariants of real abelian fields and the cyclotomic elements*, preprint (1995).

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

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

[OT] Ozaki, M. and H. Taya, *A note on Greenberg's conjecture of real abelian number fields*, Manuscripta Math. **88** (1995), 311–320.

[S] Sumida, H., *Greenberg's conjecture and the Iwasawa polynomial*, to appear in J. Math. Soc. Japan.

[T] Taya, H., *On the Iwasawa λ-invariants of real quadratic fields*, Tokyo J. Math. **16** (1993), 121–130.

[W] Washington, L., *Introduction to Cyclotomic Fields*, Graduate Texts in Math. no. 83, Springer: New York (1982).

Humio ICHIMURA
Department of Mathematics
Yokohama City University
22-2 Seto, Kanazawa-ku, Yokohama, 236, Japan
ichimura@ yokohama-cu.ac.jp

Hiroki SUMIDA
Department of Mathematical Sciences
University of Tokyo
3-8-1 Komaba, Meguro-ku, Tokyo, 153, Japan
sumida@ ms.u-tokyo.ac.jp