Iwasawa invariants and exceptional pairs of certain abelian fields

Kazato NADA, Haruma SASAKI and Hiroki SUMIDA-TAKAHASHI *

Department of Mathematical Sciences,
Tokushima University,
Minamijosanjima-cho 2-1, Tokushima 770-8506, JAPAN
e-mail address : hirokit@tokushima-u.ac.jp

Abstract

Let p be an odd prime number and ζ_p a primitive p-th root of unity. By computing special arithmetic elements modulo prime ideals, we have investigated the Iwasawa invariants and exceptional pairs $(p, \chi\omega_p^k)$ of $\mathbf{Q}(\sqrt{d}, \zeta_p)$. Here χ denotes the Dirichlet character associated to $\mathbf{Q}(\sqrt{d})$, and ω_p the Teichmüller character at p. First, we determine Λ-isomorphism classes of Iwasawa modules, and describe structural differences between exceptional and non-exceptional pairs in terms of unramified extensions outside p. Next, we report 14 new exceptional pairs in the range $|d| < 200$ and $p < 2{,}000{,}000$, or $|d| < 10$ and $p < 30{,}000{,}000$, including $(p, k, d) = (28{,}679{,}999,\ 2{,}284{,}521, -8)$ for which the $\chi\omega_p^{1-k}$-part of the Iwasawa λ-invariant is equal to two.

Key words: Iwasawa invariant, exceptional pair, unramified extension, ideal class group
2020 Mathematics Subject Classification: Primary 11R23; Secondary 11R18, 11R29, 11R70

1 Introduction

Let χ be either the trivial character or a primitive quadratic Dirichlet character of conductor $f = f_\chi$, and let p be an odd prime number such that $p \nmid f$. We

*ORCID:0000-0003-3928-9481 The author was partially supported by JSPS KAKENHI Grant Number JP25K06934 and JP26K00600.

fix an embedding $\overline{\mathbf{Q}}$ to $\mathbf{C}_p$. Define $d = d_\chi = \chi(-1)f_\chi$, $K = \mathbf{Q}(\sqrt{d}, \zeta_p)$, and $K_n = \mathbf{Q}(\sqrt{d}, \zeta_{p^{n+1}})$, where ζ_m denotes a primitive m-th root of unity. Let A_n be the p-part of the ideal class group of K_n.

Set $K_\infty = \cup_{n\geq 0} K_n$, $\Gamma = \mathrm{Gal}(K_\infty/K)$, $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty) \simeq \mathrm{Gal}(K_0/\mathbf{Q})$ and define $e_\varphi = \frac{1}{\sharp\Delta}\sum_{\delta\in\Delta}\varphi(\delta)\delta^{-1}$ for a character φ of Δ.

For a $\mathbf{Z}_p[\Delta]$-module A, We denote by A^φ the φ-part $e_\varphi A$. Let $\lambda_p(\varphi)$, $\mu_p(\varphi)$ and $\nu_p(\varphi)$ be the Iwasawa invariants associated to A_n^φ, i.e.,

$$\sharp A_n^\varphi = p^{\lambda_p(\varphi)n+\mu_p(\varphi)p^n+\nu_p(\varphi)}$$

for sufficiently large n. By Ferrero-Washington's theorem, we have $\mu_p(\varphi) = 0$ for all p and φ.

We put $f_0 = fp$ and identify Δ with a subquotient of $(\mathbf{Z}/f_0\mathbf{Z})^\times$ in the usual way. Then, we can identify φ with a $\mathbf{Q}_p$-valued Dirichlet character. In the following, we assume that a character ψ of Δ is identified with an even primitive Dirichlet character of conductor f_0. The Iwasawa polynomial $g_\psi(T) \in \mathbf{Z}_p[T]$ for the p-adic L-function is defined as follows. Let $L_p(s,\psi)$ be the p-adic L-function constructed by [13]. By [9, §6], there uniquely exists a unique power series $G_\psi(T) \in \mathbf{Z}_p[[T]]$ satisfying

$$G_\psi((1+f_0)^{1-s}-1) = L_p(s,\psi)$$

for all $s \in \mathbf{Z}_p$ with $\psi \neq \chi^0$. By [4], p does not divide $G_\psi(T)$. By the p-adic Weierstrass preparation theorem, we can uniquely write $G_\psi(T) = g_\psi(T)u_\psi(T)$, where $g_\psi(T)$ is a distinguished polynomial of $\mathbf{Z}_p[T]$ and $u_\psi(T)$ is an invertible element of $\mathbf{Z}_p[[T]]$. Similarly we can define $g_\psi^*(T) \in \mathbf{Z}_p[T]$ from $G_\psi^*(T) \in \mathbf{Z}_p[[T]]$ satisfying

$$G_\psi^*((1+f_0)^s-1) = L_p(s,\psi).$$

Put

$$\tilde{\lambda}_p(\psi) = \deg g_\psi(T) = \deg g_\psi^*(T).$$

Put $f_n = f_0p^n$ and let $\gamma \in \Gamma \simeq \mathrm{Gal}(\cup_{n\geq 0}\mathbf{Q}(\zeta_{f_n})/\mathbf{Q}(\zeta_{f_0}))$ be the generator of Γ such that $\zeta_{f_n}^{\tilde{\gamma}} = \zeta_{f_n}^{1+f_0}$ for all $n \geq 0$. As usual, we can identify the complete group ring $\mathbf{Z}_p[[\Gamma]]$ with the formal power series ring $\Lambda = \mathbf{Z}_p[[T]]$ by $\gamma = 1+T$. By this identification, we can consider a $\mathbf{Z}_p[[\Gamma]]$-module as a Λ-module. For a finitely generated torsion Λ-module A, we define the Iwasawa polynomial $\mathrm{char}_\Lambda(A)$ to be the characteristic polynomial of the action T on $A \otimes \mathbf{Q}_p$ (cf. [26, §13]). Let L_n be the maximal unramified abelian extension of K_n and M_n the maximal abelian extension of K_n unramified outside p. By the class field theory, we have $A_n \simeq \mathrm{Gal}(L_n/K_n)$. Set $L_\infty = \cup_{n\geq 0}L_n$, $M_\infty = \cup_{n\geq 0}M_n$, $X_\infty = \mathrm{Gal}(L_\infty/K_\infty)$ and $Y_\infty = \mathrm{Gal}(M_\infty/K_\infty)$. By the Iwasawa main conjecture proved by [6, 14],

$$\mathrm{char}_\Lambda(X_\infty^{\psi^{-1}\omega}) = g_\psi^*(T) \quad \text{and} \quad \mathrm{char}_\Lambda(Y_\infty^\psi) = g_\psi(T).$$

In the following, we assume that

$$\psi = \chi\omega^k \text{ is even, and } \psi^* = \psi^{-1}\omega = \chi\omega^{p-k} \text{ is odd}$$

with $2 \leq k \leq p-2$. Since p does not divide f,

$$\text{(C)} \qquad \psi(p) \neq 1 \text{ and } \psi^*(p) \neq 1.$$

By (C), we have that $A_n^\psi \simeq X_\infty^\psi/\omega_n X_\infty^\psi$ and $A_n^{\psi^*} \simeq X_\infty^{\psi^*}/\omega_n X_\infty^{\psi^*}$, where $\omega_n = (1+T)^{p^n}-1$ (cf. [8, Lemma 3 and Remark 4]). Moreover, if A_0^ψ is trivial, we have $\lambda_p(\psi) = \nu_p(\psi) = 0$, $X_\infty^\psi = \{0\}$, $\quad Y_\infty^\psi \simeq \Lambda/(g_\psi(T))$ $\quad$ and $\quad X_\infty^{\psi^*} \simeq \Lambda/(g_\psi^*(T))$. Put

$$a_0 = a_0(\psi) = L_p(1,\psi) = G_\psi(0) \quad \text{and} \quad b_0 = b_0(\psi) = L_p(0,\psi) = G_\psi^*(0).$$

Note that $v_p(a_0) = v_p(\sharp\mathrm{Gal}(M_0/K_0)^\psi)$ and $v_p(b_0) = v_p(\sharp\mathrm{Gal}(L_0/K_0)^{\psi^*})$.

We call $(p, \chi\omega^k)$ an exceptional pair when one of the following conditions holds:

$$[\nu]:\ A_0^{\chi\omega^k} \neq \{0\},\ \ [a_0]:\ v_p(a_0) > 1,\ \ [b_0]:\ v_p(b_0) > 1 \ \text{ or } \ [\mathrm{lmd}]:\ \tilde{\lambda}_p(\chi\omega^k) > 1.$$

Many authors, including Kummer, Vandiver, D.H. Lehmer, E. Lehmer, Selfridge, Nicol, Pollack, Johnson, Wada, Wagstaff, Tanner, Ernvall, Metsänkylä, Buhler, Crandall, Sompolski, Shokrollahi, Hart, Harvey and Ong, have computed irregular pairs, and verified that no exceptional pair exists for $d = 1$ and $p < 2^{31} = 2{,}147{,}483{,}648$ (cf. [2, 3, 7]).

In [19, 20, 21, 22, 23], by computing special arithmetic elements modulo prime ideals, we computed irregular and exceptional pairs in the range $|d| < 200$ (resp. $|d| < 10$) and $p < 1{,}000{,}000$ (resp. $p < 20{,}000{,}000$). These data are useful for computing the p-part of the ideal class group of K_n and higher K-groups of the integer ring of $\mathbf{Q}(\sqrt{d})$, and for verifying generalized Greenberg's conjecture for $\mathbf{Q}(\sqrt{d}, \zeta_p)$ (cf. [25]).

This paper is organized as follows. In Section 2, we determine Λ-isomorphism classes of Iwasawa modules, and describe structural differences between exceptional and non-exceptional pairs in terms of unramified extensions outside p. In Section 3, we review algorithms for the computation, and report new exceptional pairs obtained by further computation in the range $|d| < 200$ (resp. $|d| < 10$) and $p < 2{,}000{,}000$ (resp. $p < 30{,}000{,}000$), including $(p, k, d) = (28{,}679{,}999,\ 2{,}284{,}521, -8)$ with $\lambda_p(\chi\omega_p^{1-k}) = 2$.

2 Unramified abelian extensions outside p

We use the notation in the previous section and assume that $\psi = \chi\omega^k$ satisfies (C). Let D_n be the subgroup of A_n which is generated by the class of prime ideals lying above p and put $A_n' = A_n/D_n$. Let E_n be the unit group of K_n and

E'_n the p-unit group of K_n. By (C), $D_n^{\psi} = D_n^{\psi^*} = \{0\}$, $A_n^{\psi} \simeq {A'_n}^{\psi}$, $A_n^{\psi^*} \simeq {A'_n}^{\psi^*}$ and $H^1(K_n/K, E_n)^{\psi} \simeq H^1(K_n/K, E'_n)^{\psi}$,where $\psi^* = \psi^{-1}\omega = \chi\omega^{1-k}$.

In the following, we determine the Λ-isomorphism classes of Iwasawa modules by the Iwasawa main conjecture and [10, Theorem 12, 17, 18 and Lemma 12]. Note that (C) is (A) in [8]. In [18], we define the set of Λ-isomorphism classes for a distinguished polynomial $f(T) \in \Lambda$:

$$\mathcal{M}_{f(T)} = \{[M] \mid \mathrm{char}_{\Lambda}(M) = f(T), \ \ M \text{ has no nontrivial finite } \Lambda-\text{submodule}\}$$

and show that $\sharp\mathcal{M}_{f(T)}$ is finite if and only if $f(T)$ is square-free. If (p, ψ) does not satisfy $[\nu]$, it is easy to determine the Λ-isomorphism classes of Iwasawa modules, because they are cyclic Λ-modules. If (p, ψ) satisfies $[\nu]$, it is not easy to determine the Λ-isomorphism classes of Iwasawa modules especially when $\deg f(T) \geq 3$ in general. When $\deg f(T) = 1$ or $f(T)$ is an Eisenstein polynomial, $\sharp\mathcal{M}_{f(T)} = 1$. When $\deg f(T) = 2$, $\mathcal{M}_{f(T)}$ is explicitly determined in [12, 18]. However, when $\deg f(T) \geq 3$, $\mathcal{M}_{f(T)}$ is not explicitly determined except for some cases (cf. [5, 15, 16, 17, 18]).

First, if $(p, \chi\omega^k)$ is a regular pair, we have $v_p(a_0(\psi)) = 0$, $v_p(b_0(\psi)) = 0$ and $\tilde{\lambda}_p(\psi) = \lambda_p(\psi^*) = \nu_p(\psi) = \nu_p(\psi^*) = 0$. Then, we have the following simple Λ-module structures of Galois groups.

Case [R]

$$\begin{array}{lll} X_{\infty}^{\psi} = \{0\}, & & Y_{\infty}^{\psi} = \{0\}, \\ X_{\infty}^{\psi^*} = \{0\} & \text{and} & Y_{\infty}^{\psi^*} \simeq \Lambda. \end{array}$$

Next, we assume that $(p, \chi\omega^k)$ is an irregular pair. Then, $v_p(a_0(\psi)) > 0$, $v_p(b_0(\psi)) > 0$ and $\tilde{\lambda}_p(\psi) = \lambda_p(\psi^*) > 0$, where $\psi^* = \chi\omega^{1-k}$.

If (p, ψ) is not an exceptional pair,

Case [nE]

$$\begin{array}{lll} X_{\infty}^{\psi} = \{0\}, & & Y_{\infty}^{\psi} \simeq \Lambda/(T-\alpha), \\ X_{\infty}^{\psi^*} \simeq \Lambda/(T-\alpha^*) & \text{and} & Y_{\infty}^{\psi^*} \simeq \Lambda \end{array}$$

for some α, $\alpha^* \in p\mathbf{Z}_p \setminus p^2\mathbf{Z}_p$.

Finally, we consider four cases that (p, ψ) satisfies only one of conditions $[\nu]$, $[a_0]$, $[b_0]$ and [lmd], which is usual when p is large.

Case $[\nu]$

(i) If Greenberg's conjecture is true for p and ψ,

$$\begin{array}{lll} X_{\infty}^{\psi} \simeq \Lambda/(T-\alpha, p^{\nu}), & & Y_{\infty}^{\psi} \simeq \Lambda/(T-\alpha), \\ X_{\infty}^{\psi^*} \simeq \Lambda/(T-\alpha^*) & \text{and} & Y_{\infty}^{\psi^*} \simeq (T, p) \subset \Lambda \end{array}$$

for some α, $\alpha^* \in p\mathbf{Z}_p \setminus p^2\mathbf{Z}_p$ and $\nu \in \mathbf{Z}_{\geq 1}$.

(ii) If Greenberg's conjecture is false for p and ψ,

$$\begin{array}{lll} X_{\infty}^{\psi} \simeq \Lambda/(T-\alpha), & & Y_{\infty}^{\psi} \simeq \Lambda/(T-\alpha), \\ X_{\infty}^{\psi^*} \simeq \Lambda/(T-\alpha^*) & \text{and} & Y_{\infty}^{\psi^*} \simeq \Lambda/(T-\alpha^*) \oplus \Lambda \end{array}$$

for some α, $\alpha^* \in p\mathbf{Z}_p \setminus p^2\mathbf{Z}_p$.

Case $[a_0]$

$$\begin{array}{lll} X_\infty^\psi = \{0\}, & & Y_\infty^\psi \simeq \Lambda/(T-\alpha), \\ X_\infty^{\psi^*} \simeq \Lambda/(T-\alpha^*) & \text{and} & Y_\infty^{\psi^*} \simeq \Lambda \end{array}$$

for some $\alpha \in p^2\mathbf{Z}_p$, $\alpha^* \in p\mathbf{Z}_p \setminus p^2\mathbf{Z}_p$.

Case $[b_0]$

$$\begin{array}{lll} X_\infty^\psi = \{0\}, & & Y_\infty^\psi \simeq \Lambda/(T-\alpha), \\ X_\infty^{\psi^*} \simeq \Lambda/(T-\alpha^*) & \text{and} & Y_\infty^{\psi^*} \simeq \Lambda \end{array}$$

for some $\alpha \in p\mathbf{Z}_p \setminus p^2\mathbf{Z}_p$, $\alpha^* \in p^2\mathbf{Z}_p$.

Case [lmd]

$$\begin{array}{lll} X_\infty^\psi = \{0\}, & & Y_\infty^\psi \simeq \Lambda/(g(T)), \\ X_\infty^{\psi^*} \simeq \Lambda/(g^*(T)) & \text{and} & Y_\infty^{\psi^*} \simeq \Lambda \end{array}$$

for some distinguished polynomials $g(T)$, $g^*(T) \in \mathbf{Z}_p[T]$ such that $g(0)$, $g^*(0) \in p\mathbf{Z}_p \setminus p^2\mathbf{Z}_p$, $\deg g(T) = \deg g^*(T) \geq 2$.

From the above Λ-structures, we obtain the following structural differences of Galois groups over finite extensions in each case.

Theorem 2.1. *Assume that ψ satisfies* (C) *and that (p, ψ) is an irregular pair. In* Case $[\nu]$*, there is a unramified abelian p-extension L'_n of K_n such that $\mathrm{Gal}(L'_n/K_n)^\psi$ is not trivial for $n \geq 0$. In* Case $[a_0]$*, there is an unramified abelian p-extension M'_n of K_n outside p such that the exponent of $\mathrm{Gal}(M'_n/K_n)^\psi$ is larger than p^{n+1} for $n \geq 0$. In* Case $[b_0]$*, there is an unramified abelian p-extension L'_n of K_n such that the exponent of $\mathrm{Gal}(L'_n/K_n)^{\psi^*}$ is larger than p^{n+1} for $n \geq 0$. In* Case [lmd]*, there is an unramified abelian p-extension L'_n of K_n such that the p-rank of $\mathrm{Gal}(L'_n/K_n)^{\psi^*}$ is larger than one for $n \geq 1$. On the other hand, those extensions do not exist if (p, ψ) is not an exceptional pair.*

Proof. Put $X' = \mathrm{Gal}(L_\infty/K_\infty)^\psi$ and $Y' = \mathrm{Gal}(M_\infty/K_\infty)^{\psi^*}$. Then, the subgroup of X'(resp. Y') which corresponds to the maximal abelian extension of K_n is $\omega_n X'$(resp. $\omega_n Y'$). Since $X' \simeq \mathrm{Gal}(L_n/K_n)^\psi$ and $Y' \simeq \mathrm{Gal}(M_n/K_n)^{\psi^*}$, the Λ-structures of X' and Y' imply the assertions. □

In the above theorem, we use the Δ-decomposition of Galois groups. Let us give another statement which characterizes Case [lmd]. We consider the following two typical cases with $X_\infty \simeq \mathbf{Z}_p^\lambda$.

Case [lmd $\times$ 1]

$$X_\infty^{\psi^*} \simeq \Lambda/(g^*(T)) \quad (\text{Case [lmd]}) \quad \text{and} \quad X_\infty = X_\infty^{\omega^{1-k}}.$$

Case [nE $\times$ λ]

$$X_\infty^{\chi\omega^{1-k_i}} \simeq \Lambda/(T-\alpha_i^*) \quad (\text{Case [nE]}) \quad \text{and} \quad X_\infty = \bigoplus_{i=1}^{\lambda} X_\infty^{\omega^{1-k_i}}.$$

Theorem 2.2. *In* Case [lmd $\times$ 1]*, there is no unramified abelian p-extension* L_n' *of* K_n *such that*

$$\mathrm{Gal}(L_n'/K_n) \simeq (\mathbf{Z}/p^{a_1}\mathbf{Z}) \oplus (\mathbf{Z}/p^{a_2}\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/p^{a_r}\mathbf{Z})$$

with $r \leq \lambda$ *and* $a_1 \leq a_2 \leq \ldots \leq a_r$ *such that* $a_r - a_1 \geq 2$ *and that* L_n' *is a Galois extension of* K_0 *for* $n \geq 0$*. On the other hand, in* Case [nE $\times$ λ]*, there exists such an unramified abelian extension of* K_n *which is a Galois extension of* K_0 *for* $n \geq 1$*.*

Proof. Put $X' = \mathrm{Gal}(L_\infty/K_\infty)^{\psi^*}$. Then, the subgroup of X' which corresponds to the maximal abelian extension of K_n is $\omega_n X'$. Further, subgroups of X' which correspond to Galois extensions of K_0 are Λ-submodules of X'. We show that a Λ-submodule M' of $M = \Lambda/(g^*(T))$ is determined by its index when $g^*(T)$ is an Eisenstein polynomial, along the proof in [24, Theorem 2.4]. Put $\lambda = \deg g^*(T) \geq 2$. Let $h(T) \in \Lambda \setminus (g^*(T))$. By p-adic Weierstrass preparation theorem, $h(T) \equiv p^{s'-1}u(T)f(T) \mod (g^*(T))$, where $s' \geq 1$, $u(T) \in \Lambda^\times$, and $f(T)$ is a distinguished polynomial of degree $b' < \lambda$. Then, we have $(g^*(T), h(T)) = (g^*(T), p^{s'-1}f(T)) = (g^*(T), p^{s'-1}f(T), p^{s'-1}g^*(T) - p^{s'-1}T^{\lambda-b'}f(T)) = (g^*(T), p^{s'-1}T^{b'}, p^{s'})$. Let s be the minimum number of such s' contained in M' modulo $(g^*(T))$. Further let b be the minimum number of such b' with $s' = s$ contained in M' modulo $(g^*(T))$. M' is determined by s and b, i.e., $|M/M'| = p^{\lambda(s-1)+b}$. Then, as an abelian group,

$$M/M' \simeq (\mathbf{Z}/p^{(s-1)}\mathbf{Z})^{\lambda-b} \oplus (\mathbf{Z}/p^s\mathbf{Z})^b.$$

This implies the non-existence of a Galois extension of K_0 which satisfies the condition in the theorem for $n \geq 0$.

On the other hand, for $M = \bigoplus_{i=1}^{\lambda} \Lambda/(T-\alpha_i^*)$, $\langle p^{a_1}e_1, p^{a_2}e_2, \ldots, p^{a_\lambda}e_\lambda\rangle$ is a Λ-submodule of M for any $a_i \in \mathbf{Z}_{\geq 0}$, where $e_1 = (1,0,0,\ldots,0)$, $e_2 = (0,1,0,\ldots,0)$, …, $e_\lambda = (0,0,\ldots,0,1)$. Since $\omega_1 M = p^2 M$, this implies the existence of a Galois extension of K_0 which satisfies the condition in the theorem for $n \geq 1$. □

Remark 2.1. *When* $f(T)$ *is an Eisenstein polynomial, the* Λ*-isomorphism classes of Galois groups are similar to Case* [ν]*. By the above proof, there*

is only one submodule $(f(T), p^{s-1}T^b, p^s)/(f(T))$ *in* $\Lambda/(f(T))$ *of index* $p^\nu = p^{\tilde{\lambda}(s-1)+b}$.

Case $[\nu]'$ (Eisenstein polynomial)

(i) *If Greenberg's conjecture is true for* p *and* ψ,

$$\begin{array}{lll} X_\infty^\psi \simeq \Lambda/(f(T), p^{s-1}T^b, p^s), & & Y_\infty^\psi \simeq \Lambda/(f(T)), \\ X_\infty^{\psi^*} \simeq \Lambda/(f^*(T)) & \text{and} & Y_\infty^{\psi^*} \simeq (T,p) \subset \Lambda \end{array}$$

for some b, $s \in \mathbf{Z}_{\geq 1}$.

(ii) *If Greenberg's conjecture is false for* p *and* ψ,

$$\begin{array}{lll} X_\infty^\psi \simeq \Lambda/(f(T)), & & Y_\infty^\psi \simeq \Lambda/(f(T)), \\ X_\infty^{\psi^*} \simeq \Lambda/(f^*(T)) & \text{and} & Y_\infty^{\psi^*} \simeq \Lambda/(f^*(T)) \oplus \Lambda. \end{array}$$

3 Algorithms and numerical results

We use the notation in the previous sections. First, we briefly review algorithms for computing Iwasawa invariants and exceptional pairs of $\mathbf{Q}(\sqrt{d}, \zeta_p)$.

We compute the following arithmetic special elements (cf. [1], [19, §2], [20, §5] and [§3][21]):

(I) the generalized Bernoulli numbers modulo p, i.e., $\sum_{k=0}^{p-2} B_{k,\chi} t^k/k! \bmod p$,

(II)$_n$ the Iwasawa polynomial $g_\psi(T) \mod p^{n+1}$,

(III)$_n$ the special cyclotomic unit $(c_n^\psi)^{Y_n(T)}$ modulo a prime ideal $\mathfrak{L}_n$,

(IV)$_n$ the Gauss sum $g_0(N_{K_n/K_0}\mathfrak{L}_n)^{\psi^*}$ modulo a prime ideal $\mathfrak{L}_0^*$, where $\mathfrak{L}_n$ (resp. $\mathfrak{L}_n^*$) is a prime ideal above $l = 1 + \kappa f_n$ (resp. $l^* = 1 + \kappa^*(2f_n l)$) of K_n.

In (I), we use the Fast Fourier Transform algorithm for multiplication of polynomials (see [11, §4.3.3]). In (II)$_n$, we use the approximate formula for $L(s, \psi)$ [26, Theorem 5.11]. In (III)$_n$, we define $Y_n(T) \in \mathbf{Z}[T]$ by $g_\psi(T) \bmod p^{n+1}$ and compute $c = (c_n^\psi)^{Y_n(T)} \mod \mathfrak{L}_n$ for an auxiliary prime number l. We check a criterion for c. If the criterion is satisfied, we obtain $\lambda_p(\psi) = 0$ (Greenberg's conjecture) and an upper bound of $\nu_p(\psi)$ (see [8, §2]). In (IV)$_n$, we compute $g = g_0(N_{K_n/K_0}\mathfrak{L}_n)^{\psi^*} \mod \mathfrak{L}_0^*$ for auxiliary prime l^* by using the Fast Fourier Transform algorithm once again. We check a criterion for g. If the criterion is satisfied, we obtain an lower bound of $\nu_p(\psi)$. Finally we obtain the exact value of $\nu_p(\psi)$ if Greenberg's conjecture hold for p and ψ (see [19, §3]).

In [19, 20, 21, 22, 23], by using the above special elements, we efficiently computed irregular pairs and exceptional pairs for $|d| < 200$ and $p < 1{,}000{,}000$. By further computation, we obtain the following.

Proposition 3.1. *For* $10 < |d| < 200$ *and* $1{,}000{,}000 < p < 2{,}000{,}000$, *all exceptional pairs* $(p, \chi\omega^k)$ *are given in* Table 1.

Table 1: Exceptional pairs for $10 < |d| < 200$ and 1,000,000 $< p <$ 2,000,000.

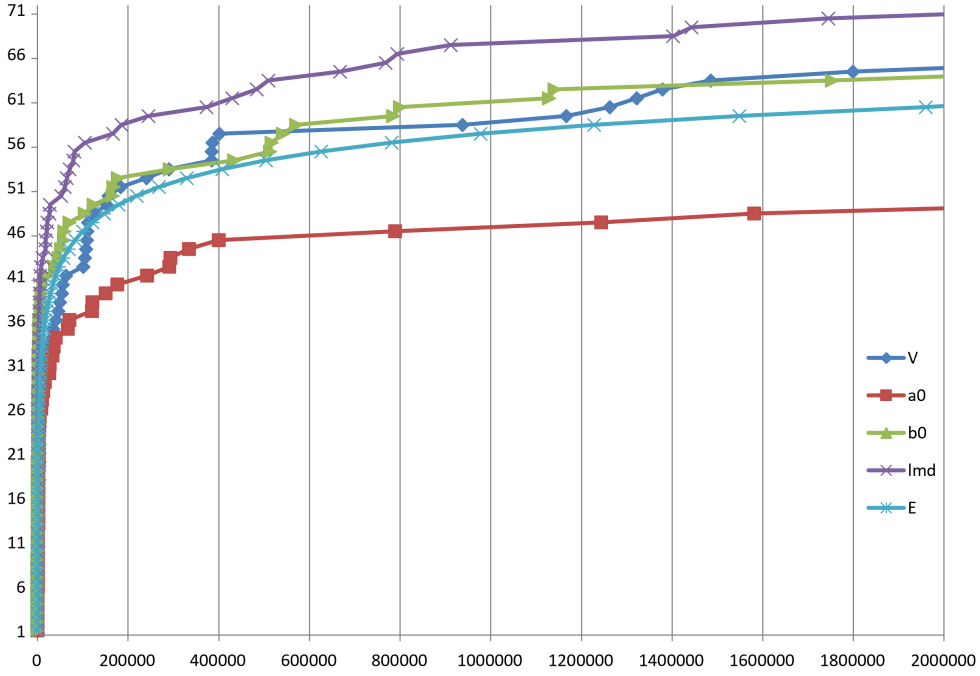
$[\nu]$			$[a_0]$		
p	k	d	p	k	d
1166927	871940	145	1243093	1052719	-183
1262483	816621	-167	1580483	878413	-116
1321927	1087373	-35			
1378691	497941	-167			
1485761	566272	73			
1798813	984380	97			
$[b_0]$			[lmd]		
p	k	d	p	k	d
1128233	191315	-67	1402147	944163	-87
1140949	611954	56	1442899	1057203	-151
1752481	557278	24			

In Figure 1, we compare actual numbers of exceptional pairs in the range $f_\chi < 200$ and $200 < p < x$ with the expected number

$$E_1(x) = 123 \sum_{200<p<x} \frac{p-3}{2} \left(\frac{1}{p}\right)^2,$$

where 123 is the number of the trivial character χ^0 and quadratic characters χ with $f_\chi < 200$.

Figure 1: Actual numbers and the expected number ($200 < p <$ 2,000,000).

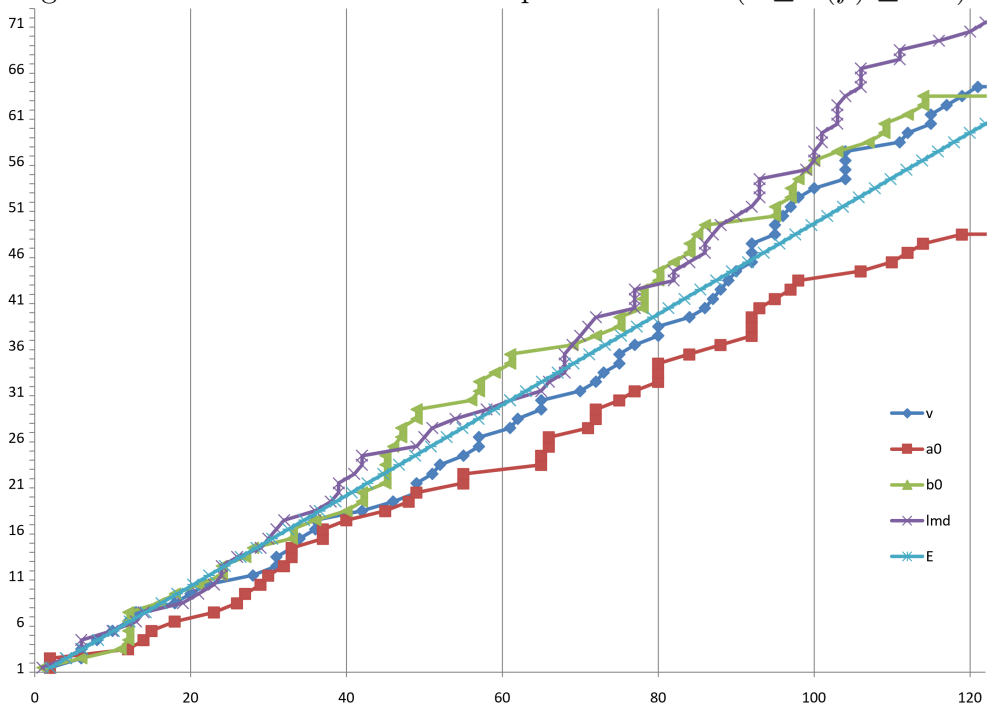


In Figure 2, we compare actual numbers of exceptional pairs in the range $f_\chi < f$ and $200 < p < 2{,}000{,}000$ with the expected number

$$E_2(n) = n \sum_{200<p<2{,}000{,}000} \frac{p-3}{2} \left(\frac{1}{p}\right)^2,$$

where $n = n(f) = \sharp\{\chi \,|\, \chi^2 = \chi^0,\ f_\chi \le f\}$. From our data, actual numbers still seem to be near the expected number.

Figure 2: Actual numbers and the expected number ($0 \le n(f) \le 123$).



In [22, 23], we computed exceptional pairs for $|d| < 10$ and $10 < p < 20{,}000{,}000$. The largest prime number among them is 5,911,877 which was found in 2012 and satisfies the condition $[a_0]$ for $(k, d) = (1{,}629{,}992, 5)$. By further computation, we obtain the following new exceptional pair which was found in 2024.

Proposition 3.2. *For* $|d| < 10$ *and* $6{,}000{,}000 < p < 30{,}000{,}000$, *there is only one exceptional pair* $(p, \chi\omega^k)$ *which is given in* Table 2.

Table 2: The exceptional pair for $|d| < 10$ and $6{,}000{,}000 < p < 30{,}000{,}000$.

	[lmd]	
p	k	d
28679999	2284521	-8

Proposition 3.3. *In the range* $|d| < 200$ (*resp.* $|d| < 10$) *and* $200 < p <$ 2,000,000 (*resp.* $10 < p <$ 30,000,000)*, every exceptional pair* (p, ψ) *satisfies only one of conditions* $[\nu]$, $[a_0]$, $[b_0]$ *and* [lmd].

For details of computation, see [23]. The programs and further data have been available in our web page: https://hiro2.pm.tokushima-u.ac.jp/~hiroki/major/galois1-e.html. These data were obtained by seven personal computers with 76 cores (152 threads) for about five years. We computed twice for $|d| < 200$ and $p < 2,000,000$, and only once for $|d| < 10$ and $p < 30,000,000$.

Though temporary hardware errors are rare, they could occur in long-term computation. We are afraid that they occur in the latter computation. However, these rare errors would not affect Proposition 3.2, because the expected number is very small. In fact,

$$\sum_{x_0<p<x_1} \frac{p-3}{2}\left(\frac{1}{p}\right)^2 \approx \frac{1}{2}(\log\log 30{,}000{,}000 - \log\log 6{,}000{,}000) = 0.04907\cdots$$

for $x_0 =$ 6,000,000 and $x_1 =$ 30,000,000. It might be hard to find a new exceptional pair for $|d| < 10$, because

$$\sum_{x_0<p<x_1} \frac{p-3}{2}\left(\frac{1}{p}\right)^2 \approx \frac{1}{2}(\log\log 100{,}000{,}000 - \log\log 30{,}000{,}000) = 0.03379\cdots$$

for $x_0 =$ 30,000,000 and $x_1 =$ 100,000,000.

References

[1] M. Aoki and T. Fukuda, *An algorithm for computing p-class groups of abelian number fields*, Lecture Notes in Computer Science **4076** (2006), 56–71.

[2] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and A. M. Shokrollahi, *Irregular primes and cyclotomic invariants to* 12 *million*, J. Symbolic Comput. **31** (2001), 89–96.

[3] J. Buhler and D. Harvey, *Irregular primes to 163 million*, Math. Comp. **80** (2011), 2435–2444.

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

[5] C. Franks, *Classifying* Λ*-modules up to isomorphism and application to Iwasawa theory*, Ph D dissertation, Arizona State University (2011).

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

[7] W. Hart, D. Harvey, and W. Ong, *Irregular primes to two billion*, Math. Comp. **86** (2017), 3031–3049.

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

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

[10] ———, *On $\mathbf{Z}_l$-extensions of algebraic number fields*, Ann. of Math.,(2) **98** (1973), 246–326.

[11] E. Knuth, *The art of computer programming, vol. 2: Seminumerical algorithms. 2nd edition*, Addison-Wesley Publishing Co., Reading, Mass, 1981.

[12] M. Koike, *On the isomorphism classes of Iwasawa modules associated to imaginary quadratic fields with $\lambda = 2$*, J. Math. Sci. Univ. Tokyo **6** (1999), 371–396.

[13] T. Kubota and H.W. Leopoldt, *Eine p-adische Theorie der Zetawerte, I. Einführung der p-adischen Dirichletschen L-Funktionen*, J. reine angew. Math. **214/215** (1964), 328–339.

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

[15] K. Murakami, *On the isomorphism classes of Iwasawa modules with $\lambda = 3$ and $\mu = 0$*, Osaka J. Math. **51** (2014), no. 4, 829–865 (English).

[16] ———, *Isomorphism classes of modules over Iwasawa algebra with $\lambda = 4$*, Tokyo J. Math. **39** (2016), no. 1, 101–132 (English).

[17] ———, *On a new invariant determining the isomorphism classes of Λ-modules with $\lambda = 3$*, Manuscr. Math. **164** (2021), 409–430.

[18] H. Sumida, *Greenberg's conjecture and the Iwasawa polynomial*, J. Math. Soc. Japan **49** (1997), 689–711.

[19] H. Sumida-Takahashi, *Computation of Iwasawa invariants of certain real abelian fields*, J. Number Theory **105** (2004), 235–250.

[20] ———, *The Iwasawa invariants and the higher K-groups associated to real quadratic fields*, Exp. Math. **14** (2005), 307–316.

[21] ———, *Computation of the p-part of the ideal class group of certain real abelian fields*, Math. Comp. **76** (2007), 1059–1071.

[22] ———, *Examples of the Iwasawa invariants and the higher K-groups associated to quadratic fields*, J. Math. Univ. Tokushima **41** (2007), 33–41.

[23] ———, *A generalized problem associated to the Kummer-Vandiver conjecture*, Arnold Math. J. **9** (2023), 381–391.

[24] H. Sumida-Takahashi, N. Furuya, and K. Kitano, *On the l-part of the class groups of imaginary cyclic fields of conductor p and degree $2l^n$*, J. Math. Tokushima Univ. **56** (2022), 1–10.

[25] ———, *Greenberg's generalized conjecture and pairings of p-units in the $4p$-cyclotomic field*, J. Ramanujan Math, Soc. **39** (2024), 79–90.

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