MATHEMATICS OF COMPUTATION
Volume 78, Number 267, July 2009, Pages 1797–1808
S 0025-5718(09)02124-3
Article electronically published on January 28, 2009

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

TAKASHI FUKUDA AND KEIICHI KOMATSU

In memory of Professor H. Ogawa

Abstract. We study the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p}\,)$ for an odd prime number p which satisfies $p \equiv 1 \pmod{16}$ relating it to units having certain properties. We give an upper bound of λ and show $\lambda = 0$ in certain cases. We also give new numerical examples of $\lambda = 0$.

1. Introduction

Let k be a finite algebraic number field, ℓ a prime number and ζ_{ℓ^n} a primitive ℓ^n-th root of unity. There exists the unique intermediate field k_∞ of $\bigcup_{n=0}^{\infty} k(\zeta_{\ell^n})/k$ such that the Galois group $G(k_\infty/k)$ is topologically isomorphic to the additive group of the ring of ℓ-adic integers $\mathbb{Z}_\ell$, which is called the cyclotomic $\mathbb{Z}_\ell$-extension of k. Let k_n be the unique intermediate field of k_∞/k with degree ℓ^n over k. Then the class number of k_n is controlled by the Iwasawa invariants $\mu_\ell(k)$, $\lambda_\ell(k)$ and $\nu_\ell(k)$ of k_∞/k, which were introduced by Iwasawa [10] and [12]. Namely, if ℓ^{e_n} denotes the ℓ-part of the ideal class number of k_n, then

$$e_n = \mu_\ell(k)\ell^n + \lambda_\ell(k)n + \nu_\ell(k)$$

for all sufficiently large n.

Iwasawa pointed out that $\mu_\ell(k)$ always seems to be zero and Ferrero and Washington [2] proved that $\mu_\ell(k)$ is zero for any abelian number field k and any prime number ℓ. Furthermore, Greenberg [7] suggests the possibility that $\lambda_\ell(k)$ is zero for any totally real number field k and any prime number ℓ, which is now called Greenberg conjecture.

In 1986, the authors [4] provided a criterion of verifying Greenberg conjecture numerically for a real quadratic field k and an odd prime number ℓ, and showed numerical evidence for the conjecture by giving a considerable amount of examples which satisfy $\lambda_\ell(k) = 0$. At the end of the twentieth century, Kraft and Schoof [15] and Ichimura and Sumida [9] developed a powerful computational technique verifying $\lambda_\ell(k) = 0$ for any odd prime number ℓ and any abelian number field k with degree prime to ℓ based on a new idea of using cyclotomic units. In particular, Ichimura and Sumida showed that $\lambda_3(\mathbb{Q}(\sqrt{m}\,)) = 0$ for all positive integers $m < 10000$. In 2003, Tsuji generalized the Ichimura-Sumida criterion to be applicable to the case that ℓ divides the degree $[k : \mathbb{Q}]$.

Received by the editor May 30, 2007 and, in revised form November 16, 2007.
2000 *Mathematics Subject Classification.* Primary 11G15, 11R27, 11Y40.
Key words and phrases. Iwasawa invariants, real quadratic fields.

In 1973, preceding the work of Ferrero and Washington, Iwasawa [11] indicated the importance of studying the cyclotomic $\mathbb{Z}_\ell$-extension of k when k is a cyclic extension of $\mathbb{Q}$ with degree ℓ. In fact, he proved that $\mu_\ell(k) = 0$ for such a k. It is then considered a fundamental step to study $\lambda_2(k)$ for real quadratic fields k from the viewpoint of Greenberg conjecture. It is essentially important to study $\lambda_2(\mathbb{Q}(\sqrt{p}\,))$ for a prime number p. The first breakthrough was brought by Ozaki and Taya [19] in 1997. They constructed certain families of infinitely many quadratic fields k which satisfy $\lambda_2(k) = 0$ and, in particular, obtained the following result:

Theorem 1.1 (cf. Ozaki and Taya [19])**.** *Let p be a prime number which satisfies one of the following conditions*:

(1) $p \equiv 3 \pmod 4$,
(2) $p \equiv 5 \pmod 8$,
(3) $p \equiv 9 \pmod{16}$,
(4) $p \equiv 1 \pmod{16}$ *and* $2^{\frac{p-1}{4}} \equiv -1 \pmod p$.

Then $\lambda_2(\mathbb{Q}(\sqrt{p}\,))$ is zero.

After Ozaki and Taya [19], the properties of $\lambda_2(k)$ for real quadratic fields k have been studied by several mathematicians (cf. [5], [18]). The purpose of this paper is to prove Theorem 1.2 below and Theorem 3.7 in §3.

Theorem 1.2. *Let p be any prime number with $p \equiv 1 \pmod{16}$, ε_0 the fundamental unit of $\mathbb{Q}(\sqrt{p})$, and $\varepsilon_0' = a + b\sqrt{2p}$ the fundamental unit of $\mathbb{Q}(\sqrt{2p})$, where a is a positive rational integer and $b \in \mathbb{Z}$. Let 2^s be the highest power of 2 which divides $p-1$. Then we have the following criteria concerning the Iwasawa λ-invariant $\lambda_2(\mathbb{Q}(\sqrt{p}))$:*

(1) *If $a \equiv 1 \pmod p$, then $\lambda_2(\mathbb{Q}(\sqrt{p})) \le 2^{s-2} - 3$.*
(2) *If $a^2 \equiv -1 \pmod p$ and if $\varepsilon_0^2 \not\equiv 1 \pmod{32}$, then $\lambda_2(\mathbb{Q}(\sqrt{p})) = 0$.*

Remark 1.1. Since ε_0' is a unit of $\mathbb{Q}(\sqrt{2p})$, $N_{\mathbb{Q}(\sqrt{2p})/\mathbb{Q}}(\varepsilon_0') = a^2 - 2pb^2 = \pm 1$. This means $a^2 \equiv \pm 1 \pmod p$.

The proofs of Theorems 1.2 and 3.7 are carried out in a different way from that of Theorem 1.1. The key idea is based on the property of units in k_n, which enables us to evaluate the 2-rank of the subgroup of the ideal class group of k_n generated by primes lying above p.

As a computational application of Theorem 3.7, we show in §4 that $\lambda_2(\mathbb{Q}(\sqrt{p})) = 0$ for all prime numbers p less than 10^4.

2. Notations

We denote by $\mathbb{Z}$ and $\mathbb{Q}$ the ring of integers and the field of rational numbers, respectively. For elements $g_1, g_2, \dots, g_r$ of a group G, we denote by $\langle\, g_1, g_2, \dots, g_r \,\rangle$ the subgroup of G generated by $g_1, g_2, \dots, g_r$. Let N be a normal subgroup of G. We denote by G/N the factor group of G over N and by $[G : N]$ the group index of N in G. For a finite algebraic extension K over k, $N_{K/k}$ means the norm mapping of K over k and if K is a Galois extension over k, $G(K/k)$ means the Galois group of K over k. If k is an algebraic number field, we denote by Ω_k and E_k the integer ring of k and the unit group of k, respectively. For an element α of Ω_k, we denote by $\alpha\Omega_k$ the principal ideal of Ω_k generated by α. We denote by ζ_{2^n} a primitive 2^n-th root of unity in the complex number field $\mathbb{C}$. Let ℓ be a prime number and

$\mathbb{Z}_\ell$ the ℓ-adic integer ring. We denote by $\Lambda = \mathbb{Z}_\ell[[T]]$ the ring of formal power series in an indeterminate T over $\mathbb{Z}_\ell$.

3. Proof of Theorem 1.2

Let p be a prime number, n a nonnegative integer and $k = \mathbb{Q}(\sqrt{p})$. We put $\alpha_n = 2\cos(2\pi/2^{n+2})$. It is well known that the field $\mathbb{Q}(\alpha_n)$ is a cyclic extension over $\mathbb{Q}$ with degree 2^n. Since $\alpha_{n+1} = \sqrt{2+\alpha_n}$, we have $\mathbb{Q}(\alpha_n) \subset \mathbb{Q}(\alpha_{n+1})$. Hence $\mathbb{Q}_\infty = \bigcup_{n=0}^\infty \mathbb{Q}(\alpha_n)$ is the unique $\mathbb{Z}_2$-extension of $\mathbb{Q}$, which is called the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$. We put $k_n = k(\alpha_n)$ and $k_\infty = k\mathbb{Q}_\infty$. Then k_∞ is the unique $\mathbb{Z}_2$-extension of k. Let M_n be the maximal abelian 2-extension of k_n unramified outside 2 and L_n the maximal abelian unramified 2-extension of k_n. Then $M_\infty = \bigcup_{n=0}^\infty M_n$ and $L_\infty = \bigcup_{n=0}^\infty L_n$ are the maximal abelian 2-extension of k_∞ unramified outside 2 and the maximal abelian unramified 2-extension of k_∞, respectively. Moreover, we put $I_n = G(M_n/L_n)$, $I_\infty = G(M_\infty/L_\infty)$, $\mathfrak{X}_\infty = G(M_\infty/k_\infty)$ and $X_\infty = G(L_\infty/k_\infty)$. As usual, we regard $\mathfrak{X}_\infty$ as a $\Lambda = \mathbb{Z}_2[[T]]$-module, where $1+T$ acts as a fixed topological generator γ of $G(k_\infty/k)$. Then we have the following exact sequence of Λ-modules:

$$1 \longrightarrow I_\infty \longrightarrow \mathfrak{X}_\infty \longrightarrow X_\infty \longrightarrow 1. \tag{1}$$

Since $\mu_2(k(\sqrt{-1}\,))$ is zero by [2] and since $\mathfrak{X}_\infty$ has no finite Λ-submodule by Theorem 1 of [8], $\mathfrak{X}_\infty$ is a finitely generated free $\mathbb{Z}_2$-module. Let $\lambda(I_\infty)$, $\lambda(\mathfrak{X}_\infty)$ and $\lambda(X_\infty)$ be $\mathbb{Z}_2$-ranks of I_∞, $\mathfrak{X}_\infty$, and X_∞, respectively. Then we have

$$\lambda(\mathfrak{X}_\infty) = \lambda(X_\infty) + \lambda(I_\infty) \tag{2}$$

by (1). Hereafter, we denote by λ_k the Iwasawa invariant $\lambda_2(k)$ of the cyclotomic $\mathbb{Z}_2$-extension of k_∞/k. By definition of λ_k, we have $\lambda_k = \lambda(X_\infty)$. Let 2^s be the highest power of 2 which divides $p-1$. We have $\lambda(\mathfrak{X}_\infty) = 2^{s-2}-1$ for $s \geq 2$ by [14, Theorem 1] and [25]. If $s \leq 3$, then $\lambda_k = 0$ by Theorem 1.1. So we assume $s \geq 4$. Now, there exist distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_{2^{s-2}}$ in k_{s-2} with $\sqrt{p}\,\Omega_{k_{s-2}} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{2^{s-2}}$ and the ideal $\mathfrak{p}_i\Omega_{k_n}$ generated by $\mathfrak{p}_i$ in Ω_{k_n} is a prime ideal of k_n for any integer $n \geq s-2$. Since 2 does not divide the class number of $\mathbb{Q}(\alpha_{s-2})$ (cf. p. 186 in [23]), there exists an odd integer t such that $\mathfrak{p}_i^{2t}$ is a principal ideal of k_{s-2} for $1 \leq i \leq 2^{s-2}$. We denote by $\mathrm{cl}(\mathfrak{p}_i^t\Omega_{k_n})$ the ideal class of k_n containing the ideal $\mathfrak{p}_i^t\Omega_{k_n}$ and by ρ_n the 2-rank of a subgroup $\langle\,\mathrm{cl}(\mathfrak{p}_1^t\Omega_{k_n}), \mathrm{cl}(\mathfrak{p}_2^t\Omega_{k_n}), \ldots, \mathrm{cl}(\mathfrak{p}_{2^{s-2}}^t\Omega_{k_n})\,\rangle$ in the ideal class group of k_n. The 2-rank of the ideal class group of k_n is stable for sufficiently large n because of $\mu_2(k) = 0$ and ρ_n is also stable. More precisely, there exists an integer $N \geq s-2$ such that $\lambda_k = \rho_n$ for all $n \geq N$ by [13, pp. 272, 287] and [6, Lemma 3.3]. Thus we have proved the following:

Lemma 3.1. *Notations and assumptions being as above, the following four assertions hold:*

(1) $\lambda_k = \lambda(X_\infty)$.
(2) $\lambda(\mathfrak{X}_\infty) = \lambda(X_\infty) + \lambda(I_\infty)$.
(3) $\lambda(\mathfrak{X}_\infty) = 2^{s-2} - 1$.
(4) *The 2-rank of the ideal class group of* k_n *is stable and* $\lambda_k = \rho_n$ *for* $n \geq N$.

Let σ be a generator of $G(k_\infty/\mathbb{Q}_\infty)$ and $\mathfrak{l}_n$ a prime ideal of k_n lying above 2. Then we have $\mathfrak{l}_n\mathfrak{l}_n^\sigma = \alpha_n\Omega_{k_n}$ $(n \geq 1)$, $(\mathfrak{l}_n\mathfrak{l}_n^\sigma)^{2^n} = 2\Omega_{k_n}$ and $\mathfrak{l}_n \neq \mathfrak{l}_n^\sigma$. We denote by E_n the unit group E_{k_n} of Ω_{k_n} for simplicity. Let $k_{n\,\mathfrak{l}_n}$ be the completion of k_n at

$\mathfrak{l}_n$, $\Omega_{\mathfrak{l}_n}^{\times}$ the unit group of $k_{n\,\mathfrak{l}_n}$ and $U_n = \Omega_{\mathfrak{l}_n}^{\times} \times \Omega_{\mathfrak{l}_n}^{\times}$. We embed E_n in U_n by the injective homomorphism

$$\varphi : E_n \ni \varepsilon \mapsto (\varepsilon, \varepsilon^{\sigma}) \in U_n. \tag{3}$$

Then we have

$$G(M_n/L_n) \simeq U_n/\,\overline{\varphi(E_n)}$$

by class field theory, where $\overline{\varphi(E_n)}$ is the topological closure of $\varphi(E_n)$ in U_n. Now, we need the following lemma:

Lemma 3.2. *The element* $(1, -1)$ *of* U_n *does not belong to* $\overline{\varphi(E_n)}$.

Proof. Let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2^{n+1}-1}$ be fundamental units of k_n. We assume $(1,-1) \in \overline{\varphi(E_n)}$. Then there exist 2-adic integers $x_1, x_2, \ldots, x_{2^{n+1}-1}$ with

$$(1,-1) = \pm\,(\varepsilon_1, \varepsilon_1^{\sigma})^{x_1}(\varepsilon_2, \varepsilon_2^{\sigma})^{x_2} \cdots (\varepsilon_{2^{n+1}-1}, \varepsilon_{2^{n+1}-1}^{\sigma})^{x_{2^{n+1}-1}}.$$

Hence we have

$$\prod_{i=1}^{2^{n+1}-1} \varepsilon_i^{2x_i} = 1 \quad \text{and} \quad \prod_{i=1}^{2^{n+1}-1} (\varepsilon_i^{\sigma})^{2x_i} = 1.$$

Let γ be a generator of $G(k_{n\,\mathfrak{l}_n}/\mathbb{Q}_2)$, where $\mathbb{Q}_2$ is the 2-adic number field. Then we have

$$\prod_{i=1}^{2^{n+1}-1} (\varepsilon_i^{\gamma^j})^{2x_i} = 1 \quad \text{and} \quad \prod_{i=1}^{2^{n+1}-1} (\varepsilon_i^{\sigma\gamma^j})^{2x_i} = 1$$

for $1 \le j \le 2^n$. This means

$$\sum_{i=1}^{2^{n+1}-1} x_i \log_2(\varepsilon_i^{\gamma^j})^2 = 0 \quad \text{and} \quad \sum_{i=1}^{2^{n+1}-1} x_i \log_2(\varepsilon_i^{\sigma\gamma^j})^2 = 0,$$

where $\log_2$ is a 2-adic log function. Therefore, we have

$$x_1 = \cdots = x_{2^{n+1}-1} = 0$$

by Leopoldt conjecture, which was proved in [1]. This is a contradiction. □

Remark 3.1. Using $(1,-1) \notin \overline{\varphi(E_0)}$, Ozaki proved in his thesis that $\lambda_k = 0$ if $s = 3$.

Let C_n be the unit group of $\mathbb{Q}(\alpha_n)$ and V_n the unit group of $\mathbb{Q}_2(\alpha_n)$. We put $W_n = \{\, u \in V_n : u \equiv 1 \pmod{4\alpha_n} \,\}$. Then we prove the following lemmas.

Lemma 3.3. *We have* $V_n = \langle\, 3 \,\rangle C_n W_n$.

Proof. Since the maximal 2-extension of $\mathbb{Q}$ unramified outside 2 is $\mathbb{Q}_\infty$, the maximal 2-extension of $\mathbb{Q}(\alpha_n)$ unramified outside 2 is also $\mathbb{Q}_\infty$. Hence we have $G(\mathbb{Q}_\infty/\mathbb{Q}(\alpha_n)) \simeq V_n/\,\overline{C}_n$, where $\overline{C}_n$ is the topological closure of C_n in V_n. Since $V_n/\,\overline{C}_n$ is generated by $3\overline{C}_n$ as a topological group and since W_n is an open subgroup of V_n, we have $V_n = \langle\, 3 \,\rangle C_n W_n$. □

Lemma 3.4. *We have* $N_{\mathbb{Q}_2(\alpha_n)/\mathbb{Q}_2}(u) \equiv 1 \pmod{2^{n+3}}$ *for any element* u *in* W_n.

Proof. Let v_n be the normalized additive α_n-adic valuation of $\mathbb{Q}(\alpha_n)$ and γ a generator of $G(\mathbb{Q}(\alpha_n)/\mathbb{Q})$. At first, we prove

$$v_n(\alpha_n^{\gamma^i} - \alpha_n) \le 2^n + 1 \quad \text{for } 1 \le i \le 2^n - 1$$

by induction on n. We have $v_n(\alpha_n^{\gamma^{2^{n-1}}} - \alpha_n) = v_n(2\alpha_n) = 2^n + 1$. Hence we have $v_1(\alpha_1^{\gamma} - \alpha_1) = 2 + 1$. We assume $v_m(\alpha_m^{\gamma^i} - \alpha_m) \leq 2^m + 1$ for $m < n$ and $1 \leq i \leq 2^m - 1$. Since $\alpha_n^2 = \alpha_{n-1} + 2$, we have

$$\begin{aligned} v_n(\alpha_n^{\gamma^i} - \alpha_n) + v_n(\alpha_n^{\gamma^i} + \alpha_n) &= v_n(\alpha_n^{2\gamma^i} - \alpha_n^2) \\ &= v_n(\alpha_{n-1}^{\gamma^i} - \alpha_{n-1}) \\ &= 2v_{n-1}(\alpha_{n-1}^{\gamma^i} - \alpha_{n-1}) \leq 2^n + 2 \end{aligned}$$

for $1 \leq i \leq 2^n - 1$ and $i \neq 2^{n-1}$. Hence we have $v_n(\alpha_n^{\gamma^i} - \alpha_n) \leq 2^n + 1$ for $1 \leq i \leq 2^n - 1$ noting that $v_n(\alpha_n^{\gamma^i} + \alpha_n) \geq 1$. Therefore, we have $N_{\mathbb{Q}_2(\alpha_n)/\mathbb{Q}_2}(u) \equiv 1 \pmod{2^{n+3}}$ by (1) of Corollary 1 to Proposition 11 of Chapter XII in [24]. □

Lemma 3.5. *Let $\mathbb{F}_2$ be the prime field of characteristic 2, G a cyclic group of order 2^n generated by γ, and $V = \mathbb{F}_2[G]$ the group ring of G over $\mathbb{F}_2$. Let $i_1, i_2, \ldots, i_r$ be integers with $0 \leq i_1 < i_2 < \cdots < i_r \leq 2^n - 1$ and v an element of V with $v = \gamma^{i_1} + \gamma^{i_2} + \cdots + \gamma^{i_r}$. If r is odd, then V is generated by $\{\gamma^i v : 0 \leq i \leq 2^n - 1\}$ over $\mathbb{F}_2$.*

Proof. Let f be a function of G into $\mathbb{C}$ such that $f(\gamma^i) = 1$ for $i = i_1, i_2, \ldots, i_r$ and that $f(\gamma^i) = 0$ for $i \neq i_1, i_2, \ldots, i_r$, where i is an integer with $0 \leq i \leq 2^n - 1$. Then we have

$$\det(f(\gamma^{i-j}))_{0 \leq i,j \leq 2^n - 1} = \prod_{\chi \in \widehat{G}} \sum_{i=0}^{2^n - 1} \chi(\gamma^i) f(\gamma^i) \equiv r^{2^n} \equiv 1 \pmod{\zeta_{2^n} - 1}$$

by [23, p. 71], where $\widehat{G}$ is the character group of G. □

Recall that φ is the isomorphism of E_n into U_n defined by (3).

Lemma 3.6. *If $n \geq s - 2$, we assume that $\mathfrak{p}_1^t \Omega_{k_n}$ is not principal in k_n. Then, for any unit ε of k_n with $N_{k_n/\mathbb{Q}(\alpha_n)}(\varepsilon) = 1$, there exists an element c of C_n such that $\varphi(\varepsilon c)$ is a square in U_n.*

Proof. Since $N_{k_n/\mathbb{Q}(\alpha_n)}(\varepsilon) = 1$, there exists an element α in Ω_{k_n} with $\varepsilon = \alpha^{\sigma - 1}$. First we assume $n \geq s - 2$. Since prime ideals $\mathfrak{p}_1\Omega_{k_n}, \mathfrak{p}_2\Omega_{k_n}, \ldots, \mathfrak{p}_{2^{s-2}}\Omega_{k_n}$ are the prime ideals in k_n which are ramified in k_n over $\mathbb{Q}(\alpha_n)$, we may assume that $\alpha\Omega_{k_n}$ is a product of the finite number of $\mathfrak{p}_i\Omega_{k_n}$. Since each $\mathfrak{p}_i\Omega_{k_n}$ is conjugate to $\mathfrak{p}_1\Omega_{k_n}$ over k and not principal in k_n, Lemma 3.5 leads to a conclusion that $\alpha\Omega_{k_n}$ is a product of an even number of $\mathfrak{p}_i\Omega_{k_n}$. Hence we have

$$N_{k_n/\mathbb{Q}}(\alpha) \equiv \pm 1 \pmod{2^{n+3}} \tag{4}$$

by $p \equiv 1 \pmod{2^s}$ and $s \geq 3$. Now we have $\alpha\alpha^\sigma \in C_n W_n$ or $\alpha\alpha^\sigma \in 3C_n W_n$ by Lemma 3.3. If we assume $\alpha\alpha^\sigma \in 3C_n W_n$, then we have

$$N_{\mathbb{Q}(\alpha_n)/\mathbb{Q}}(\alpha\alpha^\sigma) \equiv \pm(1 + 2^{n+2}) \pmod{2^{n+3}} \tag{5}$$

by Lemma 3.4, which contradicts (4). Hence we have $\alpha\alpha^\sigma \in C_n W_n$. Since any element of W_n is a square in $\Omega_{\mathfrak{l}_n}^\times$ (cf. [23, Exercises 9.3]), there exists an element c of C_n such that both $\varepsilon c = \alpha\alpha^\sigma c/\alpha^2$ and $\varepsilon^\sigma c = \alpha\alpha^\sigma c/(\alpha^\sigma)^2$ are squares in $\Omega_{\mathfrak{l}_n}^\times$.

Now, we assume $s - 2 > n$. If $\alpha\alpha^\sigma \in 3C_n W_n$, then (5) again holds, which contradicts $p \equiv 1 \pmod{2^s}$. Hence $\alpha\alpha^\sigma \in C_n W_n$ and a similar argument leads to the conclusion. □

Let E_n^2 be the set of squares of units in k_n and let $c_1, c_2, \ldots, c_{2^n-1}$ be fundamental units of $\mathbb{Q}(\alpha_n)$. Since $\mathfrak{p}_1\Omega_{k_n}, \mathfrak{p}_2\Omega_{k_n}, \ldots, \mathfrak{p}_{2^{s-2}}\Omega_{k_n}$ are ramified in k_n over $\mathbb{Q}(\alpha_n)$, elements $c_1E_n^2, c_2E_n^2, \ldots, c_{2^n-1}E_n^2$ of E_n/E_n^2 are independent over $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Hence there exist units $\eta_1, \ldots, \eta_{2^n}$ in E_n such that elements $\eta_1 C_n E_n^2, \ldots, \eta_{2^n} C_n E_n^2$ of $E_n/C_nE_n^2$ are independent over $\mathbb{F}_2$. Then we can prove the following:

Theorem 3.7. *Let m be a rational nonnegative integer with $m \leq 2^{s-2} - 2$ and $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_m$ unit in k_n such that $\varepsilon_1 C_n E_n^2, \varepsilon_2 C_n E_n^2, \ldots, \varepsilon_m C_n E_n^2$ are independent over $\mathbb{F}_2$ in $E_n/C_nE_n^2$. If $N_{k_n/\mathbb{Q}(\alpha_n)}(\varepsilon_i) = 1$ and if $N_{k_n/k_0}(\varepsilon_i) = \pm 1$ for $1 \leq i \leq m$, then $\lambda_k \leq 2^{s-2} - m - 2$.*

Proof. If $\mathfrak{p}_1^t$ is principal in k_n, then $\lambda_k = 0$ by (4) of Lemma 3.1. So we assume $\mathfrak{p}_1^t$ is not principal in k_n. We identify $k_{n,\mathfrak{l}_n}$ with $\mathbb{Q}_2(\alpha_n)$. Since $\varepsilon_i \in V_n$ and since $N_{\mathbb{Q}_2(\alpha_n)/\mathbb{Q}_2}(\varepsilon_i) = N_{k_n/k_0}(\varepsilon_i) = \pm 1$, we have $\varepsilon_i \in \overline{C}_n$ by class field theory. Since there exists an element c_i' in C_n with $\varepsilon_i c_i' \in V_n^2$ by Lemma 3.6 and since $V_n/\overline{C}_n \simeq \mathbb{Z}_2$, there exists an element $c_i'' \in \overline{C}_n$ with $\varepsilon_i c_i' = (c_i'')^2$. Hence we have $(\varepsilon_i c_i', \varepsilon_i^\sigma c_i') = ((c_i'')^2, (c_i''/\varepsilon_i)^2)$. Since $(c_i'', c_i''/\varepsilon_i) \equiv (1, 1/\varepsilon_i) \pmod{\overline{\varphi(E_n)}}$, $(c_i'', c_i''/\varepsilon_i)\overline{\varphi(E_n)}$ is an element of the inertia group of $\mathfrak{l}_n^\sigma$ in $G(M_n/k_\infty)$ whose order is two. Hence the 2-rank of the torsion part of $I_\infty G(M_\infty/M_n)/G(M_\infty/M_n)$ is greater than $m+1$ because $(1, -1) \notin \overline{\varphi(E_n)}$ by Lemma 3.2. This shows our assertion by Lemma 3.1. $\square$

After these preparations, we can now conclude our proof of Theorem 1.2.

(1) We assume $a \equiv 1 \pmod p$, which implies $a^2 - 2pb^2 = 1$. We note that the greatest common divisor of $a+1$ and $a-1$ is 2. We put $\varepsilon_1 = \frac{\sqrt{a+1}}{2}\sqrt{2} + \frac{b}{\sqrt{a+1}}\sqrt{p}$. Then we have $\varepsilon_1^2 = \varepsilon_0'$. If $a \equiv 1 \pmod 4$, then

$$\frac{a+1}{2}\frac{a-1}{4p} = \left(\frac{b}{2}\right)^2$$

implies $\varepsilon_1 \in \mathbb{Q}(\sqrt{2p})$, which is a contradiction. Hence we have $a \equiv -1 \pmod 4$. Then $\sqrt{a+1}/2$ and $b/\sqrt{a+1}$ are rational integers, which imply that ε_0, ε_1 and $1+\sqrt{2}$ are fundamental units in $\mathbb{Q}(\sqrt{p}, \sqrt{2})$ by [16]. Since $N_{k_1/\mathbb{Q}(\alpha_1)}(\varepsilon_1) = 1$ and $N_{k_1/k}(\varepsilon_1) = -1$, we have $\lambda_k \leq 2^{s-2} - 3$ by Theorem 3.7.

(2) We assume $a^2 \equiv -1 \pmod p$, which implies $a^2 - 2pb^2 = -1$. Let h_k be the class number of k. We note that h_k is odd. Hence the order of the ideal class containing $(\mathfrak{l}_1 \cap \mathbb{Q}(\sqrt{2p}))^{h_k}$ is two in the ideal class group of $\mathbb{Q}(\sqrt{2p})$ by the genus formula. This shows that $\mathrm{cl}(\mathfrak{l}_n^{h_k})$ is nontrivial in the 2-Sylow subgroup A_n of the ideal class group of k_n. Since $\varepsilon_0^2 \not\equiv 1 \pmod{32}$, the order of

$$B_n = \{\, a \in A_n \mid a^\tau = a \text{ for any element } \tau \in G(k_n/k) \,\}$$

is less than or equal to 2. Hence we have $B_n = \langle\, \mathrm{cl}(\mathfrak{l}_n^{h_k}) \,\rangle$. This shows $\lambda_k = 0$ by [7].

4. Examples

It is important to see how large an m we can choose in Theorem 3.7 for a number of numerical examples in order to deepen our understanding of Greenberg conjecture. So we examine the largest m in Theorem 3.7. We calculated certain subgroups of

$$E_n/C_nE_n^2 \qquad (6)$$

for $1 \leq n \leq 7$. Since the degree $[k_7 : \mathbb{Q}] = 256$ is large, special techniques are required for the calculations. In this section we explain our particular algorithms.

4.1. **Integral basis.** The first task is a construction of an integral basis of k_n. It is well known that powers of α_n form an integral basis of $\mathbb{Q}(\alpha_n)$. Since the discriminant of k is prime to that of $\mathbb{Q}(\alpha_n)$, an integral basis of k_n is easily constructed by [17, Propositon 17 in Chapter III].

4.2. **Unit group.** The next task is a construction of unit groups C_n and E_n. Since the group $E_n/C_nE_n^2$ in Theorem 3.7 has 2-power order, subgroups of C_n and E_n with odd indices are enough for our purpose. Since the methods for C_n and E_n are the same, we restrict our interest to E_n.

Let $r = 2^{n+1} - 1$. We use a cyclotomic unit $1 + \alpha_n$ of $\mathbb{Q}(\alpha_n)$, a cyclotomic unit

$$\xi = N_{\mathbb{Q}(\zeta_f)/k_n}(\zeta_f - 1)$$

of k_n and the fundamental unit ε_0 of k, where $f = 2^{n+2}p$ is the conductor of k_n. We denote by γ the element of $G(k_n/k)$ such that $\alpha_n^\gamma = 2\cos(10\pi/2^{n+2})$ and start with $E_n' = \langle -1, \theta_0, \theta_1, \ldots, \theta_{r-1}\rangle$, where

$$\theta_i = \begin{cases} (1+\alpha_n)^{\gamma^i} & 0 \leq i \leq 2^n - 2, \\ \xi^{\gamma^{i-2^n+1}} & 2^n - 1 \leq i \leq r-2, \\ \varepsilon_0 & i = r-1. \end{cases}$$

According to an idea of Zassenhaus [21, p. 66], we examine whether the index $(E_n : E_n')$ is odd and enlarge E_n' if $(E_n : E_n')$ is even as follows. First we check whether $\sqrt{\theta_0}$ is contained in k_n using the method in 4.3. If $\sqrt{\theta_0} \in k_n$, we replace θ_0 by $\sqrt{\theta_0}$. So we may assume that $\sqrt{\theta_0} \notin k_n$. Next we find a prime number ℓ which splits completely in $k_n/\mathbb{Q}$ and satisfies

$$\theta_0^{\frac{\ell-1}{2}} \not\equiv 1 \pmod{\mathcal{L}},$$

where $\mathcal{L}$ is a prime ideal of k_n lying over ℓ (we fix arbitrary 1). For $1 \leq i \leq r-1$, we set

$$a_i = \begin{cases} 0 & \text{if } \theta_i^{\frac{\ell-1}{2}} \equiv 1 \pmod{\mathcal{L}}, \\ 1 & \text{if } \theta_i^{\frac{\ell-1}{2}} \not\equiv 1 \pmod{\mathcal{L}}, \end{cases}$$

and put $\eta_0 = \theta_0$, $\eta_i = \theta_i\theta_0^{a_i}$ $(1 \leq i \leq r-1)$. Then $E_n' = \langle -1, \eta_0, \eta_1, \ldots, \eta_{r-1}\rangle$ and

$$\sqrt{\eta_0^{e_0}\eta_1^{e_1}\cdots\eta_{r-1}^{e_{r-1}}} \in k_n \quad (0 \leq e_i \leq 1)$$

implies $e_0 = 0$. Hence we can reduce the number of trials finding a square from 2^r to 2^{r-1}. Repeating this procedure, we can enlarge E_n' within r trials.

Finally, we obtain a subgroup $E_{n,0} = \langle -1, \eta_0, \eta_1, \ldots, \eta_{r-1}\rangle$ of E_n with odd index $(E_n : E_{n,0})$. Since $N_{k_n/k}(\xi) = 1$ (note that 2 splits in $k/\mathbb{Q}$), the above algorithm automatically leads to $N_{k_n/k}(\eta_i) = \pm 1$ for $0 \leq i \leq r-2$.

4.3. **Square root.** Let $r = 2^{n+1} - 1$ and $\{v_0, v_1, \ldots, v_r\}$ be an integral basis of k_n. When an integer β of k_n is square in k_n, we wish to obtain $\sqrt{\beta}$. Namely, we want to determine $x_j \in \mathbb{Z}$ such that $(\sum_j x_jv_j)^2 = \beta$. It is difficult to solve the system of simultaneous equations

$$\sum_j x_jv_j^\sigma = \sqrt{\beta}^\sigma \quad (\sigma \in G(k_n/\mathbb{Q})) \tag{7}$$

approximately for large n (e.g. $n \geq 4$) because of the ambiguity of the sign of $\sqrt{\beta}^{\sigma}$ ($\sqrt{\beta}^{\sigma} = \sqrt{\beta^{\sigma}}$ or $\sqrt{\beta}^{\sigma} = -\sqrt{\beta^{\sigma}}$). There is another method of Fincke and Pohst [3], [20, p. 33] based on the algorithm for finding small vectors in a lattice. But it does not fit our purpose even for small n because the coefficient of the quadratic form $\sum_{\sigma \in G(k_n/\mathbb{Q})} |\beta^{\sigma}|^{-1} |\sum_{j=0}^{2^{n+1}-1} x_j v_j^{\sigma}|^2$ are very small for our targets. So we proceed as follows:

(1) Prepare prime numbers $\ell_0, \ell_1, ..., \ell_N$ which split completely in $k_n/\mathbb{Q}$.
(2) Let β be a totally positive integer of k_n. If β is not square in k_n modulo some ℓ_i, then $\sqrt{\beta} \notin k_n$. Otherwise we search $x_j \in \mathbb{Z}$ such that $(\sum_j x_j v_j)^2 = \beta$.
(3) Calculate the minimal polynomial $f(X)$ of β over $\mathbb{Q}$.
(4) Factorize $f(X^2)$ over $\mathbb{Z}$. We assume that $f(X^2)$ splits into $g_1(X)g_2(X)$.
(5) Determine $\sqrt{\beta}^{\sigma} = \pm\sqrt{\beta^{\sigma}} \bmod \ell_i$ $(\sigma \in G(k_n/\mathbb{Q}))$ using $g_1(X)$. Namely, we choose $\sqrt{\beta}^{\sigma} \bmod \ell_i$ so that $g_1(\sqrt{\beta}^{\sigma}) \equiv 0 \pmod{\ell_i}$ and $g_1(-\sqrt{\beta}^{\sigma}) \not\equiv 0 \pmod{\ell_i}$. If $g_1(\pm\sqrt{\beta^{\sigma}}) \equiv 0 \pmod{\ell_i}$, then we skip this ℓ_i.
(6) Solving the simultaneous equations (7) modulo ℓ_i, construct $\beta_i = \sum_j x_{ij} v_j$ $(x_{ij} \in \mathbb{Z})$ such that $\beta_i^2 \equiv \beta \pmod{\ell_0 \ell_1 \cdots \ell_i}$ and $2|x_{ij}| < \ell_0 \ell_1 \cdots \ell_i$.
(7) Find i such that $\beta_i = \beta_{i+1}$.
(8) Compare β_i^2 with β. If $\beta_i^2 = \beta$, then $\sqrt{\beta}$ is found.

In many cases, $f(X^2)$ splits into two factors and we can eliminate the ambiguity of $\sqrt{\beta^{\sigma}} \bmod \ell_j$ using a factor of $f(X)$. If $f(X^2)$ remains irreducible (i.e. $\deg f \leq 2^n$), we get $\sqrt{\beta\delta^2}$ for an appropriate $\delta \in k_n$ and set $\sqrt{\beta} = \sqrt{\beta\delta^2}/\delta$.

We make two technical remarks. For small n, we can determine the sign of $\sqrt{\beta}^{\sigma}$ so that $g_1(\sqrt{\beta}^{\sigma}) = 0$ and get $\sqrt{\beta}$ directly solving the equations (7) approximately. If n is large, then coefficients of $g_1(X)$ are large and the calculation becomes slow because of high precision. For example, we need an accuracy of more than 10^5 digits for $n = 7$. So we switch approximate calculations to congruence calculations.

Our next remark is related to congruence solutions of equations (7). Let $\alpha = \alpha_n + \omega$, where $\omega = (1 + \sqrt{p})/2$. Then $k_n = \mathbb{Q}(\alpha)$. We prepare the $(r+1) \times (r+1)$ integer matrix B such that

$$(1\ \alpha\ \alpha^2 \cdots \alpha^r) = (v_0\ v_1 \cdots v_r)B.$$

If $\beta = \sum_j b_j v_j$ with $b_j \in \mathbb{Z}$, then

$$\begin{aligned} \beta^{\sigma} \bmod \ell_i &\equiv (v_0^{\sigma}\ v_1^{\sigma} \cdots v_r^{\sigma})\, {}^t(b_0\ b_1 \cdots b_r) \\ &\equiv (1\ \alpha^{\sigma}\ \alpha^{2\sigma} \cdots \alpha^{r\sigma}) B^{-1}\, {}^t(b_0\ b_1 \cdots b_r) \pmod{\ell_i}. \end{aligned} \tag{8}$$

Since the entries of B are very large for large n, the calculation of B^{-1} takes a long time. So we solve a system of linear equations each time modulo each ℓ_i.

We get $\beta^{\sigma} \bmod \ell_i$ by (8) and choose $\sqrt{\beta}^{\sigma} \bmod \ell_i$ using $g_1(X)$. Then we get $\sqrt{\beta} \bmod \ell_i = \sum_j x_j \alpha^j \bmod \ell_i$ by solving a system of linear equations

$$\sum_j x_j \alpha^{j\sigma} \equiv \sqrt{\beta}^{\sigma} \pmod{\ell_i} \quad (\sigma \in G(k_n/\mathbb{Q}))$$

and get $\sqrt{\beta} \bmod \ell_i = \sum_j y_j v_j \bmod \ell_i$ by

$$(y_0\ y_1 \cdots y_r) = (x_0\ x_1 \cdots x_r)\, {}^t B.$$

The remainder is a straightforward application of the Chinese Remainder Theorem.

4.4. **Minimal polynomial.** If the degree $[k_n : \mathbb{Q}] = 2^{n+1}$ is not too large (e.g. $n \le 5$), then the approximate calculation of

$$f(X) = \prod_{\sigma \in G(k_n/\mathbb{Q})} (X - \beta^\sigma) \tag{9}$$

works well. But the size of coefficients of $f(X)$ grows rapidly (e.g. 10^4 digits for $n = 7$), and the high accuracy of approximation makes calculations slow. This phenomenon is caused by a property of β being a product of units in k_n.

So we calculate $f(X)$ modulo each ℓ_i and construct $f_i(X) \in \mathbb{Z}[X]$ such that $f_i(X) \equiv f(X) \pmod{\ell_0\ell_1 \cdots \ell_i}$ and all the absolute values of coefficients of $f_i(X)$ are less than $\ell_0\ell_1 \cdots \ell_i/2$. If $f_i(X) = f_{i+1}(X)$, then $f_i(X)$ is very likely to be $f(X)$. Of course it is not guaranteed that $f_i(X) = f(X)$; but we do not need to worry whether $f_i(X) = f(X)$ if we find $\sqrt{\beta}$ using $f_i(X)$.

In general, $f(X)$ is not always irreducible. If $f(X)$ is square-free, then $f(X)$ is the minimal polynomial of β. When $f(X)$ is not square-free, $f(X) = g(X)^m$ with irreducible $g(X) \in \mathbb{Z}[X]$ and $m \ge 2$. Then $g(X)$ is the minimal polynomial of β.

4.5. **$\alpha \bmod \ell_i$.** The minimal polynomial $f_\alpha(X) \in \mathbb{Z}[X]$ of $\alpha = \alpha_n + \omega$ over $\mathbb{Q}$ is easily obtained by an approximate calculation similar to (9). A rational prime ℓ splits completely in k_n if $\ell \equiv 1 \pmod{2^{n+2}}$ and $(p/\ell) = 1$. We build a finite set $L = \{\ell_0, \ell_1, \dots, \ell_N\}$ consisting of an appropriate number of such ℓ satisfying $\det B \not\equiv 0 \pmod{\ell}$ and $f_\alpha(\ell) \not\equiv 0 \pmod{\ell}$.

Let $\ell_i \in L$ and g_i be a primitive root of ℓ_i. If z_1 is a rational integer satisfying $z_1 \equiv g_i^{(\ell-1)/2^{n+2}} \pmod{\ell_i}$, then $2\cos(2\pi/2^{n+2}) \equiv z_1 + z_1^{-1} \pmod{\mathcal{L}_1}$ for some prime ideal $\mathcal{L}_1$ of $\mathbb{Q}(\alpha_n)$ lying above ℓ_i. We also find $z_2 \in \mathbb{Z}$ such that $z_2 \equiv \omega \pmod{\mathcal{L}_2}$ for some prime ideal $\mathcal{L}_2$ of k lying above ℓ_i by solving $x^2 \equiv p \pmod{\ell_i}$. Then $\alpha \equiv z_1 + z_2 \pmod{\mathcal{L}}$ for some prime ideal $\mathcal{L}$ of k_n lying above ℓ_i. We abbreviate this congruence as $\alpha \equiv z_1 + z_2 \pmod{\ell_i}$.

We prepare a table of $\alpha^\sigma \bmod \ell_i$ ($\sigma \in G(k_n/\mathbb{Q})$, $0 \le i \le N$) and a table of $v_j \bmod \ell_i$ ($0 \le i \le N$, $0 \le j \le 2^{n+1} - 1$) in order to verify quickly that a given $\beta = \sum_j x_j v_j$ is not square in k_n. But we do not prepare a table of $v_j^\sigma \bmod \ell_i$ ($\sigma \in G(k_n/\mathbb{Q})$, $0 \le i \le N$, $0 \le j \le 2^{n+1} - 1$) because it requires 256 times the amount of memory as for $n = 7$.

4.6. **Subgroup calculation.** It is enough to construct the subgroup

$$E_{n,1} = \{\, \varepsilon \in E_n \mid N_{k_n/\mathbb{Q}(\alpha_n)}(\varepsilon) = 1,\ N_{k_n/k}(\varepsilon) = \pm 1 \,\}$$

of E_n in order to see how many independent units there are in Theorem 3.7.

We may assume that we find positive $\eta_i \in E_n$ such that

$$\begin{aligned} C_n &= \langle -1, \eta_0, \eta_1, \dots, \eta_{2^n-2} \rangle, \\ E_n &= \langle -1, \eta_0, \eta_1, \dots, \eta_{2^n-2}, \eta_{2^n-1}, \eta_{2^n}, \dots, \eta_{2^{n+1}-2} \rangle \end{aligned}$$

with properties

$$\begin{aligned} N_{k_n/k}(\eta_i) &= \pm 1 \quad (0 \le i \le 2^{n+1} - 3), \\ N_{k_n/k}(\eta_{2^{n+1}-2}) &\ne \pm 1 \,. \end{aligned}$$

First we find $\eta \in E_n$ which satisfies $N_{k_n/\mathbb{Q}(\alpha_n)}(\eta) = -1$ and $N_{k_n/k}(\eta) = \pm 1$.

Let $t = 2^n - 1$, $u = 2^{n+1} - 2$ and let

$$N_{k_n/\mathbb{Q}(\alpha_n)}(\eta_j) = \pm \prod_{i=0}^{t-1} \eta_i^{a_{ij}} \quad (0 \le j \le u-1)$$

with $a_{ij} \in \mathbb{Z}$. Then, the norm of

$$\prod_{j=0}^{u-1} \eta_j^{x_j} \quad (x_j \in \mathbb{Z})$$

from k_n to $\mathbb{Q}(\alpha_n)$ is equal to ± 1 if and only if $x = {}^t(x_0, x_1, \ldots, x_{u-1})$ is contained in the kernel of the linear map $\psi : \mathbb{Z}^u \ni x \mapsto Ax \in \mathbb{Z}^t$, where $A = (a_{ij})$. Let v be the dimension of $\operatorname{Ker}\psi$ and $\{\omega_0, \omega_1, \ldots, \omega_{v-1}\}$ a $\mathbb{Z}$-basis of $\operatorname{Ker}\psi$. Then the above η exists if and only if $\prod_i N_{k_n/\mathbb{Q}(\alpha_n)}(\eta_i)^{x_{ij}} < 0$ for some $\omega_j = {}^t(x_{0j}, x_{1j}, \ldots, x_{u-1,j})$. In this manner we find $\eta \in E_n$. Now, for $0 \le j \le v-1$, set e_j to be 1 or 0 according to $\prod_i N_{k_n/\mathbb{Q}(\alpha_n)}(\eta_i)^{x_{ij}} < 0$ or not. Then

$$E_{n,1} = \langle -1, \eta^{e_j} \prod_{i=0}^{u-1} \eta_i^{x_{ij}} \mid 0 \le j \le v-1 \rangle.$$

The index $(E_n : E_{n,1}C_nE_n^2)$ is easily calculated using the Hermite normal form of the integer matrix. Since $(E_n : C_nE_n^2) = 2^{2^n}$, if $(E_n : E_{n,1}C_nE_n^2) = 2^d$, then there are $2^n - d$ independent units in Theorem 3.7.

4.7. **Tables.** We calculated $E_{n,1}$ $(2 \le n \le 7)$ for $k = \mathbb{Q}(\sqrt{p})$, where p is a prime number less than 10^4 which satisfies $p \equiv 1 \pmod{2^4}$ and $2^{\frac{p-1}{4}} \equiv 1 \pmod{p}$. We denote by m_n the maximal number of independent units in Theorem 3.7. Namely, $m_n = 2^n - d$, where $(E_n : E_{n,1}C_nE_n^2) = 2^d$. Let 2^s be the highest power of 2 dividing $p-1$. Once m_n has attained $2^{s-2} - 2$ for some n, then we do not need to calculate m_k for $k \ge n+1$. Our calculation summarized in the following tables, together with Theorem 1.1, shows that $\lambda_2(\mathbb{Q}(\sqrt{p})) = 0$ for all prime numbers p less than 10^4.

For $k = \mathbb{Q}(\sqrt{4481})$, which is the most difficult example, our algorithms with Pentium 4 2.0 GHz handled k_5 in 4 minutes, k_6 in 45 minutes and k_7 in 11 hours.

$2^4 \,||\, p-1$

p	m_2	m_3	p	m_2	m_3	p	m_2	m_3	p	m_2	m_3	m_4
113	2		3089	2		4721	2		7793	2		
337	1	2	3121	2		4817	2		8081	2		
593	1	2	3217	1	2	5233	1	2	8209	2		
881	1	2	3313	2		5297	2		8273	2		
1201	2		3761	2		5393	1	2	8369	2		
1553	2		4049	1	2	6353	2		9137	1	2	
1777	2		4177	2		6449	2		9521	1	1	2
2129	1	2	4273	0	2	6481	2		9649	2		
2833	2		4657	1	2	7121	1	2				

$2^5 \,||\, p-1$

p	m_3	m_4	m_5	p	m_3	m_4	m_5	m_6	p	m_3	m_4
353	6			3361	5	5	5	6	8161	4	6
1249	5	6		4001	5	6			8609	5	6
1889	3	3	6	4513	6				9377	4	6
2273	6			6689	5	6			9697	5	6
2593	6			7393	6						
2657	6			7841	4	6					

$2^6 \,||\, p-1$

p	m_4	m_5	p	m_4	m_5	p	m_4	p	m_4	p	m_4
577	13	14	1601	14		3137	14	4801	14	7489	14
1217	14		2113	13	14	4289	14	5569	14	9281	14

$2^7 \,||\, p-1$

p	m_5	m_6	p	m_5	m_6	m_7	p	m_5	m_6
1153	30		4481	29	29	30	6529	30	
2689	29	30	4993	30			9601	28	30

$2^8 \,||\, p-1$

p	m_6	m_7
257	62	
9473	61	62

References

[1] A. Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124. MR0220694 (36:3746)

[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. MR528968 (81a:12005)

[3] U. Fincke and M. Pohst, *Improved methods for calculating vectors of short length in a lattice, including a complexity analysis*, Math. Comp. **44** (1985), 463–471. MR777278 (86e:11050)

[4] T. Fukuda and K. Komatsu, *On $\mathbb{Z}_p$-extensions of real quadratic fields*, J. Math. Soc. Japan **38** (1986), 95–102. MR816225 (87d:11081)

[5] T. Fukuda and K. Komatsu, *On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of a real quadratic field*, Tokyo J. Math. **28** (2005), 259–264. MR2149635 (2006b:11134)

[6] T. Fukuda, K. Komatsu, M. Ozaki and H. Taya, *On Iwasawa λ_p-invariants of relative real cyclic extensions of degree p*, Tokyo J. Math. **20** (1997), no. 2, 475–480. MR1489480 (98k:11153)

[7] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284. MR0401702 (53:5529)

[8] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math. **47** (1978), no. 1, 85–99. MR504453 (80b:12007)

[9] H. Ichimura and H. Sumida, *On the Iwasawa invariants of certain real abelian fields II*, Inter. J. Math. **7** (1996), 721–744. MR1417782 (98e:11128c)

[10] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226. MR0124316 (23:A1630)

[11] K. Iwasawa, *On the μ-invariants of $\mathbb{Z}_\ell$-extensions*, Number Theory, Algebraic Geometry and Commutative Algebra (in honor of Y. Akizuki), Kinokuniya, Tokyo (1973), 1–11. MR0357371 (50:9839)

[12] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326. MR0349627 (50:2120)

[13] K. Iwasawa, *Riemann-Hurwitz formula and p-adic Galois representations for number fields*, Tohoku Math. J. **33** (1981), no. 2, 263–288. MR624610 (83b:12003)

[14] Y. Kida, *Cyclotomic $\mathbb{Z}_2$-extensions of J-fields*, J. Number Theory **14** (1982), no. 3, 340–352. MR660379 (84b:12010)

[15] J. Kraft and R. Schoof, *Computing Iwasawa modules of real quadratic number fields*, Compositio Math. **97** (1995), 135–155. MR1355121 (97b:11129)

[16] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. **10** (1956), 65–85. MR0083009 (18:643e)

[17] S. Lang, Algebraic Number Theory. Second edition. Graduate Texts in Mathematics, 1103. Springer-Verlag, New York, 1994. MR1282723 (95f:11085)

[18] Y. Mizusawa, *On the Iwasawa invariants of $\mathbb{Z}_2$-extensions of certain real quadratic fields*, Tokyo J. Math. **27** (2004), 255–261. MR2060089 (2005e:11140)

[19] 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. MR1484637 (99a:11122)

[20] M. E. Pohst, *Computational Algebraic Number Theory*, DMV Seminar 21, Birkhäuser, Basel, 1993. MR1243639 (94j:11132)

[21] M. E. Pohst, *Computing invariants of algebraic number fields*, in Group Theory, Algebra, and Number Theory, Ed. by H. G. Zimmer, de Gruyter, 1996, 53–73. MR1440204 (98d:11162)

[22] T. Tsuji, *On the Iwasawa λ-invariants of real abelian fields*, Trans. Amer. Math. Soc. **355** (2003), 3699–3714. MR1990169 (2004e:11122)

[23] L. C. Washington, Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997. MR1421575 (97h:11130)

[24] A. Weil, Basic number theory. Third edition. Die Grundlehren der Mathematischen Wissenschaften, Band 144. Springer-Verlag, New York-Berlin, 1974. MR0427267 (55:302)

[25] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. **131** (1990), no. 3, 493–540. MR1053488 (91i:11163)

Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan

E-mail address: `fukuda@math.cit.nihon-u.ac.jp`

Department of Mathematical Science, School of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan

E-mail address: `kkomatsu@waseda.jp`