ON THE IWASAWA $\lambda$-IN Variant 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 $\lambda$-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 $\lambda$ 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, $\ell$ a prime number and $\zeta_{\ell^n}$ a primitive $\ell^n$-th root of unity. There exists the unique intermediate field $k_\infty$ 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 $\ell$-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 $k_\infty/k$ with degree $\ell^n$ 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 $k_\infty/k$, which were introduced by Iwasawa [10] and [12]. Namely, if $\ell^n$ denotes the $\ell$-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 $\ell$. Furthermore, Greenberg [7] suggests the possibility that $\lambda_\ell(k)$ is zero for any totally real number field $k$ and any prime number $\ell$, 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 $\ell$, 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 $\ell$ and any abelian number field $k$ with degree prime to $\ell$ 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 $\ell$ 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.

©2009 American Mathematical Society
Reverts to public domain 28 years from publication

1797
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 $\ell$. In fact, he proved that $\mu_\ell(k) = 0$ for such a $k$. It is then considered a fundamental step to study $\lambda_\ell(k)$ 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 $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

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 [9].

**Theorem 1.2.** Let $p$ be any prime number with $p \equiv 1 \pmod{16}$, $\varepsilon_0$ the fundamental unit of $\mathbb{Q}(\sqrt{p})$, and $\varepsilon'_0 = a + b\sqrt{p}$ 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 $\lambda$-invariant $\lambda_2(\mathbb{Q}^{(\sqrt{p})})$:

1. If $a \equiv 1 \pmod{p}$, then $\lambda_2(\mathbb{Q}^{(\sqrt{p})}) \leq 2^{s-2} - 3$.
2. If $a^2 \equiv -1 \pmod{p}$ and if $\varepsilon'_0 \equiv 1 \pmod{32}$, then $\lambda_2(\mathbb{Q}^{(\sqrt{p})}) = 0$.

**Remark 1.1.** Since $\varepsilon'_0$ 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 [11] 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 $g_1, g_2, \ldots, g_r$ of a group $G$, we denote by $\langle g_1, g_2, \ldots, g_r \rangle$ the subgroup of $G$ generated by $g_1, g_2, \ldots, g_r$. 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 $\Omega_k$ and $E_k$ the integer ring of $k$ and the unit group of $k$, respectively. For an element $\alpha$ of $\Omega_k$, we denote by $\alpha\Omega_k$ the principal ideal of $\Omega_k$ generated by $\alpha$. We denote by $\zeta_{2^n}$ a primitive $2^n$-th root of unity in the complex number field $\mathbb{C}$. Let $\ell$ be a prime number and
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 \( k_\infty \) 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 \( M_\infty = \bigcap_{n=0}^{\infty} M_n \) and \( L_\infty = \bigcup_{n=0}^{\infty} L_n \) are the maximal abelian 2-extension of \( k_\infty \) unramified outside 2 and the maximal abelian unramified 2-extension of \( k_\infty \), 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 \( \gamma \) of \( G(k_\infty/k) \). Then we have the following exact sequence of \( \Lambda \)-modules:

\[
1 \longrightarrow I_\infty \longrightarrow \mathfrak{x}_\infty \longrightarrow X_\infty \longrightarrow 1.
\]

Since \( \mu_2(k(\sqrt{-1})) \) is zero by \( 2 \) and since \( \mathfrak{x}_\infty \) has no finite \( \Lambda \)-submodule by Theorem 1 of [3], \( \mathfrak{x}_\infty \) 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 \( I_\infty \), \( \mathfrak{x}_\infty \), and \( X_\infty \), respectively. Then we have

\[
\lambda(\mathfrak{x}_\infty) = \lambda(X_\infty) + \lambda(I_\infty)
\]

by \( 1 \). Hereafter, we denote by \( \lambda_k \) the Iwasawa invariant \( \lambda_2(k) \) of the cyclotomic \( \mathbb{Z}_2 \)-extension of \( k_\infty/k \). By definition of \( \lambda_k \), 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 \( 14 \) and \( 25 \). If \( s \leq 3 \), then \( \lambda_k = 0 \) by Theorem \( 1 \). So we assume \( s \geq 4 \). Now, there exist distinct prime ideals \( p_1, p_2, \ldots, p_{2-s} \) in \( k_{s-2} \) with \( \sqrt{p} \Omega_{k_{s-2}} = p_1 p_2 \cdots p_{2-s} \) and the ideal \( p_i \Omega_{k_{s-2}} \) generated by \( p_i \) in \( \Omega_{k_{s-2}} \) is a prime ideal of \( k_{s-2} \) 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 \( p_i^{2t} \) is a principal ideal of \( k_{s-2} \) for \( 1 \leq i \leq 2^{s-2} \). We denote by \( \text{cl}(p_i^{2t} \Omega_{k_{s-2}}) \) the ideal class of \( k_{s-2} \) containing the ideal \( p_i^{2t} \Omega_{k_{s-2}} \) and by \( \rho_n \) the 2-rank of a subgroup \( \langle \text{cl}(p_1^{2t} \Omega_{k_{s-2}}), \text{cl}(p_2^{2t} \Omega_{k_{s-2}}), \ldots, \text{cl}(p_{2-s}^{2t} \Omega_{k_{s-2}}) \rangle \) in the ideal class group of \( k_{s-2} \). The 2-rank of the ideal class group of \( k_{s-2} \) is stable for sufficiently large \( n \) because of \( \mu_2(k) = 0 \) and \( \rho_n \) 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 \( \sigma \) be a generator of \( G(k_\infty/k_\infty) \) and \( t_n \) a prime ideal of \( k_n \) lying above 2. Then we have \( t_n \mathfrak{c}_n = \alpha_n \Omega_{k_n} \) \((n \geq 1)\), \( (t_n \mathfrak{c}_n)^{2^n} = 2\Omega_{k_n} \) and \( t_n \neq \mathfrak{c}_n \). We denote by \( E_n \) the unit group \( E_{k_n} \) of \( \Omega_{k_n} \) for simplicity. Let \( k_n t_n \) be the completion of \( k_n \) at
Lemma 3.2. The element \( (1, -1) \) of \( U_n \) does not belong to \( \overline{\varphi(E_n)} \).

Proof. Let \( \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2^n-1} \) be fundamental units of \( k_n \). We assume \( (1, -1) \in \varphi(E_n) \). Then there exist 2-adic integers \( x_1, x_2, \ldots, x_{2^n-1} \) with
\[
(1, -1) = \pm (\varepsilon_1, \varepsilon_1^2)(\varepsilon_2, \varepsilon_2^2) \cdots (\varepsilon_{2^n-1}, \varepsilon_{2^n-1}^2)^{2^{n+1}-1}.
\]
Hence we have
\[
\prod_{i=1}^{2^{n+1}-1} \varepsilon_i^{2x_i} = 1 \quad \text{and} \quad \prod_{i=1}^{2^{n+1}-1} (\varepsilon_i^{\sigma^j})^{2x_i} = 1.
\]
Let \( \gamma \) be a generator of \( G(k_{n+1}/Q_2) \), where \( Q_2 \) is the 2-adic number field. Then we have
\[
\prod_{i=1}^{2^{n+1}-1} (\varepsilon_i^{\gamma^j})^{2x_i} = 1 \quad \text{and} \quad \prod_{i=1}^{2^{n+1}-1} (\varepsilon_i^{\sigma^j})^{2x_i} = 1
\]
for \( 1 \leq j \leq 2^n \). This means
\[
\sum_{i=1}^{2^{n+1}-1} x_i \log_2(\varepsilon_i^{\gamma^j})^2 = 0 \quad \text{and} \quad \sum_{i=1}^{2^{n+1}-1} x_i \log_2(\varepsilon_i^{\sigma^j})^2 = 0,
\]
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 \( \boxed{\text{[1]}} \). This is a contradiction. \( \square \)

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

Let \( C_n \) be the unit group of \( Q(\alpha_n) \) and \( V_n \) the unit group of \( Q_2(\alpha_n) \). 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 \( V_n = (3)C_nW_n \).

Proof. Since the maximal 2-extension of \( Q \) unramified outside 2 is \( Q_\infty \), the maximal 2-extension of \( Q(\alpha_n) \) unramified outside 2 is also \( Q_\infty \). Hence we have \( G(Q_\infty/Q(\alpha_n)) \cong V_n/\overline{C_n} \), where \( \overline{C_n} \) is the topological closure of \( C_n \) in \( V_n \). Since \( V_n/\overline{C_n} \) is generated by \( 3C_n \) as a topological group and since \( W_n \) is an open subgroup of \( V_n \), we have \( V_n = (3)C_nW_n \). \( \square \)

Lemma 3.4. We have \( N_{Q_2(\alpha_n)/Q_2}(u) \equiv 1 \pmod{2^{n+3}} \) for any element \( u \) in \( W_n \).

Proof. Let \( v_n \) be the normalized additive \( \alpha_n \)-adic valuation of \( Q(\alpha_n) \) and \( \gamma \) a generator of \( G(Q(\alpha_n)/Q) \). At first, we prove
\[
v_n(\alpha_n^i - \alpha_n) \leq 2^n + 1 \quad \text{for} \quad 1 \leq i \leq 2^n - 1
\]
by induction on $n$. We have $v_n(\alpha_n^{2^n-1} - \alpha_n) = v_n(2\alpha_n) = 2^n + 1$. Hence we have $v_1(\alpha_1^2 - \alpha_1) = 2 + 1$. We assume $v_m(\alpha_m^2 - \alpha_m) \leq 2^m + 1$ for $m < n$ and $1 \leq i \leq 2^m - 1$. Since $\alpha_1^2 = \alpha_{n-1} + 2$, we have

$$v_n(\alpha_n^i - \alpha_n) + v_n(\alpha_n^i + \alpha_n) = v_n(\alpha_n^{2^i} - \alpha_n^2) = v_n(\alpha_{n-1} - \alpha_{n-1}) = 2v_n(\alpha_{n-1}^i - \alpha_{n-1}) \leq 2^n + 2$$

for $1 \leq i \leq 2^n - 1$ and $i \neq 2^{n-1}$. Hence we have $v_n(\alpha_n^i - \alpha_n) \leq 2^n + 1$ for $1 \leq i \leq 2^n - 1$ noting that $v_n(\alpha_n^i + \alpha_n) \geq 1$. 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 $\gamma$, 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 $\{\gamma^iv : 0 \leq i \leq 2^n - 1\}$ 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

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

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

Recall that $\varphi$ is the isomorphism of $E_n$ into $U_n$ defined by [4].

**Lemma 3.6.** If $n \geq s - 2$, we assume that $p^s \Omega_{k_n}$ is not principal in $k_n$. Then, for any unit $\varepsilon$ 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 $\alpha$ of $\Omega_{k_n}$ with $\varepsilon = \alpha^{s-1}$. First we assume $n \geq s - 2$. Since prime ideals $p_1 \Omega_{k_n}, p_2 \Omega_{k_n}, \ldots, p_{s-1} \Omega_{k_n}$ 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 $p_i \Omega_{k_n}$. Since each $p_i \Omega_{k_n}$ is conjugate to $p_1 \Omega_{k_n}$ over $k$ and not principal in $k_n$, Lemma 3.3 leads to a conclusion that $\alpha \Omega_{k_n}$ is a product of an even number of $p_i \Omega_{k_n}$. Hence we have

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

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

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

by Lemma 3.3, which contradicts [4]. Hence we have $\alpha \sigma \in C_n W_n$. Since any element of $W_n$ is a square in $\Omega_{k_n}^\vee$ (cf. [23] Exercies 9.3), there exists an element $c$ of $C_n$ such that both $\varepsilon c = \alpha \sigma c/\alpha^2$ and $\varepsilon^c = \alpha \sigma c/(\alpha^2)^2$ are squares in $\Omega_{k_n}^\vee$.

Now, we assume $s - 2 > n$. If $\alpha \sigma \in 3C_n W_n$, then (5) again holds, which contradicts $p \equiv 1 \pmod{2^n}$. Hence $\alpha \sigma \in C_n W_n$ and a similar argument leads to the conclusion. \qed
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 $Q(\alpha_n)$. Since $p_1\Omega_n, p_2\Omega_n, \ldots, p_{2^n-2}\Omega_n$ are ramified in $k_n$ over $Q(\alpha_n)$, 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 $F_2 = \mathbb{Z}/2\mathbb{Z}$. Hence there exists units $\eta_1, \ldots, \eta_{2^n}$ in $E_n$ such that elements $\eta_1C_nE_n^2, \ldots, \eta_{2^n}C_nE_n^2$ of $E_n/C_nE_n^2$ are independent over $F_2$. Then we can prove the following:

**Theorem 3.7.** Let $m$ be a rational nonnegative integer with $m \leq 2^{n-2} - 2$ and $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m$ unit in $k_n$ such that $\varepsilon_1C_nE_n^2, \varepsilon_2C_nE_n^2, \ldots, \varepsilon_mC_nE_n^2$ are independent over $F_2$ in $E_n/C_nE_n^2$. If $N_{k_n}/Q(\alpha_n)(\varepsilon_i) = 1$ and if $N_{k_n/k_0}(\varepsilon_i) = \pm 1$ for $1 \leq i \leq m$, then $\lambda_k \leq 2^{n-2} - m - 2$.

**Proof.** If $p_i^1$ is principal in $k_n$, then $\lambda_k = 0$ by (4) of Lemma 3.1. So we assume $p_i^1$ is not principal in $k_n$. We identify $k_{n_{i_{n}}}$ with $Q_2(\alpha_n)$. Since $\varepsilon_i \in V_n$ and since $N_{Q_2(\alpha_n)}/Q_2(\varepsilon_i) = N_{k_n/k_0}(\varepsilon_i) = \pm 1$, we have $\varepsilon_i \in C_n$ by class field theory. Since there exists an element $c_i^1$ in $C_n$ with $\varepsilon_i c_i^1 \in V_n$ by Lemma 3.6 and since $V_n/C_n \simeq \mathbb{Z}_2$, there exists an element $c_i^1 \in C_n$ with $\varepsilon_i c_i^1 = (c_i^1)^2$. Hence we have $\varepsilon_i c_i^1 \varepsilon_i c_i^1 = (c_i^1)^2$. Since $c_i^1 (c_i^1 \varepsilon_i) = 1$, we have $(c_i^1, c_i^1 \varepsilon_i) \equiv (1, 1) (\mod \varphi(E_n))$, $(c_i^1, c_i^1 \varepsilon_i) \equiv (c_i^1, c_i^1 \varepsilon_i) \varphi(E_n)$ is an element of the inertia group of $\varphi(E_n)$ 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 $(1, -1) \not\equiv \varphi(E_n)$ by Lemma 3.2. This shows our assertion by Lemma 3.1. \qed

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

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

$$a + 1 + a - 1 = \frac{4b^2}{2} \frac{a}{4p}$$

implies $\varepsilon_1 \in Q(\sqrt{2p})$, which is a contradiction. Hence we have $a \equiv -1 (\mod 4)$. Then $\sqrt{a+1}/2$ and $b/\sqrt{a+1}$ are rational integers, which imply that $\varepsilon_0, \varepsilon_1$ and $1 + \sqrt{2}$ are fundamental units in $Q(\sqrt{2}, \sqrt{2})$ by (10). Since $N_{k_1}/Q(\alpha_1)(\varepsilon_1) = 1$ and $N_{k_1/k_0}(\varepsilon_1) = -1$, we have $\lambda_k \leq 2^{n-2} - 3$ by Theorem 3.7.

(2) We assume $a^2 \equiv -1 (\mod p)$, 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 $(l_1 \cap Q(\sqrt{2p}))^{\text{ht}}$ is two in the ideal class group of $Q(\sqrt{2p})$ by the genus formula. This shows that $c_l(t_n^{h_k})$ is nontrivial in the 2-Sylow subgroup $A_n$ of the ideal class group of $k_n$. Since $h_k \not\equiv 1 (\mod 32)$, 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 $B_n = \langle c_l(t_n^{h_k}) \rangle$. 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

$$E_n/C_nE_n^2$$

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
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 $\alpha_n$ 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] Proposition 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 13 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 $\varepsilon_0$ of $k$, where $f = 2^{n+2}p$ is the conductor of $k_n$. We denote by $\gamma$ 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

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

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 [13]. If $\sqrt{\theta_0} \in k_n$, we replace $\theta_0$ by $\theta_0'$, where $\theta_0' = \theta_0$ if $\theta_0 \not\equiv \alpha_0$ (mod $\mathcal{L}$), and $\theta_0' = \theta_0$ otherwise. We may assume that $\sqrt{\theta_0} \not\in k_n$. Next we find a prime number $\ell$ which splits completely in $k_n/\mathbb{Q}$ and satisfies

$$
\theta_{0, \ell}^{\frac{\ell - 1}{2}} \not\equiv 1 \pmod{\mathcal{L}},
$$

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

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

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

$$
\sqrt{\eta_0^{\epsilon_0} \eta_1^{\epsilon_1} \cdots \eta_{r-1}^{\epsilon_{r-1}}} \in k_n \quad (0 \leq \epsilon_i \leq 1)
$$

implies $\epsilon_0 = 0$. 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 $N_{k_n/k}(\zeta_i) = 1$ (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 $\beta$ 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 $(\sum_j x_j v_j)\sigma = \beta$. It is difficult to solve the system of simultaneous equations

$$
\sum_j x_j v_j = \sqrt{\beta}^\sigma \quad (\sigma \in G(k_n/\mathbb{Q}))
$$

\text{License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use}
approximately for large $n$ (e.g. $n \geq 4$) because of the ambiguity of the sign of $\sqrt{\beta^\sigma}$ ($\sqrt{\beta^\sigma} = \sqrt{\beta^{2\sigma}}$ or $\sqrt{\beta^\sigma} = -\sqrt{\beta^{2\sigma}}$). There is another method of Fincke and Pohst \cite{FinckePohst1985}, \cite[p. 33]{FinckePohst1985} 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 $\sum_{\sigma \in G(k_n/\mathbb{Q})} |\beta^\sigma|^{-1} |\sum_{j=0}^{2n+1-1} x_j v_j^\sigma|^2$ 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 $\beta$ be a totally positive integer of $k_n$. If $\beta$ is not square in $k_n$ modulo some $\ell_i$, 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 $\beta$ 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 $\sqrt{\beta^\sigma} = \pm \sqrt{\beta^{2\sigma}} \bmod \ell_i$ ($\sigma \in G(k_n/\mathbb{Q})$) using $g_i(X)$. Namely, we choose $\sqrt{\beta^\sigma} \bmod \ell_i$ so that $g_1(\sqrt{\beta^\sigma}) \equiv 0 \pmod{\ell_i}$ and $g_1(-\sqrt{\beta^\sigma}) \neq 0 \pmod{\ell_i}$. If $g_1(\pm \sqrt{\beta^\sigma}) \equiv 0 \pmod{\ell_i}$, then we skip this $\ell_i$.
6. Solving the simultaneous equations \((1)\) modulo $\ell_i$, 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 $\beta_i^2$ with $\beta$. 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 $\sqrt{\beta^\sigma}$ mod $\ell_i$ using a factor of $f(X)$. If $f(X^2)$ remains irreducible (i.e. $\deg f \leq 2^n$), we get $\sqrt{\beta^{2\sigma}}$ for an appropriate $\delta \in k_n$ and set $\sqrt{\beta} = \sqrt{\beta^{2\sigma}/\delta}$.

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 \((1)\) 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 \((1)\). Let $\alpha = \alpha_n + \omega$, where $\omega = (1 + \sqrt{\beta})/2$. 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

$$\beta^\sigma \bmod \ell_i \equiv (v_0^\sigma \ v_1^\sigma \cdots v_r^\sigma)^t (b_0 \ v_1 \cdots b_r) \equiv (1 \alpha^\sigma \alpha^{2\sigma} \cdots \alpha^{r\sigma})B^{-1} (b_0 \ v_1 \cdots b_r) \pmod{\ell_i}.$$  \hspace{1cm} \((8)\)

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 $\ell_i$.

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

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

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

$$(y_0 \ y_1 \cdots y_r) = (x_0 \ v_1 \cdots v_r)^t B.$$  

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. \(n \leq 5\)), then the approximate calculation of
\[
(9) \quad f(X) = \prod_{\sigma \in G(k_n/\mathbb{Q})} (X - \beta^\sigma)
\]
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 \(\beta\) being a product of units in \(k_n\).

So we calculate \(f(X)\) modulo each \(\ell_i\) and construct \(f_i(X) \in \mathbb{Z}[X]\) such that \(f_i(X) \equiv f(X) \pmod{\ell_i \ell_1 \cdots \ell_i}\) and all the absolute values of coefficients of \(f_i(X)\) are less than \(\ell_i \ell_1 \cdots \ell_i/2\). 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 \(\beta\). When \(f(X)\) is not square-free, \(f(X) = g(X)^m\) with irreducible \(g(X) \in \mathbb{Z}[X]\) and \(m \geq 2\). Then \(g(X)\) is the minimal polynomial of \(\beta\).

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 \(\ell\) splits completely in \(k_n\) if \(\ell \equiv 1 \pmod{2^{n+2}}\) and \((p/\ell) = 1\). We build a finite set \(L = \{\ell_0, \ell_1, \ldots, \ell_N\}\) consisting of an appropriate number of such \(\ell\) satisfying \(\det B \neq 0 \pmod{\ell}\) and \(f(a, l) \neq 0 \pmod{\ell}\).

Let \(\ell_i \in L\) and \(g_i\) be a primitive root of \(\ell_i\). If \(z_1\) is a rational integer satisfying \(z_1 \equiv g_i^{(\ell_i-1)/2^{n+2}} \pmod{\ell_i}\), then \(2 \cos(2\pi/2^{n+2}) \equiv z_1 + z_1^{-1} \pmod{L}\) for some prime ideal \(L_1\) of \(\mathbb{Q}(\alpha_n)\) lying above \(\ell_i\). We also find \(z_2 \in \mathbb{Z}\) such that \(z_2 \equiv \omega \pmod{L_2}\) for some prime ideal \(L_2\) of \(k\) lying above \(\ell_i\) by solving \(x^2 \equiv p \pmod{\ell_i}\). Then \(\alpha \equiv z_1 + z_2 \pmod{L}\) for some prime ideal \(L\) of \(k_n\) lying above \(\ell_i\). We abbreviate this congruence as \(\alpha \equiv z_1 + z_2 \pmod{\ell_i}\).

We prepare a table of \(\alpha^i \bmod \ell_i\) (\(\sigma \in G(k_n/\mathbb{Q})\), \(0 \leq i \leq N\)) and a table of \(v_j \bmod \ell_i\) (\(0 \leq i \leq N\), \(0 \leq j \leq 2^{n+1} - 1\)) 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 \(v_j^2 \bmod \ell_i\) (\(\sigma \in G(k_n/\mathbb{Q})\), \(0 \leq i \leq N\), \(0 \leq j \leq 2^{n+1} - 1\)) 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 [5,7].

We may assume that we find positive \(\eta_i \in E_n\) such that
\[
C_n = \{ -1, \; \eta_0, \eta_1, \ldots, \eta_{2^n-2}\},
E_n = \{ -1, \; \eta_0, \eta_1, \ldots, \eta_{2^n-2}, \eta_{2^n-1}, \eta_{2^n}, \ldots, \eta_{2^{n+1}-2}\}
\]
with properties
\[
N_{k_n/k}(\eta_i) = \pm 1 \quad (0 \leq i \leq 2^{n+1} - 3),
N_{k_n/k}(\eta_{2^{n+1}-2}) \neq \pm 1.
\]
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
\[
N_{k_n/\mathbb{Q}(\alpha_n)}(\eta_j) = \pm \prod_{i=0}^{t-1} \eta_i^{a_{ij}} \quad (0 \leq j \leq u - 1)
\]
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 \( \pm 1 \) if and only if \( x = \langle x_0, x_1, \ldots, x_{u-1} \rangle \) is contained in the kernel of the linear map \( \psi : \mathbb{Z}^n \ni x \mapsto Ax \in \mathbb{Z}^t \), where \( A = (a_{ij}) \). Let \( v \) be the dimension of \( \ker \psi \) and \( \{\omega_0, \omega_1, \ldots, \omega_{v-1}\} \) a \( \mathbb{Z} \)-basis of \( \ker \psi \). Then the above \( \eta \) exists if and only if \( \prod_i N_{k_n/\mathbb{Q}(\alpha_n)}(\eta_i)^{x_{ij}} < 0 \) for some \( \omega_j = \langle x_{0j}, x_{1j}, \ldots, x_{uj} \rangle \).

In this manner we find \( \eta \in E_n \). Now, for \( 0 \leq j \leq v - 1 \), 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
\[
E_{n,1} = \langle -1, \eta^{e_j} \prod_{i=0}^{u-1} \eta_i^{x_{ij}} \mid 0 \leq j \leq v - 1 \rangle.
\]

The index \( (E_n : E_{n,1}C_nE_n^2) \) is easily calculated using the Hermite normal form of the integer matrix. Since \( (E_n : C_nE_n^2) = 2^{2n} \), if \( (E_n : E_{n,1}C_nE_n^2) = 2^d \), then there are \( 2^n - d \) independent units in Theorem 1.1.

4.7. Tables. We calculated \( E_{n,1} \) (\( 2 \leq n \leq 7 \)) for \( k = \mathbb{Q}(\sqrt{p}) \), where \( p \) is a prime number less than \( 10^4 \) which satisfies \( p \equiv 1 \) (mod \( 2^4 \)) and \( 2^4 \equiv 1 \) (mod \( p \)). We denote by \( m_n \) the maximal number of independent units in Theorem 1.1. 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 \( k \geq n + 1 \). 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.

\[
2^4 \mid p - 1
\]

<table>
<thead>
<tr>
<th>( p )</th>
<th>( m_2 )</th>
<th>( m_3 )</th>
<th>( p )</th>
<th>( m_2 )</th>
<th>( m_3 )</th>
<th>( p )</th>
<th>( m_2 )</th>
<th>( m_3 )</th>
<th>( m_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>113</td>
<td>2</td>
<td>3089</td>
<td>2</td>
<td>4721</td>
<td>2</td>
<td>7793</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>337</td>
<td>2</td>
<td>3121</td>
<td>2</td>
<td>4817</td>
<td>2</td>
<td>8081</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>593</td>
<td>2</td>
<td>3217</td>
<td>1</td>
<td>5233</td>
<td>1</td>
<td>8209</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>881</td>
<td>2</td>
<td>3313</td>
<td>2</td>
<td>5297</td>
<td>1</td>
<td>8273</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1201</td>
<td>2</td>
<td>3761</td>
<td>2</td>
<td>5593</td>
<td>1</td>
<td>8369</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1553</td>
<td>2</td>
<td>4049</td>
<td>1</td>
<td>6353</td>
<td>2</td>
<td>9137</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1777</td>
<td>2</td>
<td>4177</td>
<td>2</td>
<td>6449</td>
<td>2</td>
<td>9521</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2129</td>
<td>1</td>
<td>4273</td>
<td>0</td>
<td>6481</td>
<td>2</td>
<td>9649</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2833</td>
<td>2</td>
<td>4657</td>
<td>1</td>
<td>7121</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IWASAWA $\lambda$-IN Variant of the Cyclotomic $\mathbb{Z}_2$-Extension of $\mathbb{Q}(\sqrt{p})$

| $2^5$ || $p - 1$ |
|---|---|
| 353 | 6 |
| 1249 | 5 6 |
| 1889 | 3 3 6 |
| 2273 | 6 |
| 2593 | 6 |
| 2657 | 6 |

| $2^6$ || $p - 1$ |
|---|---|
| 577 | 13 14 |
| 1217 | 14 |

| $2^7$ || $p - 1$ |
|---|---|
| 1153 | 30 |
| 2689 | 29 30 |

| $2^8$ || $p - 1$ |
|---|---|
| 8161 | 4 6 |
| 8609 | 5 6 |
| 9377 | 4 6 |
| 9697 | 5 6 |

| $2^9$ || $p - 1$ |
|---|---|
| 7393 | 6 |
| 7841 | 4 6 |

| $2^{10}$ || $p - 1$ |
|---|---|
| 1401 | 14 |
| 2113 | 13 14 |
| 4289 | 14 5569 |
| 7489 | 14 |
| 9281 | 14 |

<table>
<thead>
<tr>
<th>References</th>
</tr>
</thead>
</table>


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