Imaginary quadratic fields whose Iwasawa $\lambda$-invariant is equal to 1

by

Dongho Byeon (Seoul) *†

1 Introduction and statement of results

Let $D$ be the fundamental discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$ and $\chi_D := \left( \frac{D}{.} \right)$ the usual Kronecker character. Let $p$ be prime, $\mathbb{Z}_p$ the ring of $p$-adic integers, and $\lambda_p(\mathbb{Q}(\sqrt{D}))$ the Iwasawa $\lambda$-invariant of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\sqrt{D})$. In this paper, we shall prove the following:

**Theorem 1.1** For any odd prime $p$, 

$$\sharp\{ -X < D < 0 \mid \lambda_p(\mathbb{Q}(\sqrt{D})) = 1, \chi_D(p) = 1 \} \gg \frac{\sqrt{X}}{\log X}.$$ 

Horie [9] proved that for any odd prime $p$, there exist infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ with $\lambda_p(\mathbb{Q}(\sqrt{D})) = 0$ and the author [1] gave a lower bound for the number of such imaginary quadratic fields. It is known that for any prime $p$ which splits in the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$, $\lambda_p(\mathbb{Q}(\sqrt{D})) \geq 1$. So it is interesting to see how often the trivial $\lambda$-invariant appears for such a prime. Jochnowitz [10] proved that for any odd prime $p$, if there exists one imaginary quadratic field $\mathbb{Q}(\sqrt{D}_0)$ with $\lambda_p(\mathbb{Q}(\sqrt{D}_0)) = 1$ and

---

*2000 Mathematics Subject Classification: 11R11, 11R23.
†This work was supported by grant No. R08-2003-000-10243-0 from the Basic Research Program of the Korea Science and Engineering Foundation.
χ_{D_0}(p) = 1, then there exist an infinite number of such imaginary quadratic fields.

For the case of real quadratic fields, Greenberg [8] conjectured that λ_p(Q(\sqrt{D})) = 0 for all real quadratic fields and all prime numbers p. Ono [11] and Byeon [2] [3] showed that for all prime numbers p, there exist infinitely many real quadratic fields Q(\sqrt{D}) with λ_p(Q(\sqrt{D})) = 0 and gave a lower bound for the number of such real quadratic fields.

In section 3, we shall prove the following:

**Proposition 1.2** For any odd prime p, if there is a negative fundamental discriminant D_0 < 0 such that λ_p(Q(\sqrt{D_0})) = 1 and χ_{D_0}(p) = 1, then

\[ \sharp \{ -X < D < 0 \mid \lambda_p(Q(\sqrt{D})) = 1, \chi_D(p) = 1 \} \gg \frac{\sqrt{X}}{\log X}. \]

In section 4, we shall prove the followings:

**Proposition 1.3** Let p be an odd prime and D_0 < 0 be the fundamental discriminant of the imaginary quadratic field Q(\sqrt{1 - p^2}). Then χ_{D_0}(p) = 1 and λ_p(Q(\sqrt{D_0})) = 1 if and only if 2^{p-1} \not\equiv 1 \pmod{p^2}, that is, p is not a Wieferich prime.

**Proposition 1.4** Let p be a Wieferich prime. If p \equiv 3 \pmod{4}, let D_0 < 0 be the fundamental discriminant of the imaginary quadratic field Q(\sqrt{1 - p^2}) and if p \equiv 1 \pmod{4}, let D_0 < 0 be the fundamental discriminant of the imaginary quadratic field Q(\sqrt{4 - p^2}). Then χ_{D_0}(p) = 1 and λ_p(Q(\sqrt{D_0})) = 1.

From these three propositions, Theorem 1.1 follows.

## 2 Preliminaries

Let \chi be a non-trivial even primitive Dirichlet character of conductor f which is not divisible by p^2. Let L_p(s, \chi) be the Kubota-Leopoldt p-adic L-function and \( O_{\chi} = \mathbb{Z}_p[\chi(1), \chi(2), \cdots] \). Then there is a power series F(T, \chi) ∈ O_{\chi}[[T]] such that

\[ L_p(s, \chi) = F((1 + pd)^s - 1, \chi), \]
where \( d = f \) if \( p \nmid f \) and \( d = f/p \) if \( p|f \). Let \( \pi \) be a generator for the ideal of \( O_\chi \) above \( p \). Then we may write

\[
F(T, \chi) = G(T)U(T),
\]

where \( U(T) \) is a unit of \( O_\chi[[T]] \), and \( G(T) \) is a distinguished polynomial: that is, \( G(T) = a_0 + a_1 T + \cdots + T^\lambda \) with \( \pi|a_i \) for \( i \leq \lambda - 1 \). Define \( \lambda(L_p(s, \chi)) \) be the index of the first coefficient of \( F(T, \chi) \) not divisible by \( \pi \). Let \( \omega \) be the Teichmüller character.

**Lemma 2.1** (Dummit, Ford, Kisilevsky and Sands [5, Proposition 5.1]) Let \( D < 0 \) be the fundamental discriminant of the imaginary quadratic field \( \mathbb{Q}(\sqrt{D}) \). Then

\[
\lambda_p(\mathbb{Q}(\sqrt{D})) = \lambda(L_p(s, \chi_D \omega)).
\]

**Lemma 2.2** (Washington [13, Lemma 1]) Let \( D < 0 \) be the fundamental discriminant of the imaginary quadratic field \( \mathbb{Q}(\sqrt{D}) \).

\[
\lambda(L_p(s, \chi_D \omega)) = 1 \iff L_p(0, \chi_D \omega) \not\equiv L_p(1, \chi_D \omega) \pmod{p^2}.
\]

From these lemmas, we can show the following:

**Proposition 2.3** Let \( p \) be an odd prime and \( D < 0 \) be the fundamental discriminant of the imaginary quadratic field \( \mathbb{Q}(\sqrt{D}) \) such that \( \chi_D(p) = 1 \). Then \( \frac{L(1-p, \chi_D)}{p} \) is \( p \)-integral and

\[
\lambda_p(\mathbb{Q}(\sqrt{D})) = 1 \iff \frac{L(1-p, \chi_D)}{p} \not\equiv 0 \pmod{p},
\]

where \( L(s, \chi_D) \) is the Dirichlet \( L \)-function.

**Proof:** By the construction of the \( p \)-adic \( L \)-function \( L_p(s, \chi_D) \),

\[
L_p(0, \chi_D \omega) = -(1 - \chi_D \omega \cdot \omega^{-1}(p))B_{1, \chi_D \omega \omega^{-1}}
\]

\[
= -(1 - \chi_D(p))B_{1, \chi_D},
\]

where \( B_{n, \chi_D} \) is the generalized Bernoulli number. Since \( \chi_D(p) = 1 \),

\[
L_p(0, \chi_D \omega) = 0.
\]
Similarly,
\[
L_p(1-p, \chi_D \omega) = -(1 - \chi_D \omega \cdot \omega^{-p}(p)p^{p-1})B_{p, \chi_D \omega^{-p}}/p \\
= -(1 - \chi_D(p)p^{p-1})B_{p, \chi_D}/p \\
= (1 - p^{p-1})L(1 - p, \chi_D) \\
\equiv L(1 - p, \chi_D) \pmod{p^2}.
\]

Since \( \chi_D \omega \neq 1 \) is not a character of the second kind, \( L_p(1 - p, \chi_D \omega) \) and \( L(1 - p, \chi_D) \) are \( p \)-integral (See [14]). By the congruence of \( L_p(s, \chi_D) \),
\[
L_p(1, \chi_D \omega) \equiv L_p(0, \chi_D \omega) = 0 \pmod p,
\]
and
\[
L_p(1, \chi_D \omega) \equiv L_p(1 - p, \chi_D \omega) \pmod{p^2}.
\]
Thus \( \frac{L(1 - p, \chi_D)}{p} \) is \( p \)-integral and
\[
\frac{L(1 - p, \chi_D)}{p} \not\equiv 0 \pmod p \iff L_p(1, \chi_D \omega) \not\equiv 0 \pmod{p^2}. \tag{1}
\]

From the equation (1) and Lemmas 2.1, 2.2, the proposition follows. \( \square \)

## 3 Proof of Proposition 1.2

Let \( M_k(\Gamma_{0}(N), \chi) \) denote the space of modular forms of weight \( k \) on \( \Gamma_{0}(N) \) with character \( \chi \). For a positive integer \( r \geq 2 \), let
\[
F_r(z) := \sum_{N \neq 0} H(r, N)q^{N} \in M_{r+\frac{1}{2}}(\Gamma_{0}(4), \chi_0)
\]
be the Cohen modular form [4], where \( q := e^{2\pi iz} \). We note that if \( Dn^2 = (-1)^r N \), then
\[
H(r, N) = L(1 - r, \chi_D) \sum_{d|n} \mu(d)\chi_D(d)d^{r-1}\sigma_{2r-1}(n/d), \tag{2}
\]
where \( \sigma_{\nu}(n) := \sum_{d|n} d^{\nu} \). From \( F_p(z) \), we can construct the modular form
\[
G_p(z) := \sum_{\left(\frac{\cdot}{p}\right) = 1, \left(\frac{n}{p}\right) = -1} \frac{H(p, n)}{p}q^{n} \in M_{p+\frac{1}{2}}(\Gamma_{0}(4p^4Q^4), \chi_0),
\]
where $Q$ is a prime such that $Q \neq p$. From Proposition 2.3 and the equation (2), if $D < 0$ is the fundamental discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ such that $\chi_D(p) = 1$, then

$$\frac{H(p, -D)}{p} = \frac{L(1 - p, \chi_D)}{p}$$

is $p$-integral. Using similar methods in Ono [11] and Byeon [2], that is, applying a theorem of Sturm [12] to the following two modular forms

$$(U_l | G_p)(z) = \sum_{(\frac{n}{p}) = 1, (\frac{p}{n}) = -1} \frac{H(p, \ln)}{p} q^n \in M_{p+\frac{1}{2}}(\Gamma_0(4p^4Q^4l), (\frac{Al}{-l})),

(V_l | G_p)(z) = \sum_{(\frac{n}{p}) = 1, (\frac{p}{n}) = -1} \frac{H(p, n)}{p} q^n \in M_{p+\frac{1}{2}}(\Gamma_0(4p^4Q^4l), (\frac{Al}{-l})),

where $l \neq p$ is a suitable prime and comparing the coefficients of $q^{-D_0l^3}$ of these modular forms, where $D_0 < 0$ is a fundamental discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{D_0})$ such that $\chi_{D_0}(p) = 1$ and $\frac{H(p, -D_0)}{p} \neq 0 \pmod{p}$, we can obtain the following:

**Proposition 3.1** Let $p$ be an odd prime. Assume that there is a fundamental discriminant $D_0 < 0$ of the imaginary quadratic field $\mathbb{Q}(\sqrt{D_0})$ such that

(i) $\chi_{D_0}(p) = 1$,

(ii) $\frac{H(p, -D_0)}{p} \neq 0 \pmod{p}$.

Then there is an arithmetic progression $r_p \pmod{pt_p}$ with $(r_p, pt_p) = 1$ and $(\frac{-r_p}{p}) = 1$, and a constant $\kappa(p)$ such that for each prime $l \equiv r_p \pmod{pt_p}$ there is an integer $1 \leq d_l \leq \kappa(p)l$ for which

(i) $D_l := -d_l l$ is a fundamental discriminant,

(ii) $\frac{H(p, -D_l)}{p} \neq 0 \pmod{p}$. 


Proof of Proposition 1.2: Let $D_l < 0$ be the fundamental discriminant in Proposition 3.1. Then $\chi_{D_l}(p) = 1$ and $\frac{H(p, -D_l)}{p} = \frac{L(1-p, \chi_{D_l})}{p} \not\equiv 0 \pmod{p}$. By Proposition 2.3, $\lambda_p(\mathbb{Q}(\sqrt{D_l})) = 1$. By Dirichlet’s theorem on primes in arithmetic progression, we have that the number of such $D_l < X$ is $\gg \frac{X}{\log X}$.

24 Proof of Propositions 1.3 and 1.4

To prove Propositions 1.3 and 1.4, we shall use of the following criterion of Gold.

Lemma 4.1 (Gold [7]) Let $p$ be an odd prime and $D < 0$ be the fundamental discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ such that $\chi_{D}(p) = 1$. Let $(p) = \bar{P}P$ in $\mathbb{Q}(\sqrt{D})$. Suppose that $P = (\pi)$ is principal for some integer $r$ not divisible by $p$. Then $\lambda_p(\mathbb{Q}(\sqrt{D})) = 1$ if and only if $\pi^{p-1} \not\equiv 1 \pmod{\bar{P}^2}$.

First we shall prove Proposition 1.3.

Proof of Proposition 1.3: We note that $1 - p^2$ is not a square. Let $P = (p, 1+\sqrt{1-p^2})$ and $\bar{P} = (p, 1-\sqrt{1-p^2})$. Then $(p) = P\bar{P}$ and $P^2 = (1+\sqrt{1-p^2})$, $\bar{P}^2 = (1-\sqrt{1-p^2})$. From Lemma 4.1, $\lambda_p(\mathbb{Q}(\sqrt{D_0})) = 1$ if and only if

$$(1 + \sqrt{1-p^2})^{p-1} \not\equiv 1 \pmod{(1 - \sqrt{1-p^2})}.$$ 

This is equivalent to that

$$(1 + \sqrt{1-p^2})^p - (1 + \sqrt{1-p^2}) \not\equiv 0 \pmod{(p^2 = (1 - \sqrt{1-p^2})(1 + \sqrt{1-p^2}) ).} \tag{3}$$

We see that

$$
(1 + \sqrt{1-p^2})^p - (1 + \sqrt{1-p^2}) \\
\equiv \sum_{n=0}^{p-1} \binom{p}{2n} + \sum_{n=0}^{p-1} \binom{p}{2n+1})\sqrt{1-p^2} - (1 + \sqrt{1-p^2}) \\
\equiv (\sum_{n=0}^{p-1} \binom{p}{2n} - 1) + (\sum_{n=0}^{p-1} \binom{p}{2n+1} - 1)\sqrt{1-p^2} \\
\equiv (2^{p-1} - 1)(1 + \sqrt{1-p^2}) \pmod{p^2}.
$$

4 Proof of Propositions 1.3 and 1.4

To prove Propositions 1.3 and 1.4, we shall use of the following criterion of Gold.

Lemma 4.1 (Gold [7]) Let $p$ be an odd prime and $D < 0$ be the fundamental discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ such that $\chi_{D}(p) = 1$. Let $(p) = \bar{P}P$ in $\mathbb{Q}(\sqrt{D})$. Suppose that $P = (\pi)$ is principal for some integer $r$ not divisible by $p$. Then $\lambda_p(\mathbb{Q}(\sqrt{D})) = 1$ if and only if $\pi^{p-1} \not\equiv 1 \pmod{\bar{P}^2}$.

First we shall prove Proposition 1.3.

Proof of Proposition 1.3: We note that $1 - p^2$ is not a square. Let $P = (p, 1+\sqrt{1-p^2})$ and $\bar{P} = (p, 1-\sqrt{1-p^2})$. Then $(p) = P\bar{P}$ and $P^2 = (1+\sqrt{1-p^2})$, $\bar{P}^2 = (1-\sqrt{1-p^2})$. From Lemma 4.1, $\lambda_p(\mathbb{Q}(\sqrt{D_0})) = 1$ if and only if

$$(1 + \sqrt{1-p^2})^{p-1} \not\equiv 1 \pmod{(1 - \sqrt{1-p^2})}.$$ 

This is equivalent to that

$$(1 + \sqrt{1-p^2})^p - (1 + \sqrt{1-p^2}) \not\equiv 0 \pmod{(p^2 = (1 - \sqrt{1-p^2})(1 + \sqrt{1-p^2}) ).} \tag{3}$$

We see that

$$
(1 + \sqrt{1-p^2})^p - (1 + \sqrt{1-p^2}) \\
\equiv \sum_{n=0}^{p-1} \binom{p}{2n} + \sum_{n=0}^{p-1} \binom{p}{2n+1})\sqrt{1-p^2} - (1 + \sqrt{1-p^2}) \\
\equiv (\sum_{n=0}^{p-1} \binom{p}{2n} - 1) + (\sum_{n=0}^{p-1} \binom{p}{2n+1} - 1)\sqrt{1-p^2} \\
\equiv (2^{p-1} - 1)(1 + \sqrt{1-p^2}) \pmod{p^2}.
$$

6
where we have used the fact
\[
\sum_{n=0}^{2^{p-1}} \binom{p}{2n} = \sum_{n=0}^{2^{p-1}} \binom{p}{2n+1} = 2^{p-1}.
\]
Thus the equation (3) is true if and only if \(2^{p-1} \not\equiv 1 \pmod{p^2}\), that is, \(p\) is not a Wieferich prime and the proposition follows. \(\Box\)

Finally we shall prove Proposition 1.4.

**Proof of Proposition 1.4:** We note that \(1 - p\) is not a square if \(p \equiv 3 \pmod{4}\) and \(4 - p\) is not a square if \(p \equiv 1 \pmod{4}\). We also note that \(\chi_{D_0}(p) = 1\).

First we consider the case \(p \equiv 3 \pmod{4}\). Let \(P = (1 + \sqrt{1 - p})\) and \(\overline{P} = (1 - \sqrt{1 - p})\). Then \((p) = PP\overline{P}\) and \(P^2 = ((1+\sqrt{1 - p})^2), \overline{P}^2 = ((1-\sqrt{1 - p})^2)\). Then from Lemma 4.1, \(\lambda_p(Q(\sqrt{D_0})) = 1\) if and only if
\[
(1 + \sqrt{1 - p})^{2(p-1)} \not\equiv 1 \pmod{(1 - \sqrt{1 - p})^2}.
\]
This is equivalent to that
\[
(1 + \sqrt{1 - p})^{2p} - (1 + \sqrt{1 - p})^2 \not\equiv 0 \pmod{(1 - \sqrt{1 - p})^2(1 + \sqrt{1 - p})^2}. \quad (4)
\]
We see that
\[
(1 + \sqrt{1 - p})^{2p} \equiv \sum_{n=0}^{p} \binom{2p}{2n} (1-p)^n + \sqrt{1-p} \cdot \sum_{n=0}^{p-1} \binom{2p}{2n+1} (1-p)^n
\]
\[
\equiv \sum_{n=0}^{p} \binom{2p}{2n} (1-np) + \sqrt{1-p} \cdot \sum_{n=0}^{p-1} \binom{2p}{2n+1} (1-np)
\]
\[
\equiv \sum_{n=0}^{p} \binom{2p}{2n} - p \cdot \sum_{n=0}^{p-1} n \binom{2p}{2n} + \sqrt{1-p} \cdot \left( \sum_{n=0}^{p-1} \binom{2p}{2n+1} - p \cdot \sum_{n=0}^{p-1} n \binom{2p}{2n+1} \right) \pmod{p^2},
\]
where we have used the fact that \((1-p)^n \equiv 1 - np \pmod{p^2}\). Now, using the following facts
\[ \sum_{n=0}^{p} \binom{2p}{2n} = \sum_{n=0}^{p-1} \binom{2p}{2n+1} = 2^{2p-1}, \]
\[ \sum_{n=1}^{p} n \binom{2p}{2n} = p \cdot 2^{2p-2}, \]
\[ \sum_{n=1}^{p-1} n \binom{2p}{2n+1} = (p-1) \cdot 2^{2p-2}, \]

we find that
\[(1 + \sqrt{1-p})^{2p} \equiv 2^{2p-1} + \sqrt{1-p} \cdot (2^{2p-1} + p \cdot 2^{2p-2}) \pmod{p^2}.\]

Hence we have
\[(1+\sqrt{1-p})^{2p} - (1+\sqrt{1-p})^{2} \equiv (2^{2p-1}+p-2) + (2^{2p-1}+p \cdot 2^{2p-2} - 2) \sqrt{1-p} \pmod{p^2}.

Thus the equation (4) is true if and only if
\[2^{2p-1} + p - 2 \not\equiv 0 \pmod{p^2} \quad \text{or} \quad 2^{2p-1} + p \cdot 2^{2p-2} - 2 \not\equiv 0 \pmod{p^2}. \quad (5)\]

But it is easy to see that (5) is true if \(2^{p-1} \equiv 1 \pmod{p^2}\). Hence if \(p\) is a Wieferich prime, then \(\lambda_p(Q(\sqrt{D_0}))\) should be equal to 1.

Now we consider the case \(p \equiv 1 \pmod{4}\). Let \(P = (2 + \sqrt{4-p})\) and \(\bar{P} = (2 - \sqrt{4-p})\). Then \(p = P \overline{P}\) and \(P^2 = (2 + \sqrt{4-p})^2\), \(\bar{P}^2 = (2 - \sqrt{4-p})^2\). Then from Lemma 4.1, \(\lambda_p(Q(\sqrt{D_0})) = 1\) if and only if
\[(2 + \sqrt{4-p})^{2(p-1)} \not\equiv 1 \pmod{(2 - \sqrt{4-p})^2}.\]

This is equivalent to that
\[(2 + \sqrt{4-p})^{2p} - (2 + \sqrt{4-p})^2 \not\equiv 0 \pmod{(p^2 = (2 - \sqrt{4-p})^2(2 + \sqrt{4-p})^2)}. \quad (6)\]

By a computation similar to the above, we have
\[(2+\sqrt{4-p})^{2p} - (2+\sqrt{4-p})^2 \equiv (2^{4p-1}+p-8) + (2^{4p-2}+p \cdot 2^{4p-5} - 4) \sqrt{4-p} \pmod{p^2}.

Thus the equation (6) is true if and only if
\[2^{4p-1} + p - 8 \not\equiv 0 \pmod{p^2} \quad \text{or} \quad 2^{4p-2} + p \cdot 2^{4p-5} - 4 \not\equiv 0 \pmod{p^2}. \quad (7)\]
But it is also easy to see that (7) is true if $2^{p-1} \equiv 1 \pmod{p^2}$. Hence if $p$ is a Wieferich prime, then $\lambda_p(\mathbb{Q}(\sqrt{D_0}))$ should be equal to 1 and we prove the proposition. □

Remark. It seems interesting that Propositions 1.3 and 1.4 give criteria for the Wieferich primes. We know that the Wieferich primes are very rare. The only Wieferich primes for $p \leq 4 \times 10^{12}$ are $p = 1093$ and $p = 3511$ (See [5]).

Acknowledgements. The author thanks the referee for correcting his mistakes and many valuable suggestions.

References


School of Mathematical Sciences, Seoul National University
Seoul 151-747, Korea
E-mail: dhbyeon@math.snu.ac.kr