ACTA ARITHMETICA
120.2 (2005)

Imaginary quadratic fields whose Iwasawa λ-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 $\chi_D := \left(\frac{D}{\cdot}\right)$ the usual Kronecker character. Let p be a prime, $\mathbb{Z}_p$ the ring of p-adic integers, and $\lambda_p(\mathbb{Q}(\sqrt{D}))$ the Iwasawa λ-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 λ-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 $\chi_{D_0}(p) = 1$, then there exist an infinite number of such imaginary quadratic fields.

For the case of real quadratic fields, Greenberg [8] conjectured that $\lambda_p(\mathbb{Q}(\sqrt{D})) = 0$ 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 $\mathbb{Q}(\sqrt{D})$ with $\lambda_p(\mathbb{Q}(\sqrt{D})) = 0$ and gave a lower bound for the number of such real quadratic fields.

In Section 3, we shall prove the following:

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.

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

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

In Section 4, we shall prove the following:

Proposition 1.3. *Let p be an odd prime and $D_0 < 0$ be the fundamental discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{1-p^2})$. Then $\chi_{D_0}(p) = 1$ and $\lambda_p(\mathbb{Q}(\sqrt{D_0})) = 1$ 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 $\mathbb{Q}(\sqrt{1-p})$, and if $p \equiv 1 \pmod 4$, let $D_0 < 0$ be the fundamental discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{4-p})$. Then $\chi_{D_0}(p) = 1$ and $\lambda_p(\mathbb{Q}(\sqrt{D_0})) = 1$.*

From these three propositions, Theorem 1.1 follows.

2. Preliminaries.

Let χ 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 $O_\chi = \mathbb{Z}_p[\chi(1), \chi(2), \ldots]$. Then there is a power series $F(T,\chi) \in O_\chi[[T]]$ such that

$$L_p(s,\chi) = F((1+pd)^s - 1, \chi),$$

where $d = f$ if $p \nmid f$ and $d = f/p$ if $p \mid f$. Let π be a generator for the ideal of O_χ 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 $\pi \mid a_i$ for $i \le \lambda - 1$. Define $\lambda(L_p(s,\chi))$ to be the index of the first coefficient of $F(T,\chi)$ not divisible by π. Let ω be the Teichmüller character.

Lemma 2.1 (Dummit, Ford, Kisilevsky and Sands [6, 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 $\mathbb{Q}(\sqrt{D})$. Then*

$$\lambda(L_p(s,\chi_D\omega)) = 1 \;\Leftrightarrow\; L_p(0,\chi_D\omega) \not\equiv L_p(1,\chi_D\omega) \pmod{p^2}.$$

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 $L(1-p,\chi_D)/p$ is p-integral and*

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

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

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

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

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

$$L_p(0,\chi_D\omega)=0.$$

Similarly,

$$\begin{aligned}L_p(1-p,\chi_D\omega)&=-(1-\chi_D\omega\cdot\omega^{-p}(p)p^{p-1})B_{p,\chi_D\omega\cdot\omega^{-p}}/p\\&=-(1-\chi_D(p)p^{p-1})B_{p,\chi_D}/p=(1-p^{p-1})L(1-p,\chi_D)\\&\equiv L(1-p,\chi_D) \pmod{p^2}.\end{aligned}$$

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 $L(1-p,\chi_D)/p$ is p-integral and

$$(1)\qquad \frac{L(1-p,\chi_D)}{p}\not\equiv 0 \pmod{p} \ \Leftrightarrow\ L_p(1,\chi_D\omega)\not\equiv 0 \pmod{p^2}.$$

From (1) and Lemmas 2.1, 2.2, the proposition follows. ∎

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 χ. For a positive integer $r\geq 2$, let

$$F_r(z):=\sum_{N\neq 0}H(r,N)q^N\in M_{r+1/2}(\Gamma_0(4),\chi_0)$$

be the Cohen modular form [4], where $q:=e^{2\pi iz}$. We note that if $Dn^2=(-1)^rN$, then

$$(2)\qquad H(r,N)=L(1-r,\chi_D)\sum_{d\mid n}\mu(d)\chi_D(d)d^{r-1}\sigma_{2r-1}(n/d),$$

where $\sigma_\nu(n) := \sum_{d|n} d^\nu$. From $F_p(z)$, we can construct the modular form

$$G_p(z) := \sum_{(\frac{-n}{p})=1,\,(\frac{n}{Q})=-1} \frac{H(p,n)}{p}\, q^n \in M_{p+1/2}(\Gamma_0(4p^4Q^4), \chi_0),$$

where Q is a prime such that $Q \neq p$. From Proposition 2.3 and 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 to Ono [11] and Byeon [2], that is, applying a theorem of Sturm [12] to the following two modular forms:

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

$$(V_l|G_p)(z) = \sum_{(\frac{-n}{p})=1,\,(\frac{n}{Q})=-1} \frac{H(p,n)}{p}\, q^{ln} \in M_{p+1/2}\biggl(\Gamma_0(4p^4Q^4l), \Bigl(\frac{4l}{\cdot}\Bigr)\biggr),$$

where $l \neq p$ is a suitable prime, and comparing the coefficients of $q^{-D_0l^3}$ in 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 $H(p,-D_0)/p \not\equiv 0 \pmod{p}$, 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) $H(p,-D_0)/p \not\equiv 0 \pmod{p}$.

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

(i) $D_l := -d_l l$ *is a fundamental discriminant*,
(ii) $H(p,-D_l)/p \not\equiv 0 \pmod{p}$.

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

4. Proof of Propositions 1.3 and 1.4. To prove these propositions, we shall use 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 $(p)=\mathbf{P}\overline{\mathbf{P}}$ in $\mathbb{Q}(\sqrt{D})$. Suppose that $\mathbf{P}^r=(\pi)$ is principal for some integer r not divisible by p. Then $\lambda_p(\mathbb{Q}(\sqrt{D}))=1$ if and only if $\pi^{p-1}\not\equiv 1 \pmod{\overline{\mathbf{P}}^2}$.*

Proof of Proposition 1.3. We note that $1-p^2$ is not a square. Let $\mathbf{P}=(p,1+\sqrt{1-p^2})$ and $\overline{\mathbf{P}}=(p,1-\sqrt{1-p^2})$. Then $(p)=\mathbf{P}\overline{\mathbf{P}}$ and $\mathbf{P}^2=(1+\sqrt{1-p^2})$, $\overline{\mathbf{P}}^2=(1-\sqrt{1-p^2})$. 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

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

We see that

$$\begin{aligned}
&(1+\sqrt{1-p^2})^p-(1+\sqrt{1-p^2})\\
&\equiv \sum_{n=0}^{(p-1)/2}\binom{p}{2n}+\Bigg(\sum_{n=0}^{(p-1)/2}\binom{p}{2n+1}\Bigg)\sqrt{1-p^2}-(1+\sqrt{1-p^2})\\
&\equiv \Bigg(\sum_{n=0}^{(p-1)/2}\binom{p}{2n}-1\Bigg)+\Bigg(\sum_{n=0}^{(p-1)/2}\binom{p}{2n+1}-1\Bigg)\sqrt{1-p^2}\\
&\equiv (2^{p-1}-1)(1+\sqrt{1-p^2}) \pmod{p^2},
\end{aligned}$$

where we have used the fact that

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

Thus (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. ∎

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 $\mathbf{P}=(1+\sqrt{1-p})$ and $\overline{\mathbf{P}}=(1-\sqrt{1-p})$. Then $(p)=\mathbf{P}\overline{\mathbf{P}}$ and $\mathbf{P}^2=((1+\sqrt{1-p})^2)$, $\overline{\mathbf{P}}^2=((1-\sqrt{1-p})^2)$. Now, 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

$$(4)\qquad (1+\sqrt{1-p})^{2p}-(1+\sqrt{1-p})^2\not\equiv 0 \quad (\operatorname{mod} p^2=(1-\sqrt{1-p})^2(1+\sqrt{1-p})^2).$$

We see that

$$\begin{aligned}
&(1+\sqrt{1-p})^{2p}\\
&\quad\equiv \sum_{n=0}^{p}\left(\binom{2p}{2n}(1-p)^n\right)+\sqrt{1-p}\cdot\sum_{n=0}^{p-1}\left(\binom{2p}{2n+1}(1-p)^n\right)\\
&\quad\equiv \sum_{n=0}^{p}\left(\binom{2p}{2n}(1-np)\right)+\sqrt{1-p}\cdot\sum_{n=0}^{p-1}\left(\binom{2p}{2n+1}(1-np)\right)\\
&\quad\equiv \sum_{n=0}^{p}\binom{2p}{2n}-p\cdot\sum_{n=0}^{p}n\binom{2p}{2n}\\
&\qquad+\sqrt{1-p}\cdot\left(\sum_{n=0}^{p-1}\binom{2p}{2n+1}-p\cdot\sum_{n=0}^{p-1}n\binom{2p}{2n+1}\right)\ (\operatorname{mod} p^2),
\end{aligned}$$

where we have used the fact that $(1-p)^n\equiv 1-np \ (\operatorname{mod} p^2)$. Now, since

$$\begin{aligned}
&\sum_{n=0}^{p}\binom{2p}{2n}=\sum_{n=0}^{p-1}\binom{2p}{2n+1}=2^{2p-1},\\
&\sum_{n=1}^{p}n\binom{2p}{2n}=p\cdot 2^{2p-2},\\
&\sum_{n=1}^{p-1}n\binom{2p}{2n+1}=(p-1)\cdot 2^{2p-2},
\end{aligned}$$

we find that

$$(1+\sqrt{1-p})^{2p}\equiv 2^{2p-1}+\sqrt{1-p}\cdot(2^{2p-1}+p\cdot 2^{2p-2})\ (\operatorname{mod} p^2).$$

Hence

$$\begin{aligned}
&(1+\sqrt{1-p})^{2p}-(1+\sqrt{1-p})^2\\
&\qquad\equiv(2^{2p-1}+p-2)+(2^{2p-1}+p\cdot 2^{2p-2}-2)\sqrt{1-p}\ (\operatorname{mod} p^2).
\end{aligned}$$

Thus (4) is true if and only if

$$(5)\qquad 2^{2p-1}+p-2\not\equiv 0\ (\operatorname{mod} p^2)\quad\text{or}\quad 2^{2p-1}+p\cdot 2^{2p-2}-2\not\equiv 0\ (\operatorname{mod} p^2).$$

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

Now we consider the case $p\equiv 1 \ (\operatorname{mod} 4)$. Let $\mathbf{P}=(2+\sqrt{4-p})$ and $\overline{\mathbf{P}}=(2-\sqrt{4-p})$. Then $(p)=\mathbf{P}\overline{\mathbf{P}}$ and $\mathbf{P}^2=((2+\sqrt{4-p})^2)$, $\overline{\mathbf{P}}^2=$

$((2-\sqrt{4-p})^2)$. Then from Lemma 4.1, $\lambda_p(\mathbb{Q}(\sqrt{D_0}))=1$ if and only if

$$(2+\sqrt{4-p})^{2(p-1)}\not\equiv 1 \pmod{(2-\sqrt{4-p})^2}.$$

This is equivalent to

$$(6)\quad (2+\sqrt{4-p})^{2p}-(2+\sqrt{4-p})^2\not\equiv 0 \\ (\bmod\, p^2=(2-\sqrt{4-p})^2(2+\sqrt{4-p})^2).$$

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 (6) is true if and only if

$$(7)\quad 2^{4p-1}+p-8\not\equiv 0 \pmod{p^2} \quad\text{or}\quad 2^{4p-2}+p\cdot 2^{4p-5}-4\not\equiv 0 \pmod{p^2}.$$

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 have proved 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 $p\le 4\cdot 10^{12}$ are $p=1093$ and $p=3511$ (see [5]).

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

References

[1] D. Byeon, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields and congruence of modular forms*, Acta Arith. 89 (1999), 295–299.

[2] —, *Indivisibility of class numbers and Iwasawa λ-invariants of real quadratic fields*, Compositio Math. 126 (2001), 249–256.

[3] —, *Existence of certain fundamental discriminants and class numbers of real quadratic fields*, J. Number Theory 98 (2003), 432–437.

[4] H. Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann. 217 (1975), 271–285.

[5] R. Crandall, K. Dilcher and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. 66 (1997), 433–449.

[6] D. S. Dummit, D. Ford, H. Kisilevsky and J. W. Sands, *Computation of Iwasawa lambda invariants for imaginary quadratic fields*, J. Number Theory 37 (1991), 100–121.

[7] R. Gold, *The nontriviality of certain $\mathbb{Z}_l$-extensions*, ibid. 6 (1974), 369–373.

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

[9] K. Horie, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields*, Invent. Math. 88 (1987), 31–38.

[10] N. Jochnowitz, *A p-adic conjecture about derivatives of L-series attached to modular forms*, in: p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture (Boston, MA, 1991), Contemp. Math. 165, Amer. Math. Soc., Providence, RI, 1994, 239–263.

[11] K. Ono, *Indivisibility of class numbers of real quadratic fields*, Compositio Math. 119 (1999), 1–11.

[12] J. Sturm, *On the congruence of modular forms*, in: Number Theory (New York, 1984–1985), Lecture Notes in Math. 1240, Springer, Berlin, 1984, 275–280.

[13] L. C. Washington, *Zeros of p-adic L-functions*, in: Séminaire Delange–Pisot–Poitou (Séminaire de Théorie des Nombres, Paris, 1980/1981), Progr. Math. 22, Birkhäuser, Boston, 1982, 337–357.

[14] —, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, New York, 1997.

Department of Mathematics
Seoul National University
Seoul 151-747, Korea
E-mail: dhbyeon@math.snu.ac.kr

Received on 12.10.2004
and in revised form on 7.7.2005 (4866)