ACTA ARITHMETICA
LXXXIX.3 (1999)

A note on basic Iwasawa λ-invariants of imaginary quadratic fields and congruence of modular forms

by

DONGHO BYEON (Seoul)

1. Introduction and statement of results. For a number field k and a prime number l, we denote by $h(k)$ the class number of k and by $\lambda_l(k)$ the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_l$-extension of k, where $\mathbb{Z}_l$ is the ring of l-adic integers.

Let l be an odd prime number. Using the Kronecker class number relation for quadratic forms, Hartung [3] proved that there exist infinitely many imaginary quadratic fields k whose class numbers are not divisible by l. For the case $l = 2$, this is an immediate consequence of Gauss' genus theory. For the case $l = 3$, Davenport and Heilbronn [2] proved the stronger result that a positive proportion of imaginary quadratic fields has class number coprime to 3. Recently, using Sturm's work [11] on the congruence of modular forms, Kohnen and Ono [7] obtained a lower bound for the number of D_k, $-X < D_k < 0$, where D_k is the discriminant of an imaginary quadratic field k such that $h(k) \not\equiv 0 \pmod{l}$ and X is a sufficiently large positive real number. Using the same method, subject to a mild condition on l, Ono [9] obtained similar results for real quadratic fields.

On the other hand, using the idea of Hartung and Eichler's trace formula combined with the l-adic Galois representation attached to the Jacobian variety $J = J_0(l)$ of the modular curve $X = X_0(l)$, Horie [4] proved that there exist infinitely many imaginary quadratic fields k such that l does not split in k and l does not divide $h(k)$. Later Horie and Onishi [5] obtained more refined results. By a theorem of Iwasawa [6], these results imply that there exist infinitely many imaginary quadratic fields k with $\lambda_l(k) = 0$. For the case $l = 2$, this is also an immediate consequence of Gauss' genus theory. For the case $l = 3$, by refining Davenport and Heilbronn's result [2], Nakagawa and Horie [8] gave a positive lower bound on the density of imaginary quadratic fields k and real quadratic fields k with $\lambda_l(k) = 0$.

1991 *Mathematics Subject Classification*: 11R11, 11R29.

Recently, Taya [12] improved the result of Nakagawa and Horie on real quadratic fields for the case $l = 3$ and Ono [9] obtained a lower bound on the number of real quadratic fields k with $\lambda_l(k) = 0$ for the case $3 < l < 5000$.

In this note, refining Kohnen and Ono's method [7, 9], we obtain a lower bound for the number of D_k, $-X < D_k < 0$, where D_k is the discriminant of an imaginary quadratic field k such that $h(k) \not\equiv 0 \pmod{l}$ and l does not split in k and X is a sufficiently large positive real number. Similarly, by a theorem of Iwasawa [6], this is also a lower bound for the number of imaginary quadratic fields k with $\lambda_l(k) = 0$.

THEOREM 1.1. *Let $l > 3$ be an odd prime and p be an odd prime such that $p \equiv 1 \pmod{8}$, $p \equiv -2 \pmod{l}$ and $\left(\frac{t}{p}\right) = 1$ for all prime t, $2 < t < l$. Then there exists an integer d_{lp}, $1 \le d_{lp} \le \frac{3}{4}(l+1)(p+1)$, such that $d_{lp}lp \ne nlp^2$ for any n, $1 \le n \le l$, and if we let $k = \mathbb{Q}(\sqrt{-d_{lp}lp})$ be the imaginary quadratic field, then $h(k) \not\equiv 0 \pmod{l}$ and l does not split in k.*

COROLLARY 1.2. *Let $l > 3$ be an odd prime and $\varepsilon > 0$. Let D_k be the discriminant of an imaginary quadratic field k with $\lambda_l(k) = 0$. Then for all sufficiently large $X > 0$,*

$$\sharp\{D_k : -X < D_k < 0\} \gg_l \sqrt{X}/\log X.$$

2. Proof of results

Proof of Theorem 1.1. Let l and p be odd primes. Let $\theta(z) := \sum_{n\in\mathbb{Z}} q^{n^2}$ be the classical theta function, where $q = e^{2\pi i z}$, $z \in \mathbb{C}$. Define $r(n)$ by

$$\sum_{n=0}^{\infty} r(n)q^n := \theta^3(z) = 1 + 6q + 12q^2 + 8q^3 + 6q^4 + 24q^5 + \ldots$$

It is well known that

$$r(n) = \begin{cases} 12H(4n) & \text{if } n \equiv 1,2 \pmod{4}, \\ 24H(n) & \text{if } n \equiv 3 \pmod{4}, \\ r(n/4) & \text{if } n \equiv 0 \pmod{4}, \\ 0 & \text{if } n \equiv 7 \pmod{4}, \end{cases} \tag{1}$$

where $H(N)$ is the Hurwitz–Kronecker class number for a natural number $N \equiv 0,3 \pmod{4}$. If $-N = D_k f^2$ where D_k is the discriminant of an imaginary quadratic field k, then $H(N)$ is related to the class number of k by the formula (see [1])

$$H(N) = \frac{h(k)}{\omega(k)} \sum_{d\mid f} \mu(d)\left(\frac{D_k}{d}\right)\sigma_1(f/d), \tag{2}$$

where $\omega(k)$ is half the number of units in $k = \mathbb{Q}(\sqrt{D_k})$, $\sigma_1(n)$ denotes the sum of the positive divisors of n, and $\mu(d)$ is the Möbius function defined by $\mu(d) = (-1)^k$ if d is equal to a product of k distinct primes (including $k = 0$) and $\mu(d) = 0$ otherwise.

Define $(U_{lp}\theta^3)(z)$, $(V_{lp}\theta^3)(z)$ and $(U_lV_p\theta^3)(z)$ in the usual way, i.e.,

$$
\begin{aligned}
(U_{lp}\theta^3)(z) &:= \sum_{n\ge 0} r(lpn)q^n = 1 + \sum_{n\ge 1} r(lpn)q^n,\\
(V_{lp}\theta^3)(z) &:= \sum_{n\ge 0} r(n)q^{lpn} = 1 + \sum_{n\ge 1} r(n)q^{lpn},\\
(U_lV_p\theta^3)(z) &:= \sum_{n\ge 0} r(nl)q^{np} = 1 + \sum_{n\ge 1} r(nl)q^{np}.
\end{aligned}
\tag{3}
$$

Then $U_{lp}\theta^3$, $V_{lp}\theta^3$, and $U_lV_p\theta^3$ are modular forms of weight $3/2$ on $\Gamma_0(4lp)$ with character $\left(\frac{4lp}{\cdot}\right)$ (see [10]).

To prove Theorem 1.1, we need the following lemmas.

LEMMA 2.1. *Let l and p be odd primes. If $\left(\frac{-np}{l}\right) = 1$ for some n, $1 \le n \le p$, then $r(npl^2) \equiv 0 \pmod{l}$.*

Proof. From (2), we have

$$r(npl^2) = r(np)\left(l + 1 - \left(\frac{-np}{l}\right)\right) = r(np)l \equiv 0 \pmod{l}. \ \blacksquare$$

LEMMA 2.2. *Let l be an odd prime such that $l \equiv 5$ or $7 \pmod 8$. Let p be an odd prime such that $p \equiv 1 \pmod 8$, $p \equiv -2 \pmod l$ and $\left(\frac{t}{p}\right) = 1$ for all prime t, $2 < t < l$. Then $r(nlp^2) \equiv 0 \pmod l$ for all n, $1 \le n < l$.*

Proof. From the assumption on l and p, we easily see that $\left(\frac{-nl}{p}\right) = -1$ for all n, $1 \le n < l$. Thus from (2), we have

$$r(nlp^2) = r(nl)\left(p + 1 - \left(\frac{-nl}{p}\right)\right) \equiv 0 \pmod l$$

for all n, $1 \le n < l$. $\blacksquare$

Similarly we have

LEMMA 2.3. *Let l be an odd prime such that $l \equiv 1$ or $3 \pmod 8$. Let p be an odd prime such that $p \equiv 1 \pmod 8$, $p \equiv -2 \pmod l$ and $\left(\frac{t}{p}\right) = 1$ for all prime t, $2 < t < l$. Then $r(nlp^2) \equiv -2r(nl) \pmod l$ for all n, $1 \le n < l$.*

If $g = \sum_{n=0}^{\infty} a(n)q^n$ has integer coefficients then define

$$\mathrm{ord}_l(g) := \min\{n : a(n) \not\equiv 0 \pmod l\}.$$

Let $M_k(\Gamma_0(N), \chi)$ be the space of modular forms of weight k on $\Gamma_0(N)$ with character χ. Sturm [11] proved that if $g \in M_k(\Gamma_0(N), \chi)$ has integer coefficients and

$$\mathrm{ord}_l(g) > \frac{k}{12}[\Gamma_0(1) : \Gamma_0(N)],$$

then $g \equiv 0 \pmod l$. He proved this for integral k and trivial χ but Kohnen and Ono [7] noted that this is also true for the general case.

Now we can prove Theorem 1.1. From now on we assume that $l > 3$ is an odd prime and p is an odd prime such that $p \equiv 1 \pmod 8$, $p \equiv -2 \pmod l$ and $\left(\frac{t}{p}\right) = 1$ for all prime t, $2 < t < l$.

Case I: $l \equiv 5$ or $7 \pmod 8$. First we claim that $(U_{lp}\theta^3)(z) \not\equiv (V_{lp}\theta^3)(z) \pmod l$. To see this, by (3), it is enough to show that the coefficients of q^{lp} in $(U_{lp}\theta^3)(z)$ and $(V_{lp}\theta^3)(z)$ are not congruent modulo l, i.e., $r(l^2p^2) \not\equiv 6 \pmod l$. From (1) and (2), we see that

$$r(l^2p^2) = 12H(4l^2p^2) = 6\left(l + 1 - \left(\frac{-4}{l}\right)\right)\left(p + 1 - \left(\frac{-4}{p}\right)\right).$$

Thus from the choice of l and p, we have

$$r(l^2p^2) \equiv \begin{cases} 0 \pmod l & \text{if } l \equiv 5 \pmod 8, \\ -24 \pmod l & \text{if } l \equiv 7 \pmod 8, \end{cases}$$

which proves the claim.

Now we note that the relevant Sturm bound for the modular forms in $M_{3/2}\big(\Gamma_0(4lp), \left(\frac{4lp}{\cdot}\right)\big)$ is $\frac{3}{4}(l+1)(p+1)$. Then by applying Sturm's theorem [11] to the modular form $g(z) = (U_{lp}\theta^3)(z) - (V_{lp}\theta^3)(z)$ in $M_{3/2}\big(\Gamma_0(4lp), \left(\frac{4lp}{\cdot}\right)\big)$, we find that there exists an integer d_{lp}, $1 \le d_{lp} \le \frac{3}{4}(l+1)(p+1) < lp$ (when $l, p \ge 7$ or $l = 5$, $p > 9$), such that $r(d_{lp}lp) \not\equiv 0 \pmod l$. From Lemma 2.2, we know that for such d_{lp}, $d_{lp}lp \ne nlp^2$ for any n, $1 \le n < l$. Furthermore from Lemma 2.1, we see that if $k = \mathbb{Q}(\sqrt{-d_{lp}lp})$ is the imaginary quadratic field and D_k is the discriminant of k then $\left(\frac{D_k}{l}\right) = 0$ or $\left(\frac{D_k}{l}\right) = -1$, i.e., l does not split in k. Thus we have the assertion of Theorem 1.1 for the case $l \equiv 5$ or $7 \pmod 8$.

Case II: $l \equiv 1$ or $3 \pmod 8$. Let $f(z) = (U_{lp}\theta^3)(z) + 2(U_lV_p\theta^3)(z)$ and $g(z) = 3(V_{lp}\theta^3)(z)$ be modular forms in $M_{3/2}\big(\Gamma_0(4lp), \left(\frac{4lp}{\cdot}\right)\big)$. Then we can also show that $f(z) \not\equiv g(z) \pmod l$. Similarly to Case I, from Sturm's theorem, Lemma 2.1, and Lemma 2.3, we can prove the desired statement.

Proof of Corollary 1.2. Let $l > 3$ be an odd prime. First we note that there exists a natural number r, $1 \le r \le 8l\prod t$, where the product runs over all primes t, $2 < t < l$, such that if a natural number $s \equiv r \pmod{8l\prod t}$, then $s \equiv 1 \pmod 8$, $s \equiv -2 \pmod l$ and $s \equiv 1 \pmod t$ for all primes t, $2 < t < l$. Then we easily see that if a prime p is in an arithmetic progression such that $p \equiv r \pmod{8l\prod t}$ then p satisfies the conditions in Theorem 1.1.

Let $p_1 < p_2 < \ldots$ be the primes in such an arithmetic progression in increasing order. Then in the notation from the proof of Theorem 1.1, if $i < j < k$ and D_i, D_j, D_k are the discriminants of the imaginary quadratic fields associated with $d_{lp_i}lp_i$, $d_{lp_j}lp_j$, $d_{lp_k}lp_k$ by (1) and (2), then at least two of them are different by Theorem 1.1. Moreover, it is obvious that $D_i > -3lp_i(l+1)(p_i+1) > -4l^2p_i^2$ (when $l, p_i \ge 7$ or $l = 5$, $p_i > 9$).

Thus from Dirichlet's theorem on primes in arithmetic progression, we have the corollary.

Acknowledgements. The author would like to thank W. Kohnen and K. Ono for showing him their preprints, and L. Washington for reminding him of Ono's work [9]. The author would also like to thank the referee for many helpful suggestions.

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, New York, 1995.

[2] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. London Ser. A 322 (1971), 405–420.

[3] P. Hartung, *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3*, J. Number Theory 6 (1974), 276–278.

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

[5] K. Horie and Y. Onishi, *The existence of certain infinite families of imaginary quadratic fields*, J. Reine Angew. Math. 390 (1988), 97–113.

[6] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257–258.

[7] W. Kohnen and K. Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate–Shafarevich groups of elliptic curves with complex multiplication*, Invent. Math. 135 (1999), 387–398.

[8] J. Nakagawa and K. Horie, *Elliptic curves with no rational points*, Proc. Amer. Math. Soc. 104 (1988), 20–24.

[9] K. Ono, *Indivisibility of class numbers of real quadratic fields*, Compositio Math., to appear.

[10] G. Shimura, *On modular forms of half-integral weight*, Ann. of Math. 97 (1973), 440–481.

[11] J. Sturm, *On the congruence of modular forms*, in: Lecture Notes in Math. 1240, Springer, 1984, 275–280.

[12] H. Taya, *Iwasawa invariants and class numbers of quadratic fields for the prime 3*, Proc. Amer. Math. Soc., to appear.

School of Mathematics
Korea Institute for Advanced Study
207-43 Cheongryangri-dong
Dongdaemun-gu
Seoul 130-012, Korea
E-mail: dhbyeon@kias.re.kr

Received on 16.11.1998
and in revised form on 26.1.1999 (3513)