Compositio Mathematica **126:** 249–256, 2001.

Indivisibility of Class Numbers and Iwasawa λ-Invariants of Real Quadratic Fields

DONGHO BYEON
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: 27 October 1999; accepted: 12 May 2000)

Abstract. Let $D > 0$ be the fundamental discriminant of a real quadratic field, and $h(D)$ its class number. In this paper, by refining Ono's idea, we show that for any prime $p > 3$,

$$\sharp\{0 < D < X \mid h(D) \not\equiv 0 \ (\text{mod p})\} >>_p \frac{\sqrt{X}}{\log X}.$$

Mathematics Subject Classification (2000). 11R29.

Key words. class numbers, Iwasawa λ-invariants.

1. Introduction

Let $D > 0$ be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{D})$, and $h(D)$ its class number. Let p be 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 $\mathbb{Q}(\sqrt{D})$. Let $R_p(D)$ denote the p-adic regulator of $\mathbb{Q}(\sqrt{D})$, and $|\cdot|_p$ denote the usual multiplicative p-adic valuation normalized so that $|p|_p = 1/p$.

Although the 'Cohen–Lenstra heuristics' [3] predict that for any prime p, there are infinitely many real quadratic fields $\mathbb{Q}(\sqrt{D})$ with $p \nmid h(D)$, it is proved only for the case $p < 5000$ ([4, 14]).

On the other hand, Greenberg [6] conjectured that $\lambda_p(\mathbb{Q}(\sqrt{D})) = 0$ for any real quadratic field $\mathbb{Q}(\sqrt{D})$ and any prime number p. However, very little is known (cf. [14]). In particular, Greenberg recently asked the question whether there exist infinitely many real quadratic fields $\mathbb{Q}(\sqrt{D})$ with p splitting and $\lambda_p(\mathbb{Q}(\sqrt{D}))$ vanishing for a given odd prime p (cf. [17]). This problem is solved only for the case $p = 3$ ([17]).

In this direction, in this paper we shall prove the following theorem:

THEOREM 1.1. *Let $p > 3$ be prime and $\delta = -1$ or 1. If $\delta = -1$, then for any $p \equiv 3$ (mod 4), and if $\delta = 1$, then for any p,*

$$\sharp\left\{0 < D < X \mid h(D) \not\equiv 0 \ (\text{mod } p),\ \left(\frac{D}{p}\right) = \delta,\ \textit{and } |R_p(D)|_p = \frac{1}{p}\right\} >>_p \frac{\sqrt{X}}{\log X}.$$

For the case $(D/p) = -1$, i.e., p remains prime in the real quadratic field $\mathbb{Q}(\sqrt{D})$, and $p \nmid h(D)$, we have $\lambda_p(\mathbb{Q}(\sqrt{D})) = 0$ by a criterion of Iwasawa [12]. Further for the case $(D/p) = 1$, i.e., p splits in the real quadratic field $\mathbb{Q}(\sqrt{D})$, $p \nmid h(D)$, and $|R_p(D)|_p = 1/p$, we also have $\lambda_p(\mathbb{Q}(\sqrt{D})) = 0$ by a criterion of Fukuda and Komatsu [5]. Thus, by Theorem 1.1 we immediately have the following theorem:

THEOREM 1.2. *Let $p > 3$ be prime and $\delta = -1$ or 1. If $\delta = -1$, then for any $p \equiv 3$ (mod 4), and if $\delta = 1$, then for any p,*

$$\sharp\left\{0 < D < X \mid \lambda_p(\mathbb{Q}(\sqrt{D})) = 0,\ \left(\frac{D}{p}\right) = \delta\right\} >>_p \frac{\sqrt{X}}{\log X}.$$

To prove Theorem 1.1, first we shall refine Ono's idea [14] and prove the following theorem.

THEOREM 1.3. *Let $p > 3$ be prime and $\delta = -1$ or 1. If there is a fundamental discriminant D_0 coprime to p of a real quadratic field $\mathbb{Q}(\sqrt{D_0})$ such that*

(i) $\left(\frac{D_0}{p}\right) = \delta$,

(ii) $h(D_0) \not\equiv 0 \bmod p$,

(iii) $|R_p(D_0)|_p = \frac{1}{p}$,

then for each δ,

$$\sharp\left\{0 < D < X \mid h(D) \not\equiv 0 \pmod p,\ \left(\frac{D}{p}\right) = \delta,\ \text{and } |R_p(D)|_p = \frac{1}{p}\right\} >>_p \frac{\sqrt{X}}{\log X}.$$

Finally, we shall show that the condition in Theorem 1.3 holds for any $p \equiv 3$ (mod 4) if $\delta = -1$ and for any p if $\delta = 1$.

Remark. Similar works for imaginary quadratic fields can be found in [1, 7–9, 13, 15].

2. Proof of Theorem 1.3

To prove Theorem 1.3, we shall basically follow the proof of Theorem 1 in [14]. Consult [14] for more details.

Let D be the fundamental discriminant of a quadratic number field, $\chi_D := (D/\cdot)$ the usual Kronecker character, and χ_0 the trivial character. Let $M_k(\Gamma_0(N), \chi)$ denote the space of modular forms of weight k on $\Gamma_0(N)$ with character χ. Let r and N be nonnegative integers with $r \geqslant 2$. If $N \not\equiv 0,\ 1 \pmod 4$, then let $H(r, N) = 0$. If

$N = 0$, then let $H(r, 0) := \zeta(1 - 2r)$. If $Dn^2 = (-1)^r N$, then define $H(r, N)$ by

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

where $\sigma_v(n) := \sum_{d|n} d^v$. Cohen [2] proved that for every $r \geqslant 2$,

$$F_r(z) := \sum_{N \geqslant 0} H(r, N)q^N \ (q := e^{2\pi iz}) \in M_{r+\frac{1}{2}}(\Gamma_0(4), \chi_0).$$

By the similar arguments as in the proof of Proposition 2 in [14], which use the construction of the Kubota–Leopoldt p-adic L-function $L_p(s, \chi_D)$, the Kummer congruences, and the p-adic class number formula (cf. [18]), we have the following proposition.

PROPOSITION 2.1. *Let p be an odd prime number and $D(\neq 1)$ be the fundamental discriminant of a real quadratic field. Then $H(p(p-1), D)$ is p-integral and*

$$H(p(p-1), D) \equiv \frac{2h(D)R_p(D)}{\sqrt{D}} \pmod{p^2}.$$

Let $\varepsilon_D > 1$ be the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{D})$. Then $R_p(D) = \log_p(\varepsilon_D)$. Let $p > 3$ be prime and $\mathbf{p}$ a prime ideal of $\mathbb{Q}(\sqrt{D})$ over p. Let $n(p, D)$ be a non negative integer satisfying that

$$\mathbf{p}^{n(p,D)} \mid \varepsilon_D^{N(\mathbf{p})-1} - 1 \quad \text{but} \quad \mathbf{p}^{n(p,D)+1} \nmid \varepsilon_D^{N(\mathbf{p})-1} - 1,$$

where N is the absolute norm of $\mathbb{Q}(\sqrt{D})$. Note that $n(p, D) \geqslant 1$. Since $|\varepsilon_D^{N(\mathbf{p})-1} - 1|_p = |\log_p(\varepsilon_D^{N(\mathbf{p})-1})|_p$, we have that

$$|R_p(D)|_p = \begin{cases} p^{-n(p,D)}, & \text{if } p \text{ is unramified,} \\ p^{-n(p,D)/2}, & \text{if } p \text{ is ramified.} \end{cases}$$

Thus, by Proposition 2.1 we immediately have the following proposition:

PROPOSITION 2.2. *Let $p > 3$ be prime and $D(\neq 1)$ be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{D})$ in which p is unramified. Then $H(p(p-1), D)/p$ is p-integral and*

$$\frac{H(p(p-1), D)}{p} \equiv \frac{2h(D)R_p(D)}{p\sqrt{D}} \pmod{p}.$$

Let $\delta = -1$ or 1. Let $p > 3$ be prime and define $G_p(z) \in M_{p(p-1)+\frac{1}{2}}(\Gamma_0(4p^2), \chi_0)$ by

$$G_p(z) := F_{p(p-1)}(z) \otimes \left(\frac{\cdot}{p}\right) = \sum_{n=0}^{\infty} \left(\frac{n}{p}\right) H(p(p-1), n)q^n,$$

https://doi.org/10.1023/A:1017561005538 Published online by Cambridge University Press

and $A_p^\delta(z) \in M_{p(p-1)+12}(\Gamma_0(4p^4), \chi_0)$ by

$$A_p^\delta(z) := \frac{G_p(z) \otimes (\frac{\cdot}{p}) + \delta G_p(z)}{2} = \sum_{(\frac{n}{p})=\delta} H(p(p-1), n)q^n.$$

Similary, for a prime $Q \neq p$, define $C_p^\delta(z) \in M_{p(p-1)+\frac{1}{2}}(\Gamma_0(4p^4Q^4), \chi_0)$ by

$$C_p^\delta(z) := \sum_{(\frac{n}{p})=\delta, (\frac{n}{Q})=-1} H(p(p-1), n)q^n.$$

If $l \neq p$ is prime, then define $(U_l|C_p^\delta)(z)$ and $(V_l|C_p^\delta)(z) \in M_{p(p-1)+\frac{1}{2}}(\Gamma_0(4p^4Q^4l), (\frac{4l}{\cdot}))$ by

$$(U_l|C_p^\delta)(z) := \sum_{n=1}^{\infty} u_{p,l}^\delta(n)q^n = \sum_{(\frac{n}{p})=\delta, (\frac{n}{Q})=-1} H(p(p-1), ln)q^n,$$

$$(V_l|C_p^\delta)(z) := \sum_{n=1}^{\infty} v_{p,l}^\delta(n)q^n = \sum_{(\frac{n}{p})=\delta, (\frac{n}{Q})=-1} H(p(p-1), n)q^{ln}.$$

By the similar arguments as in the proof of Proposition 3 in [14] and Proposition 2.2, we know that there exist $\alpha(p) \in \mathbb{Z}$ coprime to p such that $(\alpha(p))/p(U_l|C_p^\delta)(z)$ and $(\alpha(p))/p(V_l|C_p^\delta)(z)$ have integer Fourier coefficients.

Now we assume that there is a fundamental discriminant of real quadratic field of $\mathbb{Q}(\sqrt{D_0})$ for which

$$\left(\frac{D_0}{p}\right) = \delta \quad \text{and} \quad \frac{H(p(p-1), D_0)}{p} \not\equiv 0 \pmod{p}.$$

Let D_n be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{n})$ and S_p denote the set of those D_n with

$$n \leqslant \kappa(p) := (2p(p-1)+1)p^3Q^3(p+1)(Q+1)/4$$

for which

$$\left(\frac{n}{Q}\right) = -1 \quad \text{and} \quad \left(\frac{n}{p}\right) = \delta.$$

Let l be a sufficiently large prime satisfying $\chi_{D_0}(l) = 1$ and

(1) $\chi_{D_n}(l) = 1$ for every $D_n \in S_p$,

(2) $\left(\frac{l}{Q}\right) = 1$ and $\left(\frac{l}{p}\right) = 1$,

(3) $l \not\equiv 1 \pmod{p}$.

Then by the properties of l and the similar arguments in the proof of Theorem 2 in [14], which use a theorem of Sturm [16] on the congruence of modular forms, we have

https://doi.org/10.1023/A:1017561005538 Published online by Cambridge University Press

that there must be an integer $1 \leqslant n \leqslant \kappa(p)l$ coprime to l for which

$$\frac{\alpha(p)}{p} u_{p,l}^{\delta}(n) = \frac{\alpha(p)}{p} H(p(p-1), nl) \not\equiv 0 \pmod{p}.$$

Thus, by Proposition 2.2, we have the following proposition:

PROPOSITION 2.3. *Let $p > 3$ be prime and $\delta = -1$ or 1. Assume that there is a fundamental discriminant D_0 coprime to p of a real quadratic field $\mathbb{Q}(\sqrt{D_0})$ such that*

(i) $\left(\frac{D_0}{p}\right) = \delta,$

(ii) $h(D_0) \not\equiv 0 \bmod p,$

(iii) $|R_p(D_0)|_p = \frac{1}{p},$

If l is a sufficiently large prime satisfying $\chi_{D_0}(l) = 1$ and (1), (2), (3), then for each δ, there is a positive fundamental discriminant $D_l := d_l l$ with $d_l \leqslant \kappa(p)l$ such that

$$h(D_l) \not\equiv 0 \pmod{p}, \quad \left(\frac{D_l}{p}\right) = \delta, \quad \text{and} \quad |R_p(D_l)|_p = \frac{1}{p}.$$

Proof of Theorem 1.3. Let $r_p \pmod{t_p}$ be an arithmetic progression with $(r_p, t_p) = 1$ and $p|t_p$ such that for every prime $l \equiv r_p \pmod{t_p}$, l satisfies $\chi_{D_0}(l) = 1$ and (1), (2), (3). Then, by the similar arguments as in the proof of Theorem 1 in [14], which use Dirichlet's theorem on primes in arithmetic progression, Theorem 1.3 easily follows from Proposition 2.3. □

3. Proof of Theorem 1.1

Theorem 1.1 follows immediately from Theorem 1.3 and the following proposition.

PROPOSITION 3.1. *Let $p > 3$ be prime and $\delta = -1$ or 1. If $\delta = -1$, then for any $p \equiv 3 \pmod{4}$, let D be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{p^2 - 1})$ and if $\delta = 1$, then for any p, let D be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{p^2 + 4})$. Then for each δ, D satisfies the condition in Theorem 1.3, i.e.,*

(i) $\left(\frac{D_0}{p}\right) = \delta,$

(ii) $h(D_0) \not\equiv 0 \bmod p,$

(iii) $|R_p(D_0)|_p = \frac{1}{p},$

To prove Proposition 3.1, we need the following lemmas:

https://doi.org/10.1023/A:1017561005538 Published online by Cambridge University Press

LEMMA 3.2 (L. K. Hua [10]). *Let D be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{D})$ and $L(s, \chi_D)$ be the Dirichlet L-function with character χ_D. Then*

$$L(1, \chi_D) < \frac{\log D}{2} + 1.$$

LEMMA 3.3 ([11]). *Let p be an odd prime and $\mathbf{p}$ a prime ideal of the real quadratic field $\mathbb{Q}(\sqrt{D})$ over p. If α is an element of $\mathbb{Q}(\sqrt{D})$ such that $\alpha^n \equiv 1 \bmod \mathbf{p}$ but $\alpha^n \not\equiv 1 \bmod \mathbf{p}^2$ for some integer n, then we have $\alpha^{N(\mathbf{p})-1} \not\equiv 1$ mod $\mathbf{p}^2$.*

Proof of Proposition 3.1. (i). If $\delta = 1$, then since

$$\left(\frac{Df^2}{p}\right) = \left(\frac{p^2+4}{p}\right) = \left(\frac{4}{p}\right) = 1 \quad (f \in \mathbb{Z}),$$

we have $(D/p) = 1$ for any p. If $\delta = -1$, then since

$$\left(\frac{Df^2}{p}\right) = \left(\frac{p^2-1}{p}\right) = \left(\frac{-1}{p}\right) \quad (f \in \mathbb{Z}),$$

we have $(D/p) = -1$ for any $p \equiv 3 \pmod 4$.

(ii) Dirichlet's class number formula says that

$$h(D) = \frac{\sqrt{D}L(1, \chi_D)}{2\log \varepsilon_D}.$$

By Lemma 3.2, we have that

$$h(D) < \sqrt{D} \cdot \frac{(2 + \log\sqrt{D})}{4 \log \varepsilon_D} < \sqrt{D} \cdot \frac{(2 + \log\sqrt{D})}{2\log(D/4)},$$

because $\varepsilon_D > \sqrt{D}/2$.

Let D be the fundamental discriminant of $\mathbb{Q}(\sqrt{p^2-1})$ or $\mathbb{Q}(\sqrt{p^2+4})$. Then by easy computation, we have $h(D) < p$ if $p \geqslant 11$. Since we can also easily check that $h(D) < p$, if $p < 11$, we prove that $p \nmid h(D)$ for any p.

(iii) Let $\delta = 1$ and D be the fundamental discriminant of the real quadratic field $\mathbb{Q}(\sqrt{p^2+4})$. Let $\varepsilon_D > 1$ be the fundamental unit of $\mathbb{Q}(\sqrt{p^2+4})$ and $\alpha := (p + \sqrt{p^2+4})/2$. Since $N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha) = -1$ and $\alpha > 1$, $\alpha = \varepsilon_D^j$ for some odd $j > 0$. Since

$$\left(\frac{p+\sqrt{p^2+4}}{2}\right)^{p-1} - 1 = p\left(\left(\frac{p-1}{2}\right)\left(\frac{p+\sqrt{p^2+4}}{2}\right)^{p-2} + p(*)\right),$$

we have that

$$\alpha^{p-1} = \varepsilon_D^{j(p-1)} \equiv 1 \bmod \mathbf{p}, \quad \text{but} \quad \alpha^{p-1} = \varepsilon_D^{j(p-1)} \not\equiv 1 \bmod \mathbf{p}^2.$$

https://doi.org/10.1023/A:1017561005538 Published online by Cambridge University Press

Thus, by Lemma 3.3 and the discussion above in Proposition 2.2, we have that $|R_p(D)|_p = 1$.

Now, we consider the case $\delta = -1$ and D is the fundamental discriminant of $\mathbb{Q}(\sqrt{p^2 - 1})$. In this case, if we let $\alpha := p + \sqrt{p^2 - 1}$, then by the same method, we can also prove that $|R_p(D)|_p = 1$. □

Acknowledgements

The author would like to thank K. Ono for kindly answering his questions and J. H. Oh for helpful discussion.

References

1. Byeon, D.: A note on the basic Iwasawa λ-invariants of imaginary quadratic fields and congruence of modular forms, *Acta Arith.* **89** (1999), 295–299.
2. Cohen, H.: Sums involving the values at negative integers of L-functions of quadratic characters, *Math. Ann.* **217** (1975), 271–285.
3. Cohen, H. and Lenstra, H. W.: Heuristics on class groups of number fields, In: *Number Theory* (Noordwijkerhout 1983), Lecture Notes in Math. 1068, Springer, New York, 1984, pp. 33–62
4. Davenport, H. and Heilbronn, H.: On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), 405–420.
5. Fukuda, T. and Komatsu, K.: On the λ-invariants of $\mathbb{Z}_p$-extensions of real quadratic fields, *J. Number Theory* **23** (1986), 238–242.
6. Greenberg, R.: On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98** (1976), 263–284.
7. Hartung, P.: 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.
8. Horie, K.: A note on basic Iwasawa λ-invariants of imaginary quadratic fields, *Invent. Math.* **88** (1987), 31–38.
9. Horie, K. and Onishi, Y.: The existence of certain infinite families of imaginary quadratic fields, *J. Reine Angew. Math.* **390** (1988), 97–113.
10. Hua, L.-K.: On the least solution of Pell's equation, *Bull. Amer. Math. Soc.* **48** (1942), 731–735.
11. Ichimura, H.: A note on Greenberg's conjecture and the abc conjecture, *Proc. Amer. Math. Soc.* **126** (1998), 1315–1320.
12. Iwasawa, H.: A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258.
13. Kohnen, W. and Ono, K.: 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.
14. Ono, K.: Indivisibility of class numbers of real quadratic fields, *Compositio Math.* **119** (1999), 1–11.
15. Ono, K. and Skinner, C.: Fourier coefficients of half-integral weight modular forms modulo l, *Ann. Math.* **147** (1998), 453–470 .
16. Sturm, J.: On the congruence of modular forms, In: *Lecture Notes in Math.* 1240, Springer, New York, 1984, pp. 275–280.

17. Taya, H.: Iwasawa invariants and class numbers of quadratic fields for the prime 3, *Proc. Amer. Math. Soc.* **128** (2000), 1285–1292.
18. Washington, L.: *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, Berlin, 1982.