ACTA ARITHMETICA
110.1 (2003)

# A note on the existence of certain infinite families of imaginary quadratic fields

by

Iwao Kimura (Toyama)

**1. Introduction.** In this paper, we give a lower bound of the number of certain families of imaginary quadratic fields whose absolute value of discriminants are less than a given number (the main result is the corollary below). We briefly review the investigations concerned with this kind of problems.

Let $\mathbb{Z}$ be the ring of rational integers, and $\mathbb{Q}$ the field of rational numbers. For any rational prime $l$, we denote by $\mathbb{Z}_l$ the ring of $l$-adic integers. If $k$ is an algebraic number field of finite degree over $\mathbb{Q}$, we denote by $h(k)$ the class number of $k$ and by $D(k)$ the discriminant of $k$. We let $\sharp S$ denote the cardinality of any set $S$. Let $(\cdot/\cdot)$ be the Legendre–Kronecker symbol.

Denote by $\mathcal{Q}^-$ the set of all imaginary quadratic fields and by $\mathcal{Q}^+$ the set of all real quadratic fields. For any real number $X > 0$, let $\mathcal{Q}^-(X) = \{k \in \mathcal{Q}^-;\ -X < D(k)\}$ and $\mathcal{Q}^+(X) = \{k \in \mathcal{Q}^+;\ D(k) < X\}$. Note that $\mathcal{Q}^-(X)$ and $\mathcal{Q}^+(X)$ are finite sets.

Hartung [13] proved that $\{k \in \mathcal{Q}^-;\ 3 \nmid h(k)\}$ is an infinite set, and remarked that his method (an application of Kronecker's class number relation) can be applied to the same statement in which 3 is replaced by any odd prime $l$. The case of $l = 3$ is also implied in Davenport–Heilbronn's investigation [10, 11] of mean 3-class numbers of quadratic fields.

Kohnen and Ono [20] obtained a lower bound of $\sharp\{k \in \mathcal{Q}^-(X);\ l \nmid h(k)\}$ where $l \geq 5$ is any prime. This is a quantitative refinement of Hartung's result. Ono [26] and Byeon [3] also obtained a similar estimate for real quadratic fields for primes $l \geq 5$.

Cohen and Lenstra [8] conjectured the "density"

$$\lim_{X\to\infty} \frac{\sharp\{k \in \mathcal{Q}^-(X);\ l \nmid h(k)\}}{\sharp\mathcal{Q}^-(X)} = \prod_{n\geq 1}(1 - l^{-n}),$$

2000 *Mathematics Subject Classification*: Primary 11R29; Secondary 11R11.

Partially supported by Grant-in-Aid for Young Scientists (B), 14740009, The Ministry of Education, Culture, Sports, Science and Technology, Japan.

$$\lim_{X\to\infty}\frac{\sharp\{k\in\mathcal{Q}^+(X);\, l\nmid h(k)\}}{\sharp\mathcal{Q}^+(X)}=\prod_{n\geq 2}(1-l^{-n}).$$

The results cited above are far from these conjectured values.

For any number field $k$ of finite degree over $\mathbb{Q}$ and any rational prime $l$, $\lambda_l(k)$, $\mu_l(k)$ denote the Iwasawa $\lambda$ and $\mu$ invariants of the basic $\mathbb{Z}_l$-extension over $k$. It is known (Iwasawa [18]) that if $l\nmid h(k)$ and $l$ does not split at all in $k$, then $\lambda_l(k)=\mu_l(k)=0$.

Horie and Horie–Ônishi [14, 17, 15] proved that there exist infinitely many $k\in\mathcal{Q}^-$ which satisfy $l\nmid h(k)$ and certain ramification conditions (e.g. $(D(k)/l)\neq 1$) if $l$ is sufficiently large prime. The method they used involves an $l$-adic Galois representation arising from Jacobians of certain modular curves and trace formulae for Hecke operators acting on certain spaces of cusp forms. They deduced, by means of Iwasawa's theorem cited above, that $\{k\in\mathcal{Q}^-;\, \lambda_l(k)=\mu_l(k)=0\}$ is an infinite set (for any abelian number field $k$ and any rational prime $l$, it is known by Ferrero–Washington that $\mu_l(k)=0$). Naito [23, 24] extended some parts of their results to the case of relative class numbers of CM-fields, and deduced similar statements for relative $\lambda$ and $\mu$ invariants.

Nakagawa–Horie [25] refined Davenport–Heilbronn's arguments and obtained estimates of

$$\liminf_{X\to\infty}\frac{\sharp\{k\in\mathcal{Q}^-(X);\, 3\nmid h(k),\,(D(k)/3)\neq 1\}}{\sharp\mathcal{Q}^-(X)}$$

and

$$\liminf_{X\to\infty}\frac{\sharp\{k\in\mathcal{Q}^+(X);\, 3\nmid h(k),\,(D(k)/3)\neq 1\}}{\sharp\mathcal{Q}^+(X)}.$$

By Iwasawa's theorem, these values are lower bounds of

$$\liminf_{X\to\infty}\frac{\sharp\{k\in\mathcal{Q}^-(X);\, \lambda_3(k)=\mu_3(k)=0\}}{\sharp\mathcal{Q}^-(X)}$$

and

$$\liminf_{X\to\infty}\frac{\sharp\{k\in\mathcal{Q}^+(X);\, \lambda_3(k)=\mu_3(k)=0\}}{\sharp\mathcal{Q}^+(X)}. \tag{1}$$

It is a longstanding conjecture (so-called Greenberg's conjecture [12]) that $\lambda_l(k)=0$ for any rational prime $l$ if $k$ is totally real. The real quadratic case of Nakagawa–Horie's investigation provides some evidence for the conjecture. Taya [29] improved their result and showed that the value of (1) is $\geq 17/24$. Nakagawa–Horie's result is also extended to a more general situation of quadratic extensions over a fixed number field case by Horie and the author [16], and to the fixed function field case by the author [19], using the theory of zeta functions associated to a certain prehomogeneous vector space (the space of binary cubic forms) developed by Datskovsky and Wright [9].

Belabas and Fouvry [1] refined Davenport and Heilbronn's investigations and estimated $\sharp\{k \in \mathcal{Q}^+(X);\ 3 \nmid h(k)$ and $D(k)$ is a rational prime$\}$.

Byeon [4] extended the investigation of Kohnen–Ono so that it covers the cases treated by Horie [14]. He obtained

$$\sharp\{k \in \mathcal{Q}^-(X);\ \lambda_l(k) = \mu_l(k) = 0\} \gg_{l,\varepsilon} \sqrt{X}/\log X$$

for any odd prime $l \geq 5$ and any real number $\varepsilon > 0$ (the subscript on $\gg$ means that the implied constant depends on the stated variables). Ono [26] and Byeon [3, 5] also discussed the case of real quadratic fields and obtained similar lower bounds. Their method relies on the fact that the coefficients of $\theta^3(z)$, where $\theta(z) = \sum_{n\in\mathbb{Z}} q^{n^2}$, are closely related to class numbers of quadratic forms, and on Sturm's theorem [28] on congruences of modular forms.

In this paper, we give a quantitative version of the investigation of Horie–Ônishi [17] and Horie [15] (the main result is the corollary below). We use Eisenstein series of half integral weight constructed by Cohen [6] and Sturm's theorem. We note that Bruinier (Theorem 7 in [2]) gave a similar result.

**Acknowledgements.** The author thanks the anonymous referee for his careful reading of the manuscript.

## 2. Results

THEOREM. *Let $l > 3$ be an odd prime. Let $S_0, S_+, S_-$ be mutually disjoint finite sets of rational primes. Take an integer $b > 0$ which satisfies the following conditions*: *$-b$ is a fundamental discriminant*, *$(-b/q) = 0, 1, -1$ according as $q \in S_0, S_+, S_-$ respectively* (*where $(\cdot/\cdot)$ is the Legendre–Kronecker symbol*). *Let $P = 4\prod_{q\in S_0\cup S_+\cup S_-} q$. For any prime $p$ which satisfies $p^2 \equiv 1 \pmod{P}$ and $(-b/p) \not\equiv p \pmod{l}$, let $\kappa = \frac{1}{2}pP^2\prod_{q\mid pP}(1+q^{-1})$. Then there exists a natural number $m_p < \kappa$ which satisfies the following conditions*: *the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-m_p})$ is not divisible by $l$*, *every prime $q \in S_0$ ramifies*, *every prime $q \in S_+$ splits and every prime $q \in S_-$ is inert*, *in $\mathbb{Q}(\sqrt{-m_p})$*, *respectively.*

COROLLARY. *Let $l > 3$ be an odd prime*, *and $\varepsilon > 0$ be an arbitrary real number. Let $S_0, S_+, S_-$ and $P$ be as in the Theorem. Then*, *for any sufficiently large $X > 0$*, *we have*

$$\sharp\{k \in \mathcal{Q}^-(X);\ l \nmid h(k) \textit{ and } (*) \textit{ holds}\} \gg_{l,\varepsilon,P} \sqrt{X}/\log X,$$

*where*

(*) *every prime $q \in S_0$ ramifies*, *every prime $q \in S_+$ splits and every prime $q \in S_-$ is inert in $k$* (*the implied constants depend on the variables in the subscript*).

Remark. An application of this kind of result is, as mentioned above, to give an estimate of $\sharp\{k \in \mathcal{Q}^-(X);\ \lambda_l(k) = \mu_l(k) = 0\}$. We give another one. B. Mazur [21] proved that if there exist imaginary quadratic fields $k$ such that $5 \nmid h(k)$ and $(D(k)/11) \neq 1$, then the 5 primary part $Ш(X_0(11), k)\{5\}$ of the Tate–Shafarevich group of a modular curve $X_0(11)$ of level 11 over $k$ is 0. It thus follows from our corollary that

$$\sharp\{k \in \mathcal{Q}^-(X);\ Ш(X_0(11), k)\{5\} = \{0\}\} \gg \sqrt{X}/\log X.$$

**3. Proofs.** Let $g(z) = \sum_{n=0}^{\infty} a(n)q^n$ be any formal power series of an indeterminate $q$ with rational integer coefficients. For any rational prime $p$, we define $(U_p g)(z), (V_p g)(z)$ by

$$(U_p g)(z) = \sum_{n=0}^{\infty} a(pn)q^n, \qquad (V_p g)(z) = \sum_{n=0}^{\infty} a(n)q^{pn}.$$

We define the order $\mathrm{ord}_l(g)$ of $g$ at rational prime $l$ by

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

Let $h(z) = \sum_{n=0}^{\infty} b(n)q^n$ be another formal power series with rational integer coefficients, and $m$ be any rational integer. We define $g(z) \equiv h(z) \pmod{m}$ if and only if $a(n) \equiv b(n) \pmod{m}$ for all $n \geq 0$.

For any half integer $k \in \frac{1}{2}\mathbb{Z}$ and natural number $N$ (if $k \notin \mathbb{Z}$ we assume that $4 \mid N$), let $M_k(N, \chi)$ denote the space of modular forms of weight $k$, Nebentypus character $\chi$, with respect to a congruence subgroup $\Gamma_0(N)$ (cf. Shimura [27]). If $\chi$ is the trivial character, we write $M_k(N)$ instead of $M_k(N, 1)$. Let $g(z) \in M_k(N, \chi)$ have Fourier expansion $g(z) = \sum_{n=0}^{\infty} a(n)q^n$. It is known that $(U_p g)(z), (V_p g)(z) \in M_k(Np, \chi(p/\cdot))$.

Sturm [28] proved that if $g(z) \in M_k(N, \chi)$ has rational integer coefficients and

$$\mathrm{ord}_l(g) > \kappa(N, k) = \frac{k}{12}\,[\Gamma_0(1) : \Gamma_0(N)] = \frac{k}{12}\,N \prod_{q \mid N}(1 + q^{-1}),$$

then $g(z) \equiv 0 \pmod{l}$. He proved this fact when $k$ is an integer (a detailed proof can be found in Murty [22]), but Kohnen–Ono [20] pointed out that it is easy to verify this fact when $k$ is a half integer.

Let $H(n)$ denote the Hurwitz–Kronecker class number of integral binary quadratic forms of discriminant $-n$ ($-n \equiv 0, 1 \pmod{4}$). If $-n = Df^2$ where $D$ is a negative fundamental discriminant, then $H(n)$ is related to the class number $h(D)$ of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ by the well-known formula

$$H(n) = \frac{h(D)}{w(D)} \sum_{d \mid f} \mu(d)\left(\frac{D}{d}\right)\sigma_1\left(\frac{f}{d}\right).$$

Here $w(D)$ is half the number of roots of unity in $\mathbb{Q}(\sqrt{D})$, $\mu(\cdot)$ is the Möbius function, $(\cdot/\cdot)$ is the Kronecker–Legendre symbol, and $\sigma_1(\cdot)$ is the sum of positive divisors (cf. Cohen [7, Chapter 5.3]).

Let $c, d \in \mathbb{Z}$ with $d \geq 1$. Suppose that $-c$ is a quadratic non-residue modulo $d$ (i.e., the equation $x^2 \equiv -c \pmod{d}$ has no solutions). Then we define a function $\mathcal{H}^{c,d}(z)$ by

$$\mathcal{H}^{c,d}(z) = \sum_{n \equiv c \pmod{d}} H(n) q^n \qquad (q = e^{2\pi\sqrt{-1}z}).$$

It is known that $\mathcal{H}^{c,d}(z) \in M_{3/2}(A)$ where $A = 4d^2$ ($A$ can be taken to be $d^2$ if $d$ is even) by Cohen [6].

We define $f(z) = 6\mathcal{H}^{b,P}(z)$ where $b, P$ are the same as in the Theorem. The coefficients of $f(z)$ are rational integers since $H(0) = -1/12$ does not appear in $f(z)$.

Lemma. *Let $p$ be a rational prime satisfying $p^2 \equiv 1 \pmod{P}$, $p \not\equiv (-b/p) \pmod{l}$. Then*

$$(U_p f)(z) \not\equiv (V_p f)(z) \pmod{l}.$$

*Proof.* We see, by definition,

$$(U_p f)(z) = 6 \sum_{pn \equiv b \pmod{P}} H(pn) q^n \in M_{3/2}(4P^2 p),$$

$$(V_p f)(z) = 6 \sum_{n \equiv b \pmod{P}} H(n) q^{pn} \in M_{3/2}(4P^2 p).$$

The $bp$th coefficients of $(U_p f)(z)$ and $(V_p f)(z)$ are respectively $H(bp^2) = (1 + p - (-b/p))H(b)$ and $H(b)$. Note that $H(bp^2)$ appears in $(U_p f)(z)$ because $bp^2 \equiv b \pmod{P}$. By our assumptions, these two coefficients are not congruent modulo $l$. ∎

*Proof of the Theorem.* By the Lemma and Sturm's theorem stated above, there exists a natural number $n_p < \kappa(4P^2 p, 3/2) = \frac{1}{2} P^2 p \prod_{q \mid pP}(1 + q^{-1})$ such that the $n_p$th coefficient of $(U_p f)(z) - (V_p f)(z)$ is not congruent to 0 (mod $l$), i.e.,

$$H(pn_p) \not\equiv H\left(\frac{n_p}{p}\right) \pmod{l}.$$

If $p \nmid n_p$, we read that the $n_p$th coefficient $H(n_p/p)$ of $(V_p f)(z)$ is 0. Thus

$$H(pn_p) \not\equiv 0 \pmod{l}.$$

Since $pn_p \equiv b \pmod{P}$, we also see that

$$\left(\frac{-pn_p}{q}\right) = \left(\frac{-b}{q}\right) = 0, 1, -1 \qquad \text{according as } q \in S_0, S_+, S_-.$$

On the other hand, if $n_p = pn'_p$ for some natural number $n'_p$, then

$$H(pn_p) = H(p^2 n'_p) = \left(1 + p - \left(\frac{-n'_p}{p}\right)\right) H(n'_p) \not\equiv H(n'_p) \pmod{l},$$

and $H(n'_p) \not\equiv 0 \pmod{l}$ follows. Further we have $n'_p = pn_p/p^2 \equiv pn_p \pmod{P}$ since $p^2 \equiv 1 \pmod{P}$. This shows that

$$\left(\frac{-n'_p}{q}\right) = \left(\frac{-pn_p}{q}\right) = \left(\frac{-b}{q}\right) = 0, 1, -1 \qquad \text{according as } q \in S_0, S_+, S_-.$$

Taking $m_p = pn_p$ or $n'_p$ according as $p \nmid n_p$ or not, we can prove the Theorem. ∎

*Proof of the Corollary.* It is easy to see that the conditions on $p$ stated in the Theorem are equivalent to the condition that $p$ belongs to some arithmetic progression modulo $P$. Let $p_1 < p_2 < \ldots$ be the primes contained in one of such arithmetic progressions modulo $P$, taken in increasing order. Then, if $i < j < k$ and $D_i, D_j, D_k$ are the discriminants of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-m_{p_i}}), \mathbb{Q}(\sqrt{-m_{p_j}}), \mathbb{Q}(\sqrt{-m_{p_k}})$, then at least two of them are different by the Theorem.

Moreover, clearly $D_i \ge -p_i \kappa(4P^2 p_i, 3/2)$. The result now follows by Dirichlet's theorem on arithmetic progressions. ∎

## References

[1] K. Belabas et E. Fouvry, *Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier*, Duke Math. J. 98 (1999), 217–268.

[2] J. H. Bruinier, *Nonvanishing modulo l of Fourier coefficients of half-integral weight modular forms*, ibid. 98 (1999), 595–611.

[3] D. Byeon, *Class numbers and Iwasawa invariants of certain totally real number fields*, J. Number Theory 79 (1999), 249–257.

[4] —, *A note on basic Iwasawa $\lambda$-invariants of imaginary quadratic fields and congruence of modular forms*, Acta Arith. 89 (1999), 295–299.

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

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

[7] —, *A Course in Computational Algebraic Number Theory*, Springer, Berlin, 1993.

[8] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, in: Number Theory (Noordwijkerhout, 1983), Springer, Berlin, 1984, 33–62.

[9] B. Datskovsky and D. J. Wright, *Density of discriminants of cubic extensions*, J. Reine Angew. Math. 386 (1988), 116–138.

[10] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields*, Bull. London Math. Soc. 1 (1969), 345–348.

[11] —, —, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A 322 (1971), 405–420.

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

[13] 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.

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

[15] —, *Trace formulae and imaginary quadratic fields*, Math. Ann. 288 (1990), 605–612.

[16] K. Horie and I. Kimura, *On quadratic extensions of number fields and Iwasawa invariants for basic $\mathbb{Z}_3$-extensions*, J. Math. Soc. Japan 51 (1999), 387–402.

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

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

[19] I. Kimura, *On class numbers of quadratic extensions over function fields*, Manuscripta Math. 97 (1998), 81–91.

[20] 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.

[21] B. Mazur, *On the arithmetic of special values of L functions*, ibid. 55 (1979), 207–240.

[22] M. R. Murty, *Congruences between modular forms*, in: Analytic Number Theory (Kyoto, 1996), London Math. Soc. Lecture Note Ser. 247, Cambridge Univ. Press, Cambridge, 1997, 309–320.

[23] H. Naito, *Indivisibility of class numbers of totally imaginary quadratic extensions and their Iwasawa invariants*, J. Math. Soc. Japan 43 (1991), 185–194.

[24] —, *Erratum to "Indivisibility of class numbers of totally imaginary quadratic extensions and their Iwasawa invariants"*, ibid. 46 (1994), 725–726.

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

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

[27] G. Shimura, *On modular forms of half integral weight*, Ann. of Math. (2) 97 (1973), 440–481.

[28] J. Sturm, *On the congruence of modular forms*, in: Number Theory (New York, 1984–1985), Lecture Notes in Math. 1240, Springer, Berlin, 1987, 275–280.

[29] H. Taya, *Iwasawa invariants and class numbers of quadratic fields for the prime 3*, Proc. Amer. Math. Soc. 128 (2000), 1285–1292.

Department of Mathematics
Faculty of Science
Toyama University
Gofuku 3190, Toyama city
Toyama 930-0885, Japan
E-mail: iwao@sci.toyama-u.ac.jp

*Received on 12.4.2002*
*and in revised form on 6.12.2002* (4260)