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

Dongho Byeon

School of Mathematical Sciences, Seoul National University
Seoul 151-742, Korea
E-mail address: dhbyeon@math.snu.ac.kr

Let $D < 0$ be the fundamental discriminant of a imaginary quadratic field, and $h(D)$ its class number. In this paper, we show that for any prime $p > 3$ and $\epsilon = -1, 0, \text{ or } 1$,

$$\# \{-X < D < 0 \mid h(D) \not\equiv 0 \pmod{p} \text{ and } \left(\frac{D}{p}\right) = \epsilon\} \gg_p \sqrt{X \log X}.$$ 

1 Introduction and statement of results

Let $p$ be a prime number. Let $D < 0$ be the fundamental discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ and $h(D)$ its class number.

In [4], using Kronecker’s class number relation and some trace formulae of Eichler and of Yamauchi combined with the $p$-adic Galois representaions attached to the Jacobian varites of certain modular curves, Horie and Ōnishi proved the following theorem.

**Theorem (Horie and Ōnishi)** Let $\epsilon = -1, 0, \text{ or } 1$. Then there exist infinitely many fundamental discriminants $D$ of imaginary quadratic fields such that

$$h(D) \not\equiv 0 \pmod{p} \text{ and } \left(\frac{D}{p}\right) = \epsilon.$$
Here (−) denotes as usual the kronecker symbol.

Recently Brunier [1] also proved this theorem by using an application of the $q$-expansion principle of arithmetic algebraic geometry.

In this note, as the author’s previous work [2], refining Kohnen and Ono’s method [3,5] which use Sturm’s result [6] on the congruence of modular forms, we will give another proof of the above theorem and go a step further by obtaining the following estimate.

**Theorem 1.1** Let $p > 3$ be prime and $\epsilon = -1, 0, 1$. Then

$$\# \{ -X < D < 0 \mid h(D) \not\equiv 0 \pmod{p} \text{ and } \left(\frac{D}{p}\right) = \epsilon \} \gg_p \frac{\sqrt{X}}{\log X}.$$  

2 Proof of Theorem 1.1

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

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

It is well known that

$$r(n) = \begin{cases} 12H(4n) & \text{if } n \equiv 1, 2 \pmod{4} \\ 24H(n) & \text{if } n \equiv 3 \pmod{8} \\ r(n/4) & \text{if } n \equiv 0 \pmod{4} \\ 0 & \text{if } n \equiv 7 \pmod{8}, \end{cases}$$  

where $H(N)$ is the Hurwitz-Kronecker class number for a natural number $N \equiv 0, 3 \pmod{4}$. If $-N = Df^2$ where $D$ is the fundamental discriminant of an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$, then $H(N)$ is related to class number of $\mathbb{Q}(\sqrt{D})$ by the formula

$$H(N) = \frac{h(D)}{\omega(D)} \sum_{d|f} \mu(d)\left(\frac{D}{d}\right)\sigma_1(f/d),$$  

where $\omega(D)$ is half the number of units in $\mathbb{Q}(\sqrt{D})$, $\sigma_1(n)$ denotes the sum of the positive divisors of $n$ and $\mu(d)$ is Möbius function.
Case I: $\epsilon = \pm 1$.

For $k \in \frac{1}{2}\mathbb{Z}$ and $N \in \mathbb{N}$ (with $4|N$ if $k \not\in \mathbb{Z}$), let $M_k(\Gamma_0(N), \chi)$ denote the space of modular forms weight $k$ on $\Gamma_0(N)$ with Nebentypus character $\chi$. Let $\chi_0$ denote the trivial character.

Define $A_p(z) \in M_3(\Gamma_0(4p^2), \chi_0)$ by

$$A_p(z) := \theta^3(z) \otimes \left( \frac{1}{p} \right) = \sum_{n=0}^{\infty} \left( \frac{n}{p} \right) r(n)q^n,$$

and $A_{p,\epsilon}^\prime(z) \in M_3(\Gamma_0(4p^4), \chi_0)$ by

$$A_{p,\epsilon}^\prime(z) := \frac{A_p(z) \otimes \left( \frac{1}{p} \right) + \epsilon A_p(z)}{2} = \sum_{(2) = \epsilon} r(n)q^n.$$

Let $l$ be an odd prime and define $(U_l|A_{p,\epsilon}^\prime)(z), (V_l|A_{p,\epsilon}^\prime)(z) \in M_3(\Gamma_0(4p^4l), (\frac{4}{l}))$ in the usual way,

$$\begin{align*}
(U_l|A_{p,\epsilon}^\prime)(z) &:= \sum_{n=0}^{\infty} u_{p,l}^\epsilon(n)q^n = \sum_{(2) = \epsilon} r(ln)q^n, \\
(V_l|A_{p,\epsilon}^\prime)(z) &:= \sum_{n=0}^{\infty} v_{p,l}^\epsilon(n)q^n = \sum_{(2) = \epsilon} r(n)q^{ln}.
\end{align*}$$

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

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

Sturm [6] proved that if $g \in M_k(\Gamma_0(N), \chi)$ has integer coefficients and

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

then $g \equiv 0 \pmod{l}$.

Let $\kappa(p) := 3p^3(p+1)$. For a positive integer $n$, let $D_n$ be the fundamental discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$. Let $S_p^\epsilon$ denote the set of those $D_n$ with $n \leq \kappa(p)$ for which $\left( \frac{n}{p} \right) = \epsilon$.

If $l$ is an odd prime such that $\left( \frac{D_n}{l} \right) = -1$ for all $D_n \in S_p^\epsilon$ and $\left( \frac{4}{p} \right) = 1$, then by (2), the multiplicative property for $H(N)$, we have for all $n \leq \kappa(p)$ with $\left( \frac{n}{p} \right) = \epsilon$,

$$u_{p,l}^\epsilon(nl) = (l+2)v_{p,l}^\epsilon(nl).$$
Lemma 2.1  Let \( p > 3 \) be prime. If \( l \) is an odd prime such that \( l \not\equiv -2 \pmod{p} \) and \( \left(\frac{l}{p}\right) = 1 \), then

\[
(U_l|A_p^\epsilon)(z) - (l + 2)(V_l|A_p^\epsilon)(z) \not\equiv 0 \pmod{p}.
\]

**Proof:** For the case \( \epsilon = 1 \), by (2) we easily see that \( u_{p,l}^1(l^3) \not\equiv (l + 2)v_{p,l}^1(l^3) \pmod{p} \). For the case \( \epsilon = -1 \), we choose an integer \( 1 < s < p \) such that \( \left(\frac{s}{p}\right) = -1 \). Let \( D_s \) be the fundamental discriminant of the imaginary quadratic field \( \mathbb{Q}(\sqrt{-s}) \). Then \( h(D_s) < p \), i.e., \( h(D_s) \not\equiv 0 \pmod{p} \). Thus by (2) we also easily see that \( u_{p,l}^{-1}(sl^3) \not\equiv (l + 2)v_{p,l}^{-1}(sl^3) \pmod{p} \).

From Sturm’s theorem [6], Lemma 2.1 and the relations (1) (2), we immediately have the following proposition.

**Proposition 2.2** Let \( p > 3 \) be prime and \( \epsilon = -1 \) or \( 1 \). If \( l \) is a sufficiently large prime satisfying

(i) \( \left(\frac{D_n}{l}\right) = -1 \) for all \( D_n \in S_p^\epsilon \),

(ii) \( l \not\equiv -2 \pmod{p} \),

(iii) \( \left(\frac{l}{p}\right) = 1 \),

then there is a negative fundamental discriminant \( D_l := -dl \) or \(-4dl\) with \( 1 \leq dl \leq \kappa(p)l \) such that

\[ h(D_l) \not\equiv 0 \pmod{p} \] and \( \left(\frac{D_l}{p}\right) = \epsilon \).

**Case II:** \( \epsilon = 0 \).

Define \( B_p(z) \in M_2(\Gamma_0(4p^2), \chi_0) \) by

\[ B_p(z) := (U_p|V_p|\theta^3)(z) = \sum_{n=0}^\infty r(pn)q^{pn}, \]

and \( B_{p^2}(z) \in M_2(\Gamma_0(4p^4), \chi_0) \) by

\[ B_{p^2}(z) := (U_p|V_p|B_p)(z) = \sum_{n=0}^\infty r(p^2n)q^{p^2n}, \]
and \( C_p(z) \in M_3(\Gamma_0(4p^4), \chi_0) \) by
\[
C_p(z) := B_p(z) - B_{p^2}(z) = \sum_{(n,p)=1} r(pn)q^{pn}.
\]

Let \( l \) be an odd prime and define \((U_l|C_p)(z), (V_l|C_p)(z) \in M_3(\Gamma_0(4p^4l), (\frac{l}{p}))\) by
\[
(U_l|C_p)(z) := \sum_{n=0}^{\infty} u_{p,l}^0(n)q^n = \sum_{(n,p)=1} r(lpn)q^{pn},
\]
\[
(V_l|C_p)(z) := \sum_{n=0}^{\infty} v_{p,l}^0(n)q^n = \sum_{(n,p)=1} r(pn)q^{lpn}.
\]

Let \( \kappa(p) := 3p^3(p+1) \) and \( S^0_p \) denote the set of negative fundamental discriminants \( D_{np} \) with \( np \leq \kappa(p) \). If \( l \) is an odd prime such that \((\frac{D_{np}l}{p}) = -1\) for all \( D_{np} \in S^0_p \), then by (2), we have for all \( np \leq \kappa(p) \),
\[
u_{p,l}^0(lpn) = (l+2)\nu_{p,l}^0(lpn).
\]

By the similar way to Lemma 2.1 and Proposition 2.2, we have the following lemma and proposition.

**Lemma 2.3** Let \( p > 3 \) be prime. If \( l \) is an odd prime such that \( l \not\equiv -2 \pmod{p} \), then
\[
(U_l|C_p)(z) - (l+2)(V_l|C_p)(z) \not\equiv 0 \pmod{p}.
\]

**Proposition 2.4** Let \( p > 3 \) be prime and \( \epsilon = 0 \). If \( l \) is a sufficiently large prime satisfying
\[
(i) \quad (\frac{D_{np}l}{p}) = -1 \text{ for all } D_{np} \in S^0_p,
\]
\[
(ii) \quad l \not\equiv -2 \pmod{p},
\]
then there is a negative fundamental discriminant \( D_l := -pd_l \) or \(-4pd_l \) with \( 1 \leq pd_l \leq \kappa(p)l \) such that
\[
h(D_l) \not\equiv 0 \pmod{p} \text{ and } (\frac{D_l}{p}) = \epsilon.
\]
Proof of Theorem 1.1. Let \( r_p \pmod{t_p} \) be an arithmetic progression with \( (r_p, t_p) = 1 \) such that for every prime \( l \equiv r_p \pmod{t_p} \), \( l \) satisfies (i)(ii)(iii) in Proposition 2.2 or (i)(ii) in Proposition 2.4. Then by the similar arguments as in the proof of Corollary 1.2 in [2], which use Dirichlet’s theorem on primes in arithmetic progression, Theorem 1.1 easily follows from Proposition 2.2 and Proposition 2.4.

\[ \square \]

References


