Asymptotic formulas for partial sums of class numbers of indefinite binary quadratic forms

Yasufumi Hashimoto

Abstract

Sarnak obtained the asymptotic formula of the sum of the class numbers of indefinite binary quadratic forms from the prime geodesic theorem for the modular group. In the present paper, we show several asymptotic formulas of partial sums of the class numbers by using the prime geodesic theorems for the congruence subgroups of the modular group.

1 Introduction

For integers $a, b, c$ with $\gcd(a, b, c) = 1$, let $[a, b, c](x, y) = [a, b, c] := ax^2 + bxy + cy^2$ be a quadratic form of $(x, y) \in \mathbb{Z}^2$. Denote by $D := b^2 - 4ac$ and call $D$ the discriminant of $[a, b, c]$. Throughout this paper, we treat the quadratic forms of positive discriminants $D > 0$ which are not square. Put $\mathcal{D} := \{D > 0 \mid \text{not square, } D \equiv 0, 1 \mod 4\}$, the set of discriminant of the primitive indefinite quadratic forms. For $D \in \mathcal{D}$, put $d := D$ if the square free factor of $D$ is equivalent to 1 modulo 4 and $d := D/4$ otherwise. Call that $[a, b, c]$ and $[a', b', c']$ are equivalent if there exists $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ such that $[a, b, c](x, y) = [a', b', c'](\alpha x + \beta y, \gamma x + \delta y)$. For $D \in \mathcal{D}$, denote by $h(D)$ the class number of $D$ in the narrow sense, namely the number of equivalent classes of quadratic forms of discriminant $D$. Let $(t, u) \in \mathbb{Z}^2$ be the smallest nontrivial positive solution of the Pell equation $t^2 - Du^2 = 4$ and put $\epsilon(D) := (t + u\sqrt{d})/2$ the fundamental unit of discriminant $D$ in the narrow sense.

The aim of the present paper is to study the asymptotic distributions of the class numbers $h(D)$. It is well-known that

$$D^{1/2 - \epsilon} \ll h(D) \log \epsilon(D) \ll D^{1/2 + \epsilon}, \quad (\forall \epsilon > 0, \text{unconditionally}),$$

$$\frac{D^{1/2}}{\log \log D} \ll h(D) \log \epsilon(D) \ll D^{1/2} \log \log D, \quad (\text{if GRH is true}).$$
as $D \rightarrow \infty$ (see, e.g. [Mo]). Furthermore, Gauss conjectured and Siegel [Si] actually proved that

$$\sum_{D \in \mathfrak{D}, D \leq x} h(D) \log \epsilon(D) \sim \frac{\pi^2}{18 \zeta(3)} x^{3/2},$$

where $\zeta(3) := \sum_{n \geq 1} n^{-3}$. Roughly speaking, the asymptotic formula above tells us that the average of the growth of $h(D)\epsilon(D)$ is close to $D^{1/2}$ as $D \rightarrow \infty$. The formula (1.1) was shown by the class number formula $h(D) \log \epsilon(D) = D^{1/2} L(1, \chi_D) = D^{1/2} \sum_{n \geq 1} (D/n)n^{-1}$ and the analysis of the growth of the sum of $L(1, \chi_D)$. However, there have never been good estimates of $\sum_{D \leq x} h(D)$ because the distribution of the fundamental units $\epsilon(D)$ is complicated.

In 1982, Sarnak [Sa1] proved the following asymptotic formula.

$$\sum_{D \in \mathfrak{D}, \epsilon(D) < x} h(D) \log \epsilon(D) \sim \frac{1}{2} x^2.$$ (1.2)

It is easy to see that the above is equivalent to

$$\sum_{D \in \mathfrak{D}, \epsilon(D) < x} h(D) \sim \text{li}(x^2) := \int_2^{x^2} \frac{dt}{\log t} \sim \frac{x^2}{2 \log x}.$$ (1.3)

He proved (1.2) and (1.3) by expressing the prime geodesic theorem for $\text{SL}_2(\mathbb{Z})$ in terms of quadratic forms with a one-to-one correspondence between the primitive hyperbolic conjugacy classes of $\text{SL}_2(\mathbb{Z})$ and the equivalent classes of the primitive indefinite binary quadratic forms. We note that the asymptotic formulas (1.2) and (1.3) were extended to the binary quadratic forms over imaginary quadratic integers ([Sa3]) and the ternary quadratic forms [DH] in the studies of harmonic analysis of three dimensional hyperbolic manifolds and real rank two locally symmetric symmetric Riemannian manifolds respectively.

The asymptotic behaviors (1.1) and (1.2) and their proofs are different to each other; one is obtained by the analytic number theoretic way and the other is essentially done by the harmonic analytic one. In the present paper, we study the growth of partial sums of $h(D)$ over the discriminants $D$ with $\epsilon(D) < x$ to analyze more detail distributions of the class numbers from the side of $“\epsilon(D) < x.”$ For partial sums of class numbers, Sarnak [H2] studied the growth of the sum over $D = t^{2\nu} - 4$ ($\nu \geq 1$) and the author did it over $p | D$ with a fixed prime $p \geq 3$. The main results in this paper is as follows.

**Theorem 1.1.** (i) Let $\mathcal{C}$ be a condition for discriminants $D \in \mathfrak{D}$. Denote by $\mathfrak{D}(\mathcal{C})$ the set of discriminants $D \in \mathfrak{D}$ satisfying $\mathcal{C}$ and

$$\mu(\mathcal{C}) := \lim_{x \rightarrow \infty} \left( \frac{\sum_{D \in \mathfrak{D}(\mathcal{C}), \epsilon(D) < x} h(D)}{\sum_{D \in \mathfrak{D}, \epsilon(D) < x} h(D)} \right).$$
Then we have

\[
\mu(d \mid p^m) = \begin{cases} 
45/112, & p = 2, m = 1, \\
37/112, & p = 2, m = 2, \\
17/56, & p = 2, m = 3, \\
9/56, & p = 2, m = 4, \\
3 \times 2^{3-m}/7, & p = 2, \text{odd } m \geq 5, \\
2^{5-m}/7, & p = 2, \text{even } m \geq 6, \\
2p^{3-m}/(p^3 - 1), & p \geq 3,
\end{cases}
\]

\[
\mu((d/p) = 1) = \begin{cases} 
1/224, & p = 2, \\
1/2 - p(p + 1)/(p^3 - 1), & p \geq 3,
\end{cases}
\]

\[
\mu((d/p) = -1) = \begin{cases} 
75/224, & p = 2, \\
1/2 - p(p - 1)/(p^3 - 1), & p \geq 3,
\end{cases}
\]

\[
\mu(d \equiv 3 \mod 4) = 29/112.
\]

(ii) Let \( \mathcal{C}_p \) be a set of conditions such that

\[
\mathcal{C}_p = \begin{cases} 
\{ "2^r \mid d" (r \geq 1), "(d/2) = 1", "(d/2) = -1", "d \equiv 3 \mod 4" \}, & p = 2, \\
\{ "p^r \mid d" (r \geq 1), "(d/p) = 1", "(d/p) = -1" \}, & p \geq 3.
\end{cases}
\]

Then, for any distinct \( p_1, \ldots, p_l \) and \( \mathcal{C}_{p_i} \in \mathcal{C}_p \), we have

\[
\mu(\mathcal{C}_{p_1} \cap \cdots \cap \mathcal{C}_{p_l}) = \mu(\mathcal{C}_{p_1}) \times \cdots \times \mu(\mathcal{C}_{p_l}).
\]

At the end of this paper, we give some experimental (unproven) results for the asymptotic behaviors of the class numbers and compare the results to Cohen-Lenstra’s heuristics.

## 2 Proof of the theorem

### 2.1 Quadratic forms and the modular group

It is well-known that there is a one-to-one correspondence between the primitive hyperbolic conjugacy classes of the modular group and the equivalent classes of the primitive indefinite binary quadratic forms. The correspondence is described as follows (see e.g. \[G]\)).

\[
Q(x, y) := ax^2 + bxy + cy^2 \rightarrow \left( \frac{t_1 + bu_1}{2}, \frac{au_1}{t_1 - bu_1} \right),
\]

\[
\gamma := \left( \begin{array}{cc} \gamma_{11} & \gamma_{12} \\ \gamma_{21} & \gamma_{22} \end{array} \right) \rightarrow \frac{\gamma_{12}}{u_\gamma} x^2 + \frac{\gamma_{11} - \gamma_{22}}{u_\gamma} xy - \frac{\gamma_{21}}{u_\gamma} y^2 =: Q_\gamma(x, y),
\]

(2.1)
where \( D(Q) = D := b^2 - 4ac \) is the discriminant of \( Q \), \( (t_j(Q), u_j(Q)) = (t_j(D), u_j(D)) = (t_j, u_j) \) is the \( j \)-th positive solution of the Pell equation \( t^2 - Du^2 = 4 \) and \( u_\gamma := \gcd(\gamma_{12}, \gamma_{11} - \gamma_{22}, -\gamma_{21}) > 0 \). We also put \( t_\gamma := \gamma_{11} + \gamma_{22}, D_\gamma := (t_\gamma^2 - 4)/u_\gamma^2 \) and \( \epsilon(D) := (t_1 + u_1\sqrt{D})/2 \), and denote by \( h(D) \) the class number of \( D \) in the narrow sense. We note the following elementary facts without proofs.

**Fact 2.1.** Suppose that \( \gamma \) is a primitive hyperbolic element of \( \text{SL}_2(\mathbb{Z}) \). Then we have

1. \( D(Q) = D_{\gamma_Q} \) and \( D_\gamma = D(Q_\gamma) \).
2. \( (t_1(Q), u_1(Q)) = (t_\gamma Q, u_\gamma Q) \) and \( (t_\gamma, u_\gamma) = (t_1(Q_\gamma), u_1(Q_\gamma)) \).
3. \( Q_{\gamma_j} = Q_\gamma, D_{\gamma_j} = D_\gamma \) and \( (t_{\gamma_j}, u_{\gamma_j}) = (t_j(Q_\gamma), u_j(Q_\gamma)) \) for any \( j \geq 1 \).
4. \( \epsilon(D_\gamma) = \frac{1}{2}(t_\gamma + \sqrt{t_\gamma^2 - 4}) = \frac{1}{2}(t_\gamma + u_\gamma \sqrt{D_\gamma}) \) and \( N(\gamma) = \epsilon(D_\gamma)^2 \).
5. \( Q_{g^{-1}\gamma g}(x, y) = Q_\gamma(g.(x, y)) \) for any \( g \in \text{SL}_2(\mathbb{Z}) \).
6. \( \#\{\gamma \in \text{Prim}(\text{SL}_2(\mathbb{Z})) \mid D_\gamma = D\} = h(D) \).

### 2.2 Selberg’s zeta function and the prime geodesic theorem

Let \( \mathbb{H} \) be the upper half plane with the hyperbolic metric and \( \Gamma \) a discrete subgroup of \( \text{SL}_2(\mathbb{R}) \) such that the volume of \( \Gamma \backslash \mathbb{H} \) is finite. We denote by \( \text{Prim}(\Gamma) \) the set of primitive hyperbolic conjugacy classes of \( \Gamma \) and \( N(\gamma) \) the square of the larger eigenvalue of \( \gamma \in \text{Prim}(\Gamma) \). The Selberg zeta functions for \( \Gamma \) are defined as follows.

\[
Z_\Gamma(s) := \prod_{\gamma \in \text{Prim}(\Gamma)} \prod_{n=0}^{\infty} (1 - N(\gamma)^{-s-n}) \quad \text{Res} > 1,
\]

It is known that \( Z_\Gamma(s) \) is analytically continued to the whole complex plane as a meromorphic function of order 2. By virtue of the analytic properties of \( Z_\Gamma(s) \), we can obtain the following asymptotic formula called by the prime geodesic theorem (see, e.g., [Hei]).

\[
\pi_\Gamma(x) := \#\{\gamma \in \text{Prim}(\Gamma) \mid N(\gamma) < x\} = \text{li}(x) + O(x^\delta) \quad \text{as} \quad x \to \infty,
\]

where \( \text{li}(x) := \int_2^x (\log t)^{-1} \, dt \) and the constant \( \delta \) \((0 < \delta < 1)\) depends on \( \Gamma \).

According to Fact 2.1, we have

\[
Z_{\text{SL}_2(\mathbb{Z})}(s) = \prod_{D \in \mathbb{D}} \prod_{n=0}^{\infty} (1 - \epsilon(D)^{-2(s+n)})^{h(D)} \quad \text{Res} > 1, \quad (2.2)
\]

\[
\pi_{\text{SL}_2(\mathbb{Z})}(x) = \sum_{D \in \mathbb{D} \atop \epsilon(D) < x} h(D) \sim \text{li}(x^2) \quad \text{as} \quad x \to \infty. \quad (2.3)
\]
2.3 Congruence subgroups

Let \( \hat{\Gamma}(N) \) be the principal congruence subgroup of level \( N \geq 1 \) defined by

\[
\hat{\Gamma}(N) := \text{Ker}(\text{SL}_2(\mathbb{Z}) \xrightarrow{\text{proj}} \text{PSL}_2(\mathbb{Z}/N\mathbb{Z})) = \{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv \alpha I \mod N, \alpha \in \mathbb{Z}_N^{(2)} \},
\]

where \( I \) is the identity matrix and \( \mathbb{Z}_N^{(2)} := \{ \alpha \in \mathbb{Z}/n\mathbb{Z} \mid \alpha^2 \equiv 1 \mod N \} \). It is easy to see that

\[
\hat{\Gamma}(N)\hat{\Gamma}(M) = \hat{\Gamma}(\gcd(N, M)), \quad \hat{\Gamma}(N) \cap \hat{\Gamma}(M) = \hat{\Gamma}(NM/\gcd(N, M)),
\]

\[
[\text{SL}_2(\mathbb{Z}) : \hat{\Gamma}(N)] = \frac{1}{\#\mathbb{Z}_N^{(2)}} \prod_{p|N} p^{3r-2}(p^2-1) = \prod_{p|N} \begin{cases} 6, & p = 2, r = 1, \\ 24, & p = 2, r = 2, \\ 3 \times 2^{3r-4}, & p = 2, r \geq 3, \\ \frac{1}{2}p^{3r-2}(p^2-1), & p \geq 3, \end{cases}
\]

where \( N = \prod_{p|N} p^r \) is the factorization of \( N \).

We call that \( \Gamma \subset \text{SL}_2(\mathbb{Z}) \) is a congruence subgroup of level \( N \) if \( \Gamma \supset \hat{\Gamma}(N) \) and \( \Gamma \not\supset \hat{\Gamma}(M) \) for any \( M > N \). According to [H2], for a congruence subgroup \( \Gamma \), we see that

\[
\frac{Z_\Gamma^{(s)}}{Z_\hat{\Gamma}^{(s)}} = \sum_{D \in \mathcal{D}, j \geq 1} M_{\Gamma}(D, j) h(D) \frac{2 \log \epsilon(D)}{1 - \epsilon(D)^{-2j}} \epsilon(D)^{-2js},
\]

\[
\hat{\pi}_\Gamma(x^2) := \sum_{\gamma \in \text{Prim}(\Gamma), j \geq 1 \atop N(\gamma)^i < x^2} j^{-1} = \sum_{D \in \mathcal{D}, j \geq 1 \atop \epsilon(D)^i < x} j^{-1} M_{\Gamma}(D, j) h(D),
\]

where \( M_{\Gamma}(D, j) := \text{tr}_\Gamma(g(D, j)) \), \( \chi_\Gamma \) is the representation of \( \text{PSL}_2(\mathbb{Z}/p^s\mathbb{Z}) \) induced by the trivial representation of \( \Gamma/\hat{\Gamma}(p^s) \),

\[
g(D, j) := \begin{pmatrix} \frac{1}{2}(t_j(D) + \delta u_j(D)) & \frac{1}{4}(D - \delta^2)u_j(D) \\ u_j(D) & \frac{1}{2}(t_j(D) - \delta u_j(D)) \end{pmatrix} \in \text{PSL}_2(\mathbb{Z}/p^s\mathbb{Z}),
\]

and \( \delta \in \{0, 1\} \) is given as \( 4 \mid D - \delta^2 \).

For \( N = p^r \), a power of prime number, we define the following congruence subgroups.

\[
\Gamma(p^r; 0) := \{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv \alpha \begin{pmatrix} 1 & \ast \\ 0 & 1 \end{pmatrix} \mod p^r, \alpha \in \mathbb{Z}_{p^r}^{(2)} \},
\]

\[
\Gamma(p^r; +) := \{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix} \mod p^r, \delta \in (\mathbb{Z}/p^r\mathbb{Z})^\times / \mathbb{Z}_{p^r}^{(2)} \},
\]

\[
\Gamma(p^r; -) := \{ \gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv J^{-1} \begin{pmatrix} \omega^l & 0 \\ 0 & \omega^{-l} \end{pmatrix} J \mod p^r, 1 \leq l \leq p^{r-1}(p+1)/\#\mathbb{Z}_{p^r}^{(2)} \},
\]
where $\omega$ is a generator of the cyclic subgroup of order $p^{r-1}(p+1)/\#\mathbb{Z}_p^{(2)}$ in the multiplicative group of the quadratic extension of $(\mathbb{Z}/p^r\mathbb{Z})/\mathbb{Z}_p^{(2)}$. We further define the following congruence subgroups for $N = 2^r$.

$$\Gamma(2^r; 3) := \left\{ \gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv \left( \begin{array}{cc} 2 & 1 \\ 3 & 2 \end{array} \right)^l \mod 2^r \right\},$$

$$\Gamma(2^r; 2^{2m}) := \left\{ \gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv \left( \begin{array}{cc} 17^{1/2} & 4 \\ 4 & 17^{1/2} \end{array} \right)^l \mod 2^r \right\}, \quad m = 1,$$

$$\Gamma(2^r; 2^{2m}) := \left\{ \gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv \left( \begin{array}{cc} 17^{1/2} & 2 \\ 8 & 17^{1/2} \end{array} \right)^l \mod 2^r \right\}, \quad m = 2,$$

$$\Gamma(2^r; 2^{2m}) := \left\{ \gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv \left( \frac{1 + 4^m}{1} \right)^l \mod 2^r \right\}, \quad m \geq 3.$$

Actually calculating $\chi_\Gamma(g(D, j))$, we get the following results.

**Lemma 2.1.** The definitions of congruence subgroups are as above. Then the values of $M_\Gamma(D, j)$ are as follows.

(i) The case of $p = 2$;

$$M_{\Gamma(2^r; 0)}(D, j) = \begin{cases} 3, & 2 \mid u_j, \\ 1, & 2 \nmid u_j, 2 \mid D, \\ 0, & \text{otherwise.} \end{cases}$$

$$M_{\Gamma(4; 0)}(D, j) = \begin{cases} 6, & 4 \mid u_j, \\ 2, & 2 \nmid u_j, 2 \mid D \text{ or } 2 \nmid u_j, 4 \mid d, \\ 0, & \text{otherwise.} \end{cases}$$

$$M_{\Gamma(2^r; 0)}(D, j) = \begin{cases} 3 \times 2^{2r-4}, & 2^r \mid u_j, \\ 2^{2r-4}, & 2^{r-1} \mid u_j, 2 \mid D, \\ 2^{r+k-2}, & 2^k \mid u_j, 2^{r-k+2} \mid D, 0 \leq k \leq r-2, \\ 0, & \text{otherwise.} \end{cases}$$

$$M_{\Gamma(2^r; 0)\cap \hat{\Gamma}(2^r-1)}(D, j) = \begin{cases} 3 \times 2^{3r-l-4}, & 2^r \mid u_j, \\ 2^{3r-l-4}, & 2^{r-1} \mid u_j, 2 \mid D, \\ 2^{r+k-l-2}, & 2^k \mid u_j, 2^{r-k+2} \mid D, r-l \leq k \leq r-1, \\ 0, & \text{otherwise.} \end{cases}$$

$$M_{\Gamma(2^r; 0)\cap \hat{\Gamma}(2^r-1)}(D, j) = \begin{cases} 3 \times 2^{3r-l-4}, & 2^r \mid u_j, \\ 2^{3r-l-4}, & 2^{r-1} \mid u_j, 2 \mid D, \\ 2^{r+k-l-2}, & 2^k \mid u_j, 2^{r-k+2} \mid D, r-l \leq k \leq r-1, \\ 0, & \text{otherwise.} \end{cases}$$
Partial sum of class numbers

\[ M_{\Gamma(2^r;+)}(D, j) = \begin{cases} 
3 \times 2^{2r-1}, & 2^r \mid u_j, \\
2^{2k+1}, & 2^k \mid u_j, d \equiv 1 \mod 8, 3 \leq k \leq r - 1, \\
0, & \text{otherwise}.
\end{cases} \]

\[ M_{\Gamma(2^r;+ \cap \Gamma(2^r-l))}(D, j) = \begin{cases} 
3 \times 2^{3r-l-4}, & 2^r \mid u_j, \\
2^{r+2k-l-2}, & 2^k \mid d, d \equiv 1 \mod 8, r - l \leq k \leq r - 1, \\
0, & \text{otherwise}.
\end{cases} \]

\[ M_{\Gamma(2^r;+)}(D, j) = \begin{cases} 
2, & 2 \mid u_j \text{ or } 2 \nmid u_j, d \equiv 5 \mod 8, \\
0, & \text{otherwise},
\end{cases} \]

\[ M_{\Gamma(2^r;+ \cap \Gamma(2^r-l))}(D, j) = \begin{cases} 
2^{2r-1}, & 2^r \mid u_j, \\
2^{2k+1}, & 2^k \mid u_j, d \equiv 5 \mod 8, 0 \leq k \leq r - 1 (k \neq 1, 2), \\
0, & \text{otherwise}.
\end{cases} \]

\[ M_{\Gamma(2^r;+ \cap \Gamma(2^r-l))}(D, j) = \begin{cases} 
12, & 4 \mid u_j, \\
2, & 2 \nmid u_j, d \equiv 3 \mod 4, \\
0, & \text{otherwise}.
\end{cases} \]

\[ M_{\Gamma(2^r;3)}(D, j) = \begin{cases} 
3 \times 2^{2r-3}, & 2^r \mid u_j, \\
2^{2r-3}, & 2^{r-1} \mid u_j, 2 \mid D, \\
2^{2k+1}, & 2^k \mid u_j, d \equiv 3 \mod 4, 0 \leq k \leq r - 2, k \neq 1, \\
0, & \text{otherwise}.
\end{cases} \]

\[ M_{\Gamma(2^r;3 \cap \Gamma(2^r-l))}(D, j) = \begin{cases} 
3 \times 2^{3r-l-4}, & 2^r \mid u_j, \\
2^{3r-l-4}, & 2^{r-1} \mid u_j, 2 \mid D, \\
2^{r+2k-l}, & 2^k \mid u_j, d \equiv 3 \mod 4, r - l \leq k \leq r - 2, \\
0, & \text{otherwise}.
\end{cases} \]

\[ M_{\Gamma(2^r;2^m)}(D, j) = \begin{cases} 
3 \times 2^{2r-2}, & 2^r \mid u_j, \\
2^{2r-2}, & 2^{r-1} \mid u_j, 2 \mid D, \\
2^{2k+2}, & 2^k \mid u_j, d \equiv 2^{\min(2m, r)} \mod 2^{\min(2m+2, r)}, 2 \leq k \leq r - 2, \\
0, & \text{otherwise}.
\end{cases} \]

\[ M_{\Gamma(2^r;2^m \cap \Gamma(2^r-l))}(D, j) = \begin{cases} 
3 \times 2^{3r-l-4}, & 2^r \mid u_j, \\
2^{3r-l-4}, & 2^{r-1} \mid u_j, 2 \mid D, \\
2^{r+2k-l}, & 2^k \mid u_j, d \equiv 2^{\min(2m, r)} \mod 2^{\min(2m+2, r)}, r - l \leq k \leq r - 2, \\
0, & \text{otherwise}.
\end{cases} \]
(ii) The case of $p \geq 3$;

$$M_{\Gamma(p^r:0)}(D,j) = \begin{cases} p^{2r-2}(p^2-1)/2, & p^r \mid u_j, \\ p^{r+k-1}(p-1)/2, & p^k \parallel u_j, p^{r-k} \mid d, 0 \leq k \leq r-1, \\ 0, & \text{otherwise.} \end{cases}$$

$$M_{\Gamma(p^r:0) \cap \Gamma(p^r-l)}(D,j) = \begin{cases} p^{3r-l-2}(p^2-1)/2, & p^r \mid u_j, \\ p^{r+k-l-1}(p-1)/2, & p^k \parallel u_j, p^{r-k} \mid d, r-l \leq k \leq r-1, \\ 0, & \text{otherwise.} \end{cases}$$

$$M_{\Gamma(p^r:+)}(D,j) = \begin{cases} p^{2r-1}(p+1), & p^r \mid u_j, \\ 2p^{2k}, & p^k \parallel u_j, (d/p) = 1, 0 \leq k \leq r-1, \\ 0, & \text{otherwise.} \end{cases}$$

$$M_{\Gamma(p^r:+) \cap \Gamma(p^r-l)}(D,j) = \begin{cases} p^{3r-l-2}(p^2-1)/2, & p^r \mid u_j, \\ p^{r+2k-l-1}(p-1), & p^k \parallel u_j, (d/p) = 1, r-l \leq k \leq r-1, \\ 0, & \text{otherwise.} \end{cases}$$

$$M_{\Gamma(p^r:-)}(D,j) = \begin{cases} p^{2r-1}(p-1), & p^r \mid u_j, \\ 2p^{2k}, & p^k \parallel u_j, (d/p) = -1, 0 \leq k \leq r-1, \\ 0, & \text{otherwise.} \end{cases}$$

$$M_{\Gamma(p^r:-) \cap \Gamma(p^r-l)}(D,j) = \begin{cases} p^{3r-l-2}(p^2-1)/2, & p^r \mid u_j, \\ p^{r+2k-l-1}(p+1), & p^k \parallel u_j, (d/p) = -1, r-l \leq k \leq r-1, \\ 0, & \text{otherwise.} \end{cases}$$

(iii) $N \geq 1$ is an integer;

$$M_{\Gamma(N)}(D,j) = \begin{cases} [\text{SL}_2(\mathbb{Z}) : \hat{\Gamma}(N)], & N \mid u_j, \\ 0, & \text{otherwise.} \end{cases}$$

Here $p^r \parallel K$ means that $p^r \mid K$ but $p^{r+1} \nmid K$.

Proof of the theorem. Let $\hat{\mathcal{C}}$ be a condition for $(D,j) \in \mathcal{O} \times \mathbb{N}_{\geq 1}$,

$$\hat{\mathcal{O}}(\hat{\mathcal{C}}) := \{(D,j) \mid D \in \mathcal{O}, j \geq 1, (D,j) \text{satisfies } \hat{\mathcal{C}}\}$$

and

$$\hat{\mu}(\hat{\mathcal{C}}) := \lim_{x \to \infty} \left( \sum_{(D,j) \in \hat{\mathcal{O}}(\hat{\mathcal{C}})} \frac{j^{-1}h(D)}{e(D) \leq x} \right) / \left( \sum_{(D,j) \in \hat{\mathcal{O}}} j^{-1}h(D) \right).$$

For a congruence subgroup $\Gamma$ of $\text{SL}_2(\mathbb{Z})$, denote by

$$\sigma_{\Gamma} := \lim_{x \to \infty} \left( \hat{\pi}_{\Gamma}(x^2) / \hat{\pi}_{\text{SL}_2(\mathbb{Z})}(x^2) \right).$$
Partial sum of class numbers

Of course, $\sigma_{\Gamma} = 1$ for any $\Gamma$.

First we consider the case where $p \geq 3$ and $C$ is “$p^r \mid d$”. According to Lemma 2.1, we see that

$$\sigma_{\Gamma(p^r,0)} = \frac{1}{2} p^{2r-2} (p^2 - 1) \mu(p^r \mid u_j) + \sum_{0 \leq k \leq r-1} \frac{1}{2} p^{r+k-1} (p-1) \mu(p^k \mid u_j, p^{r-k} \mid d),$$

$$\sigma_{\Gamma(p^r,0) \cap \Gamma(p^{r-1})} = \frac{1}{2} p^{3r-2} (p^2 - 1) \mu(p^r \mid u_j) + \sum_{r-1 \leq k \leq r-1} \frac{1}{2} p^{2r+k-1} (p-1) \mu(p^k \mid u_j, p^{r-k} \mid d),$$

$$\sigma_{\Gamma(p^r)} = \frac{1}{2} p^{3r-2} (p^2 - 1) \mu(p^r \mid u_j).$$

Then we have

$$\hat{\mu}(p^k \mid d, p^r \mid u_j) = \sum_{k \leq m \leq r} \frac{2}{(p-1) p^{2m-2k-1}} (\sigma_{\Gamma(p^m,0) \cap \Gamma(p^{m-k})} - \frac{1}{p} \sigma_{\Gamma(p^m,0) \cap \Gamma(p^{m-k+1})})$$

$$= \frac{2}{p^3 - 1} (p^{3-k} - p^{2k-3r-3}),$$

$$\hat{\mu}(p^k \mid d \text{ or } p^r \mid u_j) = \hat{\mu}(p^k \mid d, p^r \mid u_j) + \frac{2}{p^{3r-2} (p^2 - 1)} \sigma_{\Gamma(p^r)}$$

$$= \frac{2}{p^3 - 1} (p^{3-k} - p^{2k-3r-3}) + \frac{2}{p^{3r-2} (p^2 - 1)}.$$

Since $\hat{\mu}(p^k \mid d, p^r \mid u_j) \leq \hat{\mu}(p^k \mid d) \leq \hat{\mu}(p^k \mid d \text{ or } p^r \mid u_j)$ for any $r \geq 1$, we have

$$\hat{\mu}(p^k \mid d) = \frac{2p^{3-k}}{p^3 - 1}.$$

It is easy to see that

$$\sum_{(d,j) \in D(p^k \mid d)} j^{-1} h(d) - \sum_{d \in D(p^k \mid d)} h(d) \leq \sum_{d \in D, j \geq 2, \epsilon(d) < x^2} j^{-1} h(d) \ll x.$$

Then we have

$$\mu(p^k \mid d) = \hat{\mu}(p^k \mid d) = \frac{2p^{3-k}}{p^3 - 1}.$$

Similarly, we can get the following results from Lemma 2.1

$$\mu((d/p) = 1) = \begin{cases} 1/224, & p = 2, \\ 1/2 - p(p+1)/(p^3-1), & p \geq 3, \end{cases}$$

$$\mu((d/p) = -1) = \begin{cases} 75/224, & p = 2, \\ 1/2 - p(p-1)/(p^3-1), & p \geq 3 \end{cases}$$

$$\mu(2 \mid D) = 37/56.$$
Then we have
\[
\mu(2^{m+2} \mid D) = \frac{9}{28}, \quad m \geq 3,
\]
\[
\mu(2^{m+2} \mid D) = \frac{2^{4-m}}{7}, \quad m \geq 3,
\]
\[
\mu(d \equiv 2^{2m} \mod 2^{2m+2}) = \begin{cases} 
1/112, & m = 1, \\
1/56, & m = 2, \\
2^{4-2m}/7, & m \geq 3,
\end{cases}
\]
\[
\mu(d \equiv 3 \mod 4) = \frac{29}{112}.
\]

Since
\[
\mu(2 \mid d) = \mu(2 \mid D) - \mu(d \equiv 3 \mod 4),
\]
\[
\mu(2^{2m} \mid d) = \mu(2^{2m+2} \mid D) + \mu(d \equiv 2^{2m} \mod 2^{2m+2}), \quad m \geq 1
\]
\[
\mu(2^{2m+1} \mid d) = \mu(2^{2m+3} \mid D) + \mu(d \equiv 2^{2m+2} \mod 2^{2m+4}), \quad m \geq 1,
\]
we can get the desired results for \(N = 2^m\).

Furthermore we have the following lemma (see [H2]).

**Lemma 2.2.** Let \(\Gamma\) be a congruence subgroup of level \(N = \prod_{p \mid N} p^r\). Then there exist congruence subgroups \(\Gamma_{p^r}\) of level \(p^r\) such that \(\Gamma = \cap_{p \mid N} \Gamma_{p^r}\), and it holds that \(\text{tr}_{\chi_\Gamma}(g(D, j)) = \prod_{p \mid N} \text{tr}_{\chi_{\Gamma_{p^r}}}(g(D, j))\).

**Proof of (ii).** For simplicity, we prove only \(\mu(pq \mid d) = \mu(p \mid d)\mu(q \mid d)\). We note that it is not difficult to prove other cases.

By Lemma 2.1 and 2.2 we see that
\[
\hat{\mu}(pq \mid d, p^{r_1-1} \mid u_j, q^{r_2-1} \mid u_j) = \frac{2}{p^{3r_1-2}q^{3r_2-2}} = \hat{\mu}(p \mid d, p^{r_1-1} \mid u_j)\hat{\mu}(q \mid d, q^{r_2-1} \mid u_j).
\]

Then we have
\[
\hat{\mu}(pq \mid d, p^r \mid u_j, q^r \mid u_j) = \sum_{1 \leq r_1, r_2 \leq r} \hat{\mu}(pq \mid d, p^{r_1-1} \mid u_j, q^{r_2-1} \mid u_j)
\]
\[
= \sum_{1 \leq r_1, r_2 \leq r} \hat{\mu}(p \mid d, p^{r_1-1} \mid u_j)\hat{\mu}(q \mid d, q^{r_2-1} \mid u_j)
\]
\[
= \left( \sum_{1 \leq r_1 \leq r} \hat{\mu}(p \mid d, p^{r_1-1} \mid u_j) \right) \times \left( \sum_{1 \leq r_2 \leq r} \hat{\mu}(q \mid d, q^{r_2-1} \mid u_j) \right)
\]
\[
= \hat{\mu}(p \mid d, p^r \mid u_j)\hat{\mu}(q \mid d, q^r \mid u_j).
\]

Similarly, we have
\[
\hat{\mu}(pq \mid d \text{ or } p^r q^r \mid u_j) = \hat{\mu}(p \mid d \text{ or } p^r \mid u_j)\hat{\mu}(q \mid d \text{ or } q^r \mid u_j).
\]
Therefore we get
\[ \hat{\mu}(pq \mid d) = \hat{\mu}(p \mid d)\hat{\mu}(q \mid d). \]

\[ \square \]

### 3 Problems

In this section, we give several problems for asymptotic behaviors of the class numbers.

1. Estimate the asymptotic behavior of
\[
\sum_{D \in \mathcal{D}(\mathcal{C})} h(D) \log \varepsilon(D)
\]
for the condition \( \mathcal{C} \) in Theorem 1.1. Is it true that it behaves \( \sim \beta(\mathcal{C}) x^{3/2} \) as \( x \to \infty \) for some constant \( \beta(\mathcal{C}) > 0 \)? If it is true, compare \( \beta(\mathcal{C}) \) to \( \mu(\mathcal{C}) \) in Theorem 1.1.

2. Let \( \mathcal{D}_0 \) be the set of square-free positive integers. Estimate the asymptotic behavior of
\[
\# \{ d \in \mathcal{D}_0 \mid n \mid h(D), \varepsilon(d) < x \}
\]
for given \( n \geq 1 \).

Based on experimental results, Cohen-Lenstra [CL] conjectured that
\[
\lim_{x \to \infty} \frac{\# \{ d \in \mathcal{D}_0 \mid p \mid h(D), d < x \}}{\# \{ d \in \mathcal{D}_0 \mid d < x \}} = 1 - \prod_{k \geq 2} (1 - p^{-k})
= p^{-2} + p^{-3} + p^{-4} - p^{-7} + \cdots,
\]
for an odd prime \( p \). It has been proven that
\[
\# \{ d \in \mathcal{D}_0 \mid n \mid h(d), d < x \} \approx \begin{cases} 
  x^{1/2n-\varepsilon}, & \text{if } n \text{ is prime, } [\text{Mu}], \\
  x^{1/n-\varepsilon}, & \text{if } n \text{ is an integer, } [\text{Yu}], \\
  x^{5/6}, & \text{if } n = 3, [\text{CM}], \\
  x^{7/8}, & \text{if } n = 3, [\text{BK}], \\
  x^{1/2}, & \text{if } n = 5, 7, [\text{By}].
\end{cases}
\]

On the other hand, we computed the following values.

\[
\alpha_p(x) := \frac{\# \{ d \in \mathcal{D}_0 \mid p \mid h(D), \varepsilon(D) < x \}}{\# \{ d \in \mathcal{D}_0 \mid \varepsilon(D) < x \}}.
\]

The results for \( p = 3, 5, 7, 11 \) and \( x < 3 \times 10^6 \) is as follows.

| \( x \)  | \( \alpha_3(x) \) | \( \alpha_5(x) \) | \( \alpha_7(x) \) | \( \alpha_{11}(x) \) |
|---------|-----------------|-----------------|-----------------|-----------------|
| 10,000  | 0.3726          | 0.2009          | 0.1297          | 0.0678          |
| 100,000 | 0.4088          | 0.2265          | 0.1519          | 0.08955         |
| 500,000 | 0.4236          | 0.2326          | 0.1589          | 0.09481         |
Is the following conjecture true?

\[
\lim_{x \to \infty} \alpha_p(x) = \prod_{k \geq 1} (1 - p^{-k}) = p^{-1} + p^{-2} - p^{-5} - p^{-7} + \cdots \\
= \begin{cases} 
0.43987 \cdots, & p = 3, \\
0.23967 \cdots, & p = 5, \\
0.16320 \cdots, & p = 7, \\
0.09916 \cdots, & p = 11, \\
\vdots
\end{cases}
\]

3. Estimate the asymptotic behavior of \#\{d \in \mathcal{D}_0 \mid h(D) = 1, \epsilon(D) < x\}.

Gauss conjectured that there are infinitely many \(d \in \mathcal{D}_0\) with \(h(D) = 1\), and Cohen-Lenstra [CL] gave more precise conjecture as follows.

\[
\lim_{x \to \infty} \frac{\#\{p \equiv 1 \mod 4 \mid h(p) = n, p < x\}}{\#\{p \equiv 1 \mod 4 \mid p < x\}} = \begin{cases} 
0.754 \cdots, & n = 1, \\
0.125 \cdots, & n = 3, \\
0.037 \cdots, & n = 5, \\
\vdots
\end{cases}
\]

Note that \(h(D)\) is odd if and only if \(D\) is prime and is equivalent to 1 modulo 4. Experimentally, the number of class number one primes \(p\) with \(p < x\) is not small. However, when we count it by \(\epsilon(p) < x\), the situation is very different. The following table is the list of class number one primes and the number of them.

| \(x\) | \(\omega^{(1)}(x)\) | primes \(p\) with \(h(p) = 1\) and \(\epsilon(p) < x\) |
|-------|-----------------|----------------------------------|
| \(10^2\) | 6 | 5,2,13,29,53,17 |
| \(10^3\) | 11 | 37,173,293,101,197 |
| \(10^4\) | 16 | 61,677,149,41,317 |
| \(10^5\) | 22 | 773,629,157,557,109 |
| \(10^6\) | 26 | 461,797,2477,1013,509 |
| \(10^7\) | 38 | 89,941,181,113,1877,653,73,1493,3533,389,277,1613 |
| \(10^8\) | 44 | 397,137,2693,1637,1277,1997 |
| \(10^9\) | 53 | 373,97,821,2309,349,701,4157,853,1181 |
| \(10^{10}\) | 61 | 4973,233,2357,4373,4253,2957,3797,613 |
| \(10^{11}\) | 73 | 1109,3989,353,1949,997,1733,1973,4517,2621,7013,9173 |
| \(10^{12}\) | 84 | 1061,2333,4133,1301,2789,421,5309,877,3677,3461,10853,2141 |

Here \(\omega^{(1)}(x)\) is the number of primes \(p\) with \(h(p) = 1\) and \(\epsilon(p) < x\). While the data is not necessarily enough, we can guess that it increases in logarithmic order. The situation that the discriminants \(D\) with class number one are rare, if \(D\) is arranged according to \(\epsilon(D)\), can be explained in the following rough (not strict) argument.
The class number formula tells us that \( h(D) = D^{1/2}L(1, \chi_D)/\log \epsilon(D) \). Since

\[
\epsilon(D) = \frac{1}{2} (t_1 + u_1 \sqrt{D}) = \frac{1}{2} (t_1 + \sqrt{t_1^2 - 4}) \sim t_1,
\]

\[
d = \frac{t_1^2 - 4}{u_1} \sim \frac{t_2}{u_1},
\]

\[
L(1, \chi_D) \gg D^{-\epsilon} \quad (\forall \epsilon > 0),
\]

we see that \( h(D) \gg (t_1/u_1)^{1-\epsilon} \). If \( h(D) = 1 \) then we have \( u_1 \gg t_1^{1-\epsilon} \). Since \( u_1^2 \) is a divisor of \( t_1^2 - 4 \), the condition \( u_1 \gg t_1^{1-\epsilon} \) is very severe. Thus the number of \( D \) with \( h(D) = 1 \) is small.

However, estimating its behavior strictly and precisely is not easy.

**References**

[By] D. Byeon, *Real quadratic fields with class number divisible by 5 or 7*, Manuscripta Math. **120** (2006), 211–215.

[BK] D. Byeon and E. Koh, *Real quadratic fields with class number divisible by 3*, Manuscripta Math. **111** (2003), 261–263.

[CL] H. Cohen and H.W. Lenstra, *Heuristics on class groups of number fields*, in *Number Theory*, Lec. Notes in Math. **1068**, 33-62, Springer, (1983).

[CM] K. Chakraborty and R. Murty, *On the number of real quadratic fields with class number divisible by 3*, Proc. Amer. Math. Soc., **131** (2003), 41-44.

[DH] A. Deitmar and W. Hoffmann, *Asymptotics of class numbers*, Invent. Math. **160** (2005), 647-675.

[G] C. F. Gauss, *Disquisitiones arithmeticae*, Fleischer, Leipzig, (1801).

[H1] Y. Hashimoto, *Arithmetic expressions of Selberg’s zeta functions for congruence subgroups*, J. Number Theory, **122** (2007), 324–335.

[H2] Y. Hashimoto, *Selberg’s zeta functions for congruence subgroups of modular groups in \( SL_2(\mathbb{R}) \) and \( SL_2(\mathbb{C}) \)*, arXiv.math/0806.4829.

[He] D. Hejhal, *The Selberg trace formula of \( PSL(2, \mathbb{R}) \) I, II*, Lec. Notes in Math. **548, 1001** Springer, (1976, 1983).

[KM] Y. Kishi and K. Miyake, *Parametrization of the quadratic fields whose class numbers are divisible by three*, J. Number Theory **80** (2000), 209-217.

[Mo] R. A. Mollin, *Quadratics*, CRC Press Series on Discrete Mathematics and Its Applications, CRC Press (1995).

[Mu] R. Murty, *Exponents of class groups of quadratic fields*, in *Topics in Number Theory*, Math. Appl. **467**, 229-239, Kluwer, Netherlands (1999).
[Sa1] P. Sarnak, *Class numbers of indefinite binary quadratic forms*, J. Number Theory, 15 (1982), 229-247.

[Sa2] P. Sarnak, *Class numbers of indefinite binary quadratic forms II*, J. Number Theory, 21 (1985), 333–346.

[Sa3] P. Sarnak, *The arithmetic and geometry of some hyperbolic three-manifolds*, Acta Math. 151 (1983), 253–295.

[Si] C. L. Siegel, *The average measure of quadratic forms with given determinant and signature*, Ann. of Math. II, 45 (1944), 667-685.

[VZ] A. B. Venkov and P. G. Zograf, *Analogues of Artin’s factorization formulas in the spectral theory of automorphic functions associated with induced representations of Fuchsian groups*, Izv. Akad. Nauk SSSR Ser. Mat. 46 (1982), 1150–1158, 1343 (Russian), Math. USSR-Izv. 21 (1983), 435–443 (English translation).

[Yu] G. Yu, *A note on the divisibility of class numbers of real quadratic fields*, J. Number Theory, 97 (2002), 35-44.

HASHIMOTO, Yasufumi
Institute of Systems and Information Technologies/KYUSHU,
7F 2-1-22, Momochihama, Fukuoka 814-0001, JAPAN
e-mail:hasimoto@isit.or.jp