ASYMPTOTICS FOR AVERAGES OF CLASS NUMBERS OF REAL QUADRATIC FIELDS

KENZ KALLAL

Abstract. This is my final paper for Math 286x: arithmetic statistics, taught by Fabian Gundlach. The main topic of this paper is the asymptotic formula
\[ \sum_{0 < D < T} h_D R_D \sim c T^{3/2} \]
for weighted averages of class numbers of real quadratic fields of discriminant bounded by \( T \). This was originally stated by Gauss and proved by Siegel (with a slightly different explicit constant from ours because it was stated in the language of quadratic forms up to narrow equivalence rather than class numbers and regulators of quadratic fields). We provide a new proof of this fact, using as the main technical input the Shanks infrastructure, a contribution originally belonging to the algorithmic side of the theory. We also explain Siegel’s technique, for which the main input is a connection between the quantities \( R_D \) and lengths of closed geodesics on quotients of the Poincaré upper-half plane endowed with the usual hyperbolix metric. Siegel’s technique has the advantage of providing an opportunity for the use of the Selberg trace formula, which Sarnak used in his thesis to partially decouple the class number from the regulator in this asymptotic averaging formula.

Contents

1. Introduction 
2. Quadratic forms and real quadratic fields
   2.1. Reduction theory for indefinite binary quadratic forms
   2.2. The Shanks infrastructure
3. Proof of the asymptotic formula
   3.1. The geometry of numbers
   3.2. Sieving for fundamental discriminants and concluding the main theorem
4. Quadratic forms and hyperbolic geodesics
Appendix A. The volume computation
References

1. Introduction

For a fundamental discriminant \( D > 0 \), let \( k_D = \mathbb{Q}(\sqrt{D}) \) be the real quadratic field of discriminant \( D \), and denote its class number by \( h(k_D) \) and its regulator by \( R(k_D) \). The main theorem of this paper is

**Theorem 1.1.** For \( T \to \infty \),

\[
\sum_{0 < D < T} h(k_D) R(k_D) \sim \left( \frac{\pi^2}{36} \prod_p (1 - p^{-2} - p^{-3} + p^{-4}) \right) T^{3/2}
\]
where the sum is over all positive fundamental discriminants bounded by $T$, and the product is over all positive rational primes.

Gauss [3] was probably the first to state Theorem 1.1, but to my knowledge it was not until 1944 that it was proven, in an influential paper of Siegel [9]. In both of these works, as is also the case in this paper, the theorem is stated and proved in the language of quadratic forms: $h(k_D)$ is identified with the number of equivalence classes of quadratic forms of discriminant $D$. The main difference between our proof and Siegel’s is that while his identifies the regulator with the (hyperbolic) length of the quotient of a certain geodesic on the upper half-plane by its automorphism group, ours uses the Shanks infrastructure, a construct from computational algebraic number theory which was originally used by Shanks to efficiently compute class numbers and regulators of real quadratic fields (c.f. Shanks’ baby-step giant-step method and Buchmann’s sub-exponential algorithm [2, §5.8-9]).

The (primitive\(^1\)) quadratic forms $f(X, Y)$ of positive non-square discriminant $D$ are uniquely determined up to a sign by the two quadratic irrationals $\rho_1, \rho_2$ which are the roots of $f(X, 1)$. Siegel [9] specifically considered the geodesic $\gamma$ on the Poincaré upper half-plane $\mathbb{H}$ between $\rho_1$ and $\rho_2$ (and moreover it suffices to specify the larger one, since they are Galois conjugates). Our proof instead uses the reduction theory (see [1, Ch. 3], [2, Ch. 5]) of “indefinite” (i.e. positive discriminant) binary quadratic forms, in which the point is that the process of computing the continued fraction expansion of, say, $\rho_1$, only uses operations that correspond in the binary quadratic form world to $GL_2(\mathbb{Z})$-equivalences. The theory of continued fractions for quadratic irrationals [4, Ch. X] says that every quadratic irrational has a periodic continued fraction expansion, so in particular every primitive binary quadratic form of discriminant $D > 0$ is $GL_2(\mathbb{Z})$-equivalent to one which corresponds to a quadratic irrational with purely periodic continued fraction, and the set of such binary quadratic forms (the “reduced” forms) is therefore partitioned into finitely many cycles (this is the finiteness of the class group). It turns out that if two forms are in different cycles, then they are inequivalent, and thus the class number is equal to the number of cycles. The main inconvenience is that there is no guarantee that the cycles all have the same length. The Shanks infrastructure (see e.g. [2, 6]) provides a distance function that makes all the cycles the same length, where that length is equal to the regulator. In particular, it can be shown that if $f = aX^2 + bXY + cY^2$ is a binary quadratic form of discriminant $D > 0$, then the distance between $f$ and the next form in the cycle of $f$ is

$$\frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right).$$

Therefore, the quantity $h(k_D)R(k_D)$ is accessible: it is given by the sum of the quantity above over all reduced forms. We will use the geometry of numbers to attack this sum and prove Theorem 1.1.

It might be useful to think about whether there is a direct connection between the Shanks infrastructure and the lengths of geodesics on $\mathbb{H}$ as used by Siegel. This is particularly the case because of the further progress that Siegel’s method leads to, most notably Sarnak’s work in his thesis [7] on prime geodesic theorems which used the Selberg trace formula as a

---

\(^1\)If we want to average over all $D$ rather than just the fundamental discriminants, then it is necessary to add this condition; luckily it is a formal consequence of the definition that all binary quadratic forms over $\mathbb{Z}$ with fundamental discriminant are primitive.
crucial input and resulted in an asymptotic formula similar to Theorem 1.1 except without the class numbers being weighted by the regulator\(^2\) [8]. In particular, Sarnak proved

**Theorem 1.2.** Let \(\mathcal{D}\) be the set of all positive discriminants of quadratic orders, i.e.
\[
\mathcal{D} := \{ D \in \mathbb{N} : D \equiv 0, 1 \mod 4, D \text{ non-square} \}.
\]
Then
\[
\sum_{D \in \mathcal{D} \in \mathcal{D}} \sum_{\mathcal{O}_D \leq T} h(\mathcal{O}_D) \sim Li(T^2)
\]
where \(Li\) denotes the familiar logarithmic integral, and \(\mathcal{O}_D\) is the quadratic order of discriminant \(D\).

So it is possible that Sarnak’s results imply some useful things about the Shanks infrastructure (I haven’t thought about this rather vague question at all, though; I just wrote it down to keep a record of it).

This paper is organized as follows. In Section 2, we explain in more detail the reduction theory of binary quadratic forms and the Shanks infrastructure. In Section 3, we carry out the geometry of numbers argument to prove Theorem 1.1, conditional on the computation of an integral which is relegated to Appendix A. Finally, in Section 4, we outline Siegel’s proof of Theorem 1.1 and provide a brief account of Sarnak’s more recent results described above.

## 2. Quadratic forms and real quadratic fields

First we zoom\(^3\) through the connection between binary quadratic forms and class numbers of quadratic fields, which we talked about in class (but we will avoid discussing the composition law for quadratic forms since it is not directly relevant here). The purpose of this section is to explain how to write down the fundamental domains we will use, and where the theory of the Shanks regulator comes from. Since much of this theory is usually written directly in terms of coefficients of quadratic forms (as the intended application of a lot of the literature on quadratic forms and especially the Shanks infrastructure was originally intended for algorithmic applications), I have tried to explain more clearly what everything corresponds to in the language of ideals or at least continued fractions of quadratic irrationals.

**Definition 2.1.** For a subring \(R \subset \mathbb{R}\), or (for (i) and (iii)) an arbitrary ring \(R\),

(i) \(\mathcal{V}(R)\) is the set of binary quadratic forms over \(R\);

(ii) \(\mathcal{V}_{0<\text{disc}<T}(R)\) denotes the subset of \(\mathcal{V}(R)\) consisting of forms of discriminant in \((0, T)\);

(iii) \(\mathcal{V}_{\text{disc}=D}(R)\) denotes the subset of \(\mathcal{V}(R)\) consisting of forms of discriminant exactly \(D\);

(iv) \(\mathcal{V}^{\text{fund}}(R)\) denotes the subset of \(\mathcal{V}(R)\) consisting of forms with fundamental discriminant;

(v) \(\mathcal{V}_y(R) := \mathcal{V}^y(R) \cap \mathcal{V}_y(R)\) whenever this is defined;

In most of the literature, only the \(SL_2(\mathbb{Z})\)-action on \(\mathcal{V}_{\text{disc}=D}(\mathbb{Z})\) is considered, in which case one obtains a bijection of sets
\[
SL_2(\mathbb{Z}) \cdot \mathcal{V}_{\text{disc}=D}(\mathbb{Z}) \cong \text{Cl}^+(k_D).
\]

\(^2\)Of course there is still some dependence on the regulators, since Sarnak’s asymptotic averaging formula is about averages over sets that depend on the regulators

\(^3\)No pun intended.
This is the same as \( \text{Cl}(kD) \) in the case of imaginary quadratic fields, but in our case \( D > 0 \) and we are dealing with real quadratic fields. This issue is not very deep. One way of dealing with it is to use the narrow regulator \( R^+(kD) \) and the fact

\[
h^+(kD)R^+(kD) = 2h(kD)R(kD).
\]

In this paper, thanks to being enlightened by Fabian Gundlach, we use the somewhat more elegant

**Definition 2.2.** The twisted \( GL_2(\mathbb{Z}) \)-action on \( \mathcal{V}(\mathbb{Z}) \) is defined by

\[
(M \cdot f)(X, Y) = \frac{1}{\det M} f \left( M^T \begin{pmatrix} X \\ Y \end{pmatrix} \right).
\]

The reason I say that this definition is more elegant is that the proof of the bijection of sets

\[
GL_2(\mathbb{Z}) \backslash \mathcal{V}_{\text{disc}=D}(\mathbb{Z}) \cong \text{Cl}(kD)
\]

is then slightly less messy, and also it allows us to get directly at the class group rather than having to deal with the narrow class group. As we saw in class, the main idea of the bijection comes from

**Proposition 2.3.** We have a well-defined bijection of sets

\[
k^\times_D \backslash \{ \text{bases}(\omega_1, \omega_2) \text{ of fractional ideals of } kD \} \cong \mathcal{V}_{\text{disc}=D}(\mathbb{Z})
\]

given by

\[
[(\omega_1, \omega_2)] \mapsto \frac{N_{\mathbb{Q}}^{kD}(\omega_1 X + \omega_2 Y)}{\det S}
\]

where \( S : kD \to kD \) is the \( \mathbb{Q} \)-linear map taking the basis \((1, \frac{D+\sqrt{D}}{2})\) of \( \mathcal{O}_{kD} \) to \((\omega_1, \omega_2)\).

**Proof.** We did this in class on Feb. 25, 2020. \( \square \)

The bijection between the ideal class group and \( GL_2(\mathbb{Z}) \backslash \mathcal{V}_{\text{disc}=D}(\mathbb{Z}) \) then follows from the fact that the \( GL_2(\mathbb{Z}) \)-action on bases of fractional ideals commutes with the diagonal \( k^\times_D \)-action.

If \( f(X, Y) \) corresponds under the bijection of Proposition 2.3 to \([(\omega_1, \omega_2)]\), then it is clear that

\[
f \left( \frac{-\omega_2}{\omega_1}, 1 \right) = 0,
\]

and thus the roots of \( f(X, 1) \) have some useful meaning in terms of ideal classes: they are exactly the quadratic irrational \( -\frac{\omega_2}{\omega_1} \) and its Galois conjugate. If \( f(X, Y) = aX^2+bXY+cY^2 \), we saw in class (and in middle school) that these numbers are exactly

\[
-\frac{b \pm \sqrt{D}}{2a}.
\]

Thinking in terms of these quadratic irrationals as well as ideals (useful in general for conceptual proofs) and quadratic forms (useful in general for efficient computations) proves to be a useful middle ground. The twisted \( GL_2(\mathbb{Z}) \)-action on \( \mathcal{V}_{\text{disc}=D}(\mathbb{Z}) \) acts on the roots of \( f(X, 1) \) by fractional linear transformations. This is where the standard fundamental domain for \( GL_2(\mathbb{Z}) \backslash \mathcal{V}_{\text{disc}=D}(\mathbb{Z}) \) when \( D < 0 \) comes from: the numbers \( -\frac{b \pm \sqrt{D}}{2a} \) can be assumed to lie in
the upper half plane (since we assume that $D$ is non-square and so $a \neq 0$, and $D < 0$ means that $a, c$ have the same sign; they can be made both positive via the element of $GL_2(\mathbb{Z})$ of
determinant $-1$ which switches $X$ and $Y$), so just take the set of forms lying in the standard
fundamental domain for the action of $PSL_2(\mathbb{Z})$ on the upper half-plane $H$. It is easy to
see from this that the class group is finite (since there are finitely many points of the form
$(-b + \sqrt{D})/a$ in the fundamental domain for fixed $D$). As we saw in class, this forms an
almost fundamental domain, where we can see now that fact that the stabilizers are finite
comes the finiteness of the stabilizers of the action of $PSL_2(\mathbb{Z})$ on $H$.

Unfortunately, when $D > 0$, the roots lie on the real line, so we cannot directly use the
familiar action of $PSL_2(\mathbb{Z})$ on $H$. In fact, we saw in class that in this case the stabilizers
are infinite (as they are isomorphic to $\mathcal{O}_{k_\mathcal{O}}^\times$), so we cannot expect to get a “fundamental
domain” in the sense defined in class. On the other hand, the action on the real line is still
a familiar thing, from the theory of continued fractions. This is where the reduction theory
of indefinite binary quadratic forms comes from.

2.1. Reduction theory for indefinite binary quadratic forms. Now we switch to a
higher level of rigor, since we want to get the right answer for the constant.

Fix $D > 0$ a fundamental discriminant, and let $f \in \mathcal{V}_{\text{disc}=D}(\mathbb{Z})$. The two roots of $f(X,1)$ are

$$-b \pm \sqrt{\frac{D}{2a}}.$$ 

There are two binary quadratic forms $g$ of discriminant $D$ having these as the roots of
$g(X,1)$, namely $\pm f$. This doesn’t bother us, since the sign is determined by which order the
roots come in. In particular, we still have

**Proposition 2.4.** There is an isomorphism of sets

$$GL_2(\mathbb{Z}) \backslash \mathcal{V}_{\text{disc}=D}(\mathbb{Z}) \cong GL_2(\mathbb{Z}) \backslash \mathcal{Q}_D,$$

where

$$\mathcal{Q}_D := \left\{ \frac{-b + \sqrt{D}}{2a} \in \mathbb{R} : a, b \in \mathbb{Z}, \text{ and } 4a|(D - b^2) \right\}$$

and the left-action of $GL_2(\mathbb{Z})$ on $\mathcal{Q}_D$ is defined by $M \cdot \omega := (M^\top)^{-1}\omega$, where $(M^\top)^{-1}$ acts
on $\omega$ as a fractional linear transformation.

**Proof.** First, it’s clear that the map

$$\mathcal{V}_{\text{disc}=D}(\mathbb{Z}) \to \mathcal{Q}_D$$

sending $aX^2 + bXY + cY^2$ to $\frac{-b + \sqrt{D}}{2a}$ is a bijection, since we can recover $a$ and $b$ and $c$ directly
from $(-b + \sqrt{D})/(2a)$. We just need to check that this bijection is $GL_2(\mathbb{Z})$-equivariant, which
it suffices to do on the three generators of $GL_2(\mathbb{Z})$ given by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$ 

Each of these is pretty easy:
• Starting at \( aX^2 + bXY + cY^2 \), acting on the left by \( M \in GL_2(\mathbb{Z}) \) such that \( M^\top = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) yields \( aX^2 + (b + 2a)XY + (a + b + c)Y^2 \), whereas acting on \( \frac{b + \sqrt{D}}{2a} \) by \( M \) yields \( \frac{-(b+2a)+\sqrt{D}}{2a} \) since \( M^{-1} \) is translation by \(-1\).

• Starting at \( aX^2 + bXY + cY^2 \), acting on the left by \( M^\top = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \) yields \( cX^2 - bXY + aY^2 \), whereas acting on \( -\frac{b + \sqrt{D}}{2a} \) by \( M \) yields \( \frac{-b-\sqrt{D}}{2c} \) since \( M^{-1} \) is \( \alpha \mapsto -\frac{1}{\alpha} \).

• Starting at \( aX^2 + bXY + cY^2 \), acting on the left by \( M^\top = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \) yields \( -cX^2 - bXY - aY^2 \), whereas acting on \( -\frac{b + \sqrt{D}}{2a} \) by \( M \) yields \( -\frac{b+\sqrt{D}}{2c} \) since \( M^{-1} \) is \( \alpha \mapsto \frac{1}{\alpha} \).

Of course, this is also easy to see just by thinking about it, but I wanted to make sure I had the right answer. \( \square \)

Equipped with this convenient bijection, we can think about finding a canonical representative of the \( GL_2(\mathbb{Z}) \)-equivalence class of \( f \in V_{\text{disc}} = D(\mathbb{Z}) \) in terms of the same problem for the \( GL_2(\mathbb{Z}) \) action on \( \mathcal{O}_D \). This is where the theory of continued fractions comes in: the operation

\[
\rho(\alpha) = \frac{1}{\alpha} - \left\lfloor \frac{1}{\alpha} \right\rfloor
\]

takes \( \alpha \in \mathcal{O}_D \) to a \( GL_2(\mathbb{Z}) \)-equivalent element of \( \mathcal{O}_D \). By a classical theorem of Gauss, every quadratic irrational has a periodic continued fraction, so every \( \alpha \in \mathcal{O}_D \) is equivalent (specifically via repeated applications of \( \rho \)) to a quadratic irrational whose reciprocal has purely periodic continued fraction. More specifically, recall the following (extremely classical) fact from the theory of continued fractions:

**Lemma 2.5.** All quadratic irrationals have a periodic continued fraction expansion. A quadratic irrational \( \alpha \) has a purely periodic continued fraction expansion if and only if \( \alpha > 1 \) and \(-1 < \sigma(\alpha) < 0 \), where \( \sigma(\alpha) \) denotes the Galois conjugate of \( \alpha \).

**Proof.** See [4]. \( \square \)

So as a direct consequence, we have

**Corollary 2.6.** Every element of \( \mathcal{O}_D \) is \( GL_2(\mathbb{Z}) \)-equivalent to some \( \alpha \in \mathcal{O}_D \) with \( \alpha \in (0,1) \) and \( \sigma(\alpha) < -1 \).

**Proof.** The numbers

\[
\rho(\alpha), \rho^2(\alpha), \ldots
\]

are exactly the remainders involved in computing the continued fraction of \( 1/\alpha \), i.e. if

\[
\frac{1}{\alpha} = [a_0, a_1, \ldots]
\]

then

\[
\rho^n(\alpha) = [a_n, a_{n+1}, \ldots]
\]

for \( n \geq 1 \). By Lemma 2.5, since \( 1/\alpha \) is also a quadratic irrational, the \( a_n \)'s are eventually periodic, and thus the same is true of the \( \rho^n(\alpha) \)'s. In particular, if

\[
\frac{1}{\alpha} = [a_0, \ldots, a_k; \overline{a_{k+1}, \ldots, a_{\ell}}]
\]
with \( k \geq 0 \), then \( \rho^{k+1}(\alpha) \) has a purely periodic continued fraction, which means by Lemma 2.5 that \( \rho^{k+1}(\alpha) > 1 \) and \(-1 < \sigma(\rho^{k+1}(\alpha)) < 0\), and thus \( \frac{1}{\rho^{k+1}(\alpha)} \), which is \( GL_2(\mathbb{Z})\)-equivalent to \( \alpha \), has the desired property. On the other hand, if \( 1/\alpha \) has purely periodic continued fraction, then we already know that \( \alpha \) has the desired property. \( \square \)

Writing this in the language of Proposition 2.4, if we define

**Definition 2.7.** Call a quadratic form \( aX^2 + bXY + cY^2 \in V_{\text{disc}} = D(\mathbb{Z}) \) reduced if \( |\sqrt{D} - 2a| < b < \sqrt{D} \)

then this just means we have

**Corollary 2.8.** Every element of \( V_{\text{disc}} = D(\mathbb{Z}) \) is \( GL_2(\mathbb{Z})\)-equivalent to a reduced element.

**Proof.** The previous corollary combined with Proposition 2.4 says that every form of discriminant \( D \) is equivalent to one of the form \( aX^2 + bXY + cY^2 \) with

\[
0 < \frac{-b + \sqrt{D}}{2a} < 1
\]

and

\[
\frac{-b - \sqrt{D}}{2a} < -1.
\]

If \( a > 0 \), the second equation is equivalent to

\[
2a - \sqrt{D} < b
\]

and the first is equivalent to

\[
0 < -b + \sqrt{D} < 2a,
\]

i.e. \( b < \sqrt{D} \) and \( \sqrt{D} - 2a < b \), as desired. On the other hand, actually these equations imply already that \( a > 0 \), since if \( a < 0 \) then the second equation implies that \( b < 0 \) but the first equation implies \( b > \sqrt{D} > 0 \). \( \square \)

It’s clear at least that there are finitely many reduced elements of \( V_{\text{disc}} = D(\mathbb{Z}) \), so at least we have proved over the course of this paper that \( \text{Cl}(K) \) is finite for all quadratic fields \( K \). The problem we are having is that \( h(K) \) is not (essentially) equal to the number of reduced forms as it was in the quadratic imaginary case, because there is no guarantee that each equivalence class has a unique reduced representative, or even a constant number of reduced representatives. Instead, by Lemma 2.5 and the following discussion, there are cycles of reduced forms under the \( \rho \) operator (here we abuse notation to view \( \rho \) as acting on \( V_{\text{disc}} = D(\mathbb{Z}) \) via the bijection of Proposition 2.4), and predicting the lengths of these cycles is the same as predicting the length of the period of the continued fraction expansion of a given quadratic irrational; this is a hard problem as far as I know. Obviously if two reduced forms are in the same cycle they are equivalent (since \( \rho \) is given by acting by an element of \( GL_2(\mathbb{Z}) \)). The converse is also true:

**Lemma 2.9.** If two reduced forms \( f, g \in V_{\text{disc}} = D(\mathbb{Z}) \) are \( GL_2(\mathbb{Z})\)-equivalent, then there is some \( n \in \mathbb{N} \) such that \( f = \rho^n g \).

**Proof.** This is essentially the same as [1, Theorem 3.5]. I don’t know if there is a good conceptual reason why this is true. See also [5, Theorem 5.18]. \( \square \)

As a result, we have
Corollary 2.10. The number of cycles under the action of $\rho$ on reduced forms in $\mathcal{V}_{\text{disc}=D}(\mathbb{Z})$ is $h(k_D)$.

Remark. I have written everything here in terms of wide equivalence and the twisted $GL_2(\mathbb{Z})$-action. It seems to work out somewhat nicer than what I’ve seen in the literature using narrow equivalence, where there is an extra sign that must be kept track of. I’m curious why narrow equivalence seems to be the most popular thing to work with, especially since the class group is of more fundamental interest as far as I know. Of course, in our case we shouldn’t expect it to matter much, since $h^+ = h$ for imaginary quadratic fields (there are no real embeddings so the totally positive condition is vacuous), and for real quadratic fields $h^+ R^+ = 2h R$ where $R^+$ denotes the narrow regulator.

2.2. The Shanks infrastructure. It isn’t enough to just count reduced forms, since we don’t have precise control over the size of each cycle. This is where the Shanks infrastructure comes in. The basic premise of the infrastructure is to construct a distance function for which the cycles really do all have the same length. So far, everything we’ve written down has been leveraging the theory of continued fractions for the quadratic irrational associated to a quadratic form. The Shanks infrastructure makes more sense to define in terms of ideals, however.

Definition 2.11. Let $a, b$ be fractional ideals of $\mathcal{O}_{k_D}$, such that

$$\gamma a = b$$

for some $\gamma \in k_D^\times$. Then the Shanks infrastructure provides a distance between the two ideals given by

$$d(a, b) = \frac{1}{2} \log \left| \frac{\gamma}{\sigma(\gamma)} \right| .$$

Notice that the infrastructure might depend on the choice of $\gamma$. For any unit $u$, $\gamma u$ also works, so the infrastructure is technically multiply defined, as

$$\frac{1}{2} \log \left| \frac{\gamma u}{\sigma(\gamma u)} \right| = \frac{1}{2} \left( \log \left| \frac{\gamma}{\sigma \gamma} \right| + \log \left| \frac{u}{\sigma u} \right| \right) .$$

Since $u/\sigma u = \pm \frac{1}{\sigma(u)^2}$ (as we are in a quadratic field and the norm of $u$ is $w \sigma(u) = \pm 1$) is the square of a unit, this means that the infrastructure is well-defined modulo $R(k_D)$ (this is the reason for the factor of $1/2$ in front). This is useful for the following reason: If we have a cycle of fractional ideals which are all equivalent but distinct,

$$a_1 \sim a_2 \sim \cdots \sim a_n \sim a_{n+1} = a_1 ,$$

then from the definition of the infrastructure, it’s clear that

$$\sum_{i=1}^{n} d(a_i, a_{i+1}) = d(a_1, a_1) = 0 \in R/R(k_D)\mathbb{Z} ,$$

and $n$ is the least integer $\geq 1$ for which this is true. If we choose to take the smallest positive representative of $d(a_i, a_{i+1})$ mod $R(k_D)$, then this implies that

$$\sum_{i=1}^{n} d(a_i, a_{i+1}) = d(a_1, a_1) \in R(k_D) \cdot \mathbb{N} .$$
Associating the fractional ideal
\[ Z + \frac{-b + \sqrt{D}}{2a} Z \]
to \( f = aX^2 + bXY + cY^2 \) as usual, it is shown in [2, Proposition 5.8.3] that
\[
d(f, \rho(f)) = \frac{1}{2} \log \left| \frac{b + \sqrt{D}}{b - \sqrt{D}} \right|.
\]
It follows that summing \( \frac{1}{2} \log \left| \frac{b + \sqrt{D}}{b - \sqrt{D}} \right| \) over a cycle of reduced forms yields exactly some positive integer multiple of \( R(k_D) \). In fact, it is exactly \( R(k_D) \), so we have

**Proposition 2.12.** For any fundamental discriminant \( D \),
\[
h(k_D)R(k_D) = \sum_{\text{reduced } \mathfrak{f} \in \mathcal{V}_{\text{disc} < T}(Z)} \frac{1}{2} \log \left| \frac{b + \sqrt{D}}{b - \sqrt{D}} \right|.
\]

**Proof.** As remarked above, it suffices to show that the sum of the quantity \( \frac{1}{2} \log \left| \frac{b + \sqrt{D}}{b - \sqrt{D}} \right| \) over a cycle of reduced forms is equal to the regulator (rather than just some positive integer multiple of it). To do this, I just refer to a strengthened version of Lemma 2.9, namely the one given in [5, Theorem 5.18], with \( \kappa \) equal to the appropriate fundamental unit and \( a = b \). Lenstra [6] and seemingly everyone else leaves this detail out, so I feel okay not spelling it out completely. Maybe I should be very embarrassed by this — should I have been able to deduce this directly from the version of Lemma 2.9 I have stated here? \( \square \)

For reduced forms, we have \( b < \sqrt{D} \), so the sum we are interested in when proving Theorem 1.1 is
\[
\sum_{0 < D < T} h(k_D)R(k_D) = \sum_{\text{reduced } \mathfrak{f} \in \mathcal{V}_{\text{disc} < T}(Z)} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right).
\]

## 3. Proof of the asymptotic formula

In the previous section, we reduced Theorem 1.1 to proving asymptotics on
\[
\sum_{\text{reduced } \mathfrak{f} \in \mathcal{V}_{\text{disc} < T}(Z)} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right)
\]
as \( T \to \infty \).

### 3.1. The geometry of numbers

From now on the method is pretty much identical to the one from class. In order to derive the desired asymptotics on Equation (3.1), we start by extending to all possible discriminants (then we will sieve them out). Let
\[
\mathcal{V}_{0 < \text{disc} < T}(Z) = \left\{ aX^2 + bXY + cY^2 \in \mathcal{V}_{0 < \text{disc} < T}(Z) : |\sqrt{D} - 2a| < b < \sqrt{D} \right\}
\]
and
\[
\mathcal{V}_{0 < \text{disc} < T}(R) = \left\{ aX^2 + bXY + cY^2 \in \mathcal{V}_{0 < \text{disc} < T}(R) : |\sqrt{D} - 2a| < b < \sqrt{D} \right\}.
\]
We expect to be able to approximate
\[ \sum_{f \in V_{0 < \text{disc} < T}(\mathbb{Z})} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \]
by
\[ V_T = \int \int \int_{(a,b,c) \in V_{0 < \text{disc} < T}(\mathbb{R})} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \, da db dc, \]
which is what we will prove is true asymptotically as \( T \to \infty \) in this section. Actually, this integral converges and is equal to \( \frac{\pi^2}{36} T^{3/2} \), as we will show in Appendix A, but for now we just prove it assuming that the integral converges for fixed \( T \). It is very convenient that the integrand is invariant under scaling, and the discriminant is homogeneous of degree 2 in the three variables. This at least implies via changing variables to \( T \frac{1}{2} a, T \frac{1}{2} b, T \frac{1}{2} c \)
that \( V_T = T^{3/2} V_1 \), which reduces the work of Appendix A to showing that \( V_1 = \frac{\pi^2}{36} \).

**Proposition 3.1.** As \( T \to \infty \),
\[ \sum_{f \in V_{0 < \text{disc} < T}(\mathbb{Z})} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \sim V_T. \]

**Proof.** This proof follows the same technique as the geometry of numbers argument in [9].

Since the integral defining \( V_1 \) is improper (the integrand has singularities as \( ac \to 0 \)), we need to start with the definition
\[ V_1 = \lim_{\vartheta \to 0^+} V_{1,\vartheta} \]
where
\[ V_{1,\vartheta} = \int \int \int_{(a,b,c) \in V_{0 < \text{disc} < 1}(\mathbb{R})} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \]
Now that \( a, -c \) are bounded below, we can view \( V_{1,\vartheta} \) as the integral of the smooth function
\[ \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \]
on the compact subset of \( \mathbb{R}^3 \) given by conditions
\[ 0 \leq b^2 - 4ac \leq 1; a, -c \geq \vartheta, \left| \sqrt{b^2 - 4ac} - 2a \right| \leq b. \]

This region is not only compact, but also it has the same Lebesgue measure as its interior (the boundary is the union of some subsets of 2-dimensional submanifolds of \( \mathbb{R}^3 \)), which is why we might as well integrate on the interior, where (by compactness of the whole thing) the integrand is bounded and the integral exists. The key trick is that (again using compactness,\n\footnote{Note that we have made no claims about reduction of indefinite binary quadratic forms of arbitrary discriminant, with real or integral coefficients: we have shown that \( h(k_D)R(k_D) \) is equal to this sum whenever \( D \) is a fundamental discriminant, and find it convenient for the purposes of carrying out the geometry of numbers argument to extend the definition to arbitrary discriminants.}
\footnote{I think I have found a way to make your technique work; maybe I will add it later.}
approximating the interior with unions of boxes of length $T^{-1/2}$, and applying the dominated convergence theorem) abusing the fact that $\frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right)$ is invariant under scaling as well as the homogeneity properties of all the conditions defining the set being summed over, we have

$$V_{1,\vartheta} = \lim_{T \to \infty} T^{-3/2} \sum_{(a,b,c) \in V_{0, \text{disc} < T} \left( T^{-1/2} \mathbb{Z} \right)} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right).$$

Now we bound the error between the sum on the inside and the same sum without the bound on $a$ and $-c$. First, note that everything is symmetric in $a$ and $-c$ (see [2] for a proof of why the reduced condition is symmetric for forms over $\mathbb{Z}$ as is the case here), so it suffices to bound

$$\sum_{(a,b,c) \in V_{0, \text{disc} < T} \left( \mathbb{Z} \right)} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right).$$

The condition $aX^2 + bXY + cY^2 \in V_{0, \text{disc} < T} \left( \mathbb{Z} \right)$ and $a < \vartheta T^{1/2}$ implies (for $\vartheta < 1$ which we might as well assume)

$$1 \leq a < T^{1/2}; a \in \left[ \frac{\sqrt{D} - b}{2}, \frac{\sqrt{D} + b}{2} \right]; D < T; c \leq -1.$$ If we further require $c \leq -T^{1/2}$, then using the appropriate concavity property of $x \mapsto \sqrt{x}$, we have

$$\sqrt{D} - b \geq \frac{-4ac}{2\sqrt{D}} > 2a$$

since $\sqrt{D} < T^{1/2}$, which contradicts the condition that $a \geq \frac{\sqrt{D} - b}{2}$. As a result, it suffices to bound

$$\sum_{(a,b,c) \in V_{0, \text{disc} < T} \left( \mathbb{Z} \right); a < \vartheta T^{1/2}, -c < T^{1/2}} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right).$$

To do this, we continue to emulate the technique in [9]. Split the interval $[1, T^{1/2})$ into subintervals of the form

$$C_k = \left[ \frac{T^{1/2}}{2^{k+1}}, \frac{T^{1/2}}{2^k} \right],$$

containing at most $\frac{T^{1/2}}{2^k}$ positive integers, for integers $k \geq 0$, and $[1, \vartheta T^{1/2})$ into subintervals of the form

$$A_\ell = \left[ \frac{\vartheta T^{1/2}}{2^{\ell+1}}, \frac{T^{1/2}}{2^\ell} \right].$$
containing at most $\frac{T^{1/2}}{2\vartheta}$ positive integers, for integers $\ell \geq 0$. The fact that $1 \leq b \leq T^{1/2}$ for all the quadratic forms being summed over means that the sum we are interested in is safely bounded above by

$$\sum_{b=1}^{T^{1/2}} \sum_{a=1}^{\vartheta T^{1/2}} \sum_{-c=1}^{\vartheta T^{1/2}} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right).$$

For fixed $a, c$ the summand is clearly maximized when $b = T^{1/2}$. Moreover,

$$\log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) = \log \frac{D + b^2 + 2b\sqrt{D}}{-4ac} \leq \log \frac{T}{-ac},$$

which for $a \in A_\ell$ and $-c \in C_k$ is maximized when $a = \vartheta T^{1/2 - \ell - 1}$ and $c = T^{1/2 - k - 1}$. So we can bound the size of the cusp by

$$\sum_{(a,b,c) \in V_{\text{red}} \cap \mathbb{Z}} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \leq T^{1/2} \sum_{\ell=0}^{\infty} \sum_{k=0}^{\infty} T^{1/2} \sum_{\ell=0}^{\vartheta T^{1/2 - \ell - 1}} \frac{1}{2} \log \frac{T}{\vartheta T^{1/2 - \ell - 1} T^{1/2 - k - 1}}$$

$$= \left( \sum_{\ell=0}^{\infty} \sum_{k=0}^{\infty} 2^{-k-\ell-1} \right) \vartheta \log(\vartheta^{-1}) T^{3/2}$$

$$+ \left( \sum_{\ell=0}^{\infty} \sum_{k=0}^{\infty} 2^{-k-\ell-1}(\ell + k + 2) \right) \vartheta T^{3/2}$$

$$\ll (\vartheta + \vartheta \log(\vartheta^{-1})) T^{3/2}$$

since the infinite sums in question converge to values that do not depend on $\vartheta$ or $T$. By the symmetry argument from before, the same bound holds if you switch $a$ and $-c$. So in fact,

$$T^{-3/2} \left| \sum_{(a,b,c) \in V_{\text{red}} \cap \mathbb{Z}} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) - \sum_{(a,b,c) \in V_{\text{red}} \cap \mathbb{Z}} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \right| \ll \vartheta + \vartheta \log(\vartheta^{-1})$$

which means that for any $1 > \vartheta > 0$,

$$V_{1,\vartheta} - O(\vartheta + \vartheta \log \vartheta^{-1}) \leq \liminf_{T \to \infty} T^{-3/2} \sum_{(a,b,c) \in V_{\text{red}} \cap \mathbb{Z}} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \leq V_{1,\vartheta} + O(\vartheta + \vartheta \log \vartheta^{-1})$$

and taking $\vartheta \to 0$ we obtain

$$\lim_{T \to \infty} T^{-3/2} \sum_{(a,b,c) \in V_{\text{red}} \cap \mathbb{Z}} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) = V_1,$$

as desired. \qed
3.2. Sieving for fundamental discriminants and concluding the main theorem. We know from Section 2 that
\[ \sum_{(a,b,c) \in V_{0 < \text{disc} < T}^{\text{fund, red}}(\mathbb{Z})} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) = \sum_{0 < D < T} h(k_D) R(k_D) \]
where the sum on the right is only over fundamental discriminants. And we just computed an asymptotic expression for something very close to this, namely the larger sum
\[ \sum_{(a,b,c) \in V_{0 < \text{disc} < T}^{\text{red}}(\mathbb{Z})} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \sim V_1 T^{3/2}. \]
To deduce Theorem 1.1, we apply the same sieve technique from class. The main computation was already done on problem set 4, so I just state the result.

Lemma 3.2. A discriminant \( D \) is fundamental if and only if it is at each prime \( p \). Moreover, a form \( aX^2 + bXY + cY^2 \in \mathcal{V}(\mathbb{Z}) \) being fundamental at \( p \) depends only on the reduction of the coefficients mod \( p^3 \). Exactly \( (1 - p^{-2} - p^{-4})p^{12} \) of the \( p^{12} \) residue classes in \( \mathcal{V}(\mathbb{Z}/p^3\mathbb{Z}) \) are fundamental at \( p \).

So the set of forms \( aX^2 + bXY + cY^2 \in \mathcal{V}(\mathbb{Z}) \) with discriminant fundamental at \( p \) is the disjoint union of \( (1 - p^{-2} - p^{-4})p^{12} \) shifted lattices of covolume \( p^{-12} \) in \( \mathbb{R}^3 = \mathcal{V}(\mathbb{R}) \). As a result, the same argument from the proof of Proposition 3.1 shows that
\[ \sum_{f \in V_{0 < \text{disc} < T}^{\text{red}}(\mathbb{Z}) \text{ fundamental at } p} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \sim (1 - p^{-2} - p^{-3} + p^{-4})V_1 T^{3/2} \]
as \( T \to \infty \). In fact, by the Chinese remainder theorem, the same thing works for finite lists of primes, in the sense that for any \( M > 0 \),
\[ \sum_{f \in V_{0 < \text{disc} < T}^{\text{red}}(\mathbb{Z}) \text{ fundamental at all } p < M} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \sim \prod_{p < M} (1 - p^{-2} - p^{-3} + p^{-4})V_1 T^{3/2} \]
where the \( p < M \) always means positive rational primes less than \( M \). It remains to bound
\[ E := T^{-3/2} \sum_{f \in V_{0 < \text{disc} < T}^{\text{red}}(\mathbb{Z}) \text{ not fundamental at some } p \geq M} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right). \]
We do this by copying the technique from class and the previous section (which means copying off of Siegel by transitivity). Since we will take \( M \) large anyway, we assume at least that \( M > 2 \), so we only need to consider odd primes. First, recall that for reduced forms \( f = aX^2 + bXY + cY^2 \in V_{0 < \text{disc} < T}^{\text{red}}(\mathbb{Z}) \), we have \( 0 < a, b, -c < T^{1/2} \). If we moreover require that \( f \) is not reduced at \( p \), i.e. that \( p^2 | |b^2 - 4ac| \), then for any fixed choice of \( a, b \), one of the following must be true:

1. \( p \) does not divide \( a \), and \( c \) can be anything in a specific congruence class mod \( p^2 \) depending only on \( a \) and \( b \).
2. \( v_p(a) = 1 \), \( p | b \), and \( p | c \).
3. \( p^2 | a \) and \( p | b \), in which case \( c \) can be anything.
I will just explain how to bound the contribution from case (1), since that is the main term and the other two are easy. That contribution is

\[ \ll \sum_{1 \leq b < T^{1/2}} \sum_{1 \leq a < T^{1/2}} \sum_{-c \equiv c_{a,b} \pmod{p^2}} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \ll T^{1/2} \sum_{1 \leq a < T^{1/2}} \sum_{-c \equiv c_{a,b} \pmod{p^2}} \log \left( \frac{T}{-ac} \right). \]

\[ \leq T^{1/2} \sum_{k=0}^{\infty} \frac{T^{1/2}}{2k} \sum_{1 \leq c < T^{1/2}} \log \left( \frac{T}{T^{1/2} \frac{2^{k+1}}{2^k} c} \right). \]

To deal with the inside sum, rewrite it as the sum over \( c = c_{a,b} + p^2 m, \) where \( 0 < c_{a,b} \leq p^2 \) so that \( m \) ranges from 0 to at most \( T^{1/2}/p^2, \) and thus

\[ \sum_{1 \leq c < T^{1/2}} \log \left( \frac{T}{T^{1/2} \frac{2^{k+1}}{2^k} c} \right) \leq \sum_{1 \leq m+1 \leq \frac{T^{1/2}}{p^2+1}} \log \left( \frac{T}{T^{1/2} \frac{2^{k+1}}{2^k} (c_{a,b} + p^2 m)} \right) \]

\[ \leq \sum_{\ell=0}^{\infty} \left( \frac{T^{1/2}}{p^2 2^\ell} + \frac{1}{2^\ell} \right) \log \left( \frac{T}{T^{1/2} \frac{2^{k+1}}{2^k} (c_{a,b} + p^2 m)} \right). \]

So the contribution from (1) is bounded above by

\[ T^{1/2} \sum_{k=0}^{\infty} \sum_{\ell=0}^{\infty} \frac{T^{1/2}}{2k} \left( \frac{T^{1/2}}{p^2 2^\ell} + \frac{1}{2^\ell} \right) \log \left( \frac{T}{T^{1/2} \frac{2^{k+1}}{2^k} (c_{a,b} + p^2 m)} \right) \]

which is ultimately \( O(T + T^{3/2}/p^2). \) One can check that the contribution from (2) and (3) are dominated by this. Union bounding, it follows that

\[ \sum_{f \in \mathcal{V}_{\text{red, fund}}^{0 < \text{disc} < T} \not\text{not fundamental at some } p > M} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \ll \sum_{M < p < T^{1/2}} T + \sum_{M < p < T^{1/2}} \frac{T^{3/2}}{p^2} \]

\[ \leq o(T^{3/2}) + T^{3/2} \sum_{n=M}^{\infty} n^{-2} \]

\[ \ll o(T^{3/2}) + \frac{T^{3/2}}{M} \]

by the prime number theorem. and thus \( E \ll 1/M \) for large \( T. \) So both the \( \liminf_{T \to \infty} \) and the \( \limsup_{T \to \infty} \) of

\[ T^{-3/2} \sum_{f \in \mathcal{V}_{\text{red, fund}}^{0 < \text{disc} < T} \not\text{not fundamental at some } p > M} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \]

are within \( O(1/M) \) of \( \prod_{p < M} (1 - p^{-2} - p^{-3} + p^{-4}) V_1. \) Taking \( M \to \infty, \) we see that the limit exists and is equal to

\[ \prod_p (1 - p^{-2} - p^{-3} + p^{-4}) V_1, \]
which is exactly the statement of Theorem 1.1, conditional on the computation of $V_1 = \frac{\pi^2}{36}$ which is carried out in Appendix A.

4. Quadratic forms and hyperbolic geodesics

Appendix A. The volume computation

Here I include my computation of the integral

$$V_1 = \int \int \int_{(a,b,c) \in V_{a<\text{disc}<1}(\mathbb{R})} \frac{1}{2} \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \, dadbdc.$$

Given how simple the answer is, I’m sure there is a better way to compute it, but this is the first thing I tried that worked. Changing variables from $(a,b,c)$ to $(a,b,D)$ and then to $(a,b,\alpha)$ where $\alpha = \sqrt{D}$, we have

$$V_1 = \frac{1}{8} \int_0^1 \int_b^1 \log \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \int_{\frac{\sqrt{D} - b}{2}}^{\frac{\sqrt{D} + b}{2}} \frac{1}{a} \, da \, dD \, db$$

$$= \frac{1}{8} \int_0^1 \int_b^1 \log^2 \left( \frac{\sqrt{D} + b}{\sqrt{D} - b} \right) \, dD \, db$$

$$= \frac{1}{4} \int_0^1 \int_b^1 \alpha \log^2 \left( \frac{\alpha + b}{\alpha - b} \right) \, d\alpha \, db.$$

From here, it is a routine computation, since the indefinite integrals of $x \log^2 (x+b)$, $x \log(x+b) \log(x-b)$ are well-known. Anyway, I did it on a computer and got $\pi^2/36$.

References