Counting Cubic Number Fields

Ross Paterson

Contents

Acknowledgements

I would like to thank my essay setter Dr. Tom Fisher for his time and patience, as well as for setting such a fascinating essay. I have thoroughly enjoyed the experience, and look forward to future study in arithmetic statistics and number theory. I would also like to thank my close friends and family for their support.

1 Introduction

The field of arithmetic statistics is a fascinating subset of number theory which has recieved considerable interest in recent years; in particular one of the 2014 fields medals was awarded to Manjul Bhargava for his work in this area. The idea, loosely speaking, is to study statistical properties of collections of arithmetic objects (e.g. number fields, elliptic curves, class groups) rather than the individual objects themselves. The particular problem we will concern ourselves with, is that of counting isomorphism classes of extensions of number fields $K/\mathbb{Q}$ of a given degree n with bounded discriminant. In fact we study one of the first major results in this area, that of counting fields $K/\mathbb{Q}$ of degree 3 – cubic number fields.

In 1969 Harold Davenport and Hans Heilbronn published a paper titled *On the Density of Discriminants in Cubic Fields* [11] in which they posed and make some headway into a fascinating question. This was given as follows: let $P^+(X)$ (resp. $P^-(X)$) be the number of cubic fields of positive (resp. negative) discriminant D such that $|D| < X$; do $\lim_{X\to\infty} X^{-1}P^{\pm}(X)$ exist, and are either of them positive? In this first paper, they are unsuccessful in giving an answer and the result that they give simply establishes bounds on suprema and infima of the values of these asymptotes. Their method of counting these fields involved relating them to binary cubic forms over $\mathbb{Z}$ and counting these instead, a problem already studied by Davenport in 1951 [9, 10].

Although their initial attempt was unsuccessful, this idea of relating cubic fields to binary cubic forms is very strong. In fact two years later, in 1971, Davenport and Heilbronn developed their approach in *On the Density of Discriminants in Cubic Fields II* [12] in which they continued to relate fields to binary cubic forms and gave a strong answer to the question – yes, the limits exist and is positive. In fact, they gave a value for the limit.

Theorem 1.1 (Davenport–Heilbronn)**.** *Let $N_3(\xi,\eta)$ denote the number of cubic fields K, up to isomorphism, such that $\xi < \Delta(K) < \eta$ where $\Delta(K)$ is the discriminant of $K/\mathbb{Q}$. Then*

$$\lim_{X\to\infty} \frac{N_3(0,X)}{X} = \frac{1}{12\zeta(3)},$$
$$\lim_{X\to\infty} \frac{N_3(-X,0)}{X} = \frac{1}{4\zeta(3)}.$$

The approach taken by Davenport and Heilbronn is fascinating. They construct a form F_K allocated to a cubic field K and show that such forms (up to a sensible notion of equivalence) identify cubic fields. The majority of the work done in actually counting these is in the papers of Davenport counting binary cubic forms, but the key component established in the second paper is that the authors identify a way to characterise a suitable set of forms to count.

More generally, one might ask what we can say about the case of degree n fields, and in this case there is a folk–conjecture (see e.g. [2]).

Conjecture 1. *If $N_n(X)$ is the number of extensions $K/\mathbb{Q}$ of degree n such that $|\Delta(K)| < X$ then the limit*

$$c_n = \lim_{X\to\infty} \frac{N_n(X)}{X},$$

exists and is positive.

This is actually a specific case of a larger conjecture of Malle [6], relating to counting extensions over a fixed base field with the added restriction of having Galois closure with a specific Galois group isomorphism class. The quadratic case follows from classical theory, giving $c_2 = \zeta(2)^{-1}$ (see Cohen [7]) and by Theorem 1.1 we have $c_3 = (3\zeta(3))^{-1}$. Moreover, one might ask what happens for $n \geq 4$. Unfortunately, the method of Davenport and Heilbronn is very reliant on properties specific to binary cubic forms and so does not generalise to the further question of counting fields of degree n. The important idea however, is that of parametrising the cubic fields with another object – in fact in 2001 Manjul Bhargava developed parametrisations for quartic and quintic rings in his revolutionary PhD thesis titled *Higher Composition Laws*. Following this work, in 2004 and 2010 Bhargava used these parametrisations to prove Conjecture 1 in the cases $n = 4, 5$ and obtain the values c_4, c_5 – an incredible feat.

In this essay we set out with the goal of establishing Theorem 1.1 using the modern approach of Bhargava–Shankar–Tsimerman [3] which is adapted from the work of Bhargava in counting quartic and

quintic fields. In order to do this we must first establish the more general framework known as the Delone–Faddeev correspondence, where we relate a class of rings known as cubic rings to binary cubic forms and then show the strength of this relationship. Following this, we set out with the more modest goal of establishing a theorem of Davenport as shown in Bhargava–Shankar–Tsimerman.

Theorem 1.2 (Davenport [9, 10])**.** *Let $N_3^o(\xi, \eta)$ denote the number of cubic orders R such that $\xi < \Delta(R) < \eta$. Then*

$$N_3^o(0, X) = \frac{\pi^2}{72}X + O(X^{5/6})$$
$$N_3^o(-X, 0) = \frac{\pi^2}{24}X + O(X^{5/6})$$

In counting cubic orders, we will find a simpler case than that of cubic fields. This gives the opportunity to develop the required theory without all of the additional overhead that comes with the case of fields. Having developed this theory, the adaptation to cubic fields is surprisingly simple.

In Section 2 we establish the notion of Delone–Faddeev correspondence for a principal ideal domain Z, a bijection between $\mathrm{GL}_2(Z)$-equivalence classes of cubic rings and binary cubic forms. This is a more general framework than that of Delone and Faddeev [13], and is a natural extension from the work of Harrer [17] to the results in Bhargava–Shankar–Tsimerman and Gan–Gross–Savin [14]. Following this we show the strength of this correpondence, in particular that the discriminant of a form corresponding to a given cubic ring is precisely the discriminant of the ring. Cubic rings which are integral domains are precisely those which correspond to cubic orders, and so we go on to show that the class of forms which correspond to integral domains are those which are irreducible. This Section also contains some computed examples, to illustrate the results and show some hands–on use for the readers clarity.

In Section 3 we proceed with the results of the Delone–Faddeev correspondence as applied to $Z = \mathbb{Z}$ to count cubic orders by counting the corresponding irreducible binary cubic forms as in Bhargava–Shankar–Tsimerman. We begin by embedding the binary cubic forms over $\mathbb{Z}$ in those over $\mathbb{R}$ as an integer lattice. We then establish a fundamental domain $\mathcal{F}$ for $\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2(\mathbb{R})$ which by action on v, a form over $\mathbb{R}$ of positive (resp. negative) discriminant, gives a multiset cover of fundamental domains for $\mathrm{GL}_2(\mathbb{Z})$ action on forms of positive (resp. negative) discriminant over $\mathbb{R}$. Points with nontrivial $\mathrm{GL}_2(\mathbb{Z})$ stabliser appear less often in this region, and so we obtain an error estimate to allow us to ignore these. We obtain a further error estimate to allow us to identify the irreducible points as simply those with first coefficient nonzero. Continuing with this domain, we present Davenports geometry of numbers [8] which was originally developed with the motivation of counting binary cubic forms embedded as an integer lattice in this way. Next we motivate and apply Bhargava's method of averaging and then begin to count lattice points in a specific region. Using some work of Wood [18] presented at the Arizona Winter School, we simplify this problem by ignoring an upper triangular transformation applied through the action of $\mathcal{F}$. We finish the section by counting irreducible binary cubic forms up to $\mathrm{GL}_2(\mathbb{Z})$-equivalence, and so binary cubic orders, establishing Theorem 1.2.

Finally in Section 4, we apply the methods developed in Sections 2 and 3 to count cubic fields. Since cubic fields can be uniquely identified with maximal cubic orders (their rings of integers) we begin by finding the set of binary cubic forms which correspond to maximal cubic rings. It will turn out that these can be identified by congruence conditions mod p^2 for each prime p, and so we define a notion of lattice decomposition for such a set and apply the lattice point counting method from Section 3. Following a necessary detour to establish the p-adic density of our set, we finally bring our results together with a simple seive to count cubic fields and prove Theorem 1.1

Throughout this project, all rings will be assumed to be commutative and containing a multiplicative identity 1. Since we will apply integration methods in our arguments, it is convenient to take the definition of a fundamental domain to be the closure of the usual definition. Further, unless otherwise specified, the notation Vol will be used to mean the Euclidean volume.

2 The Delone–Faddeev Correspondence

We give an account of the Delone–Faddeev Correspondence [13] (refined by Gan–Gross–Savin [14]). In particular this will be in the general setting of a principal ideal domain, as alluded to in Harrer [17], extending some proofs of Bhargava–Shankar–Tsimerman [3] to this setting. We begin with an account of the general set of rings and forms within which we will be working. Restricting to the cubic case, we prove a general statement of Delone–Faddeev correspondence for principal ideal domains: a bijection between equivalence classes of binary cubic forms and isomorphism classes of cubic rings. Following this, we study the strength of this correspondence by relating the respective discriminants of these objects as well as automorphism groups of the rings and stabilisers of the forms. We conclude by showing that the binary cubic forms which correspond to cubic rings which are integral domains, which in the case of rings over $\mathbb{Z}$ are precisely cubic orders, are those which are irreducible.

2.1 Cubic Rings

Definition 2.1. *An **n-ic ring** R over a base ring Z (written $R|Z$) is a ring which is isomorphic to Z^n as a Z-module.*

In particular, we are going to be interested in cubic (3-ic) rings over some base ring Z. As with orders of number fields, given an n-ic ring $R|Z$ we can identify an element $\alpha \in R$ with the linear map given by multiplication by α written as

$$\begin{aligned} m_\alpha : R &\to R \\ x &\mapsto \alpha x. \end{aligned}$$

Definition 2.2. *Let $R|Z$ be a n-ic ring with Z-basis $\alpha_1, \ldots, \alpha_n$. The **trace** and **characteristic polynomial** of $\alpha \in R$ are defined to be trace and characteristic polynomial of the Z-linear map m_α:*

$$\begin{aligned} \mathrm{Tr}(\alpha) &= \mathrm{tr}(m_\alpha) \\ \chi_\alpha(T) &= \chi_{m_\alpha}(T), \end{aligned}$$

*with respect to the given basis. Further we define the **discriminant** of R with respect to a Z-basis $\alpha_1, \ldots, \alpha_n$ to be*

$$\Delta(R) = \det\left(\mathrm{Tr}(\alpha_i \alpha_j)\right). \tag{1}$$

Note that after a change of basis performed by $M \in \mathrm{GL}_n(Z)$ the matrix $\mathrm{Tr}(\alpha_i\alpha_j)$ becomes $M\,\mathrm{Tr}(\alpha_i\alpha_j)M^T$ and so the discriminant is independent of change of basis up to multiplication by an element of $(Z^\times)^2$.

In particular, for the case of $Z = \mathbb{Z}$ we have that $(\mathbb{Z}^\times)^2 = \{1\}$ and the discriminant of $R|\mathbb{Z}$ is independent of change of basis. Further, in this case if $R|\mathbb{Z}$ is an order in a number field then these agree with the usual notion of trace, characteristic polynomial and discriminant.

Definition 2.3. *A n-ic ring $R|Z$ is called **unary** if it has a Z-basis containing the identity element 1.*

Proposition 2.4. *If Z is a principal ideal domain (PID) then any n-ic ring $R|Z$ is unary.*

Proof. Consider $Z \subset R$, then from the theory of elementary divisors there exists Z-bases β of Z and $\alpha_1, \ldots, \alpha_n$ of R such that $\beta = x\alpha_1$. Since $\beta Z = Z$ we must have $\beta \in Z^\times$ and so $\beta^{-1} = (x\alpha_1)^{-1} \in Z$. Thus $\alpha_1^{-1} = (x\alpha_1)^{-1}x \in R$ and $\alpha_1 \in R^\times$ is a unit. Scaling the basis of R to a new basis $\gamma_i = \alpha_1^{-1}\alpha_i$ we have a basis containing $\gamma_1 = 1$ as required. □

Throughout we will be working with base rings $Z = \mathbb{Z}, \mathbb{Z}_p$ as well as fields and so we can always freely assume that an n-ic ring $R|Z$ has a basis containing 1 for these. Looking specifically at cubic rings we have an additional useful definition.

Definition 2.5. *A basis $1, \omega, \theta$ of a unary cubic ring $R|Z$ is called **normal** if $\omega\theta \in Z$.*

Proposition 2.6. *Every unary cubic ring has a normal basis.*

Proof. Given $1, \omega', \theta'$ a Z-basis of R, say

$$\omega'\theta' = n + s\omega' + t\theta'$$

for $n, s, t \in Z$. Refining to the Z-basis $1, \omega, \theta$ of R given by

$$\omega = \omega' - t$$
$$\theta = \theta' - s$$

We have that

$$\omega\theta = n + s\omega' + t\theta' - s\omega' - t\theta' + st = n + st \in Z$$

□

2.2 Binary Forms

Let Z be an integral domain. Recall the following definition.

Definition 2.7. *A **binary n-ic form** over Z is a degree n homogeneous polynomial in two variables, i.e.*

$$f(x, y) = \sum_{i=0}^{n} a_i x^i y^{n-i}.$$

*for $a_i \in Z$. The **standard action** of $\gamma \in \mathrm{GL}_2(Z)$ on such f is given by*

$$(\gamma \cdot f)(x, y) = f((x, y)\gamma).$$

In particular, this essay we will be concerned with binary cubic (3-ic) forms. It will be useful to consider the property Disc of such forms, known as the discriminant.

Definition 2.8. *To define the **discriminant** of a general binary form $f \in Z[x, y]$ of degree n, write f as a product of linear factors in a fixed algebraic closure of $\mathrm{Frac}(Z)$, say*

$$f(x, y) = \prod_{i=1}^{n} (\alpha_i x - \beta_i y).$$

The discriminant of f is given by

$$\mathrm{Disc}(f) = \prod_{i \neq j} (\alpha_i \beta_j - \alpha_j \beta_i) = \pm \prod_{1 \leq i < j \leq n} (\alpha_i \beta_j - \alpha_j \beta_i)^2. \tag{2}$$

Remark 2.9. *It is a standard result in the theory of symmetric polynomials that the discriminant of a binary n-ic form can be written in terms of its coefficients. For a binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ the discriminant is equivalently given by*

$$\mathrm{Disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd. \tag{3}$$

We use this statement without proof for brevity.

The discriminant is an example of an invariant.

Definition 2.10. *We call a property I of a binary n-ic form an **invariant** if for all $\gamma \in \mathrm{SL}_2(Z)$ the property satisfies*

$$I(\gamma \cdot f) = I(f).$$

*Further we say it has **weight** k if for all $\gamma \in \mathrm{GL}_2(Z)$*

$$I(\gamma \cdot f) = \det(\gamma)^k I(f).$$

Proposition 2.11. *The discriminant of a binary n-ic form over Z is an invariant of weight $n^2 - n$.*

Proof. The result is fairly computational, write

$$f(x, y) = \prod_{i=1}^{n} (\alpha_i x - \beta_i y).$$

and let $\gamma = \begin{pmatrix} k & l \\ m & n \end{pmatrix} \in \mathrm{GL}_2(Z)$. Then we have

$$\begin{aligned}
\mathrm{Disc}(\gamma \cdot f) &= \mathrm{Disc}(f(kx+my, lx+ny)) && (4)\\
&= \mathrm{Disc}\left(\prod_{i=1}^{n} (\alpha_i(kx+my) - \beta_i(lx+ny))\right) && (5)\\
&= \mathrm{Disc}\left(\prod_{i=1}^{n} ((\alpha_i k - \beta_i l)x - (\beta_i n - \alpha_i m)y)\right) && (6)\\
&= \mathrm{Disc}\left(\prod_{i=1}^{n} (\alpha_i' x - \beta_i' y)\right), && (7)
\end{aligned}$$

where

$$\begin{aligned}
\alpha_i' &= (\alpha_i k - \beta_i l)\\
\beta_i' &= (\beta_i n - \alpha_i m).
\end{aligned}$$

Examining products of these terms we obtain

$$\begin{aligned}
\alpha_i'\beta_j' &= (\alpha_i k - \beta_i l)(\beta_j n - \alpha_j m)\\
&= \alpha_i\beta_j(kn) - \alpha_i\alpha_j(km) - \beta_i\beta_j(ln) + \beta_i\alpha_j(lm)
\end{aligned}$$

and in particular

$$\begin{aligned}
\alpha_i'\beta_j' - \beta_i'\alpha_j' &= (kn-lm)\alpha_i\beta_j + (lm-kn)\beta_i\alpha_j && (8)\\
&= \det(\gamma)(\alpha_i\beta_j - \alpha_j\beta_i). && (9)
\end{aligned}$$

So bringing together the results of equations (7) and (9) with the formula for discriminant (2) we have that

$$\begin{aligned}
\mathrm{Disc}(f(kx+my, lx+ny)) &= \mathrm{Disc}\left(\prod_{i=1}^{n} \alpha_i' x - \beta_i' y\right)\\
&= \prod_{1\le i<j\le n} \left(\alpha_i'\beta_j' - \beta_i'\alpha_j'\right)^2\\
&= \prod_{1\le i<j\le n} (\alpha_i\beta_j - \beta_i\alpha_j)^2 \det(\gamma)^2\\
&= \det(\gamma)^{2\binom{n}{2}} \mathrm{Disc}(f(x,y)).
\end{aligned}$$

Thus the discriminant is an invariant of weight $2\binom{n}{2} = n^2 - n$. □

2.3 Delone–Faddeev Correspondence

For the remainder of the section, take Z to be a PID. This means that we can take the result of Proposition 2.4 and assume that all cubic rings over Z are unary.

Definition 2.12. *Denote the space of binary cubic forms over Z by V_Z. Define the* ***twisted action*** *of $\mathrm{GL}_2(Z)$ on V_Z by,*

$$(\gamma \cdot f)(x,\, y) = \frac{1}{\det(\gamma)} f((x,\, y)\gamma). \tag{10}$$

For the Delone–Faddeev correspondence to have some of the properties we require, it is necessary to take the twisted action instead of the standard action. Note that these are the same for elements of $\mathrm{SL}_2(Z)$. For the rest of the essay, unless otherwise stated, when we discuss $\mathrm{GL}_2(Z)$-equivalence or action we are referring to the twisted action.

Theorem 2.13 (Delone–Faddeev Correspondence)**.** *There is a natural bijection between $\mathrm{GL}_2(Z)$-equivalence classes in V_Z and isomorphism classes of cubic rings $R|Z$.*

Proof. Using Propositions 2.4 and 2.6 we can take $1, \omega, \theta$ to be a normal Z-basis for R. To define R as a ring, it is necessary and sufficient to specify the values of $\omega\theta, \omega^2$ and θ^2 as well as verify the associativity axiom for R. Write

$$\begin{aligned} \omega\theta &= n \\ \omega^2 &= m - b\omega + a\theta \\ \theta^2 &= l - d\omega + c\theta, \end{aligned} \tag{11}$$

for $a, b, c, d, l, m, n \in Z$. From associativity we have

$$\begin{aligned} \omega(\omega\theta) &= n\omega & (\omega\theta)\theta &= n\theta \\ \omega^2\theta &= m\theta - b\omega\theta + a\theta^2 & \omega\theta^2 &= l\omega - d\omega^2 + c\omega\theta \\ &= (al - bn) + (-ad)\omega + (m + ac)\theta & &= (cn - dm) + (l + bd)\omega + (-ad)\theta, \end{aligned}$$

and so comparing coefficients we have

$$\begin{aligned} n &= -ad \\ m &= -ac \\ l &= -bd. \end{aligned} \tag{12}$$

From this we deduce that the cubic ring $R|Z$ with normal basis $1, \omega, \theta$ is uniquely determined up to isomorphism by $a, b, c, d \in Z$. Our correspondence is between binary cubic forms written as

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3,$$

and the corresponding ring R_f defined by the coefficients of f as in (11) and (12) above. This is certainly a bijection between isomorphism classes of cubic rings over Z with a specified normal basis and V_Z.

Further, take the natural embedding $Z \hookrightarrow R_f$ given by identifying $1 \in Z$ with the basis element $1 \in R_f$. Consider the map

$$\begin{aligned} R_f/Z &\to \wedge^2(R_f/Z) \\ r &\mapsto r \wedge r^2. \end{aligned}$$

As ω, θ are representatives of a basis for R_f/Z, setting $r = x\omega + y\theta$ for $x, y \in Z$ we get

$$\begin{aligned} r \wedge r^2 &= (x\omega + y\theta) \wedge ((x\omega + y\theta)(x\omega + y\theta)) \\ &= (x\omega + y\theta) \wedge (x^2\omega^2 + y^2\theta^2) \\ &= (x\omega + y\theta) \wedge (x^2(a\theta - b\omega) + y^2(c\theta - d\omega)) \\ &= (ax^3 + cxy^2)(\omega \wedge \theta) - (bx^2y + dy^3)(\theta \wedge \omega) \\ &= f(x, y)(\omega \wedge \theta) \end{aligned}$$

where we consider f as a representative of an element of R/Z. A change of normal basis of R corresponds to a linear map

$$\begin{pmatrix} 1 & 0 & 0 \\ -s & A & B \\ -t & C & D \end{pmatrix},$$

where s and t are uniquely obtained from the element $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GL}_2(Z)$ as in the normalisation process in Proposition 2.6. As a result, the change of Z-basis corresponds to the natural $\mathrm{GL}_2(Z)$ action on the basis $\langle \omega, \theta \rangle$ of R/Z, where γ gives the new basis $\langle 1, \omega', \theta' \rangle$ where

$$\begin{aligned} \omega' &= A\omega + B\theta \\ \theta' &= C\omega + D\theta \end{aligned}$$

and in $\wedge^2(R/Z)$

$$(\omega' \wedge \theta') = (A\omega + B\theta) \wedge (C\omega + D\theta) = \det(\gamma)(\omega \wedge \theta). \tag{13}$$

Thus the map $r \mapsto r \wedge r^2$ is given by

$$\begin{aligned} x\omega' + y\theta' &= (Ax + Cy)\omega + (Bx + Dy)\theta \\ &\mapsto f(Ax + Cy, Bx + Dy)(\omega \wedge \theta) \\ &= \frac{1}{\det(\gamma)} f(Ax + Cy, Bx + Dy)(\omega' \wedge \theta') \\ &= (\gamma \cdot f)(x, y)(\omega' \wedge \theta') \end{aligned}$$

and in particular it is clear that acting on f with an element $\gamma \in \mathrm{GL}_2(Z)$ is equivalent to change of Z–basis by γ for R_f as described above. Thus $\mathrm{GL}_2(Z)$ equivalence classes of binary cubic forms $f \in V_Z$ are in bijection with isomorphism classes of rings R_f as required. □

Note that the twisted action of $\mathrm{GL}_2(Z)$ on V_Z was necessary in order for the basis change in (13) to agree with the action on a binary form f as in the closing remarks of the proof.

Remark 2.14. *We will refer to the general systems of equations in* (11) *as the* ***characterising equations*** *for a cubic ring. Those in* (12) *will be referred to as the* ***associative laws*** *for a cubic ring.*

Proposition 2.15. *For $f \in V_Z$ the group of Z-automorphisms of R_f is naturally isomorphic to the stabiliser of f in $\mathrm{GL}_2(Z)$.*

Proof. Recall from the proof of Theorem 2.13 that the action of $\gamma \in \mathrm{GL}_2(Z)$ on f is identified with the natural linear action on the basis of R_f/Z. A Z-automorphism will therefore be a change of Z-basis for which the multiplication properties in the characterising equations 11 are preserved and so the coefficients of f are preserved. □

Proposition 2.16. *Given a binary cubic form $f \in V_Z$ and an element $\gamma \in \mathrm{GL}_2(Z)$ then we have that*

$$\mathrm{Disc}(\gamma \cdot f) = \det(\gamma)^2 \,\mathrm{Disc}(f)$$

Proof. Note that by the coefficient equation for discriminant in (3) we can clearly see that for a constant $\lambda \in Z^\times$ we have $\mathrm{Disc}(\lambda f) = \lambda^4 \,\mathrm{Disc}(f)$. By Proposition 2.11, the weight of the discriminant of a binary cubic form is 6 and so we have

$$\begin{aligned}\mathrm{Disc}(\gamma \cdot f) &= \mathrm{Disc}\left(\frac{1}{\det(\gamma)} f((x,y)\gamma)\right) \\ &= \det(\gamma)^{-4} \,\mathrm{Disc}(f((x,y)\gamma)) \\ &= \det(\gamma)^2 \,\mathrm{Disc}(f(x,y))\end{aligned}$$

□

We will be interested in counting isomorphism classes of cubic rings $R|\mathbb{Z}$ up to bounded absolute discriminant $|\Delta(R)|$. In order to do this by counting equivalence classes of binary cubic forms, we require a way to see the discriminant of R_f in f.

Proposition 2.17. *The Delone–Faddeev Correspondence preserves discriminants, so that for $f \in V_Z$*

$$\Delta(R_f) = \mathrm{Disc}(f)$$

Proof. Let $1, \omega, \theta$ be the normal basis of R_f corresponding to $f \in V_Z$ as in the characterising equations (11). Now, we have that

$$\Delta(R_f) = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\omega) & \mathrm{Tr}(\theta) \\ \mathrm{Tr}(\omega) & \mathrm{Tr}(\omega^2) & \mathrm{Tr}(\omega\theta) \\ \mathrm{Tr}(\theta) & \mathrm{Tr}(\omega\theta) & \mathrm{Tr}(\theta^2) \end{pmatrix}$$

It is clear that $\mathrm{Tr}(1) = 3$ and then we us the characterising equations to obtain the trace for the remaining basis elements,

$$\begin{aligned}\omega(X + Y\omega + W\theta) &= X\omega + Y\omega^2 + W\omega\theta \\ &= (nW + mY) + (X - bY)\omega + aY\theta\end{aligned}$$

and so

$$\mathrm{Tr}(\omega) = \mathrm{tr} \begin{pmatrix} 0 & m & n \\ 1 & -b & 0 \\ 0 & a & 0 \end{pmatrix} = -b.$$

Similarly,

$$\begin{aligned}\theta(X + Y\omega + W\theta) &= X\theta + Y\omega\theta + W\theta^2 \\ &= (Yn + lW) + (-dW)\omega + (X + cW)\theta\end{aligned}$$

$$\mathrm{Tr}(\theta) = \mathrm{tr} \begin{pmatrix} 0 & n & l \\ 0 & 0 & -d \\ 1 & 0 & c \end{pmatrix} = c$$

Now we using elementary properties of the trace and the characterising equations (11) and associative laws (12) to deduce that

$$\begin{aligned}\operatorname{Tr}(\omega^2) &= \operatorname{Tr}(m - b\omega + a\theta) \\ &= m\operatorname{Tr}(1) - b\operatorname{Tr}(\omega) + a\operatorname{Tr}(\theta) \\ &= 3m + b^2 + ac \\ &= b^2 - 2ac\end{aligned} \qquad \begin{aligned}\operatorname{Tr}(\theta^2) &= \operatorname{Tr}(l - d\omega + c\theta) \\ &= l\operatorname{Tr}(1) - d\operatorname{Tr}(\omega) + c\operatorname{Tr}(\theta) \\ &= 3l + bd + c^2 \\ &= c^2 - 2bd\end{aligned}$$

and $\operatorname{Tr}(\omega\theta) = \operatorname{Tr}(n) = 3n = -3ad$. Thus we can finally compute:

$$\begin{aligned}\Delta(R_f) &= \det\begin{pmatrix} 3 & -b & c \\ -b & b^2 - 2ac & -3ad \\ c & -3ad & c^2 - 2bd \end{pmatrix} \\ &= 3((b^2 - 2ac)(c^2 - 2bd) - 9a^2d^2) + b(3acd - b(c^2 - 2bd)) + c(3abd - c(b^2 - 2ac)) \\ &= 3(b^2c^2 - 2ac^3 - 2b^3d + 4abcd - 9a^2d^2) + (2b^3d - b^2c^2 + 3abcd) + (3abcd - b^2c^2 + 2ac^3) \\ &= b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd \\ &= \operatorname{Disc}(f)\end{aligned}$$

□

So isomorphism classes of cubic rings $R|Z$ correspond $\mathrm{GL}_2(Z)$-equivalence classes of V_Z with the same discriminant. In particular counting cubic rings of discriminant bounded by some X is equivalent to counting $\mathrm{GL}_2(Z)$-equivalence classes of binary cubic forms of discriminant bounded by the same X.

Below are some computed examples to show concretely the relationships we have constructed.

Example 1. *Consider the cubic ring $\mathbb{Z}[\sqrt[3]{2}]$. This has $\mathbb{Z}$-basis $\langle 1, \sqrt[3]{2}, \sqrt[3]{4}\rangle$, which is certainly a normal basis since*

$$\sqrt[3]{2}\sqrt[3]{4} = \sqrt[3]{8} = 2 \in \mathbb{Z}.$$

Further we can compute the associated binary cubic form f since

$$\begin{aligned}(\sqrt[3]{2})^2 &= m - b\sqrt[3]{2} + a\sqrt[3]{4} \\ &= \sqrt[3]{4}, \\ (\sqrt[3]{4})^2 &= l - d\sqrt[3]{2} + c\sqrt[3]{4} \\ &= 2\sqrt[3]{2},\end{aligned}$$

and so we have the associated form $f = x^3 - 2y^3$. Notice that this form is irreducible over $\mathbb{Q}$ since the polyomial $x^3 - 2$ is Eisenstein in $\mathbb{Q}_2$. Further if we take the matrix

$$\gamma = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$$

then we want to find f', the binary cubic form which is associated to $\mathbb{Z}[\sqrt[3]{2}]$ after we act on the basis with γ, and show that it satisfies $f' = \gamma \cdot f$. Since $\det(\gamma) = 1$,

$$\begin{aligned}\gamma \cdot f &= f(x - y, y) \\ &= (x - y)^3 - 2y^3 \\ &= x^3 - 3x^2y + 3xy^2 - 3y^3\end{aligned}$$

Now, γ acts on the basis $\langle \sqrt[3]{2}, \sqrt[3]{4}\rangle$ of $\mathbb{Z}[\sqrt[3]{2}]/\mathbb{Z}$ where $\mathbb{Z}$ is identified with the $\mathbb{Z}$-span of the basis element 1. The new basis is represented by $\langle \sqrt[3]{2}, \sqrt[3]{4} - \sqrt[3]{2}\rangle$. Set the new $\mathbb{Z}$-basis elements in $\mathbb{Z}[\sqrt[3]{2}]$ to be

$$\begin{aligned}\omega' &= \sqrt[3]{2} \\ \theta' &= \sqrt[3]{4} - \sqrt[3]{2}\end{aligned}$$

Since $\omega'\theta' = 2 - \sqrt[3]{4} = 2 - \theta' - \omega' \notin \mathbb{Z}$ we need to renormalise. By the same process as in Proposition 2.6 we arrive at the normal basis

$$\langle 1, \omega, \theta\rangle = \langle 1, \omega' + 1, \theta' + 1\rangle = \left\langle 1,\ \sqrt[3]{2} + 1,\ \sqrt[3]{4} - \sqrt[3]{2} + 1\right\rangle.$$

Finding the characterising equations we have

$$\begin{aligned}\omega^2 &= \sqrt[3]{4} + 2\sqrt[3]{2} + 1 \\ &= \theta + 3\sqrt[3]{2} \\ &= \theta + 3\omega - 3 \\ &= -3 + 3\omega + \theta,\end{aligned} \qquad \begin{aligned}\theta^2 &= 1 + 2(\sqrt[3]{4} - \sqrt[3]{2}) + (\sqrt[3]{4} - \sqrt[3]{2})^2 \\ &= -3 + 3\sqrt[3]{4} \\ &= 3\sqrt[3]{2} - 6 + 3\theta \\ &= -9 + 3\omega + 3\theta.\end{aligned}$$

Comparing these to (11) *we get that* $a = 1$, $b = -3$, $c = 3$, $d = -3$ *and thus the associated cubic form is*

$$f' = x^3 - 3x^2y + 3xy^2 - 3y^3 = \gamma \cdot f.$$

2.4 Cubic Orders

We have seen how general cubic rings over a PID Z correspond to cubic forms in V_Z, but this is too general for our main goal. We seek a criterion for when a cubic form over $Z = \mathbb{Z}$ corresponds to a cubic order, or equivalently an integral domain. In keeping with the more general results thus far we will in fact find a criterion for when a cubic form over Z corresponds to a cubic ring which is an integral domain. Not all cubic forms correspond to integral domains.

Example 2. *Consider the cubic ring* $R|\mathbb{Z}$ *given by* $R = \mathbb{Z}[i] \oplus \mathbb{Z}$ *where we define multiplication to be pairwise. This is not an integral domain since* $(1,0)(0,1) = (0,0)$*, let us find the associated binary cubic form. The natural embedding* $\mathbb{Z} \hookrightarrow R$ *is given by*

$$n \mapsto (n, n)$$

This is obviously injective and multiplying $(1,1)(a,b) = (a,b)$ *gives that our embedding of* 1 *is the identity element which we will write as* $\mathbf{1}$ *for clarity. Thus we consider the* $\mathbb{Z}$*-basis of* R *given by*

$$\langle \mathbf{1}, \omega, \theta \rangle = \langle \mathbf{1},\ (i,0),\ (0,1) \rangle .$$

$\omega\theta = (0,0)$ *is in the image of* $\mathbb{Z}$ *and so we have a normal basis already. Calculating the characteristic equations gives*

$$\begin{aligned}\omega^2 &= (-1,0) = -\mathbf{1} + \theta \\ \theta^2 &= \theta\end{aligned}$$

and so the associated polynomial is given by $a = 1$, $b = 0$, $c = 1$, $d = 0$*, i.e.* $f_R = x^3 + xy^2$*. Observe that this is reducible over* $\mathbb{Q}$*.*

From Examples 1 and 2 we can observe that there may be a relationship between cubic integral domains and elements of $V_\mathbb{Z}$ which are irreducible over $\mathbb{Q}$. This actually holds in the more general setting, but before showing this it is helpful to study the action of $\mathrm{GL}_2(Z)$ on $f \in V_Z$.

Remark 2.18. *Say* $(\alpha x + \beta y)$ *is a linear factor of* $f \in V_Z$ *in an appropriate algebraic closure. If* $\gamma = \begin{pmatrix} k & l \\ m & n \end{pmatrix} \in \mathrm{GL}_2(Z)$ *then the action of* γ *on this linear factor maps*

$$(\alpha x + \beta y) \mapsto ((\alpha k + \beta l)x + (\alpha m + \beta n)y)$$

where we absorb the $\frac{1}{\det \gamma}$ *term from* (10) *into the other factors of* f*. It is clear that this action can be identified with the natural action of* $\mathrm{GL}_2(Z)$ *on* $\mathbb{P}^1_{\mathrm{Frac}(Z)}$ *via*

$$\begin{bmatrix}\alpha \\ \beta\end{bmatrix} \mapsto \gamma \begin{bmatrix}\alpha \\ \beta\end{bmatrix} = \begin{bmatrix}\alpha k + \beta l \\ \alpha m + \beta n\end{bmatrix}$$

Proposition 2.19. *In the Delone–Faddeev Correspondence, cubic rings* $R|Z$ *which are integral domains correspond to irreducible binary cubic forms over* Z*.*

Proof. We will prove the negation of the statement, that non integral domains correspond to reducible forms.

($\Rightarrow$) Say $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ is reducible. If $a, d \neq 0$ then since f is degree 3 it must have a linear factor $(\alpha x + \beta y)$ with $\alpha, \beta \in Z \setminus \{0\}$. Further, since Z is a PID we can without loss of generality consider α, β coprime, so that there exist $k, l \in Z$ with $\alpha k + \beta l = 1$. Now, consider the matrix

$$\gamma = \begin{pmatrix} \beta & -\alpha \\ k & l \end{pmatrix}$$

This is in $\mathrm{GL}_2(Z)$ since $\det(\gamma) = 1$ by our choice of k, l and in fact from our discussion in Remark 2.18 we have

$$\gamma : (\alpha x + \beta y) \mapsto (y)$$

thus the coefficient of x^3 in $\gamma \cdot f$ is 0. Since isomorphism classes of rings correspond to binary cubic forms up to $\mathrm{GL}_2(Z)$ equivalence in the Delone Faddeev correspondence, we can substitute $\gamma \cdot f$ for f. Thus without loss of generality we can assume that $a = 0$ or $d = 0$. From the characterising equations (11) for R_f we have that the basis elements $\omega, \theta \neq 0$ satisfy $\omega\theta = n = -ad = 0$ and so R_f is not an integral domain.

($\Leftarrow$) Conversely if $R|Z$ is a cubic ring which is not an integral domain then there exist $\alpha, \beta \in R_f \setminus \{0\}$ such that $\alpha\beta = 0$. Write the characteristic polynomial of α as

$$\chi_\alpha(T) = T^3 + c_1T^2 + c_2T + c_3 \in Z[T]$$

Then by Cayley-Hamilton we know that $\chi_\alpha(\alpha) = 0$ and in particular

$$\begin{aligned} 0 &= 0\beta \\ &= (\alpha^3 + c_1\alpha^2 + c_2\alpha + c_3)\beta \\ &= c_3\beta \end{aligned}$$

As $c_3 \in Z \subset R$ we must have that $c_3 = 0$ since c_3 cannot be a zero-divisor (as $R \cong Z^3$ as a Z-module). Hence we must have that

$$\alpha(\alpha^2 + c_1\alpha + c_2) = 0 \tag{14}$$

Claim: R has a quadratic subring $\langle 1, \omega \rangle$

Proof of claim. If $\alpha^2 + c_1\alpha + c_2 = 0$ then $\alpha^2 = -c_1\alpha - c_2 \in \langle 1, \alpha \rangle$ and so we can take $\omega = \alpha$.

Else let $\omega = \alpha^2 + c_1\alpha + c_2 \neq 0$ then

$$\begin{aligned} \omega^2 &= \alpha^2(\alpha^2 + c_1\alpha + c_2) + c_1\alpha(\alpha^2 + c_1\alpha + c_2) + c_2(\alpha^2 + c_1\alpha + c_2) \\ &\overset{(14)}{=} c_2(\alpha^2 + c_1\alpha + c_2) \\ &= c_2\omega \end{aligned}$$

and so $\langle 1, \omega \rangle$ generates a quadratic subring. □

Now, scaling ω by an element of Z if necessary we can assume that ω is an element of some basis $\langle 1, \omega, \theta \rangle$ of R_f. Following the normalisation process in Proposition 2.6 we still get that $\langle 1, \omega \rangle$ generates a quadratic subring, and thus from the characterising equations (11) we have that since $\omega^2 \in \langle 1, \omega \rangle$ we must have $a = 0$ and so the corresponding binary cubic form f_R is reducible. □

With this we immediately apply to $Z = \mathbb{Z}$, and sum up the results in this Section as the following.

Corollary 2.20. *Through the Delone–Faddeev correspondence,* $\mathrm{GL}_2(\mathbb{Z})$*–equivalence classes of irreducible binary cubic forms of discriminant* D *are in bijection with cubic orders of discriminant* D*.*

3 Counting Cubic Orders

In order to count cubic orders up to isomorphism, we have thus far shown that it is sufficient to count irreducible $\mathrm{GL}_2(\mathbb{Z})$ orbits of points in $V_\mathbb{Z}$. We can think of $V_\mathbb{R}$ and $V_\mathbb{Z}$ naturally as $\mathbb{R}^4$ and $\mathbb{Z}^4$ with coordinates given by coefficients,

$$f = ax^3 + bx^2y + cxy^2 + dy^3 \longleftrightarrow (a, b, c, d),$$

so that $V_\mathbb{Z}$ is an integer lattice in $V_\mathbb{R}$.

We begin by showing that $\mathrm{GL}_2(\mathbb{R})$ has 2 nondegenerate orbits in $V_\mathbb{R}$, namely those of positive and negative discriminant. Constructing a fundamental domain $\mathcal{F}$ for $\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2(\mathbb{R})$, we note that for $v \in V_\mathbb{R}$ of positive (resp. negative) discriminant then $\mathcal{F}v$ will be an m-fold cover of the positive (resp. negative) discriminant points in $V_\mathbb{R}$, with the exception of points with nontrivial stabiliser in $\mathrm{GL}_2(\mathbb{Z})$ which appear less often. We resolve this discrepancy as well as the problem of deciding which points in $V_\mathbb{Z}$ are irreducible with error estimates, allowing us to count all lattice points up to error.

Following this, we give an account of Davenports geometry of numbers for counting lattice points and use this to motivate the averaging method of Bhargava which we then perform to obtain a region in which to count lattice points. We study the shape of the region in question and discover that there is an upper triangular transformation which will potentially lead to a difficulty with using Davenports geometry of numbers. To handle this, we give a method of Wood which allows us to ignore such transformations up to an acceptable error and then proceed to count the relevant points of interest. We conclude by proving the statement of Theorem 1.2, counting the isomorphism classes of cubic orders of positive (resp. negative) discriminant bounded in absolute value by some X and giving the first order term.

This section primarily follows the work of Bhargava, Shankar and Tsimerman [3], as well as taking the additional methods of Wood [18] and Davenport [8] for counting lattice points.

3.1 Bhargava's Fundamental Domain

We will consider the fundamental domain presented by Bhargava, Shankar and Tsimmerman [3] – which is adapted from Bhargava's work counting quartic fields [1]. We begin with a useful observation

Proposition 3.1. *The action of* $\mathrm{GL}_2(\mathbb{R})$ *on* $V_\mathbb{R}$ *has 2 non-degenerate orbits, namely*

- $V_\mathbb{R}^+ = \{v \in V_\mathbb{R} \mid \mathrm{Disc}(v) > 0\}$
- $V_\mathbb{R}^- = \{v \in V_\mathbb{R} \mid \mathrm{Disc}(v) < 0\}$

Proof. Let $f \in V_\mathbb{R}$. Since $[\mathbb{C} : \mathbb{R}] = 2$, we know that f must be reducible in $\mathbb{R}$.

- If $\mathrm{Disc}(f) > 0$ then f has 3 disctinct linear factors in $\mathbb{R}$

  $$f(x, y) = \prod_{i=1}^{3} (\alpha_i x + \beta_i y)$$

  and so using Remark 2.18 and the fact that $\mathrm{SL}_2(\mathbb{R})$ acts triply-transitively on $\mathbb{P}^1_\mathbb{R}$ we know that $\exists \gamma' \in \mathrm{SL}_2(\mathbb{R})$ which maps the points $[\alpha_i : \beta_i]$ to the points $\{[1 : 0], [0 : 1], [1 : 1]\}$. Thus

  $$\gamma' \cdot f = k(x^2y + y^2x)$$

  for some $k \in \mathbb{R}\backslash\{0\}$. Finally taking $\gamma = \begin{pmatrix} \frac{1}{k} & 0 \\ 0 & \frac{1}{k} \end{pmatrix} \gamma' \in \mathrm{GL}_2(\mathbb{R})$ we have that $\gamma \cdot f = x^2y + y^2x$. Further since two distinct projective points cannot be sent to the same point by an element of $\mathrm{GL}_2(\mathbb{R})$ we must have that $V_\mathbb{R}^+$ is indeed a $\mathrm{GL}_2(\mathbb{R})$ orbit in $V_\mathbb{R}$.

- If $\mathrm{Disc}(f) < 0$ then f has 2 factors, a linear and an irreducible quadratic factor. As in the proof of Proposition 2.19, up to $\mathrm{GL}_2(\mathbb{R})$ action we can consider this linear factor to be (y). Now considering the two factors, as in Remark 2.18 we will identify them with points in $\mathbb{P}^1_\mathbb{C}$. The linear factor corresponds to a point in $\mathbb{P}^1_\mathbb{C}$ given by $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$, whereas the quadratic factor corresponds to a pair of conjugate points $\begin{bmatrix} \alpha + i\beta \\ 1 \end{bmatrix}, \begin{bmatrix} \alpha - i\beta \\ 1 \end{bmatrix}$ for $\beta > 0$. The action of $\mathrm{GL}_2(\mathbb{R})$ here is equivalently

mobius transformation where the first of the points is the point at ∞. From complex analysis since $\alpha + \beta i$ is in the upper half plane, we know that there exists a mobius transformation which sends $\begin{bmatrix} \alpha + \beta i \\ 1 \end{bmatrix}$ to $\begin{bmatrix} i \\ 1 \end{bmatrix}$ and fixes the point at infinity. Thus we can use $\mathrm{GL}_2(\mathbb{Z})$ action to send f to a real multiple $ky(x^2 + y^2)$, and as above we can scale to get $(x^2 + y^2)$. Further, since this action amounts to a rational function with real coefficients, it cannot send real points to complex (or the converse) and two conjugate points can only map to conjugates of one another. Hence this is a complete orbit.

Since we have exhausted all points with no repeating factors these are all nondegenerate orbits. □

We will extend this notation to mean that $V_{\mathbb{Z}}^{\pm} = V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{\pm}$. In order to construct a fundamental domain for $\mathrm{GL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2(\mathbb{R})$ we will use a significant simplification, reducing to constructing a fundamental domain for $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2^+(\mathbb{R})$ where $\mathrm{GL}_2^+(\mathbb{R})$ is the subgroup of elements with positive determinant.

Lemma 3.2. *If $\mathcal{G}$ is a fundamental domain for $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2^+(\mathbb{R})$ then it is also a fundamental domain for $\mathrm{GL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2(\mathbb{R})$.*

Proof. Observe that $[\mathrm{GL}_2(\mathbb{Z}) : \mathrm{SL}_2(\mathbb{Z})] = [\mathrm{GL}_2(\mathbb{R}) : \mathrm{GL}_2^+(\mathbb{R})] = 2$. Further, we can take coset representatives

$$\mathrm{GL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) \cup \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \mathrm{SL}_2(\mathbb{Z})$$
$$\mathrm{GL}_2(\mathbb{R}) = \mathrm{GL}_2^+(\mathbb{R}) \cup \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \mathrm{GL}_2^+(\mathbb{R})$$

Thus as $\mathcal{G}$ is a minimal set of coset representatives for $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2^+(\mathbb{R})$ then

$$\begin{aligned} \mathrm{GL}_2(\mathbb{Z})\mathcal{G} &= \left(\mathrm{SL}_2(\mathbb{Z}) \cup \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}) \right) \mathcal{G} \\ &= \mathrm{SL}_2(\mathbb{Z})\mathcal{G} \cup \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \mathrm{SL}_2(\mathbb{Z})\mathcal{G} \\ &= \mathrm{GL}_2^+(\mathbb{R}) \cup \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \mathrm{GL}_2^+(\mathbb{R}) \\ &= \mathrm{GL}_2(\mathbb{R}) \end{aligned}$$

and so $\mathcal{G}$ is a fundamental domain for $\mathrm{GL}_2(\mathbb{Z}) \backslash \mathrm{GL}_2(\mathbb{R})$. □

Define the well known subgroups $K_1, A_+, N, \Lambda \subset \mathrm{GL}_2(\mathbb{R})$

$$\begin{aligned} K_1 &= \{\text{orthogonal transformations in } \mathrm{GL}_2(\mathbb{R})\} \\ A_+ &= \{a'(t) \mid t \in \mathbb{R}_{>0}\}, \quad a'(t) = \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \\ N &= \{n(u) \mid u \in \mathbb{R}\}, \quad n(u) = \begin{pmatrix} 1 & \\ u & 1 \end{pmatrix} \\ \Lambda &= \left\{ \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} \mid \lambda \in \mathbb{R}_{>0} \right\} \end{aligned}$$

Then the natural product map $N \times A_+ \times K_1 \times \Lambda \to \mathrm{GL}_2(\mathbb{R})$ can easily be seen to be an analytic diffeomorphism (see Bump [5]). The fact that this is a diffeomorphism immediately gives us that every element $g \in \mathrm{GL}_2(\mathbb{R})$ can be written uniquely as $g = na'k\lambda$ for $n \in N$, $a' \in A_+$, $k \in K_1$ and $\lambda \in \Lambda$, however we also provide a more elementary proof.

Lemma 3.3 (Iwasawa Decomposition)**.** *Every $g \in \mathrm{GL}_2(\mathbb{R})$ can be uniquely expressed as $na'k\lambda$ for some $n \in N$, $a' \in A_+$, $k \in K_1$ and $\lambda \in \Lambda$.*

Proof. Consider $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$. Multiplying γ on the right by other elements of $\mathrm{GL}_2(\mathbb{R})$, we can consider the rows as distinct points in $\mathbb{R}^2$. Thus, up to action by K_1 we can consider $A, D > 0$ and

$B = 0$ since K_1 is just the orthogonal transformations of the plane. Further, the matrix $\begin{pmatrix} A^{-1} & \\ & A^{-1} \end{pmatrix} \in \Lambda$ and so every $\delta \in \mathrm{GL}_2(\mathbb{R})$ can be uniquely expressed as

$$\begin{pmatrix} 1 & 0 \\ C & D \end{pmatrix} k\lambda \tag{15}$$

for some $k \in K_1$ and $\lambda \in \Lambda$ for some $D > 0$. Now looking at the elements $n \in N$ and $a' \in A_+$ we have that

$$na' = \begin{pmatrix} 1 & \\ u & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} = \begin{pmatrix} t^{-1} & \\ ut^{-1} & t \end{pmatrix}$$

and thus since $t \in \mathbb{R}_{>0}$, $\begin{pmatrix} t & \\ & t \end{pmatrix} \in \Lambda$, we can see that multplying na' by this gives us a unique expression for each matrix $\begin{pmatrix} 1 & \\ C & D \end{pmatrix}$ in (15) and this gives the required result. □

We now use the Iwasawa decomposition to construct the required fundamental domain for $\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2(\mathbb{R})$

Theorem 3.4 (Fundamental Domain)**.** *Let*

$$\mathcal{F} = \{na'k\lambda \mid n \in N'(a'),\, a' \in A',\, k \in K,\, \lambda \in \Lambda\}$$

where

$$K = \mathrm{SO}_2(\mathbb{R}) \qquad A' = \left\{ \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \mid t \geq \frac{\sqrt[4]{3}}{\sqrt{2}} \right\}$$

$$\Lambda = \left\{ \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} \mid \lambda > 0 \right\} \qquad N'(a') = \left\{ \begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} \mid n \in \nu(a') \right\}$$

and

$$\nu(a') = \begin{cases} [-\frac{1}{2}, \frac{1}{2}] & t \geq 1 \\ [-\frac{1}{2}, -\sqrt{1-t^4}] \cup [\sqrt{1-t^4}, \frac{1}{2}] & t < 1 \end{cases}$$

Then $\mathcal{F}$ is a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})\backslash \mathrm{GL}_2^+(\mathbb{R})$.

Proof. Take the action on the upper half plane $\mathfrak{H}$ by $\mathrm{GL}_2^+(\mathbb{R})$ given by

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot z = \frac{Dz + C}{Bz + A}$$

which is the conjugate of the usual mobius action by $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$. Note that Λ is in the kernel of this action, and in the quotient $\mathrm{GL}_2^+(\mathbb{R})/\Lambda$ we consider the stabiliser of $i \in \mathfrak{H}$.

Claim: The stabiliser of $i \in \mathfrak{H}$ is K.

Proof of claim.

$$\begin{aligned} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot i = i &\iff \frac{Di + C}{Bi + A} = i \\ &\iff Di + C = Ai - B \\ &\iff D = A,\ C = -B \end{aligned}$$

and since we are considering representatives of $\mathrm{GL}_2^+(\mathbb{R})/\Lambda$, we can assume that they have determinant 1. Thus

$$1 = AD - BC = A^2 + C^2$$

and so $A = \cos\theta$, $B = \sin\theta$ for some $\theta \in \mathbb{R}$, and

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in K$$

And so the stabiliser is K. □

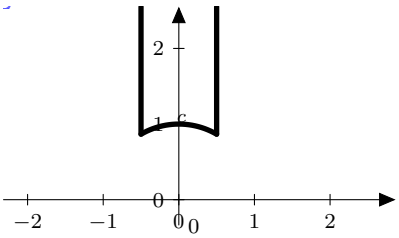


Figure 1: The fundamental domain $\mathcal{D}$ for $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$

Recall that

$$\mathcal{D} = \left\{ z \in \mathfrak{H} \mid |z| \geq 1,\ \mathrm{Re}(z) \in [-\frac{1}{2}, \frac{1}{2}],\ \right\}$$

is the classical fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{H}$. Considering the action of the remaining factors of the decomposition,

$$a' \cdot i = \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \cdot i = t^2 i$$
$$n \cdot i = \begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} \cdot i = i + n$$

we see that the set $\mathcal{F} \cdot i = \mathcal{D}$. Since elements $z \in \mathcal{D}$ are uniquely identified with elements of $N'(a')A'$, and then similarly to the proof of Lemma 3.3 each matrix in $\mathrm{GL}_2^+(\mathbb{R})$ can be obtained uniquely from these by rotations (without the possibility of reflection in K_1 since this is not in K) and scaling by appropriate λ. □

From Proposition 3.1 and Lemma 3.2, given a point $v \in V_{\mathbb{R}}^{\pm}$ then $\mathcal{F}v$ is almost a 'multi-fundamental domain' for $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}$ in the language of Wood [18]. By a multi-fundamental domain, we mean that it is a multiset which evenly covers $V_{\mathbb{R}}$

Let $n_{\pm}$ denote the cardinality of the stabiliser in $\mathrm{GL}_2(\mathbb{R})$ of $v \in V_{\mathbb{R}}^{\pm}$. Then the multiset $\mathcal{F}v$ is a union of $n_{\pm}$ fundamental domains for the action of $\mathrm{GL}_2(\mathbb{Z})$ on $V_{\mathbb{R}}^{\pm}$. Using the Delone Faddeev Correspondence, we must have that $V_{\mathbb{R}}^{+}$ corresponds to $\mathbb{R}^3$ since this has positive discriminant, and similarly $V_{\mathbb{R}}^{-}$ corresponds to $\mathbb{R} \oplus \mathbb{C}$. Thus by Proposition 2.15 we have that

$$n_{\pm} = \begin{cases} \#\operatorname{Aut}_{\mathbb{R}}(\mathbb{R}^3) = 6 & \text{if } + \\ \#\operatorname{Aut}_{\mathbb{R}}(\mathbb{R} \oplus \mathbb{C}) = 2 & \text{if } - \end{cases}$$

Of course, this need not necessarily tell us that every element in $\mathrm{GL}_2(\mathbb{Z})\backslash V_{\mathbb{Z}}$ is represented in $\mathcal{F} \cdot v$ precisely $n_{\pm}$ times. In particular, the number of times that the $\mathrm{GL}_2(\mathbb{Z})$ equivalence class of $x \in V_{\mathbb{Z}}$ is represented in $\mathcal{F}v$ is $n_{\pm}/m(x)$ where $m(x)$ is the size of the stabilizer of x in $\mathrm{GL}_2(\mathbb{Z})$. We will be counting the cases where x is irreducible and so corresponds to a cubic order R_x. In this case, using Proposition 2.15 we know that $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x)$ must be isomorphic to a subgroup of the Galois group of $\mathrm{Frac}(R_x)$ and so is either C_3 or trivial. If the irreducible point x satisfies $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(x) \cong C_3$ then we shall refer to x as a **C_3-point**.

Definition 3.5. *For $v \in V_{\mathbb{R}}^{\pm}$ define the multiset*

$$\mathcal{R}_X(v) = \{x \in \mathcal{F}v \mid |\mathrm{Disc}(x)| < X\}$$

Then we have shown the following:

Theorem 3.6. *Let $v \in V_{\mathbb{R}}^{\pm}$, $S \subset V_{\mathbb{Z}}^{\pm}$ be a $\mathrm{GL}_2(\mathbb{Z})$-invariant subset and $N(S;X)$ be the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of irreducible points in S. Then the number of irreducible points in $\mathcal{R}_X(v) \cap S$ (counting C_3-points with weight 3) is precisely the product $n_{\pm} \cdot N(S;X)$.*

Using this result with $S = V_{\mathbb{Z}}^{\pm}$, if we can obtain an error estimate for the number of C_3 points, we can use $\mathcal{F}$ as if it were a fundamental domain and count the irreducible points in $\mathcal{R}_X(v)$, and then divide by $n_{\pm}$.

3.2 Error Estimates

The result in Theorem 3.6 will be instrumental in our argument going forward. However, there are two key difficulties that this has left us with: identifying irreducible forms in the multiset $\mathcal{R}_X(v)$ and counting C_3-points. We present error estimates from Bhargava–Shankar–Tsimerman [3] to allow us to effectively ignore these. In particular, since we count orders with absolute discriminant bounded by X in Theorem 1.2 up to $O(X^{5/6})$, we seek error estimates within this error term. During our proofs we will frequently rely on the result that the number of divisors of an integer n is $O(n^\varepsilon)$ for every $\varepsilon > 0$ (see Appendix D).

Lemma 3.7 (Reducibility Estimate)**.** *Let $E \subset V_\mathbb{R}$ be a fixed compact subset with all points $x \in E$ having nonzero discriminant. Then for $v \in E$, the number of points $(a,b,c,d) \in V_\mathbb{Z} \cap \mathcal{R}_X(v)$ which are reducible binary cubic forms with $a \neq 0$ is $O(X^{3/4+\varepsilon})$ where the implied constant is only dependent on the set E.*

Proof. For $f = (a,b,c,d) \in V_\mathbb{Z} \cap \mathcal{R}_X(v)$, we have that $f \in \mathcal{F}v$ and so we can write $f = na'k\lambda v$ where $|\mathrm{Disc}(f)| < X$. By choice of v and Proposition 2.16 $|\mathrm{Disc}(f)| = \lambda^4 |\mathrm{Disc}(v)| \geq \lambda^4$ and so $\lambda < X^{1/4}$. Note that the elements n and k have bounded action on the point v. Whereas λ and a' apply the transformation

$$a'\lambda \cdot (\alpha,\beta,\gamma,\delta) = (\lambda t^{-3}\alpha, \lambda t^{-1}\beta, \lambda t\gamma, \lambda t^3\delta) = (a,b,c,d)$$

and so we can estimate $a = O(\lambda t^{-3})$. Since t is positive and bounded below by $\sqrt[4]{3}/\sqrt{2}$, we have that $t^{-k} \leq (\sqrt[4]{3}/\sqrt{2})^{-k} = O(1)$ for any fixed $k \geq 0$. Thus we can simplify to $a = O(\lambda) = O(X^{1/4})$. Similarly we can compute estimates for all products having a nonpositive power of t, giving $ab = O(X^{1/2})$, $ac = O(X^{1/2})$, $ad = O(X^{1/2})$, $abd = O(X^{3/4})$ and $abc = O(X^{3/4})$.

Consider the latter estimate, since the number of divisors of abc is $O((abc)^\delta) = O(X^{3\delta/4}) = O(X^\varepsilon)$ for any $\delta > 0$ (and hence $\varepsilon > 0$) there are $O(X^{3/4+\varepsilon})$ choices for c and hence ab. Similarly the number of choices for a from ab is $O(X^\varepsilon)$ and so the number of choices for a,b,c is $O(X^{3/4+\varepsilon})$. Hence there are this many choices of integer points (a,b,c,d) such that $a \neq 0$ and $d = 0$, which is the trivial case of reducibility (since $x \mid f$).

It remains to consider $a,d \neq 0$. Again using the estimates for the size of the products we can see that the number of choices for a,b,d in this situation is $O(X^{3/4+\varepsilon})$. Thus it is sufficient to consider how many choices remain for c if f is reducible. As f is degree 3, reducibility is equivalent to having a linear factor and so we may assume that f has the linear factor $(\alpha x - \beta y)$ where $\alpha,\beta \in \mathbb{Z}$ are coprime. Since $\alpha \mid a$ and $\beta \mid d$ we have that α,β are determined by a,d up to $O(X^\varepsilon)$. Further,

$$0 = f(\beta,\alpha) = -a\beta^3 + b\beta^2\alpha - c\beta\alpha^2 + d\alpha^3$$

and so we can uniquely obtain c from a,b,d,α,β and thus the choice of c is determined by a,b,d up to $O(X^\varepsilon)$. Hence the number of reducible integer points with $a,d \neq 0$ is $O(X^{3/4+\varepsilon})$. Since we have estimated the number of reducible points with $a \neq 0$ and $d = 0$ or $d \neq 0$ we have estimated the total at the sum which is also $O(X^{3/4+\varepsilon})$. □

Since a lattice point $(a,b,c,d) \in V_\mathbb{Z}$ with $a = 0$ has y as a factor we can use this Lemma to reduce the complicated problem of counting irreducible lattice points in a given region to counting all lattice points (a,b,c,d) with $a \neq 0$ up to error $O(X^{3/4+\varepsilon})$.

In order to estimate the number of C_3-points in the region $\mathcal{R}_X(v)$, it is extremely helpful to note that there are no C_3-points in $V_\mathbb{Z}^-$. The reason for this is that if $v \in V_\mathbb{Z}^-$ were to be a C_3-point then it would correspond through the Delone–Faddeev correspondence to a cubic order of negative discriminant with automorphism group C_3. The fraction field of this in turn is a cubic field K with negative discriminant and nontrivial Galois group – which cannot exist since the defining polynomial has one real and 2 complex roots. Thus it is only necessary to count the C_3-points in $V_\mathbb{Z}^+$, which we do by using a class of associated binary quadratic forms known as Hessian covariants.

Definition 3.8. *Every binary cubic form $f \in V_\mathbb{R}$ has a naturally associated quadratic form which we shall call the* ***Hessian covariant*** *of $f = (a,b,c,d)$ given by*

$$\mathcal{H}_f(x,y) = (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2$$

Note that this is a factor of -4 different from the usual Hessian given by $\det(\partial f/\partial x^i \partial y^j)_{i+j=2}$, and such a choice here is purely for notational convenience.

We will use this construction to give an estimate for the number of C_3-points in $V_\mathbb{R}^+$.

Lemma 3.9 (C_3-points Estimate)**.** *Let $v \in V_{\mathbb{R}}^+$. Then the number of C_3-points in $\mathcal{R}_X(v)$ is $O(X^{3/4+\varepsilon})$, where the implied constant is independent of v.*

Proof. Firstly, the number of C_3 points in $\mathcal{R}_X(v)$ is independent of v since the multiset of points $\mathcal{F}v$ is independent of choice of v. Thus it is sufficient to prove the lemma for $v = x^3 - 3x^2y$. Our reason for choosing this particular element is that it has Hessian covariant given by $\mathcal{H}_v = 9(x^2 + y^2)$, which is positive definite with fundamental root $i \in \mathbb{C}$. It is easily verified with a computer algebra system (see Appendix A Script 1) that for $\gamma \in \mathrm{SL}_2(\mathbb{R})$ we have $\gamma \cdot \mathcal{H}_v = \mathcal{H}_{\gamma \cdot v}$. Further it is clear from the definition of the Hessian covariant that since the action of $\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} \in \Lambda$ on v scales coefficients by λ, then $\mathcal{H}_{\lambda v} = \lambda^2 \mathcal{H}_v = \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} \cdot \mathcal{H}_v$. Since $\mathcal{F}\mathcal{H}_v$ consists of all reduced binary quadratic forms (see Appendix Proposition B.4), every element of $\mathcal{F}v$ must satisfy

$$|bc - 9ad| \leq b^2 - 3ac \leq c^2 - 3bd$$

In order to recognise C_3-points, note that that the characterising root (see Appendix Remark B.7) changes under action of $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ via $\theta_{\gamma \mathcal{H}_f} = \gamma \theta_{\mathcal{H}_f}$ where the latter action is the conjugate of the usual mobius action as in the proof of Theorem 3.4. So if $f \in \mathcal{F}v$ then $\mathcal{H}_f$ having stabiliser C_3 in $\mathrm{GL}_2^+(\mathbb{R})$ is equivalent to $\theta_{\mathcal{H}_f}$ having stabiliser C_3. We know from modular forms and L-functions that this means that $\theta_{\mathcal{H}_f}$ must be $\mathrm{SL}_2(\mathbb{Z})$ equivalent to one of $\frac{1 \pm \sqrt{-3}}{2}$. Since $\tau_f \in \mathcal{D}$, the classical fundamental domain (see Theorem B.3) this means that we must precisely have $\theta_{\mathcal{H}_f} = \frac{1 \pm \sqrt{-3}}{2}$ and so up to a scalar multiple $\mathcal{H}_f = x^2 \pm xy + y^2$. Hence f satisfies

$$|bc - 9ad| = b^2 - 3ac = c^2 - 3bd$$

and there are at most 2 solutions for c given any choice of a, b, d. Recall that C_3 points are irreducible by definition and so as in the proof of the reducibility estimate (Lemma 3.2), we have that the number of choices of a, b, d for $a, d \neq 0$ is $O(X^{3/4+\varepsilon})$. Since c is one of 2 choices of from a, b, d, we have the result. □

3.3 Geometry of Numbers

Using the error estimates in Lemmas 3.7 and 3.9 we can now reduce our problem to counting lattice points in $\mathcal{R}_X(v)$ for some $v \in V_{\mathbb{R}}^{\pm}$. The problem of counting lattice points in a region of $\mathbb{R}^n$ is central to counting binary cubic forms, and so appears also in the counting method of Davenport [9, 10]. As a result, Davenport publishes a useful result on this problem [8] in the same journal as his counting argument. We shall give some motivation towards the result.

Let $E \subset \mathbb{R}^n$ be a closed bounded region. We would like an estimate for the number $N(E)$ of points in $\mathbb{Z}^n \cap E$. Naive examples, such as the $M \times M$ cube in $\mathbb{R}^n$, suggest that there is some merit to estimating $N(E)$ with $\mathrm{Vol}(E)$ and so we seek an estimate for the error $|N(E) - \mathrm{Vol}(E)|$.

Let $M \in \mathbb{Z}_{>1}$, then if E is a $M \times \frac{1}{M}$ box in $\mathbb{R}^2$ we can see that E could contain as many as $M + 1$ or as few as 0 lattice points and has volume 1. Note however, that the 1-dimensional projections of E given by setting a coordinate to 0 have volumes $\frac{1}{M}$ and M. So in this case, we have that $|N(E) - \mathrm{Vol}(E)| = O(P) = O(M)$ where P is the greatest volume of 1-dimensional projections of E.

Looking at the dimension 3 example of E a cylinder of radius $\frac{1}{M}$ and length M then again E can contain as few as 0 and as many as $M + 1$ lattice points. Further E has volume $\frac{\pi}{M}$ so we seek an error of M. Looking at 2-dimensional projections however, we get volumes $1, 1, \frac{\pi}{M^2}$, which certainly do not account for the error. However, moving to dimension 1 projections we get volumes $\frac{2}{M}, \frac{2}{M}, M$, and the last of these allows us to account for this error.

From these examples, we would expect that the error estimate for $|N(E) - \mathrm{Vol}(E)|$ to be related to the largest volume of projections. Before going further, of course only restricting to E being closed and bounded is far too general. Thus Davenport restricts $E \subset \mathbb{R}^n$ to having particularly nice properties:

I Any line L parallel to a coordinate axis is either disjoint from E or $L \cap E$ is a union of at most h intervals.

II For all $m \in \{1, \ldots, n-1\}$, any m-dimensional projection obtained by setting $n - m$ coordinates of E to 0 also satisfies I.

and goes on to prove that in this case, the results in our discussion above hold generally.

Theorem 3.10 (Davenport [8]). *If $E \subset \mathbb{R}^n$ satisfies I and II above then*

$$|N(E) - \mathrm{Vol}(E)| = O(\max\{\mathrm{Vol}(\mathrm{Proj}(E)), 1\})$$

Where $\mathrm{Vol}(\mathrm{Proj}(E))$ *is the largest volume of any m-dimensional projection of E obtained by setting $n-m$ coordinates to 0. The additional 1 is to recall the 0 dimensional projection.*

In particular, since a semi-algebraic region (finite union of regions defined by finitely many polynomial equalities and inequalities) satisfies the axioms, he notes that this holds for such E. Further Davenport proves that implied constant in the error term is dependent only on n, k, l, where k is the number of algebraic conditions defining E and l the maximal degree of these.

When considering this result, it is important to note that naive use has severe limitations. In particular, Wood [18] gives the example of a $M \times 1$ region in $\mathbb{R}^2$ for $M \in \mathbb{Z}_{>0}$. Using this result we have that the number of lattice points this contains is $M + O(M)$, which is not very helpful. However, if we average over M of these regions by stacking them vertically to obtain a region which is $M \times M$ then Theorem 3.10 tells us that the number of lattice points in this larger region is $M^2 + O(M)$, and so in any one $M \times 1$ we can average to get $M + O(1)$ lattice points. This idea of averaging is central to Bhargavas approach to counting cubic orders, and then fields. Note that theorems relating to lattice points in this way naturally extend to multisets, where we define the volume of the a multiset $\mathcal{R}$ to be $\mathrm{Vol}(\mathcal{R}) = \sum_{k \geq 1} k \,\mathrm{Vol}(\mathcal{R}_i)$ where $\mathcal{R}_k$ is the set of points which occur in $\mathcal{R}$ with multiplicity k.

3.4 Bhargava's Method of Averaging

We would like to use Theorem 3.10 to count lattice points in $\mathcal{R}_X(v)$ for $v \in V_{\mathbb{R}}^{\pm}$. As noted at the end of subsection 3.3, this result is best used in some averaging argument and in particular we will average continuously to get a strong estimate. Given $C > 1$ define

$$B = B(C) = \left\{x = (a,b,c,d) \in V_{\mathbb{R}} \mid 3a^2 + b^2 + c^2 + 3d^2 \leq C,\ |\mathrm{Disc}(x)| \geq 1\right\} \tag{16}$$

then we will average over B. Our choice of B is motivated by the fact that this is a compact subset of $V_{\mathbb{R}}$ which is also $K = SO_2(\mathbb{R})$-invariant (see Appendix A Script 2). Let dv be the usual measure on $V_{\mathbb{R}}$ (identified with $\mathbb{R}^4$) given by $da\,db\,dc\,dd$ normalised to give the lattice $V_{\mathbb{Z}}$ (identified with $\mathbb{Z}^4$) covolume 1. Further, let $dg = t^{-2}\,dn\,d^\times t\,dk\,d^\times\lambda$ be the Haar measure of $\mathrm{GL}_2(\mathbb{R})$ induced by the Iwasawa decomposition (see subsection 3.1 and [3, 15]). Note that the usual measure dk on $K = SO_2(\mathbb{R})$ satisfies $\int_K dk = \int_0^{2\pi} d\theta = 2\pi$ where we write $k \in K$ as $k = \begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}$. In order to reduce notation in the main calculations, we take dk to be $\frac{1}{2\pi}$ of this usual measure so that the volume $\int_K dk = 1$.

Proposition 3.11. *Let $f \in C_0(V_{\mathbb{R}}^{\pm})$ be a function and $v_\pm \in V_{\mathbb{R}}^{\pm}$ be any element. Then*

$$\int_{g \in \mathrm{GL}_2(\mathbb{R})} f(g \cdot v_\pm) dg = \frac{1}{4\pi} \int_{v \in \mathrm{GL}_2(\mathbb{R}) \cdot v_\pm} f(v) |\mathrm{Disc}(v)|^{-1} dv = \frac{n_\pm}{4\pi} \int_{v \in V_{\mathbb{R}}^{\pm}} f(v) |\mathrm{Disc}(v)|^{-1} dv$$

where $n_\pm$ is $\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(v_\pm)$ and so $n_+ = 6, n_- = 2$ as in the discussion of subsection 3.1.

Proof. We obtain the first equality by means of a Jacobian calculation for change of variables between $g = (n,k,t,\lambda)$ and $g \cdot v_\pm$. The actions of the elements n, t, λ in the Iwasawa decomposition on $v_\pm = (a,b,c,d)$ are given by

$$\begin{array}{lcl} n \cdot (a,b,c,d) & = & (a, 3an + b, 3an^2 + 2bn + c, an^3 + bn^2 + cn + d) \\ t \cdot (a,b,c,d) & = & (t^{-3}a, t^{-1}b, tc, t^3 d) \\ \lambda \cdot (a,b,c,d) & = & (\lambda a, \lambda b, \lambda c, \lambda d) \end{array} \tag{17}$$

These expressions differentiate with respect to n, t, λ respectively to give the corresponding rows for the Jacobian. In particular, since the measure dg is a Haar measure it is left $\mathrm{GL}_2(\mathbb{R})$ invariant and we need only evaluate the Jacobian at the element $g = \begin{pmatrix}1 & \\ n & 1\end{pmatrix}\begin{pmatrix}t^{-1} & \\ & t\end{pmatrix} k \begin{pmatrix}\lambda & \\ & \lambda\end{pmatrix} = \begin{pmatrix}1 & \\ & 1\end{pmatrix}$ and so $t = \lambda = 1$ and $n = 0$. The corresponding rows for n, t, λ are thus

$$\begin{aligned} n &: (0, 3a, 2b, c) \\ t &: (-3a, -b, c, 3d) \\ \lambda &: (a, b, c, d) \end{aligned}$$

For the element k the calculation is messy. Before this however, we make the intermediary change of variables $k \mapsto 2\pi k$ so that we can use $d\theta$ as above. The action of $k = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ gives

$$\begin{aligned} k \cdot (a,b,c,d) = (&a\cos^3\theta - b\cos^2\theta\sin\theta + c\cos\theta\sin^2\theta - d\sin^3\theta, \\ &3a\cos^2\theta\sin\theta + b(\cos^3\theta - 2\cos\theta\sin^2\theta) + c(\sin^3\theta - 2\cos^2\theta\sin\theta) + 3d\cos\theta\sin^2\theta, \\ &3a\cos\theta\sin^2\theta - b(\sin^3\theta - 2\cos^2\theta\sin\theta) + c(\cos^3\theta - 2\cos\theta\sin^2\theta) - 3d\cos^2\theta\sin\theta, \\ &a\sin^3\theta + b\sin^2\theta + c\cos^2\theta\sin\theta + d\cos^3\theta) \end{aligned}$$

It is only necessary to note that since we evaluate the derivative at $g = 1$ (and so $\theta = 0$) then the only term which differentiates to not have a factor of $\sin\theta$ (and so be evaluated to 0) is $\cos^2(\theta)\sin(\theta)$. This differentiates to $2\cos\theta\sin^2\theta + \cos^3\theta$, and so evaluates at $\theta = 0$ to be 1, meaning that the k (equivalently θ) row of the Jacobian is given by

$$k : (-b, 3a - 2c, 2b - 3d, c)$$

Thus we calculate the determinant of the Jacobian matrix to get that this is $2\,\mathrm{Disc}(v)$ and since we scaled the variable k by 2π then we have

$$dv = 4\pi|\mathrm{Disc}(v)|dg$$

as required. The second equality in the Proposition statement is simply a result of the fact that $\mathrm{GL}_2(\mathbb{R}) \cdot v_\pm$ is a $n_\pm$-fold cover of $V_{\mathbb{R}}^\pm$ (see Subsection 3.1). □

We will now use the result in Theorem 3.6 by averaging the number of lattice points in $\mathcal{R}_X(v)$ over $v \in B$ from (16). Recall $\mathcal{R}_X(v) = \{x \in \mathcal{F}v \mid |\mathrm{Disc}(v)| < X\}$ where $\mathcal{F}$ is the fundamental domain for $\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R})$ as in subsection 3.1. Further for any $T \subset V_{\mathbb{Z}}$ let T^{irr} denote the subset of irreducible elements of T.

Let $S \subset V_{\mathbb{R}}^\pm$ be a $\mathrm{GL}_2(\mathbb{Z})$-invariant subset, by Theorem 3.6 the number of $\mathrm{GL}_2(\mathbb{Z})$-orbits of irreducible points in S is precisely

$$N(S;X) = \frac{\int_{v\in B\cap V_{\mathbb{R}}^\pm} \#(\mathcal{R}_X(v)\cap S^{\mathrm{irr}})|\mathrm{Disc}(v)|^{-1}dv}{(n_\pm)\int_{v\in B\cap V_{\mathbb{R}}^\pm}|\mathrm{Disc}(v)|^{-1}dv} \tag{18}$$

where we count C_3-points in the right hand side with weight 3. Though this does not hold for a general $S \subset V_{\mathbb{Z}}^\pm$, we will take this as the definition of $N(S;X)$ whenever S is not $\mathrm{GL}_2(\mathbb{Z})$-invariant. This will be useful in Section 4, when we split S into a disjoint union $S = \cup_{i=1}^k S_i$ and then use this definition to write

$$N(S;X) = \sum_{i=1}^k N(S_i;X).$$

Returning to our counting argument, given $a' = \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \in A', n \in N'(a'), \lambda \in \Lambda$ as in the definition of $\mathcal{F}$, define

$$B^\pm(n,t,\lambda,X) = n\begin{pmatrix} t^{-1} & \\ & t \end{pmatrix}\lambda B \cap \left\{x \in V_{\mathbb{R}}^\pm \mid |\mathrm{Disc}\, x| < X\right\}.$$

Then we can reformulate (18) in terms of $B^\pm(n,t,\lambda,X)$.

Lemma 3.12. *For any $S \subset V_{\mathbb{Z}}^\pm$,*

$$N(S;X) = \frac{1}{M_\pm}\int_{g\in N'(t)A'\Lambda} \#\left\{x \in S^{\mathrm{irr}} \cap B^\pm(n,t,\lambda,X)\right\} t^{-2}dn\, d^\times t\, d^\times\lambda$$

where we count C_3-points on the right hand side with weight 3, $M_\pm = \frac{n_\pm}{4\pi}\int_{v\in B\cap V_{\mathbb{R}}^\pm}|\mathrm{Disc}(v)|^{-1}dv$ and we shorten notation to $N'(t) := N'(\begin{pmatrix} t^{-1} & \\ & t \end{pmatrix})$.

Proof. Fix $v_\pm \in V_{\mathbb{R}}^\pm$ and let $H^\pm \subset \mathrm{GL}_2(\mathbb{R})$ be the maximal subset such that $H^\pm \cdot v_\pm = B \cap V_{\mathbb{R}}^\pm$. Thus $H^\pm \cdot v_\pm$ as a multiset is a $n_\pm$-fold cover of $B \cap V_{\mathbb{R}}^\pm$.

Notice that we have from (18) we have that $N(S;X) = \frac{1}{4\pi M_\pm}\int_{v\in B\cap V_{\mathbb{R}}^\pm} \#(\mathcal{R}_X(v)\cap V_{\mathbb{Z}}^{\mathrm{irr}})|\mathrm{Disc}(v)|^{-1}dv$. Then we can separate the integral,

$$\begin{aligned}\int_{v\in B\cap V_{\mathbb{R}}^\pm} \#(\mathcal{R}_X(v)\cap S^{\mathrm{irr}})|\mathrm{Disc}(v)|^{-1}dv &= \int_{v\in B\cap V_{\mathbb{R}}^\pm} \#\left\{x\in \mathcal{F}v\cap S^{\mathrm{irr}} \mid |\mathrm{Disc}(x)|<X\right\}|\mathrm{Disc}(v)|^{-1}dv\\ &= \sum_{\substack{x\in S^{\mathrm{irr}}\\ |\mathrm{Disc}(x)|<X}} \int_{v\in B\cap V_{\mathbb{R}}^\pm} \#\left\{g\in\mathcal{F}\mid g\cdot v = x\right\}|\mathrm{Disc}(v)|^{-1}dv.\end{aligned}$$

Now applying a change of variables using Proposition 3.11 and rearranging, this is

$$\begin{aligned}\sum_{\substack{x\in S^{\mathrm{irr}}\\ |\mathrm{Disc}(x)|<X}} \int_{v\in B\cap V_{\mathbb{R}}^\pm} \#\left\{g\in\mathcal{F}\mid g\cdot v = x\right\}|\mathrm{Disc}(v)|^{-1}dv &= \frac{4\pi}{n_\pm}\sum_{\substack{x\in S^{\mathrm{irr}}\\ |\mathrm{Disc}(x)|<X}} \int_{h\in H^\pm} \#\left\{g\in\mathcal{F}\mid gh\cdot v_\pm = x\right\}dh\\ &= \frac{4\pi}{n_\pm}\sum_{\substack{x\in S^{\mathrm{irr}}\\ |\mathrm{Disc}(x)|<X}} \int_{g\in\mathcal{F}} \#\left\{h\in H^\pm\mid gh\cdot v_\pm = x\right\}dg\\ &= \frac{4\pi}{n_\pm}\int_{g\in\mathcal{F}} \#\left\{x\in S^{\mathrm{irr}}\cap(gH^\pm v_\pm)\mid |\mathrm{Disc}\,x|<X\right\}dg\\ &= 4\pi\int_{g\in\mathcal{F}} \#\left\{x\in S^{\mathrm{irr}}\cap g(B\cap V_{\mathbb{R}}^\pm)\mid |\mathrm{Disc}\,x|<X\right\}dg\end{aligned}$$

where the last equality is because $H^\pm\cdot v_\pm$ is an $n_\pm$-fold cover of $B\cap V_{\mathbb{R}}^\pm$. Note that as B is K-invariant, $kB = B$ and so

$$g(B\cap V_{\mathbb{R}}^\pm) = gB\cap V_{\mathbb{R}}^\pm = n\begin{pmatrix}t^{-1} & \\ & t\end{pmatrix}k\lambda B\cap V_{\mathbb{R}}^\pm = n\begin{pmatrix}t^{-1} & \\ & t\end{pmatrix}\lambda B\cap V_{\mathbb{R}}^\pm.$$

Applying this to our integrand we see that

$$\begin{aligned}\left\{x\in S^{\mathrm{irr}}\cap g(B\cap V_{\mathbb{R}}^\pm)\mid |\mathrm{Disc}\,x|<X\right\} &= \left\{x\in S^{\mathrm{irr}}\cap n\begin{pmatrix}t^{-1} & \\ & t\end{pmatrix}\lambda B\cap V_{\mathbb{R}}^\pm \mid |\mathrm{Disc}\,x|<X\right\}\\ &= \left\{x\in S^{\mathrm{irr}}\cap B^\pm(n,t,\lambda,X)\right\}.\end{aligned}$$

Considering this, the development of the integral and (18) we have,

$$\begin{aligned}N(S;X) &= \frac{1}{4\pi M_\pm}\int_{v\in B\cap V_{\mathbb{R}}^\pm} \#(\mathcal{R}_X(v)\cap V_{\mathbb{Z}}^{\mathrm{irr}})|\mathrm{Disc}(v)|^{-1}dv\\ &= \frac{1}{M_\pm}\int_{g\in\mathcal{F}} \#\left\{x\in S^{\mathrm{irr}}\cap B^\pm(n,t,\lambda,X)\right\}dg\\ &= \frac{1}{M_\pm}\int_{g\in N'(t)A'K\Lambda} \#\left\{x\in S^{\mathrm{irr}}\cap B^\pm(n,t,\lambda,X)\right\}t^{-2}\,dn\,d^\times t\,dk\,d^\times\lambda\\ &= \frac{1}{M_\pm}\int_{g\in N'(t)A'\Lambda} \#\left\{x\in S^{\mathrm{irr}}\cap B^\pm(n,t,\lambda,X)\right\}t^{-2}\,dn\,d^\times t\,d^\times\lambda\end{aligned}$$

where the last equality is from the lack of k dependence of the integrand, and the fact that we normalised the measure dk to give $\int_K dk = 1$. Thus we have the result. □

There is an immediate corollary of this result using our error estimates in Lemmas 3.7 and 3.9.

Corollary 3.13. *Up to error $O(X^{3/4+\varepsilon})$, for $S\subset V_{\mathbb{Z}}^\pm$ we have*

$$N(S;X) = \frac{1}{M_\pm}\int_{g\in N'(t)A'\Lambda} \#\left\{x\in S\cap B^\pm(n,t,\lambda,X)\mid \substack{x=(a,b,c,d)\\ a\neq 0}\right\}t^{-2}\,dn\,d^\times t\,d^\times\lambda$$

where all points are counted with equal weight.

3.5 Counting Lattice Points

Corollary 3.13 gives us a method of establishing $N(V_{\mathbb{Z}}^{\pm}; X)$, once we have some way of counting the number of points in $V_{\mathbb{Z}}^{\pm} \cap B^{\pm}(n, t, \lambda, X)$ with first coordinate nonzero. In particular, since $B^{\pm}(n, t, \lambda, X)$ contains no points from $V_{\mathbb{R}}^{\mp}$ this is equivalent to counting points in $V_{\mathbb{Z}} \cap B^{\pm}(n, t, \lambda, X)$ with first coordinate nonzero. We would like to apply Davenport's Theorem 3.10 to our region $B^{\pm}(n, t, \lambda, X)$, to do this we will need to understand the shape in order to look at the $1, 2$ and 3 dimensional projections. The points $x \in B$ satisfy $1 \leq |\mathrm{Disc}(x)|$, we must have $|\mathrm{Disc}(\lambda x)| = \lambda^4 |\mathrm{Disc}(x)| \geq \lambda^4$. Since points in $B^{\pm}(n, t, \lambda, X)$ have absolute discriminant at most X, $B^{\pm}(n, t, \lambda, X)$ is nonempty only for $\lambda < X^{1/4}$. Note that the action of n, t, λ on the coordinates of a point $(a, b, c, d) \in B$ are given as in (17) by

$$\begin{aligned}
\lambda \cdot (a, b, c, d) &= (\lambda a, \lambda b, \lambda, c, \lambda d), \\
t \cdot (a, b, c, d) &= (t^{-3} a, t^{-1} b, tc, t^3 d), \\
n \cdot (a, b, c, d) &= (a, 3an + b, 3an^2 + 2bn + c, an^3 + bn^2 + cn + d).
\end{aligned}$$

As λ simply scales the volumes of the projections of B of dimension j by λ^j, and $B(n, t, \lambda, X) \neq \emptyset$ only if $\lambda < X^{1/4}$ then these projected volumes are easily approximated in terms of X. The action of the t variable is a little more difficult, and in particular around $a = 0$ there is a long thin cusp caused by the t^3 term on d. However as mentioned in Corollary 3.13 we will only be interested in points with $a \neq 0$ – so we have 'cut off' this cusp. Thus the only projection where large t can cause an increase in volume is $b = 0$, and in this projection the scaling is linear and we will be able to put a simple bound on t. As is perhaps immediately clear from the action of n, it is hard to comment on the action that n has on volumes of projections. We will deal with this unipotent upper triangular transformation (or lower if we consider (a, b, c, d) as a column vector) via a method of Wood [18]. Let $N(E)$ denote the number of $\mathbb{Z}^n$ points in $E \subset \mathbb{R}^n$ as in subsection 3.3.

Lemma 3.14. *For any semialgebraic region $E \subset \mathbb{R}^m$ and upper (or lower) triangular unipotent transformation T of $\mathbb{R}^n$, we have that*

$$|N(E) - N(T(E))| = O(\mathrm{NProj}(E)),$$

where $\mathrm{NProj}(E)$ *is the greatest number of $\mathbb{Z}^m$ points in any projection of E of dimension at most $m-1$. The implied constant depends only on m and the degree* $\deg(E)$ *of E (the maximal degree of the algebraic conditions defining E).*

Proof. Write the coordinates of a point $x \in E$ as $x = (x_1, \ldots, x_m)$ and write the projection onto variable x_i as $\pi_i(x)$. Decomposing T into its action on each coordinate, write $T = t_k \circ \cdots \circ t_2$ where t_i is the linear transformation given by

$$\begin{cases} \pi_j(t_i(x)) = x_j & j \neq i \\ \pi_j(t_i(x)) = x_i + \lambda_{i-1} x_{i-1} + \cdots + \lambda_1 x_1 & j = i. \end{cases}$$

We induct on k, the number of t_i in the decomposition of T.

If we can write $T = t_i$, then for $c_j \in \mathbb{Z}$ consider the line

$$L = \{(x_1, \ldots, x_m) \in \mathbb{R}^m \mid x_j = c_j \text{ for } j \neq i\}$$

Since T only acts on the coordinate x_i then T preserves L. Thus $T(E \cap L) = T(E) \cap L$. Further, as E is semialgebraic, we can write $E \cap L$ as a union of h intervals and in particular since T is determinant 1, it simply translates the intervals of $E \cap L$ along L. An interval in $E \cap L$ of length ℓ must contain between $\ell - 1$ and $\ell + 1$ lattice points, and so

$$|N(E \cap L) - N(T(E) \cap L)| \leq 2h$$

and $h = O(\deg(E))$. It remains to estimate the number of choices of line giving $E \cap L \neq \emptyset$, but this is precisely the number of choices c_j for $i \neq j$ which is the number of lattice points in the projection $x_i = 0$ and so is $O(\mathrm{NProj}(E))$. Thus

$$|N(E) - N(t_i(E))| = O(\mathrm{NProj}(E))$$

For $T = t_k \circ \cdots \circ t_2$, we use the inductive hypothesis by writing $T = t_k \circ T'$ where T' is able to be written with strictly less t_i factors. By the inductive hypothesis,

$$|N(E) - N(T'(E))| = O(\mathrm{NProj}(E)) \tag{19}$$

Let $T'(E)_k$ be the projection of $T'(E)$ onto $x_k = 0$, then from the base case argument above

$$|N(T'(E)) - N(t_k \circ T'(E))| = O(N(T'(E)_k)). \tag{20}$$

Now, for a point $x = (x_1, \ldots, x_m)$ then the values of each coordinate x_i' of $T'(x)$ are independent of x_k for $i \neq k$. Thus $T'(E)_k = T'(E_k)$ where E_k is the projection of E onto $x_k = 0$. Again using the inductive hypothesis

$$|N(T'(E_k)) - N(E_k)| = O(\mathrm{NProj}(E_k)), \tag{21}$$

bringing this together we have that

$$\begin{aligned}
|N(E) - N(T(E))| &\leq |N(E) - N(T'(E))| + |N(T'(E)) - N(T(E))| \\
&\overset{(19),(20)}{=} O(\mathrm{NProj}(E)) + O(N(T'(E)_k)) \\
&= O(\mathrm{NProj}(E)) + O(N(T'(E_k))) \\
&\overset{(21)}{=} O(\mathrm{NProj}(E)) + O(N(E_k)) + O(\mathrm{NProj}(E_k)) \\
&= O(\mathrm{NProj}(E))
\end{aligned}$$

where the last equality holds because E_k is itself a projection of E. □

This has left the problem of estimating the number of lattice points in a projection. Adapting the error with Davenport's Theorem we obtain

Theorem 3.15 (Wood [18])**.** *For a semialgebraic region $E \subset \mathbb{R}^m$ and T an upper (or lower) triangular transformation of $\mathbb{R}^m$,*

$$|N(E) - N(T(E))| = O(\max\{\mathrm{Vol}(\mathrm{Proj}(E)), 1\}).$$

Proof. From Lemma 3.14 we know that $|N(E) - N(T(E))| = O(\mathrm{NProj}(E))$. Let E' be a projection of E such that $N(E') = \mathrm{NProj}(E)$. Applying Daveports Theorem 3.10,

$$\mathrm{NProj}(E) = N(E') = \mathrm{Vol}(E') + O(\max\{\mathrm{Vol}(\mathrm{Proj}(E')), 1\}).$$

Since E' and any projection of E' are projections of E we have that

$$\mathrm{Vol}(E') + O(\max\{\mathrm{Vol}(\mathrm{Proj}(E')), 1\}) = O(\max\{\mathrm{Vol}(\mathrm{Proj}(E)), 1\}),$$

giving the required result. □

Returning to the problem of counting lattice points in $B^{\pm}(n, t, \lambda, X)$, since $\det(n) = 1$ we know from Proposition 2.16 that $\mathrm{Disc}(n \cdot v) = \mathrm{Disc}(v)$ and thus $B^{\pm}(n, t, \lambda, X) = nB^{\pm}(t, \lambda, X)$ where

$$B^{\pm}(t, \lambda, X) = \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \lambda B \cap \left\{ x \in V_{\mathbb{R}}^{\pm} \mid |\mathrm{Disc}(x)| < X \right\}.$$

Using Theorem 3.15 since n exerts a unipotent triangular transformation on $V_{\mathbb{R}}$ identified with $\mathbb{R}^4$, we can count points in $V_{\mathbb{Z}} \cap B^{\pm}(n, t, \lambda, X)$ by counting those in $V_{\mathbb{Z}} \cap B^{\pm}(t, \lambda, X)$ up to an error term. Formalising this we obtain:

Theorem 3.16. *The number of points (a, b, c, d) found in $V_{\mathbb{Z}} \cap B^{\pm}(n, t, \lambda, X)$ with $a \neq 0$ is*

$$\begin{cases} 0 & \text{if } C\lambda t^{-3} < 1 \\ \mathrm{Vol}(B^{\pm}(n, t, \lambda, X)) + O(\max\left\{C^3 t^3 \lambda^3, 1\right\}) & \text{otherwise,} \end{cases}$$

where $B = B(C)$ as in (16)*.*

Proof. Every point $(\alpha, \beta, \gamma, \delta) \in B^{\pm}(n, t, \lambda, X)$ satisfies $\alpha = at^{-3}\lambda$ (see (17)) for a a first coordinate of a point in B. In particular, by definition of B we have the (in general fairly loose) bound $|a| \leq C$ and so,

$$|\alpha| = |at^{-3}\lambda| \leq C\lambda t^{-3} \tag{22}$$

Thus if $C\lambda t^{-3} < 1$ then every point $(\alpha, \beta, \gamma, \delta) \in V_{\mathbb{Z}} \cap B^{\pm}(n, t, \lambda, X)$ satisfies $|\alpha| < 1$ and so $\alpha = 0$.

Otherwise $C\lambda t^{-3} \geq 1$ and so since $t \geq \frac{\sqrt[4]{3}}{\sqrt{2}}$ we have that $\lambda \geq \left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3 /C$. As discussed above, up to error $O(\max\{\mathrm{Vol}(\mathrm{Proj}(B^{\pm}(t,\lambda,X))),1\})$ we need only count such points in $V_{\mathbb{Z}} \cap B^{\pm}(t,\lambda,X)$. Using Davenport's Theorem 3.10 then up to the same error term this is just $\mathrm{Vol}(B^{\pm}(t,\lambda,X))$. As n gives a unipotent triangular transformation of $\mathbb{R}^4$ (so has determinant 1 as a linear map), $\mathrm{Vol}(B^{\pm}(t,\lambda,X)) = \mathrm{Vol}(B^{\pm}(n,t,\lambda,X))$ as in the theorem statement. Now it is sufficient to show that the suggested error bound holds. Points in $B^{\pm}(t,\lambda,X)$ can be written as

$$(\lambda t^{-3}a, \lambda t^{-1}b, \lambda tc, \lambda t^3 d)$$

for $(a,b,c,d) \in B$. Using the definition of B to bound each coordinate a,b,c,d by C the coordinates of such a point are $O(C\lambda t^{-3})$, $O(C\lambda t^{-1})$, $O(C\lambda t)$, $O(C\lambda t^3)$ respectively. Computing volumes of projections we get that the projection onto the last 3 coordinates is $O(\lambda^3 t^3 C^3)$. Further, since $C\lambda \geq t^3$ it is clear that the projection onto the last 2 coordinates has volume $O(C^2\lambda^2 t^4) \leq O(C^3\lambda^3 t^3)$. All other projections have volume bounded by $O(C^3\lambda^3 t^3)$ in the same way and so we have that the error term $O(\max\{\mathrm{Vol}(\mathrm{Proj}(B^{\pm}(t,\lambda,X))),1\}) = O(\max\left\{C^3t^3\lambda^3, 1\right\})$ as required. □

We will apply this theorem directly to Corollary 3.13 obtained from Bhargava's averaging argument to count cubic orders.

3.6 Counting Cubic Orders

We now apply the tools we have developed to count cubic orders with absolute discriminant less than some X by calculating $N(V_{\mathbb{Z}}^{\pm}; X)$.

Recall Corollary 3.13 which, when applied to $V_{\mathbb{Z}}^{\pm}$, says that up to error $O(X^{3/4+\varepsilon})$

$$N(V_{\mathbb{Z}}^{\pm}; X) = \frac{1}{M_{\pm}} \int_{g \in N'(t)A'\Lambda} \#\left\{x \in V_{\mathbb{Z}} \cap B^{\pm}(n,t,\lambda,X) \mid {}^{x=(a,b,c,d)}_{a\neq 0}\right\} t^{-2}\, dn\, d^{\times}t\, d^{\times}\lambda.$$

where we can take $V_{\mathbb{Z}}$ in the integrand instead of $V_{\mathbb{Z}}^{\pm}$ because $B(n,t,\lambda,X) \cap V_{\mathbb{Z}}^{\mp} = \emptyset$. As in the discussion of the shape of the region $B(n,t,\lambda,X)$ at the beginning of 3.5, this integrand is 0 for $\lambda \geq X^{1/4}$. Further by Theorem 3.16 the integrand is 0 for $t > (C\lambda)^{1/3}$ and $\lambda < t^3/C$. Thus again by Theorem 3.16,

$$N(V_{\mathbb{Z}}^{\pm}; X) = \frac{1}{M_{\pm}} \int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}} \int_{t=\frac{\sqrt[4]{3}}{\sqrt{2}}}^{(C\lambda)^{1/3}} \int_{N'(t)} \mathrm{Vol}(B^{\pm}(n,t,\lambda,X)) + O(\max\left\{C^3t^3\lambda^3, 1\right\}) t^{-2}\, dn\, d^{\times}t\, d^{\times}\lambda \tag{23}$$

up to error $O(X^{3/4+\varepsilon})$. We compute this by separating into the integral for each integrand and label each as a Lemma.

Lemma 3.17 (First Integrand)**.** *For any $v_{\pm} \in V_{\mathbb{R}}^{\pm}$, the first integrand in* (23) *is*

$$\frac{1}{M_{\pm}} \int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}} \int_{t=\frac{\sqrt[4]{3}}{\sqrt{2}}}^{(C\lambda)^{1/3}} \int_{N'(t)} \mathrm{Vol}(B^{\pm}(n,t,\lambda,X))\, t^{-2}\, dn\, d^{\times}t\, d^{\times}\lambda = \frac{1}{n_{\pm}} \mathrm{Vol}(\mathcal{R}_X(v_{\pm})) + O(C^{10/3}X^{5/6}M_{\pm}^{-1})$$

Where $n_{\pm} = \#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(v_{\pm})$ and $\mathcal{R}_X(v_{\pm}) = \{x \in \mathcal{F}v_{\pm} \mid |\mathrm{Disc}(x)| < X\}$ as in the discussion at the end of subsection 3.1.

Lemma 3.18 (Second Integrand)**.** *The second integrand in* (23) *is*

$$\frac{1}{M_{\pm}} \int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}} \int_{t=\frac{\sqrt[4]{3}}{\sqrt{2}}}^{(C\lambda)^{1/3}} \int_{N'(t)} O(\max\left\{C^3t^3\lambda^3, 1\right\}) t^{-2}\, dn\, d^{\times}t\, d^{\times}\lambda = O(C^{10/3}X^{5/6}M_{\pm}^{-1})$$

Combining Lemmas 3.17 and 3.18, noting that the error from these includes the $O(X^{3/4+\varepsilon})$ from Corollary 3.13 we have,

Corollary 3.19. *For $v_{\pm} \in V_{\mathbb{R}}^{\pm}$*

$$N(V_{\mathbb{Z}}^{\pm}; X) = \frac{1}{n_{\pm}} \mathrm{Vol}(\mathcal{R}_X(v_{\pm})) + O(C^{10/3}X^{5/6}M_{\pm}^{-1})$$

And so since $C > 1$ is a chosen constant, and $M_\pm$ is a constant only dependent on the region B (and hence only on C), we need only calculate $\frac{1}{n_\pm}\operatorname{Vol}(\mathcal{R}_X(v_\pm))$ in order to obtain Theorem 1.2. Note that the volume of $\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2^{\pm 1}(\mathbb{R})$ calculated with respect to the measure $dh = t^{-2}\,dn\,d^\times t\,dk$ on the restricted Iwasawa decomposition as defined in Subsection 3.4 is $\frac{\zeta(2)}{2\pi}$ (see Appendix C). Recall that λ scales discriminant of $v_\pm$ by λ^4 and the other components of the Iwasawa decomposition do not affect the discriminant; taking $v_\pm \in V_\mathbb{R}^\pm$ we apply a change of variables from Proposition 3.11 to get

$$\begin{aligned}
\frac{1}{n_\pm}\operatorname{Vol}(\mathcal{R}_X(v_\pm)) &= \frac{1}{n_\pm}\int_{v\in\mathcal{R}_X(v_\pm)} dv \\
&= \frac{4\pi}{n_\pm}\int_{g\in\mathcal{F}} |\mathrm{Disc}(g\cdot v_\pm)|dg \\
&= \frac{4\pi}{n_\pm}\int_{\lambda=0}^{X^{1/4}} \lambda^4\,d^\times\lambda \int_{\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2^{\pm 1}(\mathbb{R})} dh \\
&= \frac{4\pi}{n_\pm}\frac{X}{4}\frac{\zeta(2)}{2\pi} \\
&= \frac{\pi^2}{12n_\pm}X.
\end{aligned}$$

Recalling the values of $n_\pm$ are 6 and 2 for $+$ and $-$ respectively from Subsection 3.1, we have obtained

Theorem 3.20. *The number of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of irreducible binary quadratic forms of positive and negative discriminant bounded in absolute value by X are*

$$\begin{aligned}
N(V_\mathbb{Z}^+;X) &= \frac{\pi^2}{72}X + O(X^{5/6}) \\
N(V_\mathbb{Z}^-;X) &= \frac{\pi^2}{24}X + O(X^{5/6}).
\end{aligned}$$

Thus by the Delone–Faddeev correspondence, these are the number of cubic orders (up to isomorphism) of positive (resp. negative) discriminant bounded in absolute value by X giving Theorem 1.2.

Proof of first integrand (Lemma 3.17). Performing a standard trick, we split this integral into a 'whole region' and 'region without' and subtract the latter from the former. At the same time it is convenient to apply a change of variables as in Proposition 3.11. Proceeding thus, the integral in the Lemma statement is equal to

$$\frac{1}{M_\pm}\left(\frac{1}{4\pi}\int_{v\in B\cap V_\mathbb{R}^\pm}\operatorname{Vol}(\mathcal{R}_X(v))|\mathrm{Disc}(v)|^{-1}dv \;-\; \int_{\lambda=\left(\frac{4\sqrt{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}}\int_{t=(C\lambda)^{1/3}}^{\infty}\int_{N'(t)}\operatorname{Vol}(B^\pm(n,t,\lambda,X))\,t^{-2}\,dn\,d^\times t\,d^\times\lambda\right) \tag{24}$$

Looking at each term independently, note firstly that Proposition 3.11 gives that the measure $|\mathrm{Disc}(v)|^{-1}dv$ is $\mathrm{GL}_2(\mathbb{R})$-invariant (since dg is a Haar measure) and so $\operatorname{Vol}(\mathcal{R}_X(v))$ is independent of choice of $v \in V_\mathbb{R}^\pm$. Hence the first term can be written as

$$\begin{aligned}
\frac{1}{4\pi M_\pm}\int_{v\in B\cap V_\mathbb{R}^\pm}\operatorname{Vol}(\mathcal{R}_X(v))|\mathrm{Disc}(v)|^{-1}dv &= \frac{1}{4\pi M_\pm}\int_{v\in B\cap V_\mathbb{R}^\pm}\operatorname{Vol}(\mathcal{R}_X(v_\pm))|\mathrm{Disc}(v)|^{-1}dv \\
&= \frac{\operatorname{Vol}(\mathcal{R}_X(v_\pm))}{4\pi M_\pm}\int_{v\in B\cap V_\mathbb{R}^\pm}|\mathrm{Disc}(v)|^{-1}dv
\end{aligned}$$

and since $M_\pm = \frac{n_\pm}{4\pi}\int_{v\in B\cap V_\mathbb{R}^\pm}|\mathrm{Disc}(v)|^{-1}dv$, we have that this simplifies to

$$\frac{1}{n_\pm}\operatorname{Vol}(\mathcal{R}_X(v_\pm))$$

giving the main term in the lemma statement. Now it is sufficient to show that the second term in (24) is within the suggested error bound. Firstly, $\operatorname{Vol}(B^\pm(n,t,\lambda,X)) = \operatorname{Vol}(B^\pm(t,\lambda,X))$ since n applies a determinant 1 transformation to $V_\mathbb{R}$. Secondly, the coefficients of a point $(a\lambda t^{-3}, b\lambda t^{-1}, c\lambda t, d\lambda t^3) \in B^\pm(t,\lambda,X)$ have absolute value bounded (in general very loosely) by $C\lambda t^{-3}$, $C\lambda t^{-1}$, $C\lambda t$, $C\lambda t^3$. Thus

the volume $\mathrm{Vol}(B(n,t,\lambda,X)) < C^4\lambda^4$. Now we estimate the second term using this bound and the fact that by the definition of $N'(t)$, we must have $\int_{N'(t)} dn \leq 1$.

$$\begin{aligned}
&\frac{1}{M_\pm}\int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}}\int_{t=(C\lambda)^{1/3}}^{\infty}\int_{N'(t)}\mathrm{Vol}(B^\pm(n,t,\lambda,X))\,t^{-2}\,dn\,d^\times t\,d^\times\lambda\\
<&\frac{1}{M_\pm}\int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}}\int_{t=(C\lambda)^{1/3}}^{\infty}\int_{N'(t)}C^4\lambda^4\,t^{-2}\,dn\,d^\times t\,d^\times\lambda\\
\leq&\frac{1}{M_\pm}\int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}}\int_{t=(C\lambda)^{1/3}}^{\infty}C^4\lambda^4\,t^{-2}\,d^\times t\,d^\times\lambda\\
=&\frac{1}{2M_\pm}\int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}}C^{10/3}\lambda^{10/3}\,d^\times\lambda\\
&=O(C^{10/3}X^{5/6}M_\pm^{-1})
\end{aligned}$$

as required. □

Proof of second integrand (Lemma 3.18). In our domain $C^3t^3\lambda^3 >> 1$ in general, and again by definition of $N'(t)$ we have that $\int_{N'(t)} dn \leq 1$ so this integral is estimated for some $W \in \mathbb{R}$ by

$$\begin{aligned}
&\frac{1}{M_\pm}\int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}}\int_{t=\frac{\sqrt[4]{3}}{\sqrt{2}}}^{(C\lambda)^{1/3}}\int_{N'(t)}O(\max\left\{C^3t^3\lambda^3,1\right\})\,t^{-2}\,dn\,d^\times t\,d^\times\lambda\\
\leq&\frac{W}{M_\pm}\int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}}\int_{t=\frac{\sqrt[4]{3}}{\sqrt{2}}}^{(C\lambda)^{1/3}}\int_{N'(t)}C^3t\lambda^3\,dn\,d^\times t\,d^\times\lambda\\
\leq&\frac{W}{M_\pm}\int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}}\int_{t=\frac{\sqrt[4]{3}}{\sqrt{2}}}^{(C\lambda)^{1/3}}C^3t\lambda^3\,d^\times t\,d^\times\lambda\\
<&\frac{W}{M_\pm}\int_{\lambda=\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3/C}^{X^{1/4}}C^{10/3}\lambda^{10/3}\,d^\times\lambda\\
=&O(C^{10/3}X^{5/6}M_\pm^{-1})
\end{aligned}$$

□

4 Counting Cubic Fields

Having developed a suite of methods in the process of counting cubic orders in Section 3, we would like to apply these to counting cubic fields. A cubic field K is can be uniquely identified with a maximal cubic order, namely its ring of integers $\mathcal{O}_K$ which has by definition the same discriminant. Thus counting cubic fields up to discriminant X is equivalent to counting maximal cubic orders up to discrimant X. We begin by establishing the set of forms $\mathcal{U}$ in $V_\mathbb{Z}$ which correspond to maximal rings, and can immediately state the region within which we need to count irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits in $\mathcal{U}$ from the results in Section 3. The remainder of the approach for cubic orders relies specifically on the fact that we are counting all lattice points in a given region, but $\mathcal{U}$ is certainly not the whole lattice $V_\mathbb{Z}$ which presents a barrier.

Fortunately, $\mathcal{U}$ can be defined by congruence conditions and so we can view it as a union of several translations of an inflated lattice $mV_\mathbb{Z}$, and so we adapt the previous methods for this approach. Following through the methods of the previous section for a set S which is defined by congruence conditions modulo m, we arrive at a result dependent on the density of the k translates of $mV_\mathbb{Z}$ which make up S – which can be easily translated into a product of p-adic densities of $\mathcal{U}$. Computing the relevant densities for $\mathcal{U}$, we then give the final argument to obtain the first order term of the number of of positive (resp. negative) discriminant up to absolute value X in terms of X.

4.1 Maximal Cubic Orders

We wish to establish a set of binary cubic forms in $V_\mathbb{Z}$ which correspond to maximal cubic rings. We will say that a cubic ring R is **maximal at** p if $R \otimes_\mathbb{Z} \mathbb{Z}_p$ (a cubic ring over $\mathbb{Z}_p$) is maximal. In particular, since cubic rings containing $R \otimes_\mathbb{Z} \mathbb{Z}_p$ restrict to cubic rings containing R over $\mathbb{Z}$ with index a multiple of p, we have that R is maximal if and only it is maximal at p for every p.

Lemma 4.1. *Let R be a cubic ring, then R is not maximal at p if and only if there exists a $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ such that at least one of the following forms a ring:*

- $\mathbb{Z} + \frac{\omega}{p}\mathbb{Z} + \frac{\theta}{p}\mathbb{Z}$,
- $\mathbb{Z} + \frac{\omega}{p}\mathbb{Z} + \theta\mathbb{Z}$.

Proof. ($\Leftarrow$) Either of these rings will strictly contain R so that R is not maximal at p.

($\Rightarrow$) Since R is not maximal at p, i.e. $R \otimes_\mathbb{Z} \mathbb{Z}_p$ is not maximal, we can take a cubic ring $R' \supset R$ which has index a multiple of p. Now define

$$R_1 = R' \cap \left(R \otimes_\mathbb{Z} \mathbb{Z}\left[\frac{1}{p}\right] \right) = \{ x \in R' \mid p^m x \in R \}.$$

By definition, $R_1 \supsetneq R$ and is itself a cubic ring over $\mathbb{Z}$. Thus by Proposition 2.6 we choose normal $\mathbb{Z}$-bases for R and R', since $R \subset R_1$ we can write the basis for R in terms of that of R_1 to obtain a matrix

$$A = \begin{pmatrix} 1 & 0 & 0 \\ \alpha & \beta & \gamma \\ \delta & \varepsilon & \eta \end{pmatrix}.$$

Since $R_1 \subset R \otimes_\mathbb{Z} \mathbb{Z}[\frac{1}{p}]$, A must be invertible over $\mathbb{Z}[\frac{1}{p}]$ and thus have determinant $\pm p^k$ for some k. As in the theory of elementary divisors, we can perform row operations over $\mathbb{Z}$ in a determinant preserving way and thus obtain

$$A' = \begin{pmatrix} 1 & & \\ & p^j & \\ & & p^i \end{pmatrix}.$$

Therefore there exist $i \geq j \geq 0$ and a basis $\langle 1, \omega, \theta \rangle$ of R such that

$$R_1 = \mathbb{Z} + \frac{\omega}{p^i}\mathbb{Z} + \frac{\theta}{p^j}\mathbb{Z} \tag{25}$$

If $i = 1$ then the result is immediate. Assuming $i > 1$, we can without loss of generality assume that the

basis $\langle 1, \omega, \theta \rangle$ for R is normal. Then using the characterising equations (11) for such a basis we obtain,

$$\begin{aligned}
\frac{\omega}{p^i}\frac{\theta}{p^j} &= \frac{-ad}{p^{i+j}}, \\
\left(\frac{\omega}{p^i}\right)^2 &= \frac{-ac}{p^{2i}} - \frac{b}{p^i}\left(\frac{\omega}{p^i}\right) + \frac{a}{p^{2i-j}}\left(\frac{\theta}{p^j}\right), \\
\left(\frac{\theta}{p^j}\right)^2 &= \frac{-bd}{p^{2j}} - \frac{d}{p^{2j-i}}\left(\frac{\omega}{p^i}\right) + \frac{c}{p^j}\left(\frac{\theta}{p^j}\right).
\end{aligned}$$

Using (25) we deduce that these are equivalent to

$$b \equiv 0 \mod p^i, \quad a \equiv 0 \mod p^{2i-j}, \quad c \equiv 0 \mod p^j, \quad d \equiv 0 \mod p^{2j-i}, \tag{26}$$

where we have taken the convention that every $x \in \mathbb{Z}$ satisfies $x \equiv 0 \mod p^e$ for any $e \leq 0$. If $j = 0$ then replacing i with 1 the conditions of (26) still hold and so R_1 is still a ring and is second case in the lemma statement. Further if $j \neq 0$ then replacing (i, j) with $(i-1, j-1)$ these conditions still hold and R_1 is still a ring. Iterating a finite number of times, we can take $i = 1$ and $j = 1, 0$ and so R_1 is as in the lemma statement. □

In particular, we can translate these conditions through the Delone–Faddeev correspondence to the binary cubic forms we will be counting. Let $\mathcal{U}_p \subset V_\mathbb{Z}$ be the set of irreducible forms $f = (a, b, c, d)$ such that not all coefficients of f are divisible by p and f is not $\mathrm{GL}_2(\mathbb{Z})$-equivalent to a form with

$$a \equiv 0 \mod p^2, \quad b \equiv 0 \mod p,$$

then in fact are precisely the forms with the properties we seek.

Theorem 4.2. *Given a binary cubic form $f \in V_\mathbb{Z}$, the cubic ring $R_f|\mathbb{Z}$ is maximal at p if and only if $f \in \mathcal{U}_p$.*

Proof. This follows immediately from the proof of Lemma 4.1. The congruence equations in (26) with $i = 1$ and $j = 0, 1$ as in the result of the lemma are equivalent to the conditions rejecting points from being in $\mathcal{U}_p$. □

Maximality is a local property, and so $\mathcal{U} = \cap_p \mathcal{U}_p \subset V_\mathbb{Z}$ is the set of binary quadratic forms corresponding to maximal cubic rings. The theory described in Lemma 4.1 can be used to derive another interesting result (essentially due to Bhargava [3, prop. 15]) which will be of use when we apply a seive method in subsection 4.4.

Proposition 4.3. *Given $f \in V_\mathbb{Z}$, the number of index p subrings of R_f is equal to the number of roots of f in R/pR. In particular this number is at most 3.*

Proof. Let $S \subset R$ be an index p subring, then S is a cubic ring which is not maximal. By Lemma 4.1, we can choose a normal $\mathbb{Z}$-basis $1, \omega, \theta$ of R such that $1, p\omega, \theta$ is a normal $\mathbb{Z}$-basis for S. Let $f_R = ax^3 + bx^2y + cxy^2 + dy^3$. Then S is a well defined ring if and only if the characterising equations for S 11 give $(p\omega)^2 \in S$ and $\theta^2 \in S$. It is plain that the former of these two holds trivially, but the latter gives,

$$\theta^2 = l - \frac{d}{p}(p\omega) + \theta \in S \iff d \equiv 0 \mod p$$

Thus S is an index p subring if and only if $d \equiv 0 \mod p$. Further $f(p\omega, \theta) \equiv 0$ in R/pR if and only if $d \equiv 0$. Since the basis $1, p\omega, \theta$ uniquely establishes the cubic ring of index p S we have the required bijection. □

4.2 Counting Congruence–Condition Subsets

We would like to count maximal cubic orders which, by the Delone–Faddeev correspondence, is equivalent to counting irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits in $\mathcal{U} = \cap_p \mathcal{U}_p$. It is immediate from the definition that $\mathcal{U}_p$ is $\mathrm{GL}_2(\mathbb{Z})$-invariant, and hence so is $\mathcal{U}$. We would like to take a similar approach to that taken in Section 3 when counting cubic orders, beginning with Corollary 3.13. The immediate barrier which stops us from just continuing from there is that $\mathcal{U}$ is not every point in $V_\mathbb{Z}$, and our methods have involved finding all lattice points in a region up to some error.

From the definition of $\mathcal{U}_p$ we can see that it is defined by congruence conditions mod p^2, and further from the Chinese remainder theorem $\bigcap_{p<Y} \mathcal{U}_p$ is defined precisely by congruence conditions mod $\prod_{p<Y} p^2$. More generally, let $S \subset V_{\mathbb{Z}}$ be defined by congruence conditions mod m for some $m \in \mathbb{Z}$. Then we can specify a set $\bar{S}$ of binary cubic forms mod m such that $f \in S$ if and only if $\bar{f} \in \bar{S}$ where $\bar{f} \equiv f \mod m$. Thus if we imagine tiling $\mathbb{R}^4$ evenly with boxes of side length m, the intersection of $\mathcal{U}_p$ with any two boxes should be identical up to translations in any variable by a multiple of m. In particular we can see S as a union of $k = \#\bar{S}$ translates of the inflated lattice $mV_{\mathbb{Z}}$.

Definition 4.4. *For any set $S \subset V_{\mathbb{Z}}$ which is defined by congruence conditions mod m for some $m \in \mathbb{Z}$, the **Lattice Decomposition** of S is the disjoint union*

$$S = \bigcup_{i=1}^{k} S_i$$

where the S_i are the translates of the inflated lattice $mV_{\mathbb{Z}}$ as described above and necessarily $k = \#\bar{S}$ the number of congruence classes mod m occupied by forms in S.

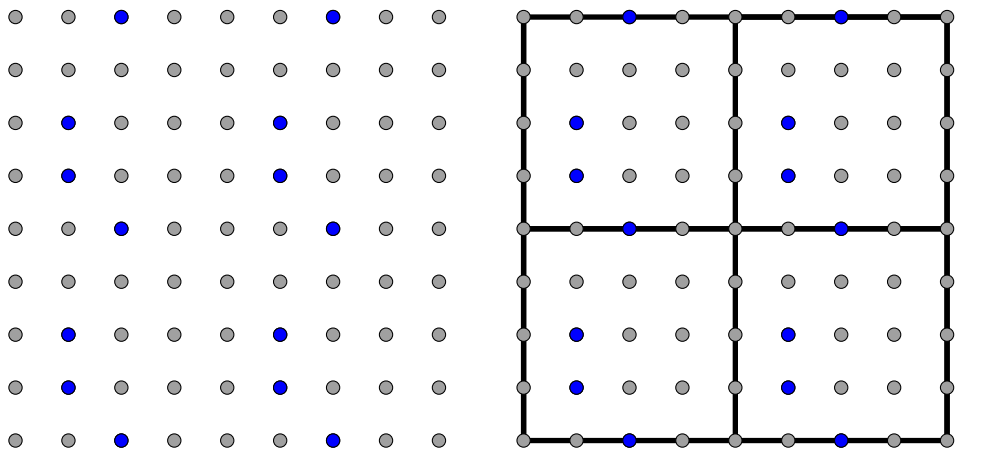
It is precisely this notion of Lattice decomposition which will allow us to use the previous methods established.

Example 3. *Seeing as the confines of this essay do not allow us to adequately capture $V_{\mathbb{R}}$, consider an example of the above concept in the set of linear forms $ax + by$ over $\mathbb{R}$ which can be identified with $\mathbb{R}^2$. Define the set of forms*

$$L = \{f = ax + by \in \mathbb{Z}[x, y] \mid f \equiv x + y, 2x \text{ or } x + 2y \mod 4\}$$

Then looking at the boxes of side length 4, consider $[0, 4]^2$ and $[4, 8] \times [0, 4]$ as in Figure 2. These have an identical arrangement of points from L. In fact it should be clear that this repeating pattern exists in $[5A, 5B] \times [5C, 5D]$ for any $A, B, C, D \in \mathbb{Z}$. Thus we can see that this particular example has lattice decomposition $L = L_1 \cup L_2 \cup L_3$ where

$$L_1 = \{(5a + 1, 5b + 1)\} \quad L_2 = \{(5a + 2, 5b)\} \quad L_3 = \{(5a + 1, 5a + 2)\}$$



(a) Points in L (b) Points in L alongside boxes of width 4

Figure 2: Points in L (blue) plotted inside the lattice $\mathbb{Z}^2$ (grey) in $[0, 8]^2$

For $S \subset V_{\mathbb{Z}}$ defined by congruence conditions mod m, recall the definition of $N(S; X)$ for arbitrary S given by (18) which agrees with the usual 'number of irreducible $\mathrm{GL}_2(\mathbb{Z})$-orbits' definition for S which are $\mathrm{GL}_2(\mathbb{Z})$-invariant. In particular even if S is $\mathrm{GL}_2(\mathbb{Z})$-invariant, the translates $\{S_i\}_{i=1}^k$ in the lattice decomposition of S are not in general. However, since the $\{S_i\}_{i=1}^k$ are disjoint it is certainly true from this definition that if $S_i^{\pm} = S_i \cap V_{\mathbb{Z}}^{\pm}$ then

$$N(S \cap V_{\mathbb{Z}}^{\pm}; X) = \sum_{i=1}^{k} N(S_i^{\pm}; X).$$

Hence it is sufficient to calculate $N(S_i^{\pm}; X)$, which is similar to the case of $N(V_{\mathbb{Z}}; X)$ in Section 3 since S_i is just an inflation and translation of $V_{\mathbb{Z}}$. From Corollary 3.13 we have up to error $O(X^{3/4+\varepsilon})$

$$N(S_i^{\pm}; X) = \frac{1}{M_{\pm}} \int_{g \in N'(t)A'\Lambda} \# \left\{ x \in S_i \cap B^{\pm}(n,t,\lambda,X) \mid \substack{x=(a,b,c,d) \\ a \neq 0} \right\} t^{-2}\, dn\, d^{\times}t\, d^{\times}\lambda. \tag{27}$$

where we have S_i and not $S_i^{\pm}$ in the integrand since $S_i^{\mp} \cap B^{\pm}(n,t,\lambda,X) = \emptyset$. Thus we will require an analogue of Theorem 3.16 to estimate the integrand.

Theorem 4.5. *For a translate S_i of the inflated lattice $mV_{\mathbb{Z}}$, the number of points in $S_i \cap B^{\pm}(n,t,\lambda,X)$ with first coordinate nonzero is*

$$\begin{cases} 0 & \text{if } C\lambda t^{-3} < q \\ m^{-4} \operatorname{Vol}(B^{\pm}(n,t,\lambda,X)) + O(\max\left\{m^{-3}C^3t^3\lambda^3, 1\right\}) & \text{otherwise,} \end{cases}$$

where $B = B(C)$ as in (16) and q is the smallest absolute value of any nonzero first coordinate in S_i.

Proof. Identically to the proof of Theorem 3.16, every point $(\alpha,\beta,\gamma,\delta) \in B^{\pm}(n,t,\lambda,X)$ satisfies $\alpha = a\lambda t^{-3}$ for a a first coordinate of a point in B. In particular, we still have $|a| \leq C$ and so

$$|\alpha| \leq |a\lambda t^{-}3| \leq C\lambda t^{-3}.$$

If $C\lambda t^{-3} < q$ then $|\alpha| < q$ and so $\alpha = 0$ for any point $(\alpha,\beta,\gamma,\delta) \in S_i \cap B^{\pm}(n,t,\lambda,X)$.

Otherwise, $C\lambda t^{-3} \geq q$ and so since $t \geq \frac{\sqrt[4]{3}}{\sqrt{2}}$ we must have $\lambda \geq \frac{q}{C}(\frac{\sqrt[4]{3}}{\sqrt{2}})^3$. Note that the number of points in $S_i \cap B^{\pm}(n,t,\lambda,X)$ is invariant if we scale both sets simultaneously. So that we can count points in $V'_{\mathbb{Z}} \cap B^{\pm}(n,t,m^{-1}\lambda,X)$ for $V'_{\mathbb{Z}}$ a not necessarily integer translation of the lattice $V_{\mathbb{Z}}$. Then translating this by the appropriate real values we are counting points in $V_{\mathbb{Z}} \cap \beta$ for β a translation of $B(n,t,m^{-1}\lambda,X)$. Since none of the theory in the proof of Theorem 3.16 explicitly relied on more than the volumes of $B(n,t,\lambda,X)$ and its projections, which are unchanged under translation, we immediately have that the number of lattice points in $V_{\mathbb{Z}} \cap \beta$ is

$$\operatorname{Vol}(B^{\pm}(n,t,m^{-1}\lambda,X)) + O(\max\left\{C^3t^3(m^{-1}\lambda)^3\right\}) = m^{-4}\operatorname{Vol}(B^{\pm}(n,t,\lambda,X)) + O(\max\left\{m^{-3}C^3t^3\lambda^3, 1\right\})$$

□

We now directly compute the integral (27) using Theorem 4.5 in the same way as when we counted cubic orders (subsection 3.6). Before we do so, we will require a particular definition to state the result efficiently.

Definition 4.6. *For $S \subset V_{\mathbb{Z}}$, we define $\mu_p^l(S)$ to be the proportion of congruence classes mod p^l occupied by forms in S. We define the* ***p-adic density*** *of S to be*

$$\mu_p(S) = \lim_{l \to \infty} \mu_p^l(S)$$

Note that in our current setting, if S is defined by congruence conditions mod p^r then $\mu_p(S)$ must be precisely $(\#\bar{S})/p^{4r}$ where $\bar{S}$ is the reduction mod p^r of elements in S.

Theorem 4.7. *For $S \subset V_{\mathbb{Z}}$ a subset defined by congruence conditions at powers of primes for finitely many primes p,*

$$\lim_{X \to \infty} \frac{N(S \cap V_{\mathbb{Z}}^{\pm}; X)}{X} = \frac{\pi^2}{12 n_{\pm}} \left(\prod_p \mu_p(S) \right)$$

Proof. An immediate application of Chinese remainder theorem gives that S is defined by congruence conditions mod m which is the product of the prime powers in the theorem statement. Write S in terms of its lattice decomposition $S = S_1 \cup \cdots \cup S_k$, evalutating $N(S_i^{\pm}; X)$. As discussed above, from Corollary 3.13 up to error $O(X^{3/4+\varepsilon})$ we have (27). As discussed when we counted cubic orders, the integrand is 0 for $\lambda > X^{1/4}$. By Theorem 4.5, the integrand is also zero for $t > (\frac{C\lambda}{q})^{1/3}$ and $\lambda < \frac{q}{C}(\frac{\sqrt[4]{3}}{\sqrt{2}})^3$ where q is the least absolute value of first coordinates of points in S_i. Hence,

$$N(S_i^{\pm}; X) = \frac{1}{M_{\pm}} \int_{\lambda = \frac{q}{C}\left(\frac{\sqrt[4]{3}}{\sqrt{2}}\right)^3}^{X^{1/4}} \int_{t = \frac{\sqrt[4]{3}}{\sqrt{2}}}^{(\frac{C\lambda}{q})^{1/3}} \int_{N'(t)} m^{-4} \operatorname{Vol}(B^{\pm}(n,t,\lambda,X)) + O(\max\left\{m^{-3}C^3t^3\lambda^3, 1\right\}) t^{-2}\, dn\, d^{\times}t\, d^{\times}\lambda$$

Computing this integral in exactly the same way as Lemmas 3.17 and 3.18 we obtain error terms of $O(m^{-4}C^{10/3}X^{5/6}q^{-2/3}M_{\pm}^{-1})$ and $O(m^{-3}C^{10/3}X^{5/6}q^{-1/3}M_{\pm}^{-1})$ respectively. Thus for any $v_{\pm} \in V_{\mathbb{R}}^{\pm}$,

$$N(S_i^{\pm}; X) = \frac{1}{m^4 n_{\pm}} \operatorname{Vol}(\mathcal{R}_X(v_{\pm})) + O(m^{-3}C^{10/3}X^{5/6}q^{-1/3}).$$

where we can neglect $C, M_{\pm}$ terms in the error since these are only dependent on C which is a fixed constant. Taking the value for the volume term as in subsection 3.6 we get

$$N(S_i^{\pm}; X) = m^{-4}\frac{\pi^2}{12n_{\pm}}X + O(m^{-3}X^{5/6}q^{-1/3}).$$

Thus

$$N(S \cap V_{\mathbb{Z}}^{\pm}) = \sum_{i=1}^{k} N(S_i^{\pm}; X) = km^{-4}\frac{\pi^2}{12n_{\pm}}X + O(km^{-3}X^{5/6}q^{-1/3}).$$

Notice that k is bounded by the constant m^4, and q is bounded by m and so the error term can be written $O(m^{2/3}X^{5/6})$. Under the assumption that $m = O(X^{1/6})$ we have that the error bound vanishes when dividing by X and taking asymptote in X. Further km^{-4} is the proportion of congruence classes mod m occupied by forms in S and so by Chinese remainder theorem $km^{-4} = \prod_p \mu_p(S)$. Thus we have the result. □

We will apply this result in the case $S = \bigcap_{p<Y} \mathcal{U}_p$.

4.3 p-adic Densities

We would like to calculate the p-adic density of $\mathcal{U}_p$ so that we can use Theorem 4.7. In order to do this, we will need to separate the forms according to their behaviour mod p.

Definition 4.8. *Given $f \in V_{\mathbb{Z}}$ and $p \in \mathbb{Z}$ a prime such that $f \not\equiv 0 \mod p$, define the Davenport–Heilbronn symbol (f, p) to be*

$$(f, p) = (f_1^{e_1} \dots)$$

where f_i are the degrees of the factors of f in $\mathbb{F}_p[x, y]$ and e_i are their multiplicities. We denote by $T_p(\cdot)$ the set of $f \in V_{\mathbb{Z}}$ such that $(f, p) = (\cdot)$.

We shall calculate $\mu_p(\mathcal{U}_p)$ by splitting into cases according to the Davenport–Heilbronn symbol and taking the p-adic density of

$$\mathcal{U}_p(\cdot) = T_p(\cdot) \cap \mathcal{U}_p.$$

Note that by definition no form which is a multiple of p (and hence 0 mod p) is contained in $\mathcal{U}_p$, so a sum over the Davenport–Heilbronn symbol of these values gives us precisely $\mu_p(\mathcal{U}_p)$.

Lemma 4.9. *The p-adic densities of $T_p(\cdot)$ are given by,*

$$\begin{aligned}
\mu_p(T_p(111)) &= \tfrac{1}{6}(p-1)^2p(p+1)/p^4 \\
\mu_p(T_p(12)) &= \tfrac{1}{2}(p-1)^2p(p+1)/p^4 \\
\mu_p(T_p(3)) &= \tfrac{1}{3}(p-1)^2p(p+1)/p^4 \\
\mu_p(T_p(1^21)) &= (p-1)p(p+1)/p^4 \\
\mu_p(T_p(1^3)) &= (p-1)(p+1)/p^4.
\end{aligned}$$

Proof. Since $T_p(\cdot)$ is reliant only on conditions mod p, $\mu_p(T_p(\cdot))$ is just the proportion of congruence classes mod p occupied by forms in $T_p(\cdot)$.

Claim: The number of irreducible binary forms of degree 1 and 2 in $\mathbb{F}_p[x, y]$ with leading coefficient 1 are $(p + 1)$ and $\frac{1}{2}p(p - 1)$ respectively.

Proof of claim. Linear forms $\alpha x + \beta y$ are uniquely defined by the point $(\alpha, \beta) \in \mathbb{P}^1_{\mathbb{F}_P}$ that they define up to scalar multiplication. Since we are taking those with leading coefficient 1, the number of such is just $\#\mathbb{P}^1_{\mathbb{F}_p} = p + 1$. For quadratic forms, note that there are $p^2 + p + 1$ quadratic forms over $\mathbb{F}_p$ which have leading coefficient 1. If a quadratic form f is reducible, then it is either g^2 or gh for g, h two distinct

linear forms with leading coefficient 1. The number of such forms in each of these cases is $p+1$ and $\binom{p+1}{2}$ respectively. Thus the number of irreducible quadratic forms is

$$p^2+p+1-(p+1)-\binom{p+1}{2} = p^2 - \frac{p(p-1)}{2}$$
$$= \frac{1}{2}p(p-1)$$

□

We apply the claim, multiplying by $(p-1)$ for the scalar factor of the leading coefficient, to obtain the density for all but $T_p(3)$. However, since every form is either in $T_p(\cdot)$ or is the degenerate case $f \equiv 0 \mod p$, we simply calculate

$$\mu_p(T_p(3)) = \frac{p^4-1}{p^4} - \sum_{(\cdot)\neq(3)} \mu_p(T_p(\cdot)) = \frac{1}{3}(p-1)^2 p(p+1)/p^4$$

□

Now, we apply this to counting the various cases in $\mathcal{U}_p$.

Lemma 4.10. *The p-adic density of $\mathcal{U}_p$ is*

$$\mu_p(\mathcal{U}_p) = (1-p^{-3})(1-p^{-2})$$

Proof. Firstly, if $f \in T_p(111), T_p(12), T_p(3)$ then the discriminant of f is coprime to p. Using the coefficient formula for discriminant (3) we immediately deduce that the coefficients of f cannot be all divisible by p. Similarly, since $\mathrm{GL}_2(\mathbb{Z})$-equivalence preserves discriminant, f cannot be $\mathrm{GL}_2(\mathbb{Z})$-equivalent to one with coefficients satisfying $a \equiv 0 \mod p^2$ and $b \equiv 0 \mod p$. Thus for these three cases, $\mathcal{U}_p(\cdot) = T_p(\cdot)$. If $f \in T_p(1^21)$ or $T_p(1^3)$ then it has a factor of multiplicity at least 2. Using $\mathrm{GL}_2(\mathbb{Z})$ action as in the proof of Proposition 2.19 we can send this factor to y and so $a \equiv b \equiv 0 \mod p$. Further a proportion of $\frac{1}{p}$ will satisfy $a \equiv 0 \mod p^2$ and so in these two cases $\mathcal{U}_p(\cdot) = \frac{p-1}{p} T_p(\cdot)$.

We then simply calculate

$$\mu_p(\mathcal{U}_p) = \sum_{(\cdot)} \mu_p(\mathcal{U}_p(\cdot)) = \frac{(p^3-1)(p^2-1)}{p^5}$$

as required. □

Notice that $\mu_p(\mathcal{U}_q) = 1$ for $p, q \in \mathbb{Z}$ distinct primes by Chinese remainder theorem.

4.4 Counting Cubic Fields

We will use the results established in the previous subsections to count maximal cubic orders and thus cubic fields. Using Theorem 4.7 we have obtained that if $\mathcal{U}^{(Y)} = \cap_{p<Y} \mathcal{U}_p$

$$\lim_{X\to\infty} \frac{N(\mathcal{U}^{(Y)} \cap V_{\mathbb{Z}}^{\pm}; X)}{X} = \frac{\pi^2}{12 n_{\pm}} \prod_p \mu_p(\mathcal{U}^{(Y)}).$$

In order to use the p-adic density values in subsection 4.3, note that by Chinese remainder theorem for a prime q

$$\mu_q(\mathcal{U}^{(Y)}) = \prod_{p<Y} \mu_q(\mathcal{U}_p) = \begin{cases} \mu_q(\mathcal{U}_q) & q < Y \\ 1 & \text{otherwise.} \end{cases}$$

Therefore by Lemma 4.10

$$\lim_{X\to\infty} \frac{N(\mathcal{U}^{(Y)} \cap V_{\mathbb{Z}}^{\pm}; X)}{X} = \frac{\pi^2}{12 n_{\pm}} \prod_{p<Y} \mu_p(\mathcal{U}_p) \tag{28}$$

$$= \frac{\pi^2}{12 n_{\pm}} \prod_{p<Y} (1-p^{-3})(1-p^{-2}). \tag{29}$$

Letting $Y \to \infty$ in (29) we immediately obtain

$$\limsup_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbb{Z}}^{\pm}; X)}{X} \leq \frac{\pi^2}{12 n_{\pm}} \prod_p (1-p^{-3})(1-p^{-2}) \tag{30}$$

In order to take limits in Y to obtain a lower bound, we will require an elementary seive method. Let $\mathcal{W}_p = V_{\mathbb{Z}} \backslash \mathcal{U}_p$, so that the forms in $\mathcal{W}_p$ correspond to the cubic rings which are not maximal at p. Note that $\mathcal{W}_p$ is $\mathrm{GL}_2(\mathbb{Z})$ invariant since $\mathcal{U}_p$ is.

Lemma 4.11. *We have that the number of irreducible* $\mathrm{GL}_2(\mathbb{Z})$ *orbits of points in* $\mathcal{W}_p$ *is*

$$N(\mathcal{W}_p; X) = O(X p^{-2}).$$

As $\mathcal{U}^{(Y)} \subset (\mathcal{U} \cup \bigcup_{p \geq Y} \mathcal{W}_p)$ we immediately obtain that

$$\begin{aligned} \lim_{X\to\infty} \frac{N(\mathcal{U}^{(Y)} \cap V_{\mathbb{Z}}^{\pm}; X)}{X} &\leq \lim_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbb{Z}}^{\pm}; X)}{X} + \lim_{X\to\infty} \frac{N((\cup_{p\geq Y} \mathcal{W}_p) \cap V_{\mathbb{Z}}^{\pm}; X)}{X} \\ &\leq \lim_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbb{Z}}^{\pm}; X)}{X} + \sum_{p \geq Y} \lim_{X\to\infty} \frac{N(\mathcal{W}_p \cap V_{\mathbb{Z}}^{\pm}; X)}{X}, \end{aligned}$$

where the second inequality is because the $\mathcal{W}_p$ are not necessarily disjoint. Applying Lemma 4.11 and (29),

$$\lim_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbb{Z}}^{\pm}; X)}{X} \geq \frac{\pi^2}{12 n_{\pm}} \left(\prod_{p<Y} (1-p^{-3})(1-p^{-2}) \right) - \sum_{p \geq Y} O(p^{-2}). \tag{31}$$

Letting $Y \to \infty$ we obtain and then comparing to (30) we have proved that

$$\begin{aligned} \lim_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbb{Z}}^{\pm}; X)}{X} &= \frac{\pi^2}{12 n_{\pm}} \prod_p (1-p^{-3})(1-p^{-2}) \\ &= \frac{1}{2 n_{\pm} \zeta(3)}. \end{aligned}$$

Recalling the values of $n_{\pm}$ as $6, 2$ for $+, -$ respectively from Subsection 3.1 we have shown

$$\begin{aligned} \lim_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbb{Z}}^{+}; X)}{X} &= \frac{1}{12\zeta(3)} \\ \lim_{X\to\infty} \frac{N(\mathcal{U} \cap V_{\mathbb{Z}}^{-}; X)}{X} &= \frac{1}{4\zeta(3)}. \end{aligned}$$

The Delone–Faddeev correspondence and the construction of $\mathcal{U}$ in Subsection 4.1 imply that this is equivalent to Theorem 1.1 and so we have counted cubic fields asymtotically in their discriminant.

Proof of Lemma 4.11. Through the Delone Faddeev correspondence we need only count cubic orders R which are not maximal at p with $|\Delta(R)| < X$, something we have certainly established tools to do in Section 3 and Subsection 4.1. By Lemma 4.1 if R is such a cubic order then it has a $\mathbb{Z}$-basis $\langle 1, \omega, \theta \rangle$ such that one of the following is a ring:

$$\begin{aligned} R' &= \mathbb{Z} + \tfrac{\omega}{p}\mathbb{Z} + \theta\mathbb{Z} \\ R'' &= \mathbb{Z} + \tfrac{\omega}{p}\mathbb{Z} + \tfrac{\theta}{p}\mathbb{Z} \end{aligned}$$

Write $f_R(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, the element from the Delone–Faddeev correspondence which relates to R with the basis $\langle 1, \omega, \theta \rangle$. Without loss of generality we can assume that the basis of

If R' is a ring, then we separate into two cases. If $f_{R'}$ is not a multiple of p then the characteristic equations for R give that

$$\begin{aligned} (\tfrac{\omega}{p})^2 &= \tfrac{m}{p^2} - \tfrac{b}{p}(\tfrac{\omega}{p}) + \tfrac{a}{p^2}\theta \\ \theta^2 &= l - dp(\tfrac{\omega}{p}) + c\theta. \end{aligned}$$

By the quartic equation for discriminant (3) of $f_{R'}$ we get that

$$\Delta(R') = \mathrm{Disc}(f_{R'}) = \mathrm{Disc}(f_R) p^{-2} = \Delta(R) p^{-2} < X p^{-2}.$$

By Theorem 1.2 we know that the number of such R' is $O(Xp^{-2})$. Further since R is an index p subring of R' then by Proposition 4.3 the number of R is at most 3 times the number of R' which is still $O(Xp^{-2})$. If f is a multiple of p then note that from the characterising equations we can deduce that R'' is also a ring.

If R'' is a ring, then the characterising equations for R give

$$\left(\frac{\omega}{p}\right)^2 = \frac{m}{p^2} - \frac{b}{p}\frac{\omega}{p} + \frac{a}{p}\frac{\theta}{p}$$
$$\left(\frac{\theta}{p}\right)^2 = \frac{l}{p^2} - \frac{d}{p}\frac{\omega}{p} + \frac{c}{p}\frac{\theta}{p}$$

.

Again using the quartic equation for discriminant (3) we obtain $\Delta(R'') = \Delta(R)p^{-4}$, thus by Theorem 1.2 we have that there are $O(Xp^{-4})$ such R''. Since $R = \mathbb{Z} + pR''$, this means there are $O(Xp^{-2})$ such R and we have shown

$$N(\mathcal{W}_p; X) = O(Xp^{-4}) + O(Xp^{-2}) = O(Xp^{-2})$$

□

A Computer Algebra Code

Below are some scripts used to carry out some particularly intractible calculations from this essay. Their use is referenced in the relevant locations throughout.

Script 1. *A Magma script which compares $\mathcal{H}_{\gamma \cdot f}$ and $\gamma \cdot \mathcal{H}_f$ for $\gamma \in \mathrm{SL}_2(\mathbb{R})$.*

```
MC := MonomialCoefficient;
K<R,S,T,U> := PolynomialRing(Rationals(), 4);
Q<A,B,C,D> := quo<K | R*U - S*T - 1>;
R<a,b,c,d> := PolynomialRing(Q,4);
RR<x,y> := PolynomialRing(R,2);

// Function to output Hessian of a binary cubic as in Bhargava
hessian := function(binary_cubic)
    coeffs := [MC(binary_cubic,x^(3-i)*y^i): i in [0..3]];
    H := (coeffs[2]^2-3*coeffs[1]*coeffs[3])*x^2
            + (coeffs[2]*coeffs[3]-9*coeffs[1]*coeffs[4])*x*y
            + (coeffs[3]^2-3*coeffs[2]*coeffs[4])*y^2;
    return H;
end function;

// Function sending f(x,y) --> f(Ax+Cy,Bx+Dy)
GL_Action := function(binary_form)
    return Evaluate(binary_form, [A*x+C*y, B*x+D*y]);
end function;

f := a*x^3 + b*x^2*y + c*x*y^2 + d*y^3;

assert hessian(GL_Action(f)) eq GL_Action(hessian(f));
```

Script 2. *A magma script to verify that K fixes $B(C)$ as defined in 16. This code is due to Dr. Tom Fisher.*

```
MC := MonomialCoefficient;
K<cc,ss> := FunctionField(Rationals(),2);
R<a,b,c,d> := PolynomialRing(K,4);
RR<x,y> := PolynomialRing(R,2);

f := a*x^3 + b*x^2*y + c*x*y^2 + d*y^3;

// We transform f using a matrix in SO(3,R)
// Here cc and ss stand for cos(theta) and sin(theta)
F := Evaluate(f,[cc*x + ss*y,-ss*x + cc*y]);
coeffs := [MC(F,x^(3-i)*y^i): i in [0..3]];

// The coefficients of the binary cubic change according
// to the following 4 by 4 matrix
N := Matrix(K,4,4,[MC(coeff,R.i): i in [1..4],coeff in coeffs]);

// We check that the quadratic form 3*a^2 + b^2 + c^2 + 3*d^2
// is preserved by this transformation
D := DiagonalMatrix(K,[3,1,1,3]);
assert Transpose(N)*D*N eq (cc^2 + ss^2)^3*D;
```

B Binary Quadratic Forms

Here we give a brief discussion of some material regarding positive definite binary quadratic forms over $\mathbb{Z}$ and $\mathbb{R}$. In particular, the results here are either attributed to the text by Buell [4] or to the *Modular Forms and L-Functions* course at the university of Cambridge in Michaelmas term 2017. Some results from Buell are presented with alternative proofs, which more efficiently convey the structures at play. We denote by $\mathrm{GL}_2^+(\mathbb{R})$ the set of positive determinant matrices over $\mathbb{R}$.

Definition B.1. *A binary quadratic form*

$$f = ax^2 + bxy + cy^2$$

*with each $A_i \in \mathbb{R}$, written as $f = (a, b, c)$ is said to be **positive definite** if it has discriminant* $\mathrm{Disc}(f) < 0$. *Moreover f is said to be **reduced** if the coefficients of f satisfy*

$$|b| \leq a \leq c$$

We take the action of $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ on binary quadratic forms given by $(\gamma \cdot f)(x, y) = f((x, y)\gamma)$ and write $f \sim f'$ to mean that f is $\mathrm{GL}_2^+(\mathbb{R})$ equivalent to f'. Note that positive definite binary quadratic forms are irreducible, since as dehomogenised polynomials they have the same discriminant and so are irreducible.

Definition B.2. *Given a positive definite binary quadratic form $f = (a, b, c)$ of discriminant $-D$ the **principal root** is*

$$\tau_f = \frac{-b + i\sqrt{D}}{2a}$$

This is also the root of the dehomogenised polynomial $ax^2 + bx + c$ which lies in the upper half plane. In particular we can write $f = a(x - \tau_f y)(x - \overline{\tau_f} y)$.

Theorem B.3 ([4])**.** *A positive definite binary quadratic form f is reduced if and only if the principal root $\tau_f \in \mathcal{D}$ the classical fundamental domain in the upper half plane given by*

$$\left\{ z \in \mathbb{C} \mid \mathrm{Im}(z) > 0,\ \mathrm{Re}(z) \in \left[-\frac{1}{2}, \frac{1}{2}\right],\ |z| \geq 1 \right\}$$

Proof. This is a simple equivalence between conditions. Let $f = (a, b, c)$ be a binary quadratic form over $\mathbb{R}$, by definition $\mathrm{Im}(\tau_f) > 0$. Further, $\mathrm{Re}(\tau_f) = \frac{-b}{2a}$, so $|b| \leq a$ is equivalent to $\mathrm{Re}(\tau_f) \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. Finally, we can note that since $a\tau_f\overline{\tau_f} = c$, then $|\tau| = \frac{c}{a}$ and then the condition $a \leq c$ is equivalently $|\tau_f| \geq 1$. Thus f is reduced if and only if $\tau_f \in \mathcal{D}$. □

Proposition B.4. *Given a binary quadratic form of the form $f = a(x^2 + y^2)$ for $a \in \mathbb{R}$ let $\mathcal{F} = N'A'K\Lambda$ be the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})\backslash \mathrm{GL}_2^+(\mathbb{R})$ as established in Theorem 3.4. Then $\mathcal{F} \cdot f$ is the set of all positive definite reduced binary quadratic forms.*

Proof. Decompose the element $g \in \mathcal{F}$ into the components of the domain $\mathcal{F}$ so that $g = \begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} k \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}$. Then note that

$$\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} \cdot f = \lambda^2 f$$

so that we can obtain any scalar multiple of a form $g \cdot f$. Further the action of K is trivial since

$$(\cos\theta x + \sin\theta y)^2 + (\cos\theta y - \sin\theta x)^2 = x^2 + y^2$$

Finally, note that the action of the remaining two components is:

$$\begin{aligned} \begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \cdot a(x^2 + y^2) &= \begin{pmatrix} t^{-1} & \\ nt^{-1} & t \end{pmatrix} \cdot a(x + iy)(x - iy) \\ &= a(t^{-1}x + (nt^{-1} + it)y)(t^{-1}x - (it - nt^{-1})y) \\ &= at^{-2}(x + (n + it^2)y)(x - (it^2 - n)y) \end{aligned}$$

and so the principal root of $g \cdot f$ is $\tau = -n + it^2$ and given the definition of N' and A' we must have that $\tau \in \mathcal{D}$ and moreover this characterises all of the elements of the classical domain $\mathcal{D}$, and so by Theorem B.3 we have that $\mathcal{F} \cdot f$ is the set of all positive definite binary quadratic forms. □

Finally, we recall a fact from part II number theory (also in [4])

Theorem B.5. *Every positive definite binary quadratic form is* $\mathrm{SL}_2(\mathbb{Z})$ *equivalent to a unique reduced form, with the exception of the cases*

$$(a, b, a) \sim (a, -b, a)$$
$$(a, a, c) \sim (a, -a, c)$$

Definition B.6. *For a positive definite binary quadratic form* f*, we will call* $\theta_f = -\overline{\tau_f}$ *the* ***characterising root*** *of* f*. Note that* θ_f *is in the upper half plane.*

Remark B.7. *Note that the action of* $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ *on* f *acts via*

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} a(x + \theta_f y)(x + \overline{\theta_f} y) = a((A + \theta_f B)x + (C + \theta_f D)y)((A + \overline{\theta_f} B)x + (C + \overline{\theta_f} D)y)$$

which has characterising root $\frac{D\theta_f + C}{B\theta_f + A}$*. Thus the action of* $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ *on a binary quadratic form* f *satisfies*

$$\theta_{\gamma f} = \gamma \theta_f$$

where the right hand side is given by the conjugate of the usual mobius action by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

C Volume of $\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2^{\pm 1}(\mathbb{R})$

Let $\mathrm{GL}_2^{\pm 1}(\mathbb{R})$ be the group of real matrices with determinant of absolute value 1. We wish to derive the value of $\int_{\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2^{\pm 1}(\mathbb{R})} dh$, where dh is the measure ascertained from the Iwasawa decomposition in Subsection 3.1 without Λ. We will do so by a geometric method (essentially due to Garrett [15]) which computes this from $\int_{\mathcal{D}} y^{-2} dx dy$ where $\mathcal{D}$ is the usual fundamental domain in the upper half plane.

Note that a fundamental domain for $\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2^{\pm 1}(\mathbb{R})$ can be obtained from the domain $\mathcal{F}$ for $\mathrm{GL}_2(\mathbb{Z})\backslash \mathrm{GL}_2(\mathbb{R})$ in Theorem 3.4 by restricting to

$$\mathcal{G} = \{na'k \mid n \in N'(a'),\, a' \in A',\, k \in K\}\,.$$

Consider the identification of such matrices with the elements if $\mathcal{D}$ as given in the proof of Theorem 3.4 by $g \mapsto g \cdot i$, where g has the twisted action on the upper half plane

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot i = \frac{Di + C}{Bi + A}.$$

As before, K is the stabiliser of i and further since the central elements ± 1 of $\mathrm{GL}_2(\mathbb{Z})$ act trivially on the upper half plane and are in K, we see that in this setting $\{\pm 1\}\backslash K$ has volume 1. Thus in the identification K will have volume 2, and not 1 (from our normalisation of dk), so we scale accordingly.

The action of elements in na' is given by

$$\begin{pmatrix} 1 & \\ n & 1 \end{pmatrix} \begin{pmatrix} t^{-1} & \\ & t \end{pmatrix} \cdot i = t^2 i + n.$$

so applying a change of variables $y = t^2$ we obtain $dy = 2t\,dt$ and so restricting the measure from Subsection 3.4:

$$\begin{aligned} \int_{g \in \mathcal{G}} t^{-2} dn\, d^\times t\, dk &= \frac{1}{2} \int_{N'(t)} \int_{t=\frac{\sqrt{3}}{\sqrt{2}}}^{\infty} t^{-3}\, dn\, dt \\ &= \frac{1}{4} \int_{N'(\sqrt{y})} \int_{y=\frac{\sqrt{3}}{2}}^{\infty} y^{-2}\, dn\, dy \\ &= \frac{1}{4} \int_{x+iy \in \mathcal{D}} y^{-2}\, dx\, dy \\ &= \frac{\pi}{12} = \frac{\zeta(2)}{2\pi}. \end{aligned}$$

D Order Estimate for Divisibility

In Subsection 3.2 we frequently use the fact that for an integer n, the divisors of n are determined up to $O(n^\varepsilon)$ for any $\varepsilon > 0$. We give a proof of this from Hardy and Wright [16], after establishing some elementary bounds. Let $d(n)$ be the 'number of divisors' function given by

$$d(n) = \sum_{d|n} 1$$

We are interested in estimating $d(n)$.

Lemma D.1. *For $x > 0$ we have that $e^x > x + 1$.*

Proof. Consider $g(x) = e^x - x$, for $x > 0$ we have that $g'(x) = e^x - 1 > 0$. Thus g is increasing, and since $g(0) = 1$ we have that $g(x) = e^x - x > 1$ as required. □

Lemma D.2. *For any $\varepsilon > 0$, $p, m \in \mathbb{Z}$ such that $p \geq 2$ and $m \geq 1$ then*

$$\frac{m+1}{p^{m\varepsilon}} < \begin{cases} 1 & \text{if } p \geq 2^{1/\varepsilon} \\ e^{1/(\log(2)\varepsilon)} & \text{otherwise.} \end{cases}$$

Proof. Note firstly that if $p \geq 2^{1/\varepsilon}$ then using Lemma D.1 we can write

$$\frac{m+1}{p^{m\varepsilon}} \leq \frac{m+1}{2^m} = \frac{m+1}{e^{\log(2)m}} < \frac{m+1}{\log(2)m+1} < 1$$

where the final inequality is because $\log(2) > 1$.

Otherwise, note that by Lemma D.1

$$p^{m\varepsilon} \geq 2^{m\varepsilon} = e^{\log(2)m\varepsilon} > \log(2)m\varepsilon + 1 > \log(2)m\varepsilon.$$

Applying this alongside Lemma D.1 we have

$$\begin{aligned} \frac{m+1}{p^{m\varepsilon}} &< \frac{m}{p^{m\varepsilon}} + 1 \\ &< \frac{m}{\log(2)m\varepsilon} + 1 \\ &= \frac{1}{\log(2)\varepsilon} + 1 \\ &< e^{1/(\log(2)\varepsilon)} \end{aligned}$$

as required. □

In particular this holds for p prime. Note that $d(n)$ is a multiplicative function and so this bound will give us behaviour at each prime.

Proposition D.3. *Let $d(n)$ be the number of divisors of a natural number n, then*

$$d(n) = O(n^\varepsilon)$$

for all $\varepsilon > 0$.

Proof. It is sufficient to prove that $d(n)/n^\varepsilon = O(1)$ for $\varepsilon > 0$. Writing n as a decomposition into primes $n = \prod_{i=1}^r p_i^{m_i}$, with each $m_i \geq 1$, note that

$$d(n) = \prod_{i=1}^r (m_i + 1).$$

and moreover,

$$\frac{d(n)}{n^\varepsilon} = \prod_{i=1}^r \frac{(m_i+1)}{p_i^{m_i\varepsilon}}$$

By Lemma D.2, and the fact that the number of primes less than $2^{1/\varepsilon}$ is certainly less than $2^{1/\varepsilon}$ we can then write

$$\begin{aligned}\frac{d(n)}{n^{\varepsilon}} &< \prod_{\substack{i=1 \\ p_i<2^{1/\varepsilon}}}^{r} e^{1/(\log(2)\varepsilon)} \\ &< e^{2^{1/\varepsilon}/(\log(2)\varepsilon)}\end{aligned}$$

So in particular, since the exponent has nominator dominating at 0 and denominator dominating at ∞ we can see that this term is $O(1)$ as required. □

References

[1] M. Bhargava. The density of discriminants of quartic rings and fields. *Annals of Mathematics*, pages 1031–1063, 2005.

[2] M. Bhargava. The density of discriminants of quintic rings and fields. *Annals of mathematics*, pages 1559–1591, 2010.

[3] M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport–Heilbronn theorems and second order terms. *Inventiones mathematicae*, 193(2):439–499, Aug 2013.

[4] D. A. Buell. *Binary Quadratic Forms: Classical theory and modern computations*. Springer–Verlag, 1989.

[5] D. Bump. *Lie Groups*. Springer–Verlag, 2013.

[6] H. Cohen. Constructing and counting number fields. *arXiv preprint math/0304231*, 2003.

[7] H. Cohen and M. Olivier. Counting discriminants of number fields. *J. Théor. Nombres Bordeaux*, 18(3):573–593, 2006.

[8] H. Davenport. On a principle of lipschitz. *Journal of the London Mathematical Society*, s1-26(3):179–183, 1951.

[9] H. Davenport. On the class-number of binary cubic forms I. *Journal of the London Mathematical Society*, s1-26(3):183–192, 1951.

[10] H. Davenport. On the class-number of binary cubic forms II. *Journal of the London Mathematical Society*, s1-26(3):192–198, 1951.

[11] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. *Bulletin of the London Mathematical Society*, 1(3):345–348, 1969.

[12] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 322(1551):405–420, 1971.

[13] B. Delone and D. Faddeev. *The theory of irrationalities of the third degree*, volume 10. AMS Providence, Rhode Island, 1964.

[14] W. T. Gan, B. Gross, and G. Savin. Fourier coefficients of modular forms on G_2. *Duke Math. J.*, 115:105–169, 2002.

[15] P. Garrett. Volume of $SL_n(\mathbb{Z})\backslash SL_n(\mathbb{R})$ and $Sp_n(\mathbb{Z})\backslash Sp_n(\mathbb{R})$. `http://www-users.math.umn.edu/~garrett/m/v/volumes.pdf`, 2014.

[16] G. H. Hardy and E. Wright. *An introduction to the theory of numbers*. Clarendon Press, Oxford, 3rd ed. edition, 1954.

[17] D. Harrer. Parametrization of cubic rings. *Ludwig-Maximilians-Universitat Munchen*, 2012.

[18] M. Wood. *Asymptotics For Number Fields and Class Groups*. Arizona Winter School Course Notes, 2014.