CHAPTER 2

The determinant and the discriminant

In this chapter we discuss two *indefinite* quadratic forms: the *determinant* quadratic form

$$\det(a,b,c,d) = ad - bc,$$

and the discriminant

$$\mathrm{disc}(a,b,c) = b^2 - 4ac.$$

We will be interested in the integral representations of a given integer n by either of these, that is the set of solutions of the equations

$$ad - bc = n,\ (a,b,c,d) \in \mathbb{Z}^4$$

and

$$b^2 - ac = n,\ (a,b,c) \in \mathbb{Z}^3.$$

For q either of these forms, we denote by $\mathrm{R}_q(n)$ the set of all such representations. Consider the three basic questions of the previous chapter:

(1) When is $\mathrm{R}_q(n)$ non-empty ?
(2) If non-empty, how large $\mathrm{R}_q(n)$ is ?
(3) How is the set $\mathrm{R}_q(n)$ distributed as n varies ?

In a suitable sense, a good portion of the answers to these question will be similar to the four and three square quadratic forms; but there will be major differences coming from the fact that

– det and disc are indefinite quadratic forms (have signature $(2,2)$ and $(2,1)$ over the reals),
– det and disc admit *isotropic* vectors: there exist $\mathbf{x} \in \mathbb{Q}^4$ (resp. $\mathbb{Q}^3$) such that $\det(\mathbf{x}) = 0$ (resp. $\mathrm{disc}(\mathbf{x}) = 0$).

1. Existence and number of representations by the determinant

As the name suggest, determining $\mathrm{R}_{\det}(n)$ is equivalent to determining the integral 2×2 matrices of determinant n:

$$\mathrm{R}_{\det}(n) \simeq M_2^{(n)}(\mathbb{Z}) = \{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}),\ \det(g) = n\}.$$

Observe that the diagonal matrix $a = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$ has determinant n, and any other matrix in the orbit $\mathrm{SL}_2(\mathbb{Z}).a$ is integral and has the same determinant. Thus

LEMMA. *For any $n \in \mathbb{Z}$, $\mathrm{R}_{\det}(n)$ is non empty and in fact infinite.*

We have exploited the faithful action of the infinite group $\mathrm{SL}_2(\mathbb{Z})$ on $M_2^{(n)}(\mathbb{Z})$ to establish its infiniteness; therefore to "count" the number of representations it is natural to consider the number of orbits under this action.

PROPOSITION 1.1. *For $n \neq 0$, the quotient $\mathrm{SL}_2(\mathbb{Z})\backslash M_2^{(n)}(\mathbb{Z})$ is finite and*

$$|\mathrm{SL}_2(\mathbb{Z})\backslash M_2^{(n)}(\mathbb{Z})| = \sum_{d|n} d = \prod_{p^\alpha \| n} \frac{p^{\alpha+1}-1}{p-1}. \tag{1.1}$$

Therefore

$$|\mathrm{SL}_2(\mathbb{Z})\backslash M_2^{(n)}(\mathbb{Z})| = n^{1+o(1)}. \tag{1.2}$$

PROOF. It is easy to verify that a set of representatives is given by

$$\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}),\ ad = n,\ 0 \leq b \leq d-1\}.$$

□

Written in this form the ressemblence between formulas (1.1) and (2.1) is pretty striking, the two number agreeing as long as $4 \nmid n$. This may be "explained" by the fact that the $\mathbb{Q}$-algebras B and M_2 are "forms" of each other, and precisely, for any prime $p \neq 2$, one has

$$\mathrm{B}(\mathbb{Z}_p) := \mathrm{B}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq M_2(\mathbb{Z}_p).$$

1.1. The algebra of matrices as a quaternion algebra. As we see, the algebra of 2×2 matrices play the same role as the Hamilton quaternions for sums of four squares. In fact $M_2(\mathbb{Q})$ is a *quaternion algebra* (in the sense of Chap. 10) and is the simplest possible one, the *split (unramified)* quaternion algebra. For instance, $M_2(\mathbb{Q})$ may be written into the form

$$M_2(\mathbb{Q}) = \mathbb{Q}\mathrm{Id} + \mathbb{Q}I + \mathbb{Q}J + \mathbb{Q}K$$

with

$$I = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

satisfying

$$I^2 = J^2 = \mathrm{Id},\ IJ = -JI = K.$$

The canonical anti-involution on $M_2(\mathbb{Q})$ is given by

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \overline{g} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = w^{-1}\,{}^t\begin{pmatrix} a & b \\ c & d \end{pmatrix} w$$

$$\text{with } w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

and corresponding reduced trace and reduced norm are just the usual trace and determinant (up to identifying $\mathbb{Q}$ with the algebra of scalar matrice $Z = \mathbb{Q}.\mathrm{Id}$):

$$m + \overline{m} = (a+d)\mathrm{Id} = \mathrm{tr}(m)\mathrm{Id},\ m\overline{m} = \det(m)\mathrm{Id};$$

and, again the "trace" and the "determinant" of $m \in M_2(\mathbb{Q})$ acting on $M_2(\mathbb{Q})$ by left multiplication is twice and the square of the usual trace and determinant.

The group of units $M_2^\times(\mathbb{Q})$ is the linear group $\mathrm{GL}_2(\mathbb{Q})$, and the subgroup of units of norm one $M_2^{(1)}(\mathbb{Q})$ is the special linear group $\mathrm{SL}_2(\mathbb{Q})$. Considering $(M_2(\mathbb{Q}), \det)$ as a quadratic space, one has an isomorphism of $\mathbb{Q}$-algebraic groups

$$\mathrm{GL}_2 \times \mathrm{GL}_2/\Delta Z^\times \simeq \mathrm{SO}_{M_2}$$

($\Delta Z^\times$ the subgroup of scalar matrices diagonally embedded in $\mathrm{GL}_2 \times \mathrm{GL}_2$) induced by

$$\rho : \begin{array}{ccc} \mathrm{GL}_2 \times \mathrm{GL}_2 & \mapsto & \mathrm{SO}_{M_2} \\ (g, g') & \mapsto & \rho_{g,g'} : m \mapsto gmg'^{-1} \end{array}$$

1.1.1. *Trace zero matrices.* As for Hamilton quaternions, the stabilizer of the subspace of scalar matrices in $\mathrm{GL}_2 \times \mathrm{GL}_2/\Delta Z^\times$ is

$$\Delta\mathrm{GL}_2/\Delta Z^\times = \mathrm{PGL}_2,$$

and the orthogonal subspace to the scalars is the space of trace-zero matrices

$$M_2^0(\mathbb{Q}) = \{m \in M_2(\mathbb{Q}),\ \mathrm{tr}(m) = 0\} :$$

in other terms the action of GL_2 on M_2^0 by conjugation induces the isomorphism

$$\rho : \begin{array}{ccc} \mathrm{PGL}_2 & \mapsto & \mathrm{SO}_{M_2^0} \\ g & \mapsto & m \mapsto gmg^{-1} \end{array} .$$

1.1.2. *The order of integral matrices.* The order corresponding to the integral Hamilton quaternions $\mathrm{B}(\mathbb{Z})$ is the ring of 2×2 integral matrices

$$M_2(\mathbb{Z}) = \mathscr{O}_{M_2} = \mathbb{Z}[I, J, K, \frac{\mathrm{Id} + I + J + K}{2}].$$

Its groups of units, and of units of norm one are, respectively,

$$\mathscr{O}_{M_2}^\times = \mathrm{GL}_2(\mathbb{Z}),\ \mathscr{O}_{M_2}^{(1)}(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}).$$

The analog of Theorem **??** and its corollary is

Proposition 1.2. *One has*

- *The order $\mathscr{O}_{M_2}$ is a maximal order and any maximal order of $M_2(\mathbb{Q})$ is conjugate to $M_2(\mathbb{Z})$.*
- *It is principal: any left (resp. right) $\mathscr{O}_{M_2}$-ideal $I \subset M_2(\mathbb{Q})$ is of the form $\mathscr{O}_{M_2}.g$ (resp. $g.\mathscr{O}_{M_2}$) for some $g \in \mathrm{GL}_2(\mathbb{Q})$ uniquely defined up to left (resp. right) multiplication by an element of $\mathrm{GL}_2(\mathbb{Z})$.*

Proof. We merely sketch the proof: the main point is the introduction of the lattices in $\mathbb{Q}^2$ (ie. the finitely generated $\mathbb{Z}$-modules of $\mathbb{Q}^2$ of maximal rank, for instance the square lattice $\mathbb{Z}^2$) and the fact that $\mathrm{GL}_2(\mathbb{Q})$ act transitively on the space of lattices. One show that any order $\mathscr{O} \subset M_2(\mathbb{Q})$ is contained in

$$\mathscr{O}_L := \mathrm{End}_{\mathbb{Z}}(L)$$

where $L \subset \mathbb{Q}^2$ is a lattice (check that $\mathscr{O}_L$ is an order). For instance, $\mathscr{O} \subset \mathscr{O}_L$ for L the lattice

$$L := \{x \in \mathbb{Z}^2,\ x\mathscr{O} \subset \mathbb{Z}^2\}.$$

Writing $L = \mathbb{Z}^2.g,\ g \in \mathrm{GL}_2(\mathbb{Q})$, one obtain that

$$g\mathscr{O}g^{-1} \subset \mathscr{O}_{M_2} = \mathscr{O}_{\mathbb{Z}^2}.$$

Similarly, if $I \subset M_2(\mathbb{Q})$ is a left $\mathscr{O}_{M_2}$-ideal,

$$L = \mathbb{Z}^2.I$$

is a lattice and $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Z}^2, L) = I$. Writing $L = \mathbb{Z}^2.g$ one has

$$I = \mathscr{O}_{M_2}.g.$$

We refer to [**Vig80**, Chap. 2, Thm. 2.3] for greater details (there the above statements are proven for non-archimedean local field, but the proof carry over since $\mathbb{Z}$ is principal.) □

2. The distribution of integral matrices of large determinant

Having counted the "number" of representation on an integer by the determinant (and found that there are "more and more" asthe integer grows) we adress the third question:

How are these many representations distributed as $n \to \infty$?

Firstly we may assume that n is non-negative since $M_2^{(n)}(\mathbb{Z}) = m.M_2^{(-n)}(\mathbb{Z})$ where m is any integral matrix of determinant -1. Next we may proceed as before, and, dividing by $n^{1/2}$, project $M_2^{(n)}(\mathbb{Z})$ on the set of matrices of determinant 1

$$n^{-1/2}M_2^{(n)}(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{R}).$$

Now $\mathrm{SL}_2(\mathbb{R})$ is a locally compact (unimodular) group and endowed with some Haar measure (well defined up to multiplication by a positive scalar) μ_{SL_2}. One has the following equidistribution theorem

THEOREM 2.1. *As $n \to +\infty$, $n^{-1/2}M_2^{(n)}(\mathbb{Z})$ becomes equidistributed into $\mathrm{SL}_2(\mathbb{R})$ w.r.t. μ_{SL_2} in the following sense: for $\varphi_1, \varphi_2 \in \mathscr{C}_c(\mathrm{SL}_2(\mathbb{R}))$ such that $\mu_{\mathrm{SL}_2}(\varphi_2) \neq 0$, then*

$$\frac{\sum_{g \in M_2^{(n)}(\mathbb{Z})} \varphi_1(|\det g|^{-1/2}g)}{\sum_{g \in M_2^{(n)}(\mathbb{Z})} \varphi_2(|\det g|^{-1/2}g)} \to \frac{\mu_{\mathrm{SL}_2}(\varphi_1)}{\mu_{\mathrm{SL}_2}(\varphi_2)},\ n \to \infty.$$

More precisely, there is a positive constant $\lambda > 0$ depending only on the choice of the measure μ_{SL_2} such that for any $\varphi \in \mathscr{C}_c(\mathrm{SL}_2(\mathbb{R}))$,

$$\sum_{g \in M_2^{(n)}(\mathbb{Z})} \varphi(|\det g|^{-1/2}g) = \tag{2.1}$$

$$\lambda \mu_{\mathrm{SL}_2(\mathbb{R})}(\varphi)|\mathrm{SL}_2(\mathbb{Z})\backslash M_2^{(n)}(\mathbb{Z})| + o(|\mathrm{SL}_2(\mathbb{Z})\backslash M_2^{(n)}(\mathbb{Z})|).$$

REMARK. This definition of equidistribution takes care of the fact that μ_{SL_2} is a not a finite measure.

2.0.3. *Sketch of the proof of Theorem 2.1.* Clearly the first part of the theorem follows from the second one.

Let $G = \mathrm{SL}_2(\mathbb{R})$ and $\Gamma = \mathrm{SL}_2(\mathbb{Z})$; this is a discrete subgroup therefore acting properly on G and the (right-invariant) quotient of the Haar measure μ_G by the counting measure on Γ, $\mu_{\Gamma\backslash G}$ is *finite*; in a way this is a measure analog of the fact that the quotient $\Gamma\backslash M_2^{(n)}(\mathbb{Z})$ is finite. Up to multiplying μ_G by a scalar, we will therefore assume that $\mu_{\Gamma\backslash G}$ is a probability measure.

For $g \in \mathrm{GL}_2(\mathbb{R})$ we set

$$\tilde{g} = |\det g|^{-1/2} g.$$

Let φ be a smooth compactly supported function on G, one has

$$\sum_{g_n \in M_2^{(n)}(\mathbb{Z})} \varphi(\tilde{g}_n) = \sum_{g_n \in \Gamma\backslash M_2^{(n)}(\mathbb{Z})} \varphi_\Gamma(\tilde{g}_n)$$

where $\varphi_\Gamma(g)$ is the function on $\Gamma\backslash G$ defined by

$$\varphi_\Gamma(g) = \sum_{\gamma \in \Gamma} \varphi(\gamma g), \tag{2.2}$$

(the notation $\tilde{g}_n$ for $g_n \in \Gamma\backslash M_2^{(n)}(\mathbb{Z})$ is (well) defined in the evident way). The function φ_Γ is compactly supported on $\gamma\backslash G$ and smooth: this is an example of an *automorphic function*.

Given ϕ a function on $\Gamma\backslash G$, let

$$T_n\phi : g \mapsto \frac{1}{|\Gamma\backslash M_2^{(n)}(\mathbb{Z})|} \sum_{g_n \in \Gamma\backslash M_2^{(n)}(\mathbb{Z})} \phi(\tilde{g}_n g);$$

$T_n\phi$ is a well defined function on $\Gamma\backslash G$ and the map

$$T_n : \phi \mapsto T_n\phi$$

is the n-th (normalized) *Hecke operator*. Let

$$L^2(\Gamma\backslash G) = \{\phi : \Gamma\backslash G \mapsto \mathbb{C},\ \langle\phi,\phi\rangle_{\Gamma\backslash G} = \int_{\Gamma\backslash G} |\phi(g)|^2 d\mu_{\Gamma\backslash G}(g) < \infty\}$$

denote the space of square integrable functions on $\Gamma\backslash G$ with respect to $\mu_{\Gamma\backslash G}$; this space contains the constant functions. The operator T_n is a self-adjoint operator on $L^2(\Gamma\backslash G)$ which may be diagonalized (in a suitable sense); the space of constant functions on $\Gamma\backslash G$ is an eigenspace of T_n with eigenvalue 1. Let $L_0^2(\Gamma\backslash G)$ be the subspace orthogonal to the constant functions. It follows from the work of Selberg that the L^2-norm of the restriction of T_n to that subspace is bounded by

$$\|T_n\|_{L_0^2(\Gamma\backslash G)} \ll \frac{n^{1-\delta+o(1)}}{|\Gamma\backslash M_2^{(n)}(\mathbb{Z})|} \tag{2.3}$$

for some absolute constant $\delta > 0$. Since $|\Gamma\backslash M_2^{(n)}(\mathbb{Z})| = n^{1+o(1)}$, we have for any $\phi \in L^2(\Gamma\backslash G)$

$$\begin{aligned}\|T_n\phi - \mu_{\Gamma\backslash G}(\phi)\|_{\Gamma\backslash G} &= \|T_n(\phi - \mu_{\Gamma\backslash G}(\phi))\|_{\Gamma\backslash G} \\ &\ll_\phi \|T_n\|_{L^2_0(\Gamma\backslash G)}\|\phi\|_{\Gamma\backslash G} \ll n^{-\delta+o(1)}\|\phi\|_{\Gamma\backslash G} = o_\phi(1).\end{aligned}$$

2.0.4. *Pointwise bounds and mixing.* We would like to pass from this L^2-estimate to a pointwise estimate: ie. for any compactly supported function $\phi \in \mathscr{C}_c(\Gamma\backslash G)$

$$T_n\phi(e) = \mu_{\Gamma\backslash G}(\phi) + o_\phi(1),\ n \to +\infty. \tag{2.4}$$

Applying this to $\phi = \varphi_\Gamma$, this conclude the proof of (2.1) since

$$\sum_{g_n \in M_2^{(n)(\mathbb{Z})}} \varphi(\tilde{g}_n) = T_n\varphi_\Gamma(e) \text{ and } \mu_{\Gamma\backslash G}(\varphi_\Gamma) = \mu_G(\varphi).$$

To prove (2.4), we use an approximation argument: note first that, by the Cauchy-Schwarz inequality, for any $\phi, \delta \in L^2(\Gamma\backslash G)$,

$$\begin{aligned}\langle T_n\phi, \delta\rangle_{\Gamma\backslash G} - \mu_{\Gamma\backslash G}(\phi)\mu_{\Gamma\backslash G}(\delta) &= \langle T_n(\phi - \mu_{\Gamma\backslash G}(\phi)), \delta\rangle_{\Gamma\backslash G} \\ &\ll \|T_n\|_{L^2_o(G)}\|\phi\|\|\delta\| = o_{\phi,\delta}(1);\end{aligned} \tag{2.5}$$

this express the *mixing* property of the operator T_n.

Now, if ϕ is continuous compactly supported, it is uniformly continuous and (since G acts continuously on $\Gamma\backslash G$ by right multiplication), for any $\varepsilon > 0$, there exists an open precompact neighborhood of the identity $e \in \Omega_\varepsilon \subset G$ such that for any $g \in G$ and $h \in \Omega_\varepsilon$,

$$|\phi(gh) - \phi(g)| \leq \varepsilon. \tag{2.6}$$

Shrinking, Ω_ε is necessary, we may also assume that for any $\gamma \in \Gamma$, $\gamma \neq e$

$$\gamma\Omega_\varepsilon \cap \Omega_\varepsilon = \emptyset$$

so that Ω_ε is identified with an open neighborhood of the class $\Gamma\backslash\Gamma.e \in \Gamma\backslash G$. Let δ_ε be a non-negative continuous function supported on Ω_ε such that

$$\int_G \delta_\varepsilon(h)dh = 1, \tag{2.7}$$

and let $\delta_{\varepsilon\Gamma}$ be defined as in (2.2). By the mixing property (2.5), we have

$$\begin{aligned}\langle T_n\phi, \delta_{\varepsilon\Gamma}\rangle_{\Gamma\backslash G} &= \mu_{\Gamma\backslash G}(\phi)\mu_{\Gamma\backslash G}(\delta_{\varepsilon\Gamma}) + o_{\phi,\delta_\varepsilon}(1) = \mu_{\Gamma\backslash G}(\phi)\mu_G(\delta_\varepsilon) + o_{\phi,\delta_\varepsilon}(1) \\ &= \mu_{\Gamma\backslash G}(\phi) + o_{\phi,\delta_\varepsilon}(1)\end{aligned}$$

On the other hand, by (6.1),

$$\begin{aligned}\langle T_n\phi, \delta_{\varepsilon\Gamma}\rangle_{\Gamma\backslash G} &= \int_{\Omega_\varepsilon} T_n\phi(h)\delta_\varepsilon(h)dh \\ &= \frac{1}{|\Gamma\backslash M_2^{(n)}(\mathbb{Z})|}\sum_{g_n\in\Gamma\backslash M_2^{(n)}(\mathbb{Z})}\int_{\Omega_\varepsilon}\phi(\tilde{g}_n h)\delta_\varepsilon(h)dh \\ &= \frac{1}{|\Gamma\backslash M_2^{(n)}(\mathbb{Z})|}\sum_{g_n\in\Gamma\backslash M_2^{(n)}(\mathbb{Z})}\phi(\tilde{g}_n) + O(\varepsilon) \\ &= T_n\phi(e) + O_\phi(\varepsilon),\end{aligned}$$

on using (2.6), the non-negativity of δ_ε and (2.7). This conclude the proof of (2.4). □

2.1. Equidistribution of rotations. As for the Hamilton quaternion, we may visualize this equidistribution property, through the action by conjugation of GL_2 on the space of trace zero matrices M_2^0; recall that this is an isometric action on the quadratic space $(M_2^0, \det)$ (§1.1). For $g \in \mathrm{GL}_2$ let

$$\rho_{g,g} \in \mathrm{SO}_{M_2^0} \simeq \mathrm{PGL}_2 : m \in M_2^0 \mapsto gmg^{-1}$$

denote the corresponding rotation. The previous theorem immediately imply that the set of rotations

$$\{\rho_{g_n,g_n},\ g_n \in M_2^{(n)}(\mathbb{Z})\}$$

become equidistributed on $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{PGL}_2^+(\mathbb{R})$ (the identity component of $\mathrm{PGL}_2(\mathbb{R})$). Let us consider now the subvariety of matrices of determinant 1 in M_2^0

$$M_2^{0,(1)}(\mathbb{R}) = \{m \in M_2^0(\mathbb{R}),\ \det(m) = 1\}.$$

By Witt's theorem $M_2^{0,(1)}(\mathbb{R})$ is acted on transitively by $\mathrm{SO}_{M_2^0}(\mathbb{R})$: $M_2^{0,(1)}(\mathbb{R})$ is the $\mathrm{GL}_2(\mathbb{R})$-conjugacy class of the matrix $K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ whose stabilizer is the compact group

$$\{a\mathrm{Id} + bK,\ (a,b) \in \mathbb{R}^2 - (0,0)\}/Z^\times(\mathbb{R}) = \mathrm{SO}_2(\mathbb{R})/\pm\mathrm{Id} = \mathrm{PSO}_2(\mathbb{R}).$$

Theorefore

$$M_2^{0,(1)}(\mathbb{R}) \simeq \mathrm{PGL}_2(\mathbb{R})/\mathrm{PSO}_2(\mathbb{R})$$

carries a $\mathrm{PGL}_2(\mathbb{R})$-invariant measure (the quotient on Haar measures of $\mathrm{PGL}_2(\mathbb{R})$ and $\mathrm{PSO}_2(\mathbb{R})$) unique up to scalar; we denote it by $\mu_{M_2^{0,(1)}}$. Also $M_2^{0,(1)}(\mathbb{R})$ has two connected components, namely the two $\mathrm{PGL}_2^+(\mathbb{R})$-orbits of $\pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$; these components are interchanged by conjugation of any matrix of determinant -1.

COROLLARY 2.1. *Given any $m \in M_2^{0,(1)}(\mathbb{R})$, the set*

$$\{\rho_{g,g}(m),\ g \in M_2^{(n)}(\mathbb{Z})\}$$

becomes equidistributed on the connected component of $M_2^{0,(1)}(\mathbb{R})$ containing m w.r.t. the measure $\mu_{M_2^{0,(1)}}$ as $n \to +\infty$. In other terms, for φ_1, φ_2 continuous functions, compactly supported on this connected component and such that $\mu_{M_2^{0,(1)}}(\varphi_2) \neq 0$, one has

$$\frac{\sum_{g \in M_2^{(n)}(\mathbb{Z})} \varphi_1(\rho_g(m))}{\sum_{g \in M_2^{(n)}(\mathbb{Z})} \varphi_2(\rho_g(m))} \to \frac{\mu_{M_2^{0,(1)}}(\varphi_1)}{\mu_{M_2^{0,(1)}}(\varphi_2)},\ n \to \infty.$$

More precisely there exist $\lambda > 0$ depending on the choice of the Haar measure $\mu_{M_2^{0,(1)}}$ such that for any $\varphi \in \mathcal{C}_c(M_2^{0,(1)}(\mathbb{R}))$

$$\sum_{g_n \in M_2^{(n)}(\mathbb{Z})} \varphi(\rho_{g_n,g_n}(m)) = \lambda(\mu_{M_2^{0,(1)}}(\varphi) + o(1))|\mathrm{SL}_2(\mathbb{Z})\backslash M_2^{(n)}(\mathbb{Z})|,\ n \to +\infty.$$

PROOF. Let H denote the stabilizer of m in $G = \mathrm{PSL}_2(\mathbb{R})$; this is a compact subgroup of G conjugate to $\mathrm{PSO}_2(\mathbb{R})$. The connected component of $M_2^{0,\pm 1}(\mathbb{R})$ containing m is homeomorphic to G/H via the map

$$gH \in G/H \mapsto g.m$$

and the (restriction of) the measure $\mu_{M_2^{0,(1)}}$ on this component is the quotient measure, $\mu_{G/H}$. Since any compactly supported function on G/H may be identified with a compactly supported function on G which is right H-invariant, the result now follows. □

2.1.1. *Equidistribution on two-sheeted hyperboloid.* We can now visualize the equidistribution of the $\{\rho_g(m),\ g \in M_2^{(n)}(\mathbb{Z})\}$ by identifying $M_2^{0,(1)}(\mathbb{R})$ with the affine variety

$$V_1(\mathbb{R}) = \{(a,b,c) \in \mathbb{R}^3, ac - b^2 = 1\},$$

via the map

$$(a,b,c) \mapsto \begin{pmatrix} b & a \\ -c & -b \end{pmatrix}.$$

3. The discriminant

We consider now the ternary quadratic form:

$$\mathrm{disc}(a,b,c) = b^2 - 4ac,$$

to be called the *discriminant* as it corresponds to the discriminant of the *binary* quadratic form

$$f_{a,b,c}(X,Y) = aX^2 + bXY + cY^2$$

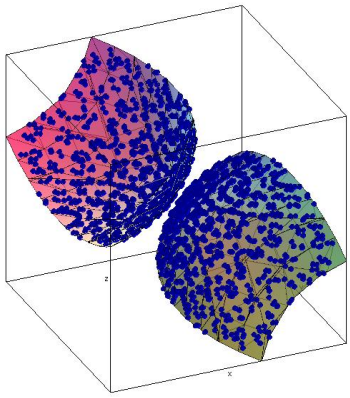

FIGURE 1. $n = 6632,\ (a, b, c) = (1, 0, 1)$

or in fancier terms, one has an isometry of the quadratic spaces

$$(\mathbb{Q}^3, \mathrm{disc}) \simeq (\mathrm{Sym}_2(\mathbb{Q}), \mathrm{disc}),$$

the space of 2×2 binary quadratic forms enquiped with the discriminant. Another interesting isometry is the following

$$\begin{array}{ccc} (\mathrm{Sym}_2(\mathbb{Q}), \mathrm{disc}) & \simeq & (M_2^0(\mathbb{Q}), -\det) \\ aX^2 + bXY + cY^2 & \mapsto & \begin{pmatrix} b & 2c \\ -2a & -b \end{pmatrix} . \end{array} \tag{3.1}$$

Thus $\mathrm{SO}_{\mathrm{disc}} \simeq \mathrm{SO}_{M_2^{0,(1)}} \simeq \mathrm{PGL}_2$ and the action of PGL_2 on the space of binary quadratic form intertwining with conjugation on M_2^0 is given explicitly for $g = \begin{pmatrix} u & v \\ w & z \end{pmatrix}$ by

$$g.f(X, Y) = \det(g)^{-1} f(uX + wY, vX + zY) = \det(g)^{-1} f((X, Y)g), \tag{3.2}$$

or if we represent the quadratic form $aX^2 + bXY + cY^2$ by the symmetric matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$, the intertwining actions are

$$g \begin{pmatrix} b & 2c \\ -2a & -b \end{pmatrix} g^{-1} \longleftrightarrow \frac{1}{\det(g)} g \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} {}^t g.$$

We are therefore essentially reduced to the study of the traceless integral matrices (with even entries on the anti-diagonal) of given discriminant.

4. Representations by the discriminant

For the discriminant quadratic form, the existence of representations is easy:

PROPOSITION 4.1. *An integer n is represented by* disc *(ie. n is a discriminant) if and only if $n \equiv 0, 1 (\mathrm{mod}\ 4)$. Moreover, the number of such representations is infinite.*

PROOF. Necessity is evident since $0, 1 \,(\mathrm{mod}\, 4)$ are exactly the squares in $\mathbb{Z}/4\mathbb{Z}$. Conversely, if $d \equiv 0, 1 \,(\mathrm{mod}\, 4)$, then $d = b^2 + 4a$ for $b = 0$ or 1 and $\mathrm{disc}(a, b, -1) = d$. Moreover for any integer k, $(a - k - k^2, b + 2k, -1)$ is another solution. □

From now on, we valid change notations and replace the letter "n" by "d" (for "discriminant"). We denote by $\mathrm{R}_{\mathrm{disc}}(d)$ the representation of d by the discriminant quadratic form and by $\mathrm{R}^*_{\mathrm{disc}}(d)$ the set of primitive representations (ie. such that $(a, b, c) = 1$). It follows from the explicit action of PGL_2 on the space of binary quadratic form (3.2), that the lattice of integral binary forms $\mathrm{Sym}^2(\mathbb{Z})$ is stable by $\mathrm{PGL}_2(\mathbb{Z})$, thus $\mathrm{PGL}_2(\mathbb{Z})$ act on $\mathrm{R}_{\mathrm{disc}}(d)$ and on $\mathrm{R}^*_{\mathrm{disc}}(d)$. While these sets are infinite, the set of $\mathrm{PGL}_2(\mathbb{Z})$-orbits is finite: this is the content of Gauss reduction theory:

THEOREM 4.1 (Gauss). *The set of primitive orbits $\mathrm{PGL}_2(\mathbb{Z})\backslash \mathrm{R}^*_{\mathrm{disc}}(d)$ is finite.*

PROOF. Specifically Gauss proved (using the fact that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$) that any such orbit has a representative (a, b, c) such that

$$\begin{cases} |d^{1/2} - 2|c|| < b < d^{1/2} & \text{if } d > 0 \\ 0 \leq |b| \leq |a| \leq |c| & \text{if } d < 0 \end{cases}.$$

□

By the discussion in §5 of the previous chapter ($\mathrm{PSL}_2(\mathbb{Z})$ has index 2 in $\mathrm{PGL}_2(\mathbb{Z})$), it follows from Dirichlet class number formula and Siegel's theorem that

THEOREM 4.2. *Given d a discriminant, one has*

$$|\mathrm{PGL}_2(\mathbb{Z})\backslash \mathrm{R}^*_{\mathrm{disc}}(d)| = |d|^{1/2+o(1)}$$
$$|\mathrm{PGL}_2(\mathbb{Z})\backslash \mathrm{R}_{\mathrm{disc}}(d)| = |d|^{1/2+o(1)}$$

4.1. Discriminant and quadratic fields. The representations of integers by the dicriminant are closely related to quadratic fields: we discuss this relation in details in the present section.

Let d be a discriminant which is not a perfect square; let $(a, b, c) \in \mathrm{R}^*_{\mathrm{disc}}(d)$ be a primitive representation, and let

$$m = m_{a,b,c} = \begin{pmatrix} b & 2c \\ -2a & -b \end{pmatrix} \tag{4.1}$$

by the trace zero matrix associated to it via the map (3.1), since

$$m^2 = d\mathrm{Id}$$

this defines an embedding of the quadratic field (d is not a square) $K = \mathbb{Q}(\sqrt{d})$ into $M_2(\mathbb{Q})$

$$\iota_m : \begin{array}{ccc} K & \mapsto & M_2(\mathbb{Q}) \\ u + v\sqrt{n} & \mapsto & u\mathrm{Id} + v.m \end{array}$$

Let

$$\mathscr{O}_m := M_2(\mathbb{Z}) \cap \iota_m(K)$$

be the order associated with m, one has

$$\iota_m^{-1}(\mathscr{O}_m) = \mathscr{O}_d = \mathbb{Z}[\frac{d+\sqrt{d}}{2}]$$

is the order of discriminant d. In other terms ι_m is an optimal embedding of $\mathscr{O}_d$ into $M_2(\mathbb{Z})$.

$$\iota_m(u + v\frac{d+\sqrt{d}}{2}) = \begin{pmatrix} u + v\frac{d+b}{2} & -av \\ cv & u + v\frac{d-b}{2} \end{pmatrix}$$

Since $d \equiv b(2)$, it is clear that $\iota_m(\mathscr{O}_d) \subset M_2(\mathbb{Z})$; conversely if $\iota_m(u + v\frac{d+\sqrt{d}}{2})$ belongs to $M_2(\mathbb{Z})$ one has

$$v \in \frac{1}{(a,c)}\mathbb{Z},\ u + v\frac{d-b}{2} \in \mathbb{Z},\ v \in \frac{1}{b}\mathbb{Z}$$

and by primitivity $v \in \mathbb{Z}$, from which follows that $u \in \mathbb{Z}$ (since $\frac{d-b}{2} \in \mathbb{Z}$).

Proposition 4.2. *The above defines a bijection between*

$$\text{Primitive representations up to sign: } \pm(a,b,c) \in \mathrm{R}^*_{\mathrm{disc}}(d)/\{\pm 1\}$$

and

$$\text{Optimal embeddings } \iota : \mathscr{O}_d \hookrightarrow M_2(\mathbb{Z}).$$

The group $\mathrm{PGL}_2(\mathbb{Z})$ acts on both sides (by conjugation on the set of optimal embeddings) and the above bijection induces a bijection between the corresponding orbits: $\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{R}^*_{\mathrm{disc}}(d)$ and the $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes of optimal embeddings.

Finally, we have the following

Proposition 4.3. *There is a bijection between*

$$\text{The } \mathrm{GL}_2(\mathbb{Z})\text{-conjugacy classes of optimal embeddings of } \mathscr{O}_d$$

and the ideal class group

$$\mathrm{Pic}(\mathscr{O}_d) = \{[I] = K^\times.I,\ I \subset K \text{ a proper } \mathscr{O}_d\text{-ideal}\}.$$

Proof. Given a proper $\mathscr{O}_d$-ideal $I \subset K$, one choose a $\mathbb{Z}$-basis $I = \mathbb{Z}.\alpha + \mathbb{Z}.\beta$ which give an identification

$$\theta : \begin{array}{ccc} I & \mapsto & \mathbb{Z}^2 \\ u\alpha + v\beta & \mapsto & (u,v) \end{array}$$

This identification induces the embedding

$$\iota : K \hookrightarrow M_2(\mathbb{Q})$$

defined by

$$\iota(\lambda)(u, v) = \theta(\lambda.(u\alpha + v\beta)),$$

(or in other terms, such that $\theta(\lambda.x) = \iota(\lambda)\theta(x)$).

Since $\mathscr{O}_d.I \subset I$, one has $\iota(\mathscr{O}_d)\mathbb{Z}^2 \subset \mathbb{Z}^2$, that is $\iota(\mathscr{O}_d) \subset M_2(\mathbb{Z})$ and the fact that I is a proper $\mathscr{O}_d$-ideal is equivalent to the fact that ι is an optimal embedding of $\mathscr{O}_d$.

If we replace the $\mathbb{Z}$-basis (α, β) by another basis, then

$$(\alpha', \beta') = (u\alpha + v\beta, w\alpha + z\beta)$$

with $\begin{pmatrix} u & v \\ w & z \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ and one see that ι is replaced by a $\mathrm{GL}_2(\mathbb{Z})$-conjugate. Finally if I is replaced by an ideal in the same class $I' = \lambda.I$ $\lambda \in K^\times$, then one check esily that the corresponding $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes coincide: $[\iota_{I'}] = [\iota_I]$.

The inverse of the map

$$[I] \mapsto [\iota_I]$$

is as follows: given $\iota : K \mapsto M_2(\mathbb{Q})$ an optimal embedding of $\mathscr{O}_d$, let $e_1 = (1, 0) \in \mathbb{Z}^2$ be the first vector of the canonical basis[1] of $\mathbb{Z}^2$, the map

$$\theta : \begin{array}{ccc} K & \mapsto & \mathbb{Q}^2 \\ \lambda & \mapsto & \iota(\lambda).e_1 \end{array}$$

is an isomorphism of $\mathbb{Q}$-vector spaces; let $I = \theta^{-1}(\mathbb{Z}^2)$, this is a lattice in K which is invariant under multiplication by $\mathscr{O}_d$: I is an $\mathscr{O}_d$-ideal and it being proper is equivalent to ι being optimal. □

5. Equidistribution of representations

To investigate the distribution of representations, we proceed as before and introduce the affine varieties of level ± 1

$$V_{\mathrm{disc},\pm 1}(\mathbb{R}) = \{(a, b, c) \in \mathbb{R}^3,\ b^2 - 4ac = \pm 1\}.$$

Given d a non zero discriminant, we may consider the projection of $\mathrm{R}_{\mathrm{disc}}(d)$ on the variety of level $\pm 1 = \mathrm{sign}(d)$:

$$|d|^{-1/2}\mathrm{R}_{\mathrm{disc}}(d) \subset V_{\mathrm{disc},\pm 1}(\mathbb{R}).$$

Observe that $V_{\mathrm{disc},-1}(\mathbb{R})$ is the variety noted $V_1(\mathbb{R})$ in §2.1.1.

$V_{\mathrm{disc},1}(\mathbb{R})$ is a one sheeted (ie. connected) hyperboloid and $V_{\mathrm{disc},-1}(\mathbb{R})$ a two sheeted hyperboloid (the two components being determined by the sign of a)

By Witt's theorem, both are acted on transitively by the orthogonal group $\mathrm{SO}_{\mathrm{disc}}(\mathbb{R}) \simeq \mathrm{PGL}_2(\mathbb{R})$ and therefore one has the identification

$$V_{\mathrm{disc},\pm 1}(\mathbb{R}) \simeq \mathrm{SO}_{\mathrm{disc}}(\mathbb{R})/\,\mathrm{SO}_{\mathrm{disc}}(\mathbb{R})_{\mathbf{x}_{\pm 1}}$$

[1] we could have choosen any primitive vector in $\mathbb{Z}^2$

for some choice of point $\mathbf{x}_{\pm 1} \in V_{\mathrm{disc},\pm 1}(\mathbb{R})$ with stabilizer $\mathrm{SO}_{\mathrm{disc}}(\mathbb{R})_{\mathbf{x}_{\pm 1}}$.

Because of this $V_{\mathrm{disc},\pm 1}(\mathbb{R})$ admit a natural $\mathrm{SO}_{\mathrm{disc}}(\mathbb{R})$-invariant measure (a quotient of Haar measures -cf. Chap. **??**-) well defined up to positive scalars, $\mu_{\mathrm{disc},\pm}$. This measure may also be described in elementary terms : for $\Omega \subset V_{\mathrm{disc},\pm 1}(\mathbb{R})$ an open subset, let

$$\mathcal{C}(\Omega) = \{r.\mathbf{x},\ \mathbf{x} \in \Omega,\ r \in [0,1]\}$$

be the solid angle supported by Ω, then

$$\mu_{\mathrm{disc},\pm}(\Omega) = \mu_{\mathbb{R}^3}(\mathcal{C}(\Omega))$$

were $\mu_{\mathbb{R}^3}$ is the Lebesgue measure.

One has then the following equidistribution statement:

THEOREM 5.1. *As $d \to \infty$, $|d|^{-1/2}\mathrm{R}_{\mathrm{disc}}(d)$ becomes equidistributed on $V_{\mathrm{disc},\pm 1}(\mathbb{R})$ ($\pm 1 = \mathrm{sign}(d)$) w.r.t. $\mu_{\mathrm{disc},\pm 1}$ in the following sense: for $\varphi_1, \varphi_2 \in \mathscr{C}_c(V_{\mathrm{disc},\pm 1}(\mathbb{R}))$ such that $\mu_{\mathrm{disc}\,.\pm 1}(\varphi_2) \neq 0$, then*

$$\frac{\sum_{x \in \mathrm{R}_{\mathrm{disc}}(d)} \varphi_1(|d|^{-1/2}x)}{\sum_{x \in \mathrm{R}_{\mathrm{disc}}(d)} \varphi_2(|d|^{-1/2}x))} \to \frac{\mu_{\mathrm{disc},\pm 1}(\varphi_1)}{\mu_{\mathrm{disc},\pm 1}(\varphi_2)},\ d \to \infty.$$

More precisely, there is a positive constant $\lambda > 0$ depending only on the choice of the measure $\mu_{\mathrm{disc},\pm 1}$ such that for any $\varphi \in \mathscr{C}_c(V_{\mathrm{disc},\pm 1}(\mathbb{R}))$,

$$\sum_{x \in \mathrm{R}_{\mathrm{disc}}(d)} \varphi(|d|^{-1/2}x) = \lambda(\mu_{\mathrm{disc},\pm 1}(\varphi) + o(1))|d|^{1/2+o(1)}. \tag{5.1}$$

6. Transition to locally homogeneous spaces

The starting point of the proof is the group theoretic interpretation of the problem.

Let Q denote the quadratic form disc. By Witt's theorem, the varieties $V_{Q,\pm 1}(\mathbb{R})$ are acted on transitively by the orthogonal group

$$\mathrm{SO}_Q(\mathbb{R}) \simeq \mathrm{PGL}_2(\mathbb{R}) =: G;$$

so the choice of some point $x_0 = (a_0, b_0, c_0) \in V_{Q,\pm 1}(\mathbb{R})$, induces an homeomorphism

$$V_{Q,\pm 1}(\mathbb{R}) = G.x_0 \simeq G/H \tag{6.1}$$

where $H := \mathrm{Stab}_{x_0}(G)$ denote the stabilizer of x_0. To be specific, we will take $x_0 = (0,1,0)$ in the $+1$ case and $x_0 = (1/2, 0, 1/2)$ in the -1 case; under the identification (3.1) correspond to the choice of the matrices

$$m_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ \text{and } m_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

so that H is is either

- the split torus $A = \mathrm{diag}_2(\mathbb{R})^\times/\mathbb{R}^\times.\mathrm{Id}$ (ie. the image of the diagonal matrices in $\mathrm{PGL}_2(\mathbb{R})$),
- the non-split torus $K := \mathrm{PSO}_2(\mathbb{R}) = \mathrm{SO}_2(\mathbb{R})/\{\pm\mathrm{Id}\}$.

The choice of Haar measures μ_G, μ_H on (the unimodular group) G and H then determine a left G-invariant quotient measure

$$\mu_{G/H}$$

on $G/H \simeq V_{Q,\pm 1}(\mathbb{R})$; that measure correspond to (a positive multiple of) $\mu_{Q,\pm 1}$.

6.1. A duality principle. It follows from the previous discussion that each representation $(a,b,c) \in \mathrm{R}_Q(d)$, or its projection $|d|^{-1/2}(a,b,c) \in V_{Q,\pm 1}(\mathbb{R})$ is identified with some class $g_{a,b,c}H/H \in G/H$ or what is the same to an orbit $g_{a,b,c}H \subset G$ for some $g_{a,b,c} \in G$ such that

$$g_{a,b,c}x_0 = |d|^{-1/2}(a,b,c).$$

Let $\Gamma = \mathrm{PGL}_2(\mathbb{Z})$; as we have seen $\mathrm{R}_Q(d)$ decomposes into a finite disjoint union of Γ-orbits; we denote by

$$[\mathrm{R}_Q(n)] = \Gamma\backslash \mathrm{R}_Q(d)$$

the set of such orbits and by

$$[a,b,c] = \Gamma\backslash\Gamma(a,b,c) \in [\mathrm{R}_Q(d)];$$

one has

$$\mathrm{R}_Q(d) = \bigsqcup_{[a,b,c]\in[\mathrm{R}_Q(d)]} \Gamma.(a,b,c)$$

and (6.1) identifies $|d|^{-1/2}.\mathrm{R}_Q(d)$ with

$$\bigsqcup_{[a,b,c]\in[\mathrm{R}_Q(d)]} \Gamma g_{a,b,c}H/H \subset G/H;$$

thus the problem of the distribution of $|d|^{-1/2}.\mathrm{R}_Q(d)$ inside $V_{Q,\pm 1}(\mathbb{R})$ is a problem about the distribution of a collection of Γ-orbits inside the quotient space G/H.

We note the tautological equivalence

$$\Gamma gH/H \longleftrightarrow \Gamma gH \longleftrightarrow \Gamma\backslash\Gamma gH, \tag{6.2}$$

between (left) Γ-orbits on G/H and (right) H-orbits on $\Gamma\backslash G$. From this equivalence and the previous identification, one could expect that studying the distribution of $|d|^{-1/2}.\mathrm{R}_Q(d)$ inside $V_{Q,\pm 1}(\mathbb{R})$ is tantamount to studying the distribution of some collection of right-H orbits, indexed by $[\mathrm{R}_Q(d)]$ inside the homogeneous space $\Gamma\backslash G$ namely

$$\mathcal{Y}_d = \bigcup_{[a,b,c]\in[\mathrm{R}_Q(d)]} x_{[a,b,c]}H \subset \Gamma\backslash G$$

with $x_{[a,b,c]} = \Gamma\backslash\Gamma g_{a,b,c}$.

6.2. The shape of orbits. Let us describe more precisely the structure of the orbit $x_{[a,b,c]}H$. For this we may assume that $(a,b,c) \in \mathrm{R}^*_{\mathrm{disc}}(d)$ is a primitive representation (otherwise it is sufficient to replace (a,b,c) and d by, respectively (a',b',c') and $d'=d/f^2$ where $(a',b',c')=f^{-1}(a,b,c)$ is the primitive representation underlying (a,b,c)). We have

$$x_{[a,b,c]}H = \Gamma\backslash\Gamma g_{a,b,c}H = \Gamma\backslash\Gamma H_{a,b,c}g_{a,b,c}$$

where

$$H_{a,b,c} = g_{a,b,c}Hg_{a,b,c}^{-1} = \mathrm{Stab}_{(a,b,c)}(G) = G_{(a,b,c)}$$

is the stabilizer of (a,b,c) in G. We have homeomorphisms

$$x_{[a,b,c]}H \simeq \Gamma\backslash\Gamma H_{a,b,c} \simeq \Gamma_{a,b,c}\backslash H_{a,b,c}$$

where

$$\Gamma_{a,b,c} := \Gamma \cap H_{a,b,c}.$$

In the present case $H_{a,b,c} = \mathbf{T}_{a,b,c}(\mathbb{R})$, the group of real points of the stabilizer $\mathbf{T}_{a,b,c}$ (say), of (a,b,c) in PGL_2 (a $\mathbb{Q}$-algebraic group); equivalently $\mathbf{T}_{a,b,c}$ is the image in PGL_2 of the centralizer Z_m of the matrix $m = m_{a,b,c}$. Let $\iota = \iota_{m_{a,b,c}} : K \hookrightarrow M_2(\mathbb{Q})$ be the embedding indiced by m, then

$$Z_m(\mathbb{Q}) = \iota(K^\times),\ \mathbf{T}(\mathbb{Q}) = \iota(K^\times)/\mathbb{Q}^\times\mathrm{Id},\ H_{a,b,c} = \iota((K\otimes\mathbb{R})^\times)/\mathbb{R}^\times\mathrm{Id},$$

and since $M_2(\mathbb{Z}) \cap \iota(K) = \mathscr{O}_m$, one has

$$\Gamma \cap H_{a,b,c} = \iota(\mathscr{O}_d^\times)/\{\pm\mathrm{Id}\}$$

and

$$\Gamma \cap H_{a,b,c}\backslash H_{a,b,c} = \iota((K\otimes\mathbb{R})^\times)/\mathbb{R}^\times\iota(\mathscr{O}_d^\times).$$

In particular, by Dirichlet's units theorem, the latter space is compact and since $[\mathrm{R}_{\mathrm{disc}}(d)]$ is finite, we obtain:

THEOREM 6.1. *For d not a square, the set $\mathcal{Y}_d$ is compact.*

REMARK. The above theorem is a consequence of two classical results of algebraic number theory: the finitness of the *class group* and Dirichlet's units theorem. In fact, it is possible to prove directly that $\mathcal{Y}_d$ is compact, which will then proves these two theorems altogether. We will describe the arguments below. Such results are in fact consequence of a much more general result on algebraic groups: the *Borel-Harish-Chandra* finiteness theorem.

6.3. A measure theoretic version of the duality principle. To consider equidistribution problems, one need to refine the identification (6.1) and the correspondance (6.2) at the level of measures. As a general fact, the choice of the counting measure on Γ, μ_Γ, and of some left-invariant Haar measure μ_H on H define a measure theoretic version of the (6.2):

FACT. *There exists bijections between the following spaces of Radon measures:*

(6.3)

left Γ*-invariant*		*left* Γ*, right* H*-invariant*		*right* H*-invariant*
Radon measures	$\longleftrightarrow$	*Radon measures*	$\longleftrightarrow$	*Radon measures*
λ *on* G/H		ρ *on* G		ν *on* $\Gamma\backslash G$.

These bijections are homeomorphisms for the weak- topology and are is characterized by the equalities: for any* $\varphi \in \mathscr{C}_c(G)$*, one has*

$$\lambda(\varphi_H) = \rho(\varphi) = \nu(\varphi_\Gamma)$$

where

$$\varphi_H(g) := \int_H f(gh) d\mu_H(h),\ \varphi_\Gamma(g) = \sum_{\gamma\in\Gamma} f(\gamma.g).$$

REMARK. Let us recall that since $\Gamma, H < G$ are closed, the maps

$$\varphi \in \mathcal{C}_c(G) \to \varphi_H \in \mathcal{C}_c(G/H),$$
$$\varphi \in \mathcal{C}_c(G) \to \varphi_\Gamma \in \mathcal{C}_c(\Gamma\backslash G)$$

are onto.

6.4. The volume of orbits and the class number formula. Let us work out this correspondance in specific cases:

– We choose for ρ, some Haar measure μ_G on G (which is unimodular hence left-Γ, right-H-invariant). We obtain via the correspondence (6.3) the quotient measures $\nu = \mu_{\Gamma\backslash G}$ on $\Gamma\backslash G$, and $\lambda = \mu_{G/H} \propto \mu_{Q,\pm 1}$ on G/H. The former measure ν is finite (Γ is a lattice in G) and we may adjust μ_G so that $\mu_{\Gamma\backslash G}$ is a probability measure.

– Let us consider now the (atomic) sum of Dirac measures on G/H

$$\begin{aligned}\lambda_d &= \sum_{(a,b,c)\in \mathrm{R}_Q(d)} \delta_{g_{a,b,c}H/H} = \sum_{[a,b,c]} \sum_{g\in\Gamma.g_{a,b,c}} \delta_{gH/H} \\ &= \sum_{[a,b,c]} \sum_{\gamma\in\Gamma/\Gamma_{a,b,c}} \delta_{\gamma g_{a,b,c}H/H} = \sum_{[a,b,c]} \lambda_{[a,b,c]}\end{aligned}$$

say. We have

$$\begin{aligned}\lambda_{[a,b,c]}(\varphi_H) &= \sum_{\gamma\in\Gamma/\Gamma_{a,b,c}} \int_H \varphi(\gamma g_{a,b,c}h)dh = \sum_{\gamma\in\Gamma/\Gamma_{a,b,c}} \int_{H_{a,b,c}} \varphi(\gamma h g_{a,b,c})dh \\ &= \sum_{\gamma\in\Gamma/\Gamma_{a,b,c}} \int_{H_{a,b,c}} \varphi(\gamma h g_{a,b,c})dh = \int_{\Gamma_{a,b,c}\backslash H_{a,b,c}} \varphi_\Gamma(h g_{a,b,c})dh \\ &= \int_{\Gamma'_{a,b,c}\backslash H} \varphi_\Gamma(g_{a,b,c}h)dh = \int_{x_{[a,b,c]}H} \varphi_\Gamma(h)dh.\end{aligned}$$

Here we have used the homeomorphism

$$x_{[a,b,c]}H \simeq \Gamma'_{a,b,c}\backslash H \text{ with } \Gamma'_{a,b,c} = g_{a,b,c}^{-1}\Gamma g_{a,b,c} \cap H$$

and, to ease notation, we have denoted successively by dh , the Haar measure μ_H, the Haar measure on $H_{a,b,c} = g_{a,b,c} H g_{a,b,c}^{-1}$ deduced from μ_H by conjugation, the quotient (by the counting measure) measure on $\Gamma_{a,b,c}\backslash H_{a,b,c}$, and the quotient measure on $\Gamma'_{a,b,c}\backslash H$ and eventually on the orbit $x_{[a,b,c]}H$.

Notice that

$$\Gamma'_{a,b,c} = g_{a,b,c}^{-1}\Gamma g_{a,b,c} \cap H = \iota_0(\mathscr{O}_d^\times)/\{\pm \mathrm{Id}\}$$

where ι_0 denote the real embedding

$$\iota_0 : \begin{array}{ccc} K & \mapsto & M_2(\mathbb{R}) \\ u + v\sqrt{d} & \mapsto & u\mathrm{Id} + v.|d|^{1/2} m_0 \end{array}$$

and it follows that the volumes of the orbits $x_{[a,b,c]}H$ (for (a,b,c) primitive) are all equal and are equal to

$$\mathrm{vol}(\mathbb{R}^\times.\iota_0(\mathscr{O}_d^\times)\backslash H).$$

This volume is related to classical arithmetical invariants of the order $\mathscr{O}_d$: there is a constant $\lambda > 0$ (depending only on the choice of the measure on H) so that, if $d < 0$ ($H = \mathrm{PSO}_2(\mathbb{R})$ is compact, $\mathscr{O}_d^\times$ is finite)

$$\mathrm{vol}(x_{[a,b,c]}H) = \lambda / w_d,\ w_d = |\mathscr{O}_d^\times/\{\pm 1\}|.$$

If $d > 0$, then

$$\mathrm{vol}(x_{[a,b,c]}H) = \mathrm{vol}(\mathbb{R}^\times.\iota_0(\mathscr{O}_d^\times)\backslash H) = \lambda \mathrm{reg}(\mathscr{O}_d)$$

where $\mathrm{reg}(\mathscr{O}_d)$ is the regulator of $\mathscr{O}_d$

Let $\mathcal{Y}_d^*$ be the union of orbits associated to primitive representations

$$\mathcal{Y}_d^* = \bigsqcup_{[a,b,c] \in [\mathrm{R}^*_{\mathrm{disc}}(d)]} x_{[a,b,c]}H$$

we have from the previous discussion

$$\mathrm{vol}(\mathcal{Y}_d^*) = \lambda |\mathrm{Pic}(\mathscr{O}_d)|/w_d, \quad \text{or } \lambda |\mathrm{Pic}(\mathscr{O}_d)|\mathrm{reg}(\mathscr{O}_d)$$

depending on the sign of d. If $d = \mathrm{disc}(\mathscr{O}_K)$ is a fundamental discriminant, a formula for the lefthand side is the content of the *Dirichlet class number formula*: up to changing the value of the constant λ, one has

$$\mathrm{vol}(\mathcal{Y}_d^*) = \lambda |d|^{1/2} L(\chi_d, 1),$$

where $\lambda > 0$ depends on the sign of d $\chi_d(.) = (\frac{d}{.})$ is the Kronecker symbol and $L((\frac{d}{.}), s)$ its associated L-function. Then by Siegel's theorem $L(\chi_d, 1) = |d|^{o(1)}$ as $d \to \infty$ so that

$$\mathrm{vol}(\mathcal{Y}_d^*) = |d|^{1/2 + o(1)}. \tag{6.4}$$

If d is not a fundamental discriminant, a comparison between the size of the class numbers and regulators of $\mathscr{O}_K$) and $\mathscr{O}_d$ shows that (6.4) holds in general and since

$$\mathcal{Y}_d = \bigsqcup_{f^2 | d} \mathcal{Y}^*_{d/f^2}$$

, one has

$$\mathrm{vol}(\mathcal{Y}_d) = \lambda |d|^{1/2+o(1)}.$$

THEOREM (Dirichlet). *for $d > 0$, one has*

$$|\operatorname{Pic}(\mathscr{O})||\operatorname{Reg}(\mathscr{O}_K)| = \frac{|\operatorname{Pic}(\mathscr{O}_d)|}{|\operatorname{Pic}(\mathscr{O}_K)|}\frac{w_K}{2}|d_K|^{1/2}L(\chi_K, 1).$$

We let

$$\mu_d := \frac{1}{\mathrm{vol}(\mathcal{Y}_d)}\nu_d.$$

This is an H-invariant probability measure on $\Gamma\backslash G$. As we now show Theorem 5.1 follows from

THEOREM 6.2. *As $d \to \infty$ (amongst the non-square discriminants) the sequence of measures μ_d weak-* converge to the probability measure $\mu_{\Gamma\backslash G}$: for any $\varphi_\Gamma \in \mathscr{C}_c(\Gamma\backslash G)$, one has*

$$\mu_d(\varphi_\Gamma) = \frac{1}{\mathrm{vol}(\mathcal{Y}_d)}\sum_{[a,b,c]}\int_{x_{[a,b,c]}H}\varphi_\Gamma(h)dh \to \mu_{\Gamma\backslash G}(\varphi_\Gamma).$$

Moreover, one has

$$\mathrm{vol}(\mathcal{Y}_d) = |d|^{1/2+o(1)}.$$

Indeed any continuous compactly supported function on G/H is of the form φ_H for $\varphi \in \mathscr{C}_c(G)$, we have

$$\begin{aligned}\lambda_d(\varphi_H) = \nu_d(\varphi_\Gamma) &= \mathrm{vol}(\mathcal{Y}_d)\mu_d(\varphi_\Gamma)\\ &= \mathrm{vol}(\mathcal{Y}_d)(\mu_{\Gamma\backslash G}(\varphi_\Gamma) + o(1)) = \mathrm{vol}(\mathcal{Y}_d)(\mu_{G/H}(\varphi_H) + o(1)).\end{aligned}$$

7. Equidistribution on the modular curve

7.1. The upper-half plane model. The linear group $\mathrm{GL}_2(\mathbb{R})$ acts on the *Riemann sphere* $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\} = \mathrm{P}_1(\mathbb{C})$ by fractional linear transformations

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} :\ z \mapsto g.z = \frac{az+b}{cz+d}.$$

This action factor through $\mathrm{G} = \mathrm{PGL}_2(\mathbb{R})$ and have two orbits, the real projective line $\mathrm{P}_1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$ and the union of the "upper" and "lower" half planes

$$\mathbb{C} - \mathbb{R} = \mathbb{H}^+ \cup \mathbb{H}^-,\ \mathbb{H}^\pm = \{z \in \mathbb{C},\ \pm\Im(z) > 0\}.$$

$\mathbb{H}^\pm$ are the two orbits of $\mathrm{PSL}_2(\mathbb{R})$ in $\mathbb{C} - \mathbb{R}$; we also note the upper-half plane by $\mathbb{H}$.

The stabilizer of $i \in \mathbb{H}$ in $\mathrm{PGL}_2(\mathbb{R})$ is $K = \mathrm{PSO}_2(\mathbb{R})$ and therefore we have and homemorphism of G-spaces

$$\mathbb{H}^+ \cup \mathbb{H}^- \simeq G/K \simeq V_{\mathrm{disc},-1}(\mathbb{R}) \simeq M_2^{0,(1)}(\mathbb{R})$$

given for $g \in G$ by

$$g.i \leftrightarrow g.x_0 = g.(1/2, 0, 1/2) \leftrightarrow g.m_0 = g.\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Explicitely we have

LEMMA 7.1. *Given $d \in \mathbb{R}_{<0}$, and $(a, b, c) \in \mathbb{R}^3$ such that $b^2 - 4ac = d$, the complex number $z_{a,b,c} \in \mathbb{C} - \{\mathbb{R}\}$ corresponding to $|d|^{-1/2}(a, b, c) \in V_{\mathrm{disc},-1}(\mathbb{R})$ under the previous identification is*

$$z_{a,b,c} = \frac{-b \pm i|d|^{1/2}}{2a}, \ \pm = \mathrm{sign}(a).$$

PROOF. Indeed $|d|^{-1/2}(a, b, c)$ correspond to the matrix

$$|d|^{-1/2} m_{a,b,c} = |d|^{-1/2} \begin{pmatrix} b & 2c \\ -2a & -b \end{pmatrix}$$

which is (obviously) invariant under conjugation by $m_{a,b,c}$; thus $z_{a,b,c}$ is fixed under the action of $m_{a,b,c}$ (ie. satisfies $m_{a,b,c}.z = \frac{bz-2a}{2cz-b} = z$). We conclude since the connected component of $V_{\mathrm{disc},-1}$ given by the (a, b, c) for a is of some given sign correspond to the z whose imaginary part has the same sign. □

7.1.1. *The hyperbolic metric and the hyperbolic measure.* he identification $\mathbb{H}^+ \cup \mathbb{H}^- \simeq G/K$ can be made explicit in terms of *Iwasawa* coordinates: any $g \in \mathrm{PGL}_2(\mathbb{R})$ is the image (in a unique way) of a matrix of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} k, \ x \in \mathbb{R}, \ y \in \mathbb{R}^\times, \ k \in \mathrm{SO}_2(\mathbb{R})$$

and then

$$g.i = \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} = z = x + iy.$$

The Killing form $B : (X, Y) \mapsto \mathrm{tr}_{\mathfrak{pgl}_2}(\mathrm{Ad}(X)\,\mathrm{Ad}(Y))$ on the Lie algebra $\mathfrak{pgl}_2$ induces a positive definite quadratic form on $\mathfrak{pgl}_2/\mathfrak{pso}_2$ hence a left G-invariant Riemannian metric on the symmetric space G/K (and so on $\mathbb{H}^+ \cup \mathbb{H}^-$). A computation in the Iwasawa coordinates show that this metric correspond to a multiplie of the *hyperbolic metric*

$$ds^2 = \frac{dx^2 + dy^2}{y^2}.$$

If a smilar way, the quotient Haar measure $\mu_{G/H}$ correspond to a multiple of the *hyperbolic measure*

$$d\mu_{\mathrm{Hyp}} = \frac{dxdy}{y^2}.$$

7.2. Equidistribution of Heegner points. From the above discussion, it follows from Theorem 6.1, that

THEOREM. *As $d \to -\infty$ amongst the negative discriminant, the sequence of sets*

$$\{z_{a,b,c} = \frac{-b + i|d|^{1/2}}{2a},\ (a,b,c) \in \mathrm{R}_{\mathrm{disc}}(d),\ a > 0\}$$

become equidistributed on $\mathbb{H}$ with respect to the hyperbolic measure μ_{Hyp}.

Equivalently, we may take the quotient by the discrete subgroup $\Gamma = \mathrm{PGL}_2(\mathbb{Z})$. Note that since K is *compact*, the discrete subgroup $\Gamma = \mathrm{PGL}_2(\mathbb{Z})$ acts properly on the quotient $G/K \simeq \mathbb{H}^+ \cup \mathbb{H}^-$ and the above identification induce an topological homeomorphism of the double quotient $\Gamma\backslash G/K$ with the *modular curve*

$$\Gamma\backslash G/K \simeq \Gamma\backslash\mathbb{H}^+ \cup \mathbb{H}^- \simeq \mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H} = Y_0(1).$$

The space of continuous compactly supported functions on $Y_0(1) \simeq \Gamma\backslash G/K$ is identified with the space of right K-invariant functions on $\Gamma\backslash G$; therefore the above theorem (equivalently Theorem 6.2) implies

THEOREM. *Let $z_{[a,b,c]} \in Y_0(1)$ denote the Γ-orbit of $z_{a,b,c}$: As $d \to -\infty$ amongst the negative discriminant, the sequence of sets*

$$\mathcal{H}_d := \{z_{[a,b,c]},\ (a,b,c) \in \mathrm{R}_{\mathrm{disc}}(d),\ a > 0\}$$

become equidistributed on $Y_0(1)$ with respect to the (quotient of the) hyperbolic probability measure $\frac{3}{\pi}\frac{dxdy}{y^2}$.

Let us recall that the map

$$z \in \mathbb{H} \mapsto E_z(\mathbb{C}) = \mathbb{C}/(\mathbb{Z} + z\mathbb{Z}),$$

$Y_0(1)$ parametrizes the set of elliptic curves defined over $\mathbb{C}$ up to isomorphism. Under this parametrization, the set

$$\mathcal{H}_d^* = \{z_{[a,b,c]} \in Y_0(1),\ (a,b,c) \in \mathrm{R}_{\mathrm{disc}}(d) \text{ primitive}\}$$

correspond bijectively with the subset of isomorphism classes of elliptic curves with *complex multiplication* (CM-elliptic curves) by the order $\mathscr{O}_d$ (see [?Silv2, Chap. I and II]): $\mathcal{H}_d^*$ is the set of so-called *Heegner points* of discriminant d. Thus the above theorem maybe interpreted by saying that set of (isomorphism classes of)CM elliptic curves with large discriminant becomes equidistributed in the space of (isomorphism classes of) complex elliptic curves.

Recall that the fundamental domain for $Y_0(1)$ is $\{z \in \mathbb{C},\ |\Re ez| < 1/2,\ |z| > 1\}$. The figure below represent the distribution of the Heegner points of discriminant $d = -104831$

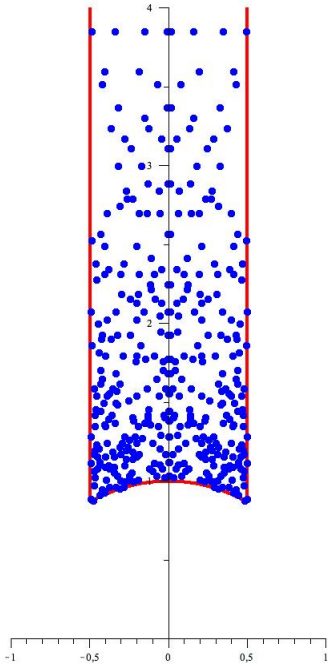

FIGURE 2. The distribution of $\mathcal{H}_d$, $d = -104831$, $h(d) =$.

7.3. Equidistribution of closed geodesics. For positive discriminants d, Theorem 6.2 may also be interpreted in terms of the modular curve $Y_0(1)$.

We refer to [?EVVol1, Chap 9.] for a more complete discussion of the following facts. As we discussed above, $\mathbb{H}^{\pm} = \mathbb{H}^{+} \cup \mathbb{H}^{-}$ a Riemannian manifold (equipped with the hyperbolic metric) is isometric to G/K (equipped with the metric coming from a suitable multiple of the Killing form); under this identification, its *unit tangent bundle*

$$\mathbf{T}^1(\mathbb{H}^{\pm}) = \{(z, v_z),\ z \in \mathbb{H}^{\pm},\ v \in \mathbf{T}_z(\mathbb{H}^{\pm}),\ \|v_z\|_z = 1\}$$

is naturally identified with G and the *geodesic flow*

$$(g_t)_{t\in\mathbb{R}} : \mathbf{T}^1(\mathbb{H}^{\pm}) \mapsto \mathbf{T}^1(\mathbb{H}^{\pm})$$

correspond to the action by right multiplication of the (image in $\mathrm{PGL}_2(\mathbb{R})$) of the diagonal matrices

$$(g_t)_{t\in\mathbb{R}} : g_t = \begin{pmatrix} e^{\alpha t} & 0 \\ 0 & e^{-\alpha t} \end{pmatrix}.$$

for some suitable $\alpha > 0$. Let

$$A^+ \subset A = \mathrm{diag}_2(\mathbb{R})/\mathbb{R}^{\times}\mathrm{Id} = H$$

(recall that $d > 0$) denote the image of that group; since $A = A^+ \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} A^+$, we see that for $(a,b,c) \in \mathrm{R}_{\mathrm{disc}}(d)$ the orbit

$$g_{a,b,c}H = g_{a,b,c}A^+ \cup g_{a,b,c} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} A^+$$

is identified with the union of two geodesic curves symmetric about the real axis:

$$\gamma_{a,b,c} \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \gamma_{a,b,c},$$

$$\gamma_{a,b,c} \subset \mathbf{T}^1(\mathbb{H}).$$

Recall that the geodesics curves projected on $\mathbb{H}$ are either vertical half-lines or half-circles centered on the real axis

LEMMA. *The geodesic $\gamma_{a,b,c}$ project (up to orientation) in $\mathbb{H}$ to the half-circle whose endpoints on $\mathbb{R}$ are*

$$x^{\pm}_{a,b,c} = \frac{-b \pm d^{1/2}}{2a}.$$

PROOF. □

Upon quotenting by Γ, the two geodesics are identified (since $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$) and we denote the resulting image $\gamma_{[a,b,c]} = \Gamma\backslash\Gamma.\gamma_{a,b,c} \simeq x_{[a,b,c]}H$; as $x_{[a,b,c]}H$ is compact, the geodesic closed; the (finite) union of these is noted

$$\Gamma_d = \bigsqcup_{[a,b,c]} \gamma_{[a,b,c]} \subset \mathbf{T}^1(Y_0(1));$$

Its volume of Γ_d is its total length of these geodesic and Theorem 6.1 may be rewritten in this case

THEOREM. *As $d \to +\infty$ amongst the non-square positive discriminants, the sequence of paquet of geodesics Γ_d become equidistributed on $\mathbf{T}^1(Y_0(1))$ with respect to the Liouville probability measure: for any $\varphi \in \mathscr{C}_c(\mathbf{T}^1(Y_0(1)))$,*

$$\frac{1}{\mathrm{length}(\Gamma_d)} \sum_{[a,b,c]} \int_{\gamma_{[a,b,c]}} \varphi(t)dt \to \int_{\mathbf{T}^1(Y_0(1))} \varphi(u)d\mu_{Liouv}(u).$$

Below we represent the projection of Γ_{377} to $Y_0(1)$; it has one one orbit (the class number of $\mathscr{O}_{377}$ equals 1) and length 22.47...

8. Principle of the proofs

During the late 50's and 60's, using Linnik's "ergodic method", Linnik and Skubenko resolved problem **??** for the appropriate integers d, subject to an extra congruence condition modulo a fixed prime p:

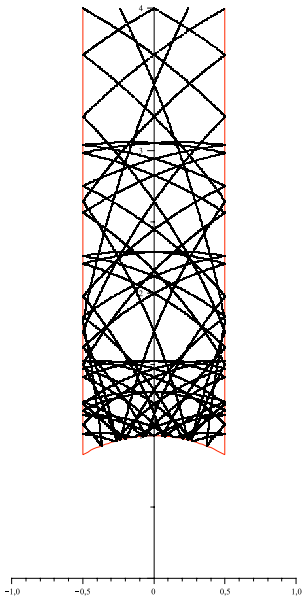

FIGURE 3. The distribution of Γ_{377}.

THEOREM 8.1 (Linnik, Skubenko). *Let Q be either the quadratic form b^2-4ac or $-(a^2+b^2+c^2)$. Let $p>2$ be a fixed prime and let d vary amongst the integers such that $\mathrm{R}_Q(d)\neq\emptyset$ and such that the prime p splits in the quadratic field $\mathbb{Q}(\sqrt{d})$.*
Then as $|d|\to\infty$, the set $|d|^{-1/2}.\mathrm{R}_Q(d)$ become equidistributed on $V_{Q,\pm 1}$ w.r.t $\mu_{Q,\pm 1}$ where $\pm 1=d/|d|$.

The (mod p)-congruence condition on d

"p splits in $\mathbb{Q}(\sqrt{d})$ for some fixed prime p"

is called a condition of Linnik's type. Such condition is quite natural in the context of Linnik's "ergodic method" but seem superfluous regarding the original equidistribution problems. In [**Lin68**], Linnik explicitely raised the problem of removing this condition; for instance, he pointed out that it could be avoided by assuming some weak form of the generalized Riemann hypothesis [**Lin68**, Chap. IV, §8]. In the following years, the ergodic method was generalized in various ways –either by considering different ternary forms or by considering similar problems over more general number fields [`?Te`]– but all these generalizations assumed a form or another of Linnik's condition. It is only in the late 80's that Duke made a fundamental breaktrough and removed Linnik's condition but by following a completely different approach avoiding the ergodic method [**Duk88**, `?DSP`]. Duke established essentially the following

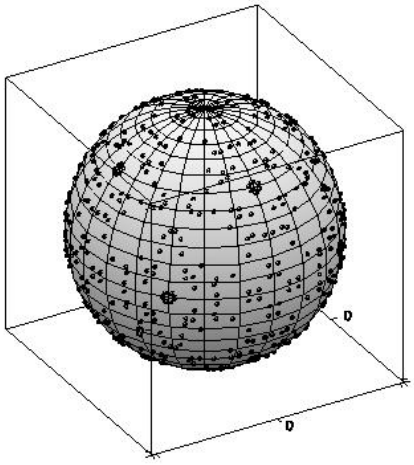

FIGURE 4. $Q(a,b,c) = -a^2 - b^2 - c^2$, d=-78540

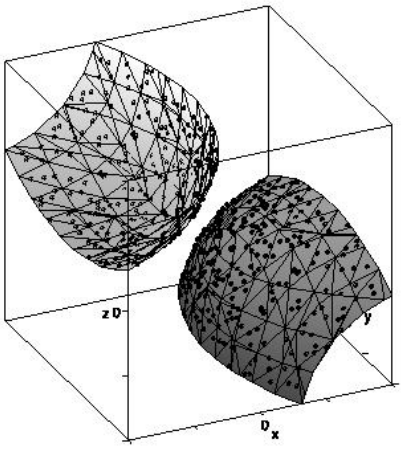

FIGURE 5. $Q(a,b,c) = b^2 - 4ac$, $d = -4620$

THEOREM 8.2 (Duke). *Let Q be either the quadratic form $-(a^2+b^2+c^2)$ or the quadratic form $b^2 - 4ac$. As $|d| \to +\infty$, amongst the d's for which $\mathrm{R}_Q(d) \neq \emptyset$ (that is $d < 0$ and $d \not\equiv 0, 1, 4 (\mathrm{mod}\ 8)$ in the former case and $d \equiv 0, 1 (\mathrm{mod}\ 4)$ in the latter case), the set $|d|^{-1/2}.\mathrm{R}_Q(d)$ becomes equidistributed on $V_{Q,\pm 1}(\mathbb{R})$ w.r.t $\mu_{Q,\pm 1}$ where $\pm 1 = d/|d|$.*

REMARK 8.1. In fact, Duke did not exactly proved his result in the generality stated above; see remark **??** below. For instance he discussed

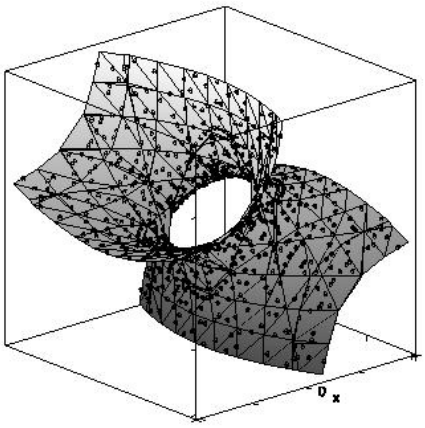

FIGURE 6. $Q(a,b,c) = b^2 - 4ac,\ d = 1540$

only the case of fundamental discriminants d which from the perpective of the present paper in the most interesting case. However, Duke's original arguments can be adapted to cover all cases.

In fact, Duke's results where not formulated exactly in this form: in the next section, we give an equivalent description of Linnik's problems which lead to Duke's results in their original form.