GEOMETRY OF NUMBERS

LECTURES BY AKSHAY VENKATESH,
NOTES BY TONY FENG AND NICCOLO RONCHETTI

CONTENTS

1. LATTICES

1.1. **Overview.** This will be an *introductory* course on the geometry of numbers. We will mostly adopt a classical approach, but here is the highbrow way of describing the goal of the course. For G a reductive group over $\mathbf{Q}$ (or really over any global field), we want to understand the size and shape of

$$G(\mathbf{R})/\mathscr{G}(\mathbf{Z})$$

(for $\mathscr{G}$ a suitably nice flat affine $\mathbf{Z}$-group of finite type with generic fiber G), or the adelic reformulation

$$G(\mathbf{A})/G(\mathbf{Q}).$$

1.2. **Lattices.** Here is a puzzle that we will be able to answer soon.

Question 1.2.1. *Choose a large prime p and an integer $1 \leq \lambda \leq p-1$ randomly. Find the smallest solution (minimizing $\sqrt{x^2+y^2}$) among non-zero solutions to $x \equiv \lambda y \bmod p$. How large should you expect $\sqrt{x^2+y^2}$ to be?*

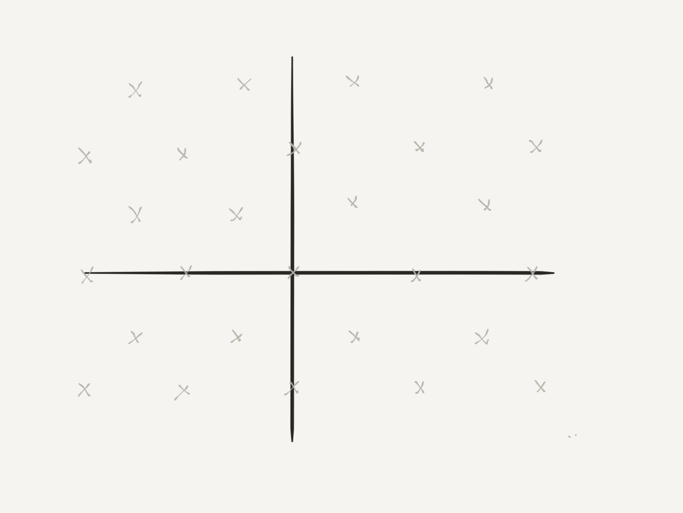
Definition 1.2.2. A *lattice* in $\mathbf{R}^n$ is a subgroup $L \subset \mathbf{R}^n$ that is generated by an $\mathbf{R}$-basis.

Example 1.2.3. $\mathbf{Z}^n \subset \mathbf{R}^n$ is a lattice. (However, for reasons we'll discuss later in the course, it does not look like a "typical" lattice.)

Definition 1.2.4. By an *n-dimensional lattice* we mean a lattice in $\mathbf{R}^n$ up to rotation. Equivalently, it is a free abelian group Λ of rank n together with a positive-definite quadratic form on $\Lambda \otimes \mathbf{R}$. (One could consider indefinite quadratic forms, but for present purposes we focus on the positive-definite case so that the associated special orthogonal group is "compact at infinity"; i.e., $\mathbf{R}$-anisotropic.)

Example 1.2.5. The D_n-lattice is the lattice associated to the D_n root system.

$$D_n = \{(x_1, \dots, x_n) \in \mathbf{Z}^n : \sum x_i \text{ even}\}.$$



Example 1.2.6. More generally, fix an integer N and integers $a_1, \dots, a_n$ not all zero. We can consider the lattice

$$\{(x_1, \dots, x_n) \in \mathbf{Z}^n : \sum a_i x_i \equiv 0 \mod N\}.$$

Example 1.2.7. For fixed $\lambda \in \mathbf{Z}$,

$$\{(x, y) \in \mathbf{Z}^2 \mid x \equiv \lambda y \mod p\}$$

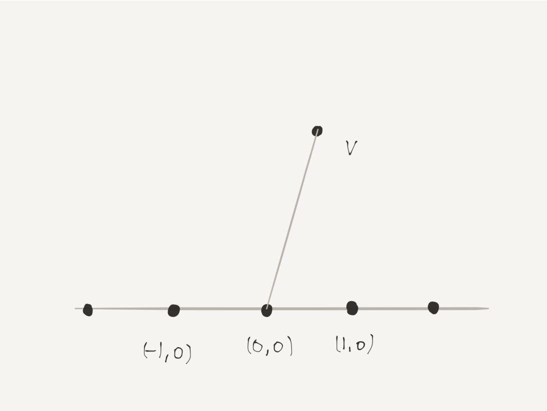
is a lattice in $\mathbf{R}^2$.

Example 1.2.8. One description of the famous E_8-lattice is

$$E_8 : s = D_8 + \left\{ D_8 + \left(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2} \right) \right\}.$$

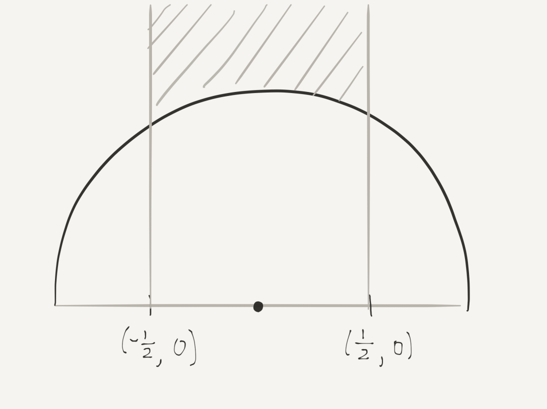
More generally, $D_n + \{D_n + (\frac{1}{2}, \dots, \frac{1}{2})\}$ is a lattice (i.e., stable under addition) when $2 \mid n$.

1.3. **Classification of 2-dimensional lattices.** In particular, 2-dimensional lattices up to isometric isomorphism are lattices in $\mathbf{R}^2$ up to rotation and reflection (orientation is not fixed). Let L be any such lattice. After rotating and *scaling* ($v \mapsto \lambda v$ with $\lambda \in \mathbf{R}^\times$) we can suppose that $(1,0) \in L$, and furthermore that it is the shortest vector in L (since by discreteness L has finite intersection with any bounded region).



Clearly $L \cap \mathbf{R}(1,0) = \mathbf{Z}(1,0)$. The connected components of $L_{\mathbf{R}} - \mathbf{R}(1,0)$ are swapped by negation. Let $v = (x, y)$ be a shortest vector in a fixed such connected component (drawn as an "upper half-plane"). This lies outside the open unit disc, which is to say $\|v\| \geq 1$. Also, we will have $-\frac{1}{2} \leq x \leq \frac{1}{2}$ because otherwise translating v by ±1 produces a shorter vector.

So, up to boundary issues, the isometry classes of 2-dimensional lattices are parameterized by points (x, y) with $x^2 + y^2 \geq 1$ and $-\frac{1}{2} \leq x \leq \frac{1}{2}$.



(In other words, up to specific boundary issues, $\mathrm{GL}_2(\mathbf{Z})$ acts freely on the union of this region and its reflection across the x-axis.)

We can now answer Question 1.2.1 in terms of this fundamental domain, as follows. If (x_0, y_0) is the smallest solution then $t = \frac{x_0^2 + y_0^2}{p}$ has a limiting disribution as $p \to \infty$. The distribution function is supported in the region $0 \leq t \leq |\lambda| \frac{2}{\sqrt{3}}$, and is given by $F(t)\,\mathrm{d}t$ where $F(t)$ is proportional to the width of the fundamental domain at $y = t^{-1}$.

1.4. **The space of lattices.** The set of lattices in $\mathbf{R}^n$ is $\mathrm{GL}_n(\mathbf{R}) / \mathrm{GL}_n(\mathbf{Z})$: given $g \in \mathrm{GL}_n(\mathbf{R})$, the image $g\mathbf{Z}^n$ is a lattice in $\mathbf{R}^n$ with basis the "column vectors" of g. This description does not account for the equivalence relation of isometric automorphisms of $\mathbf{R}^n$, so the set of lattices up to isometric isomorphism is

$$O_n(\mathbf{R})\backslash \mathrm{GL}_n(\mathbf{R})/\mathrm{GL}_n(\mathbf{Z}).$$

1.5. **Minkowski's Theorem.** *Reduction theory* is about constructing preferred and pleasant class of bases for lattices. It makes statements of the form "each lattice has a 'quasi-orthogonal' basis, and such bases are roughly unique".

First we discuss the existence of short vectors. Minkowski observed that lattices have short vectors for simple geometric reasons.

Definition 1.5.1. If $L \subset \mathbf{R}^n$ is a lattice, then we define the *volume* of L to be the (absolute value of) the determinant of any basis

$$\mathrm{vol}(L) = \left| \det \begin{pmatrix} | & | & | \\ v_1 & \dots & v_n \\ | & | & | \end{pmatrix} \right|$$

This is the same as $\mathrm{vol}(\mathbf{R}^n/L)$, and by definition also coincides with the volume of a fundamental domain for $\mathbf{R}^n/L$ (such as the parallelope arising from a $\mathbf{Z}$-basis of L).

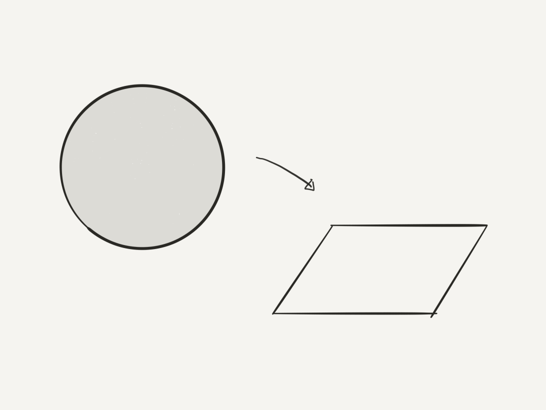
Example 1.5.2. The volume of $\{x \equiv \lambda y \mod p\}$ is p. You can calculate it using our definition, but it is easier to note that this is a sublattice of $\mathbf{Z}^2$ with about $1/p$ of the vectors.

Theorem 1.5.3 (Minkowski)**.** *Let V_n be the volume of the unit sphere in $\mathbf{R}^n$. If V_n $R^n \geq \mathrm{vol}(L)$, then L contains a nonzero vector of length $\leq 2R$.*

Remark 1.5.4. The intuition is that if we take a sphere of radius R, so that the volume of the sphere is at least that of the lattice, then there will be a lattice point inside it. The theorem statement is off by a factor of 2, but we will generally ignore absolute constant factors (so that all norms on $\mathbf{R}^n$ become equivalent).

Example 1.5.5. For $L = \{(x \equiv \lambda y \mod p)\}$, this says that if $\pi R^2 \geq p$ then L contains a vector of length at most $2R$; in other words, a nonzero vector of length at most $\sqrt{\frac{4p}{\pi}}$.

Proof. Take the ball of radius R in $\mathbf{R}^n$ and map it to $\mathbf{R}^n/L$.



By volume considerations, this cannot be injective. That means that there exist distinct x, y with $\|x\|, \|y\| \leq R$ such that $x \equiv y$ in $\mathbf{R}^n/L$, so $x - y \in L$. On the other hand, we clearly have $\|x - y\| \leq 2R$. □

1.6. **Some applications.**

Example 1.6.1. If $p \equiv 1 \mod 4$, there there exists $\lambda \in \mathbf{Z}/p\mathbf{Z}$ such that $\lambda^2 \equiv -1 \mod p$. By Theorem 1.5.3 we can find $(x,y) \neq (0,0)$ such that $x^2+y^2 \leq \frac{4p}{\pi} < 2p$ and $p \mid (x^2+y^2)$, so $x^2+y^2=p$.

From Theorem 1.5.3 you can derive all the basic finiteness theorems of algebraic number theory: finiteness of the class number, Dirichlet's unit theorem (we'll do these two later, in a more general setting), and the *finiteness of the number of field extensions* $K/\mathbf{Q}$ *with bounded discriminant.*

One manifestation of this last result is that there are no non-trivial field extensions $K/\mathbf{Q}$ with discriminant 1. To illustrate the technique, we prove that now.

Proof. (In the case where K is totally real; the general case is similar.) First we recall the meaning of the discriminant. Recall that if $[K:\mathbf{Q}]=d$, we have d embeddings

$$\sigma_1,\dots,\sigma_d \colon K \hookrightarrow \mathbf{R}$$

that are the component functions of an $\mathbf{R}$-algebra decomposition $\mathbf{R}\otimes_{\mathbf{Q}} K = \mathbf{R}^d$. Let $\mathscr{O}_K$ be the ring of algebraic integers in K. Then these embeddings identify $\mathscr{O}_K$ as a lattice in $\mathbf{R}^d$:

$$(\sigma_1,\dots,\sigma_d)\colon \mathscr{O}_K \hookrightarrow \mathbf{R}^d.$$

One definition of the discriminant, ignoring its sign, is:

$$\operatorname{disc} K := \operatorname{vol}(\mathscr{O}_K \text{ as a lattice in } \mathbf{R}^d)^2 \in \mathbf{Z}_{>0}.$$

We want to show that $\operatorname{disc} K > 1$. By Minkowski's Theorem 1.5.3, if $V_d R^d \geq \sqrt{\operatorname{disc} K}$ then there exists a nonzero element $x \in \mathscr{O}_K$ such that $\sqrt{\sum \sigma_i(x)^2} \leq 2R$.

We want to show that such a small vector can't exist. What constraint do we have? The conjugates $\sigma_i(x)$ can't all be small because their product is a nonzero integer. That is,

$$\left|\prod \sigma_i(x)\right| \geq 1$$

so by Cauchy-Schwarz (for instance),

$$\sum \sigma_i(x)^2 \geq d.$$

Using this bound in Minkowski's Theorem, we obtain

$$\sqrt{\operatorname{disc} K} \geq V_d \left(\frac{\sqrt{d}}{2}\right)^d.$$

We'll analyze how the right hand side behaves for d large; for d small you can calculate it directly.

The area of the unit sphere in $\mathbf{R}^d$ is $\frac{2\pi^{d/2}}{\Gamma(d/2)}$; you can derive this by integrating the d-dimensional Gaussian distribution:

$$\pi^{d/2} = \int_{\mathbf{R}^d} e^{-x_1^2-\dots-x_d^2}\,\mathrm{d}x = \left(\int e^{-r^2} r^{d-1}\,\mathrm{d}r\right)\cdot(\text{Area of unit sphere}).$$

Integrating, we find that

$$V_d = \frac{2\pi^{d/2}}{\Gamma(d/2)} \cdot \frac{1}{d+1}$$

so

$$\sqrt{\operatorname{disc} K} \geq \frac{2}{d+1} \left(\frac{\pi^{1/2} d}{2} \right)^d \frac{1}{\Gamma(d/2)}$$

and by Stirling's formula, for large d this grows exponentially. □

2. Reduction theory

2.1. **Reduced bases.**

Example 2.1.1. Consider the lattice $(\mathbf{Z}^3, x^2+y^2+z^2+10^7(\sqrt{2}x+ey+\pi z)^2)$. The shortest non-zero vector turns out to be

$$(x,y,z) = (17,-10,1).$$

This corresponds to the fact that

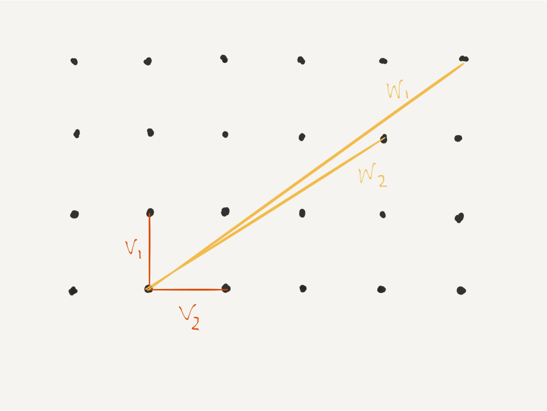
$$17\sqrt{2} - 10e + \pi = 0.0004\ldots$$

The point of this example is that you can detect approximate linear dependencies with integral coefficients over $\mathbf{Z}$ by finding short vectors. This is one application of having efficient algorithms for finding short vectors.

Definition 2.1.2. A *basis* for a lattice is a basis as a $\mathbf{Z}$-module.

There are many bases for a given lattice, but we want to codify a notion of preferred basis. Let's consider an example.

Example 2.1.3. Consider the lattice depicted below



with basis (v_1, v_2) in red and basis (w_1, w_2) in yellow. We feel like (v_1, v_2) is a "better" basis than (w_1, w_2). Why? The basis (v_1, v_2) satisfies:

- the orthogonal projection $\overline{v}_1$ of v_1 onto $v_2^{\perp}$ satisfies

$$\|\overline{v}_1\| \geq \frac{\sqrt{3}}{2} \|v_2\|.$$

- If we write $v_1 = \overline{v}_1 + \alpha v_2$ then $|\alpha| \leq \frac{1}{2}$.

Definition 2.1.4. In general, an (A,B)-*reduced basis* $v_1, \ldots, v_n$ for L is a basis such that, if $\overline{v_i}$ is the projection of v_i onto $\langle v_{i+1}, \ldots, v_n \rangle^\perp$ then

- $\|\overline{v}_i\| \geq A \|\overline{v}_{i+1}\|$,
- If we write
$$v_i = \overline{v}_i + \sum_{j>i} \alpha_{ij} \overline{v}_j,$$
then $|\alpha_{ij}| \leq B$.

The point here is to force the vectors to be "roughly" orthogonal. This is very rough, but one gets that the angle between any two is bounded away from zero.

Theorem 2.1.5. *Reduced bases enjoy the following properties:*

- *("Existence") For small enough A and large enough B (e.g. $(A,B) = (\sqrt{3}/2, 1/2)$ works), (A,B)-reduced bases exist.*
- *("Uniqueness") If $(v_1', \ldots, v_n')$ and $(v_1, \ldots, v_n)$ are reduced bases, then*
$$\|v_i\| \asymp_{n,A,B} \|v_i''\|.$$
Here the $\asymp$ means that the lengths are bounded above and below in terms of the implicit constants.
- *If you write $v_i' = \sum m_{ij} v_j$, then $\|m_{ij}\| \leq$ constant(n, A, B), independently of the lattice.*

Remark 2.1.6. Part of the proof will give an algorithm (LLL), which *finds* such a basis in polynomial time.

Reformulation of Theorem 2.1.5. if $y_1, \ldots, y_n$ is any basis for L and $v_1, \ldots, v_n$ is an (A,B)-reduced basis for L, then

$$\begin{pmatrix} | & & | \\ y_1 & \ldots & y_n \\ | & & | \end{pmatrix} = \begin{pmatrix} | & & | \\ v_1 & \ldots & v_n \\ | & & | \end{pmatrix} \cdot (M \in \mathrm{GL}_n(\mathbf{Z})).$$

The condition of being (A,B)-reduced tells us that

$$\begin{pmatrix} | & & | \\ v_1 & \ldots & v_n \\ | & & | \end{pmatrix} = \begin{pmatrix} | & & | \\ \overline{v}_1 & \ldots & \overline{v}_n \\ | & & | \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ * & * & 1 \end{pmatrix}$$

where $|*| \leq B$, and also

$$\begin{pmatrix} | & & | \\ v_1 & \ldots & v_n \\ | & & | \end{pmatrix} \in O_n \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ * & * & 1 \end{pmatrix}$$

where $* \leq B$ and $a_i / a_{i+1} \geq A$.

So if we write $F_{A,B} \subset \mathrm{GL}_n(\mathbf{R})$ given by

$$F_{A,B} = O_n \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ * & 1 & 0 \\ * & * & 1 \end{pmatrix}$$

(the subscripts A, B may be suppressed in the future) then Theorem 2.1.5 says that

$$F_{A,B}\,\mathrm{GL}_n(\mathbf{Z}) = \mathrm{GL}_n(\mathbf{R})$$

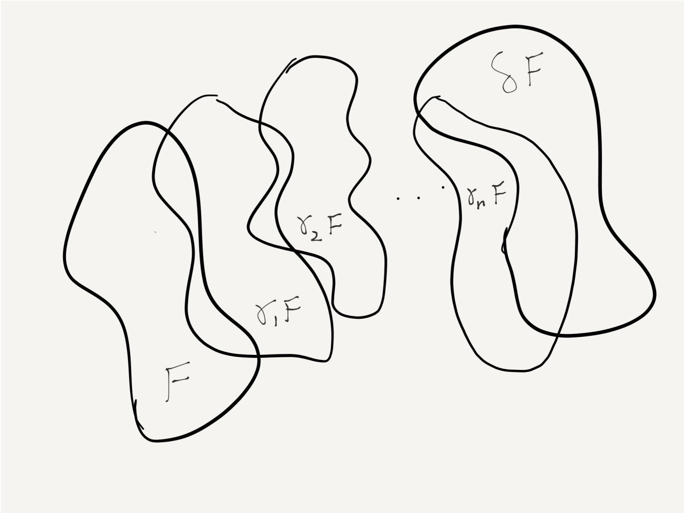
for small enough A and large enough B, and the set of $\gamma \in \mathrm{GL}_n(\mathbf{Z})$ such that $F \cap F\gamma \neq \emptyset$ is finite. This $F_{A,B}$ is a "Siegel" set, and this is saying that it is an approximate fundamental domain.

Remark 2.1.7. An actual fundamental domain must be very complicated, since we know the Betti numbers of the quotient space and they are very large.

Corollary 2.1.8. *The group* $\mathrm{GL}_n(\mathbf{Z})$ *is finitely generated. In fact, it is generated by*

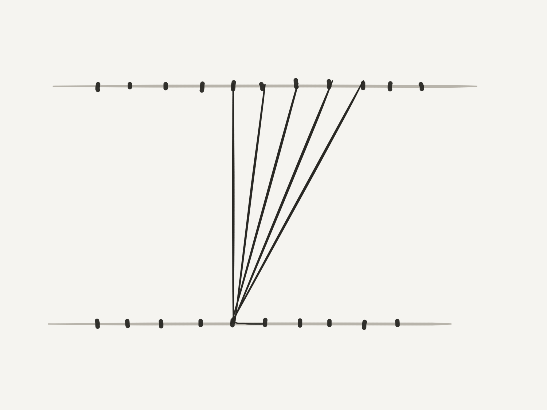
$$S := \{\gamma \mid F \cap F\gamma \neq \emptyset\}.$$

Proof. Pick $\delta \in \mathrm{GL}_n(\mathbf{Z})$. Consider $F\delta$. Then there exists a sequence of translates $F\gamma_i$ interpolating between F and δF:



and we may assume that $F\gamma_i \cap F\gamma_{i+1} \neq \emptyset$, implying that $\gamma_{i+1}\gamma_i^{-1} \in S$. □

Remark 2.1.9. Why not make a lattice by enforcing a lower bound on angles? Consider a lattice of the form below.

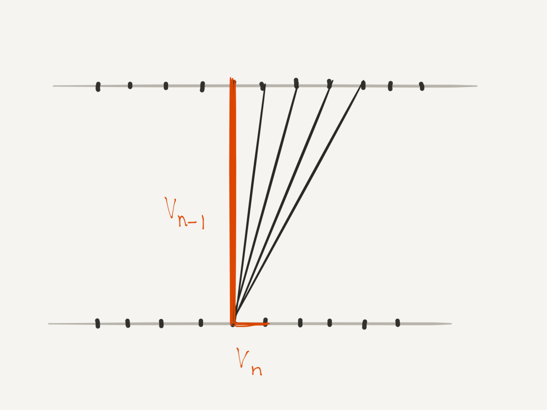


What should be a "preferred" basis? We obviously want the shortest vector. If we only demanded that the angles of the basis be bounded below, then there would be *many* options for a second basis vector, and the number of reduced bases could be arbitrarily large. In Theorem 2.1.5 the constants are bounded *independently* of the lattice.

2.2. **The LLL algorithm.**

We will now discuss a proof of Theorem 2.1.5. (Assume $A < \sqrt{3}/2$ and $B > 1/2$ throughout.)

"Existence." We first give a *non-constructive* proof, which is a "greedy" algorithm. Let v_n be the shortest non-zero vector. Project L to $v_n^{\perp}$, obtaining a lattice L_{n-1} of rank $n-1$. Let v'_{n-1} be the shortest vector in L_{n-1} and lift it to L_n in the shortest possible way, so that the coefficient of v_n is $\le B$.



By the discussion of §1.3 we have

$$\|\overline{v}_{n-1}\| \ge \frac{\sqrt{3}}{2}\|\overline{v}_n\|.$$

Next project L to $\langle v_{n-1}, v_n\rangle^{\perp}$ and call v'_{n-2} the shortest vector in L_{n-2}. Lift it to $v_{n-2} \in L$; adjusting by v_{n-1} and v_n we can assume that

$$v_{n-2} = \overline{v}_{n-2} + \alpha\overline{v}_{n-1} + \beta\overline{v}_n$$

where $|\alpha|, |\beta| \leq B$ (taking care to adjust α first). Continue.

Exercise 2.2.1. Check that algorithm indeed produces an (A, B)-reduced basis.

Now we give the constructive LLL algorithm. For $n = 2$ this is "equivalent" to the continued fraction algorithm.

The LLL algorithm.

Input. A basis $(y_1, \ldots, y_n)$ for L.

Output. An (A, B)-reduced basis ($A < \sqrt{3}/2$, $B > 1/2$).

Algorithm. At each stage form $\overline{y}_1, \ldots, \overline{y}_n$ as before (i.e. $\overline{y}_i$ is the projection of y_i to $\langle y_{i+1}, \ldots, y_n \rangle^{\perp}$). By adjusting y_i by a combination of $y_{i+1}, \ldots, y_n$ we can assume that

$$y_i = \overline{y}_i + \sum_{j>i} \alpha_{ij} \overline{y}_j \quad \text{where } |\alpha_{ij}| \leq \frac{1}{2}.$$

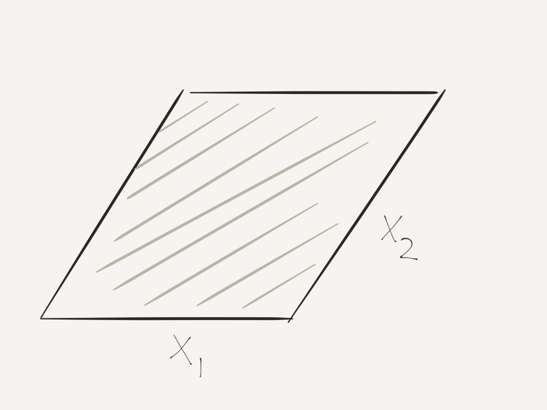
If there exists i such that $\|\overline{y}_i\| / \|\overline{y}_{i+1}\| < A$, then swap y_i and y_{i+1}. Repeat from the beginning.

Remark 2.2.2. The running time depends on the parameters; it may not be polynomial for all parameters.

Exercise 2.2.3. Run this for some examples in the case $n = 2$.

If this algorithm terminates, i.e. no swaps are necessary, then it produces an (A, B)-reduced basis. Therefore, we merely have to prove that it does terminate.

Proof of termination. We give another perspective on reduced bases. Roughly speaking, y_n is the shortest vector. But we can say more via $\|y_n\|$, $\|y_{n-1} \wedge y_n\|$, $\|y_{n-2} \wedge y_{n-1} \wedge y_n\|$, etc. (Here $\|x_1 \wedge x_2\|$ can be interpreted as the area of the parallelogram spanned by x_1 and x_2.



Generally, if V is a vector space with inner product then all $\wedge^j(V)$ also have an inner product, namely

$$\langle v_1 \wedge \ldots \wedge v_j, w_1 \wedge \ldots \wedge w_j \rangle = \det(\langle v_i, w_j \rangle).)$$

The idea is that a reduced basis (roughly) minimizes all of these at once. That is, not only is the last vector short as possible, but the sequence of parallelepipeds have the smallest possible volumes.

Once this is granted, the proof of termination is almost immediate since by discreteness, each quantity $\|y_j \wedge \ldots \wedge y_n\|$ is bounded below. Each swap $y_i \longleftrightarrow y_{i+1}$ doesn't change any of these areas except for $\|y_{i+1} \wedge y_{i+2} \wedge \ldots \wedge y_n\|$.

Exercise 2.2.4. Show that this decreases by a factor of at least $\sqrt{A^2 + 1/4}$. (i.e. the new volume is $\leq \sqrt{A^2+1/4}$ times the old volume).

□

We have seen that the LLL algorithm hinges on the following principle:

Principle. In an (A, B)-reduced basis,

- v_n is roughly the shortest vector,
- $\langle v_{n-1}, v_n \rangle$ is roughly the smallest parallelogram, etc.

The justification of this principle will be bundled up with the (approximate) uniqueness of reduced bases.

Uniqueness. If $e_1, \ldots, e_n$ and $f_1, \ldots, f_n$ are (A, B)-reduced bases, then

$$\|f_i\| \asymp_{n,A,B} \|e_i\|.$$

Also, the change of basis $e_i \mapsto f_i$ has coefficients bounded in magnitude by $\leq c(A, B, n)$.

Lemma 2.2.5. *If L is the linear transformation satisfying $e_i \mapsto \overline{e_i}$ for each i, then*

$$\|Lv\| \asymp \|v\|.$$

Proof. By the definition of a reduced basis, we have

$$L^{-1}\colon \frac{\overline{e_i}}{\|\overline{e_i}\|} \mapsto \frac{e_i}{\|\overline{e_i}\|} = \frac{\overline{e_i}}{\|\overline{e_i}\|} + \sum_{j>i} n_{ji} \frac{\overline{e_j}}{\|\overline{e_i}\|}$$

where $|n_{ji}| \leq B$. We can rewrite this as

$$L^{-1} : \frac{\overline{e_i}}{\|\overline{e_i}\|} \mapsto \frac{e_i}{\|\overline{e_i}\|} + \sum_{j>i} n_{ji} \frac{\overline{e_j}}{\|\overline{e}_j\|} \frac{\|\overline{e_j}\|}{\|\overline{e_i}\|}$$

where $\|\overline{e_j}\|/\|\overline{e_i}\| \leq A^n$. Hence, with respect to the ordered orthonormal basis $\{\overline{e_i}/\|\overline{e_i}\|\}$ the matrix of L is

$$\begin{pmatrix} 1 & & \\ * & \ddots & \\ * & * & 1 \end{pmatrix}$$

with each entry $*$ bounded uniformly in terms of A, B, and n. Lengths of vectors are computed by the habitual formula in coordinates relative to any orthonormal basis, so we are done. □

Corollary 2.2.6. *We have*

$$\|\sum x_k e_k\|^2 \asymp_{n,A,B} \sum |x_k|^2 \|\overline{e_k}\|^2.$$

Remark 2.2.7. A consequence of this is that it is "easy" to enumerate all vectors $v \in L$ with $\|v\| \leq R$: they are all of the form

$$\sum x_k e_k, \quad |x_k| \leq \gamma_n \frac{R}{\|\overline{e_k}\|}.$$

for some uniform constant $\gamma_n > 0$ and integers x_k.

Choose $v_1, \ldots, v_k \in L$, so we can write

$$v_1 \wedge \ldots \wedge v_k = \sum_{\substack{J \subset \{1,\ldots,n\} \\ \#J = k}} m_J e_J$$

where $e_J = e_{j_1} \wedge \ldots \wedge e_{j_k}$ for a strictly monotone sequence $J = \{j_1, \ldots, j_k\}$ and $m_J \in \mathbf{Z}$. By Corollary 2.2.6, the norms are changed by a bounded amount upon replacing e_j with $\overline{e_j}$, so:

$$\begin{aligned} \|\sum_{\substack{J \subset \{1,\ldots,n\} \\ \#J = k}} m_J e_J\|^2 &\asymp \|\sum m_J \overline{e_J}\|^2 \\ &= \sum |m_J|^2 \|\overline{e_J}\|^2 \end{aligned}$$

In particular, we see that

$$\|v_1 \wedge \ldots \wedge v_k\| \geq \|\overline{e}_{n-k+1} \wedge \ldots \wedge \overline{e_n}\| \asymp \|e_{n-k+1} \wedge \ldots \wedge e_n\|$$

provided the $e_{n-k+1} \wedge \ldots \wedge e_n$-coefficient in $\mathbf{Z}$ for $v_1 \wedge \cdots \wedge v_k$ is nonzero.[1]

If we have two (A,B)-reduced bases $(e_1, \ldots, e_n)$ and $(f_1, \ldots, f_n)$, we can apply this result to each with respect to the other to obtain that

$$\|e_{n-k+1} \wedge \ldots \wedge e_n\| \asymp \|f_{n-k+1} \wedge \ldots \wedge f_n\|$$

for all k, which implies that

$$\|\overline{e_i}\| \asymp \|\overline{f}_i\| \text{ for all } i$$

and also

$$\|e_i\| \asymp \|f_i\| \text{ for all } i.$$

This means that the lengths $\|e_1\|, \ldots, \|e_n\|$ are *well-defined "up to constants"* (depending on n); they are classically called the *minima* of L.

Remark 2.2.8. Prior to the notion of reduced bases, the "kth successive minimum of L" was defined to be

$$\min\{r > 0 \colon \dim \operatorname{Span}(\{v \in L \colon |v| \leq r\}) \geq k\}$$

which we now know is $\asymp \|e_{n-k+1}\|$.

[1] Need to explain why this is nonzero when $v_1, \ldots, v_k$ arises from the end of a reduced basis!

2.3. **A "Harder-Narasimhan" stratification.** Note that if there is a huge gap in the kth minimum, i.e. if

$$\|\overline{e}_k\| > C\|\overline{e}_{k+1}\|$$

for some large enough $C = C(n, A, B)$, then our previous argument shows something more precise: it shows that *if* $e_1, \ldots, e_n$ *and* $f_1, \ldots, f_n$ *are reduced then in fact*

$$e_{k+1} \wedge \ldots \wedge e_n = f_{k+1} \wedge \ldots \wedge f_n.$$

(Previously we said only that $e_{k+1} \wedge \ldots \wedge e_n \asymp_{n,A,B} f_{k+1} \wedge \ldots \wedge f_n$.)

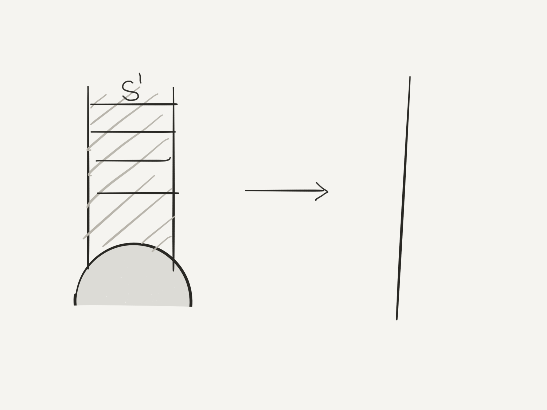
This shows that if (for instance) $\|e_2\|/\|e_3\| \geq C$ and $\|e_7\|/\|e_8\| \geq C$ then the data

- $e_8 \wedge \ldots \wedge e_n$ (equivalently, $\mathrm{Span}(e_8, \ldots, e_n)$),
- $e_3 \wedge \ldots \wedge e_n$, and
- $e_1 \wedge \ldots \wedge e_n$

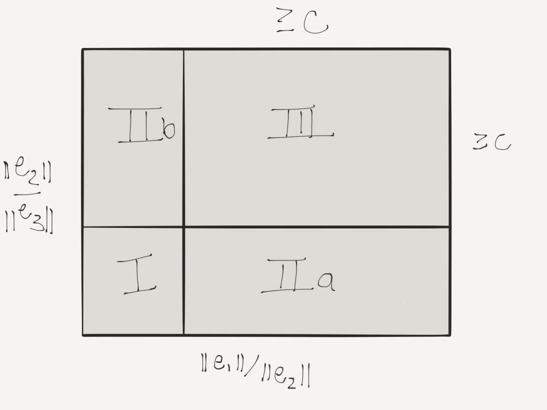
are *independent* of the reduced basis.

For a fixed C, this gives a flag in $L \otimes \mathbf{Q}$, analogous to the "Harder–Narasimhan filtration" of vector bundles on curves.

Example 2.3.1. We have already discussed the fundamental domain for the moduli space of 2-dimensional lattices. Consider the "y-height" map to $\mathbf{R}$, which one can think of as roughly specifying the length of the second-shortest vector. The fibers are S^1, corresponding to the choice of phase for this second basis vector.



Example 2.3.2. Consider the moduli of 3-dimensional lattices. Consider the map from this space to $\mathbf{R}^2$ given by $(\|e_1\|/\|e_2\|, \|e_2\|/\|e_3\|)$. It is natural to divide up the image according to how the ratios compare with C, corresponding to the "breaks" in the Harder–Narasimhan filtration.



The fiber over a point in region III is roughly similar to a product of 3 circles, corresponding to a choice of phase for the three basis vectors. More precisely, it is a "nilmanifold" $N(\mathbf{R})/N(\mathbf{Z})$ where

$$N = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

Over small compact region, the fiber is a mess. The fibers over regions IIa and IIb look like an $S^1 \times S^1$-bundle over the fundamental domain.

Finally, we show the last part of Theorem 2.1.5: if $\{e_i\}$ and $\{f_i\}$ are (A,B)-reduced bases for L and we write

$$e_i = \sum_j m_{ij} f_j,$$

then we claim that $|m_{ij}| \le C'(A,B,n)$.

Proof. We break up into two cases, according to "Harder–Narasimhan" filtration.

Case 1: no large gap. Then $\|e_i\|/\|e_{i+1}\| \le C$ for all i, where C is as in the preceding discussion. We can sandwich this value as

$$A \le \frac{\|e_i\|}{\|e_{i+1}\|} \le C$$

so all the $\|e_i\|$ are the same (up to uniform constants in A,B,n). The same applies to $\{f_i\}$ since $\|e_i\| \asymp_{n,A,B} \|f_i\|$ for all i, so

$$\|e_i\|^2 = \|\sum_j m_{ij} f_j\|^2 \asymp \|\sum_j m_{ij} \overline{f}_j\|^2 = \sum_j |m_{ij}|^2 \|\overline{f}_j\|^2.$$

Since $\|\overline{f_j}\| \asymp_{n,A,B} \|e_j\|$ for all j, we get $\|e_i\|^2 \asymp_{n,A,B} \sum_j |m_{ij}|^2 \|e_j\|^2$. But there are no large gaps, so in this final sum we can replace every e_j with e_i up to uniform constants (controlled by n, A, B, which absorbs any intervention by C as well). Hence, we obtain the desired type of upper bound on $\sum_j |m_{ij}|^2$ for each i and hence on every $|m_{ij}|$.

Case 2: there is a large gap. Then we can essentially break the problem up into smaller ones. We showed earlier that if there is a large gap at i, then

$$\langle e_{i+1}, \dots, e_n \rangle = \langle f_{i+1}, \dots, f_n \rangle$$

and we work with $\langle e_{i+1}, \dots, e_n \rangle$ and the projection of L onto $\langle e_{i+1}, \dots, e_n \rangle^{\perp}$. (There is some work required in gluing these two cases together.)

Exercise 2.3.3. Check this.

□

Remark 2.3.4. There will be $O(c^{n^3})$ reduced bases. This comes from analyzing the Gram matrix of inner products $(\langle v_i, v_j \rangle)$. The reducedness imposes only an exponential bound on each entry, so one has $(c^n)^{n^2}$ for a bound on the number of Gram matrices.

2.4. **Applications.** Let's use reduced bases to recover Minkowski's Theorem, which says that up to constants, a lattice of volume V in an n-dimensional quadratic space has a nonzero vector of length $< c_n V^{1/n}$ for some universal constant $c_n > 0$ depending only on n.

Proof via reduced bases. If $\{e_1, \dots, e_n\}$ is an (A, B)-reduced basis, we claim that

$$\|e_1\| \dots \|e_n\| \asymp_{n,A,B} V.$$

Indeed, for our purposes we can straighten the vectors (i.e., replace e_i with $\overline{e_i}$) "for free", so

$$\|e_1\| \dots \|e_n\| \asymp \|\overline{e_1}\| \dots \|\overline{e_n}\| \asymp \|\overline{e_1} \wedge \dots \wedge \overline{e_n}\| = V$$

so the shortest $\|\overline{e_j}\|$ is at most $V^{1/n}$. □

Exercise 2.4.1. For $L \subset \mathbf{R}^n$ with dual lattice

$$L^* = \{v^* \in \mathbf{R}^n \mid \langle v^*, L \rangle \subset \mathbf{Z}\},$$

find the minima of L^* in terms of the minima of L.

We end our discussion of reduction theory with the following, very useful, consequence.

Theorem 2.4.2 (Mahler compactness)**.** *Fix $\delta > 0$. Inside*

$$\mathrm{GL}_n(\mathbf{R})/\mathrm{GL}_n(\mathbf{Z}) = \{\text{lattices } L \subset \mathbf{R}^n\}$$

the set

$$S(\delta) = \{L \subset \mathbf{R}^n \mid \mathrm{vol}(L) = 1, \text{ all nonzero } v \in L \text{ have length } \geq \delta\}$$

has compact closure.

Remark 2.4.3. The topology on $\mathrm{GL}_n(\mathbf{R})/\mathrm{GL}_n(\mathbf{Z})$ is the quotient topology: concretely, we have $L_i \to L$ exactly when there exists basis B_i for each L_i approaching a basis B for L as $i \to \infty$.

Proof. For $L \in S(\delta)$, pick an (A,B)-reduced basis $\{e_1,\dots,e_n\}$ for some appropriate A,B. Recall that we think of an (A,B)-reduced basis as an "almost-orthogonal" basis; in particular, we have

$$\|e_1\|\dots\|e_n\| \asymp_{n,A,B} \mathrm{vol}(L).$$

Since $\|e_i\| \geq \delta$, we also obtain

$$\|e_i\| \leq \frac{C\,\mathrm{vol}(L)}{\delta^{n-1}}$$

and hence each lattice $L \in S(\delta)$ has columns in the compact set

$$\left\{ x \in \mathbf{R}^n \mid \delta \leq \|x\| \leq \frac{C\,\mathrm{vol}(L)}{\delta^{n-1}} \right\}.$$

In other words, inside $\mathrm{SL}_n(\mathbf{R})$ the compact subset of matrices whose columns lie in the above compact region in $\mathbf{R}^n$ has image in $\mathrm{GL}_n|(\mathbf{R})/\mathrm{GL}_n(\mathbf{Z})$ that contains $S(\delta)$, so $S(\delta)$ has compact closure. □

Informally speaking, the only way a sequence of lattices L_i with covolume 1 can go to infinity in the space of lattices is if the lengths of the shortest nonzero vectors go to zero.

3. Pell's equation

We now discuss Pell's equation:

$$x^2 - dy^2 = 1,$$

where we look for nontrivial integer solutions (that is, aside from $(\pm1,0)$). This is a very ancient problem, but our discussion will involve very flexible methods and ideas that we will generalize later.

3.1. **Existence and number of solutions.** First of all, a very rough but surprisingly effective algorithm for solving (when possible) this equation comes from the observation that $\frac{x}{y} \approx \sqrt{d}$: one then writes down the continued expansion of $\sqrt{d}$ and then proceed to guess the solution (x,y). A priori, such method only guarantees that $x^2 - dy^2$ is small, and it is unclear why in practice this yields an actual solution to Pell's equation.

Theorem 3.1.1. *Let d be a non-square. Then Pell's equation admits a nontrivial solution. Notice however that the smallest nontrivial solution may be very large (roughly $\sqrt{d}$ digits).*

Remark 3.1.2 (*Hardy-Littlewood heuristic*). Before giving the proof we describe a very useful heuristic - let's call it Hardy-Littlewood heuristic - which we will come back to when we will talk about the mass formula.

Consider the hyperbola $x^2 - dy^2 = 1$ in the half-plane $x \geq 0$. Rather than looking for integer points on this curve, consider its small thickening $0.5 \leq x^2 - dy^2 \leq 1.5$: it turns out that the area of this region is infinite, and hence we expect it to contain points with integer coordinates.

More precisely, if we look at the thickened hyperbola to the left of the vertical line $x = T$, its area turns out to be $\frac{\log T}{\sqrt{d}}$ and hence our expectation for the smallest integral solution grows exponentially in $\sqrt{d}$. Finally, observe that an integer point (x, y) in the thickened hyperbola is necessarily a solution of Pell's equation.

Proof. To show that $x^2 - dy^2 = 1$ with non-square $d > 0$ admits nontrivial solutions, it is enough to prove that for the quadratic form $Q(x, y) = x^2 - dy^2$ the Zariski closure $\mathrm{SO}_{Q,\mathbf{Z}} \subset \mathrm{SL}_2$ over $\mathbf{Z}$ of the associated algebraic group SO_Q over $\mathbf{Q}$ has infinitely many $\mathbf{Z}$-points. Indeed, explicitly we have

$$\mathrm{SO}_Q(R) = \left\{ \begin{bmatrix} a & db \\ b & a \end{bmatrix} \in \mathrm{SL}_2(R) \right\}$$

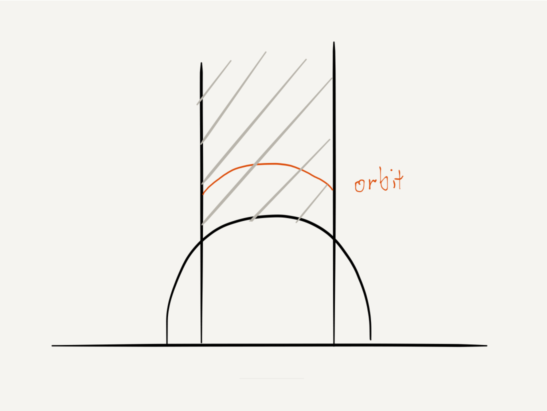
for $\mathbf{Q}$-algebras R, so elements of $\mathrm{SO}_{Q,\mathbf{Z}}(\mathbf{Z})$ corresponds to $(a, b) \in \mathbf{Z}^2$ with $a^2 - db^2 = 1$, and having infinitely many guarantees the existence of a pair with nonzero b.

Denote now $G = \mathrm{SO}_Q(\mathbf{R})$. Denote by $[\mathbf{Z}^2]$ the lattice $\mathbf{Z}^2$ thought of as a point in

$$\{\text{lattices in } \mathbf{R}^2\} = \mathrm{GL}_2(\mathbf{R}) / \mathrm{GL}_2(\mathbf{Z}).$$

We claim that the set of translates (i.e., the orbit) $G.[\mathbf{Z}^2]$ has image in $\mathrm{GL}_2(\mathbf{R}) / \mathrm{GL}_2(\mathbf{Z})$ with compact closure.

Example 3.1.3. If we picture the usual fundamental domain for the set of lattices in $\mathbf{R}^2$ we can see that the orbit goes away from $[\mathbf{Z}^2]$, then comes back and closes in on itself.

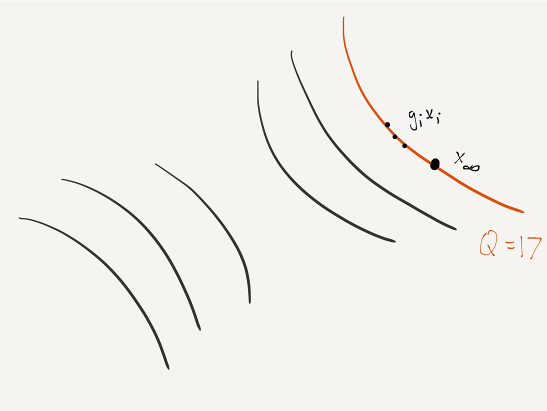


To prove the claim, notice that since G preserves Q, for each vector $v \in L$ and each $[L] \in G.[\mathbf{Z}^2]$, we have $Q(v) \in \mathbf{Z}$. This says that even though $L = g(\mathbf{Z}^2)$ where $g \in \mathrm{SL}_2(\mathbf{R})$ might have irrational entries, $Q|_L$ is $\mathbf{Z}$-valued. Hence, in coordinates arising from a $\mathbf{Z}$-basis of L the quadratic form $Q|_L$ has $\mathbf{Z}$-coefficients.

Moreover, $\mathrm{disc}(Q|_L) = \mathrm{disc}(Q) = -d$ since $g \in \mathrm{SL}_2(\mathbf{R})$. Since d is not a square, $Q|_L$ is $\mathbf{Q}$-anisotropic; i.e., the only $v \in L_{\mathbf{Q}}$ for which $Q(v) = 0$ is $v = 0$. Therefore, for each $[L] \in G.[\mathbf{Z}^2]$ and each nonzero $v \in L$, we have $|Q(v)| \geq 1$, so by staring at a hyperbola not passing through $(0, 0)$ we get $\delta > 0$ independent of L such that $\|v\| \geq \delta$. We have shown that $G.[\mathbf{Z}^2] \subset S(\delta)$, and then Mahler's compactness criterion kicks in to yield that the closure $\overline{G.[\mathbf{Z}^2]}$ is compact.

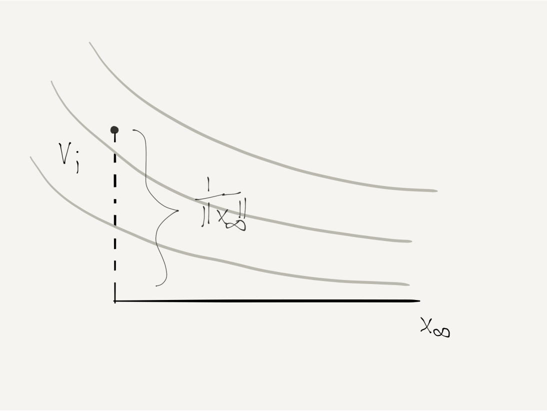
The previous argument yields then that there exists a sequence (g_i) with $g_i \to \infty$ in G such that $g_i \mathbf{Z}^2 \to L$ for some limit lattice L as $i \to \infty$. In particular, there exist primitive vectors (x_i) of $\mathbf{Z}^2$ such that $g_i x_i \to x_\infty$ in $\mathbf{R}^2$ with x_∞ primitive in L. .

Notice that all $g_i x_i$ and x_∞ lie on the same integral level set of Q, since G preserves the quadratic form.



Since G acts locally transitively on the level set, by adjusting each g_i a tiny bit we can assume that $g_i x_i = x_\infty$.

Hence, for every i we have the primitive vector $x_\infty \in g_i^{-1}\mathbf{Z}^2$; on the other hand, $\mathrm{vol}(g_i^{-1}\mathbf{Z}^2) = 1$ and we can take it to be spanned by $\{x_\infty, v_i\}$ for v_i lying on the line perpendicular to x_∞ and of length $1/\|x_\infty\|$.



Finally, notice that all v_i must lie on the same level set for Q as G preserves the quadratic form, hence there are only finitely many possibilities for the v_i's, and therefore we obtain infinitely many pairs $(i \neq j)$ such that $g_i \mathbf{Z}^2 = g_j \mathbf{Z}^2$. This yields infinitely many elements $g_i g_j^{-1} \in \mathrm{SO}_{Q,\mathbf{Z}}(\mathbf{Z})$, completing the proof. □

Remark 3.1.4. In the last step we used crucially the assumption that our original choice of $g_i \to \infty$; otherwise, when we "wiggled" the g_i to send x_i to x_∞ we could have made them the same.

Let's summarize the proof: we look at all automorphisms of Q, then firstly we notice that $G.[\mathbf{Z}^2]$ is precompact, then by discreteness arguments we prove that the orbit $G.[\mathbf{Z}^2]$ is closed, rather than just almost closed.

Remark 3.1.5. This proof is in fact constructive, because it uses lattice reduction theory for which the LLL algorithm is available. In fact, implementing the algorithm involved in the proof is equivalent (in terms of complexity) to all other algorithms to find solutions.

We will generalize the above proof to a constructive argument.

Exercise 3.1.6. Make the proof effective by showing that the smallest nontrivial solution (x, y) to Pell's equation satisfies

$$\log|x| + \log|y| \leq Cd.$$

In fact, the best bound is $C\sqrt{d}$, which can be obtained from the proof if one is very careful.

Remark 3.1.7. Answering a question of Arnav. The orbit $G.[\mathbf{Z}^2]$ gives a closed circle inside the space of 2-dimensional lattices. Projecting to the usual fundamental domain gives a closed orbit of the geodesic flow, after changing coordinates.

3.2. **Three generalizations.** We give three generalizations of the setup above, the last one being a theorem of Mostow and Tamagawa.

Suppose first that $Q : \mathbf{Z}^n \longrightarrow \mathbf{Z}$ is a quadratic form such that $Q(\mathbf{Z}^n - \{0\}) \neq 0$, or equivalently Q is $\mathbf{Q}$-anisotropic.

Proposition 3.2.1. *If* $\mathrm{SO}_Q(\mathbf{Z})$ *is large enough, the quotient* $\mathrm{SO}_Q(\mathbf{R})/\,\mathrm{SO}_Q(\mathbf{Z})$ *is compact for the quotient topology.*

One way that $\mathrm{SO}_Q(\mathbf{Z})$ can be infinite is when Q is indefinite.

Remark 3.2.2. Nonetheless, for an indefinite quadratic form Q, the anisotropicity condition can only happen for $n \leq 4$. This follows from the general theory of quadratic forms, which we will talk about later in the course.

Proof. We prove compactness of $Y = \mathrm{SO}_Q(\mathbf{R})/\,\mathrm{SO}_Q(\mathbf{Z})$. Start by defining

$$\begin{aligned} \iota : Y \colon &\to \{\text{lattices in } \mathbf{R}^n\} = \mathrm{GL}_n(\mathbf{R})/\,\mathrm{GL}_n(\mathbf{Z}) \\ g &\mapsto g[\mathbf{Z}^2]. \end{aligned}$$

We claim that ι is a homeomorphism onto its image, and that $\iota(Y)$ is compact.

First, one proves that the closure $\overline{\iota(Y)}$ is compact: this works just like before. Indeed, for each $[L] \in \iota(Y)$ the restriction $Q|_L$ is anisotropic but $\mathbf{Z}$-valued, so $|Q| \geq 1$ on $L - \{0\}$. This guarantees that the points in $L - \{0\}$ are bounded away from zero. Mahler compactness criterion yields then that $\iota(Y)$ is precompact.

Then we prove that $\iota(Y)$ is closed. By definition of quotient topology, this means showing that $\mathrm{SO}_Q(\mathbf{R})\mathrm{GL}_n(\mathbf{Z})$ is closed inside $\mathrm{GL}_n(\mathbf{R})$, or equivalently $\mathrm{GL}_n(\mathbf{Z})\mathrm{SO}_Q(\mathbf{R})$ is closed inside $\mathrm{GL}_n(\mathbf{R})$.

Look then at the action of $\mathrm{GL}_n(\mathbf{R})$ on the space of quadratic forms on $\mathbf{R}^n$ with $\mathbf{Z}$-coefficients: the $\mathrm{GL}_n(\mathbf{Z})\cdot\mathrm{SO}_Q(\mathbf{R})$-orbit of Q is obviously the same as its $\mathrm{GL}_n(\mathbf{Z})$ orbit, call this D: this is a set of integral quadratic forms.

In fact, it turns out that $\mathrm{GL}_n(\mathbf{Z})\cdot\mathrm{SO}_Q(\mathbf{R})$ is the preimage of D under the orbit map

$$\begin{aligned}\mathrm{GL}_n(\mathbf{R}) &\longrightarrow \{\text{quadratic forms}\}\\ g &\longmapsto g.Q\end{aligned}$$

This shows that $\mathrm{GL}_n(\mathbf{Z})\cdot\mathrm{SO}_Q(\mathbf{R})$ is the preimage of the discrete set D under the continuous orbit map, hence it is closed.

Proving that ι is an homeomorphism onto its image is left as an exercise to the reader. □

The general context is the following: given an algebraic group G (e.g. GL_n) and a subgroup H (e.g. SO_Q) we can understand G/H by finding a representation $\rho : G \longrightarrow \mathrm{GL}_N$ (e.g. GL_n acting on quadratic forms) and a line $\ell \subset \mathbf{A}^N$ whose stabilizer is H. The fact that such a pair (ρ,ℓ) always exists is a theorem of Chevalley. We obtain in particular an embedding

$$G/H \hookrightarrow \mathbf{P}^{N-1}$$

into projective space. (If H is semisimple, e.g. SO_Q, then it will fix ℓ pointwise and furnish an embedding into affine space.)

Let us recap the argument to prove infinitude of solutions to Pell's equation for non-square d, so that it will be easier to generalize it. Let d be a non-square integer, and $Q(x,y)=x^2-dy^2$, so that

$$\mathrm{SO}_Q=\left\{\begin{bmatrix} a & b\\ db & a\end{bmatrix} \mid a^2-db^2=1\right\}$$

and we want to show that $|\mathrm{SO}_Q(\mathbf{Z})|=\infty$.

Look at the $\mathrm{SO}_Q(\mathbf{R})\cong\mathbf{R}^*$-orbit of $[\mathbf{Z}^2]$:

Step 1. We show that the orbit is precompact, by using the fact that $Q(g[\mathbf{Z}^2])$ takes integral values, hence they are bounded away from zero.

Step 2. A discreteness argument together with the precompactness proved in the previous step shows that the orbit "closes up" by using integrality again.

This argument generalizes immediately to the following result:

Proposition 3.2.3. *Let* **Q** *be an integral quadratic form such that* $Q(x)\neq 0$ *for each* $x\in\mathbf{Z}^n-\{0\}$*, then the* $\mathrm{SO}_Q(\mathbf{R})$*-orbit of* $[\mathbf{Z}^n]$ *is compact, i.e.* $\mathrm{SO}_Q(\mathbf{R})/\mathrm{SO}_Q(\mathbf{Z})$ *is compact. In particular,* $\mathrm{SO}_Q(\mathbf{Z})$ *is an infinite group.*

Proof. Step 1. Works precisely as above.

Step 2. We outline the discreteness argument: we want to show that $\mathrm{SO}_Q(\mathbf{R})\mathrm{GL}_n(\mathbf{Z})$ is closed in $\mathrm{GL}_n(\mathbf{R})$, we show instead that $\mathrm{GL}_n(\mathbf{Z}) \longrightarrow \mathrm{GL}_n(\mathbf{R})/\,\mathrm{SO}_Q(\mathbf{R})$ is closed. The target space $\mathrm{GL}_n(\mathbf{R})/\,\mathrm{SO}_Q(\mathbf{R})$ is - up to replacing $\mathrm{SO}_Q(\mathbf{R})$ with $\mathrm{O}_Q(\mathbf{R})$ which does not influence closedness of the image of $\mathrm{GL}_n(\mathbf{Z})$ - the space of quadratic forms in $\mathbf{R}^n$.

The image of $\mathrm{GL}_n(\mathbf{Z})$ consists then of the integral quadratic forms, which is discrete inside the the space of all quadratic forms.

□

Let us now discuss more examples where generalizations of the above argument go through.

Example 3.2.4 (Dirichlet unit theorem). Let $F/\mathbf{Q}$ be a number field with ring of algebraic integers $\mathcal{O}_F$. Then the inclusion

$$\mathcal{O}_F^* \subset \left\{x \in (F \otimes \mathbf{R})^* \,|\, \mathbf{N}(x) = \pm 1\right\}$$

is co-compact, i.e. the quotient space is compact.

In particular, unless $F = \mathbf{Q}(\sqrt{d})$ for $d < 0$, the ring of integers $\mathcal{O}_F$ has infinitely many units.

Remark 3.2.5. Notice that this encompass our previous setting of the Pell's equation, by setting $F = \mathbf{Q}(\sqrt{d})$ and then $\mathcal{O}_F \supset \mathbf{Z}[\sqrt{d}]$ with

$$\mathbf{Z}[\sqrt{d}]^* = \left\{a + b\sqrt{d} \,|\, a^2 - db^2 = 1\right\}.$$

We want to prove the Dirichlet unit theorem using our results on lattices: the argument will be the same as before, but replacing the quadratic form Q with the Norm form $\mathbf{N}$ on F.

Example 3.2.6. Let's work it out in a specific example, to make it as explicit as possible. Take $F = \mathbf{Q}(^3\sqrt{2})$, so that $\mathcal{O}_F = \left\{x +^3 \sqrt{2}y + z^3\sqrt{4} \,|\, x, y, z \in \mathbf{Z}\right\}$. The Dirichlet unit theorem implies that the rank of $\mathcal{O}_F^*$ is 2.

Consider the matrix of multiplication by $x + y^3\sqrt{2} + z^3\sqrt{4}$ on the $\mathbf{Q}$-basis $\{1,^3\sqrt{2}^3\sqrt{4}\}$ of F:

$$x\begin{bmatrix}1 & & \\ & 1 & \\ & & 1\end{bmatrix} + y\begin{bmatrix} & 1 & \\ & & 1\\ 2 & & \end{bmatrix} + z\begin{bmatrix} & & 1\\ 2 & & \\ & 2 & \end{bmatrix}$$

Its determinant is the norm

$$N(x + y^3\sqrt{2} + z^3\sqrt{4}) = x^3 + 2y^3 + 4z^3 - 6xyz.$$

We want to apply the previous reasoning where we replace Q by $\mathbf{N}$ and SO_Q by

$$G = \left\{x\begin{bmatrix}1 & & \\ & 1 & \\ & & 1\end{bmatrix} + y\begin{bmatrix} & 1 & \\ & & 1\\ 2 & & \end{bmatrix} + z\begin{bmatrix} & & 1\\ 2 & & \\ & 2 & \end{bmatrix}\right\} \cap \mathrm{SL}_3$$

Looking at the $G(\mathbf{R})$-orbit of $[\mathbf{Z}^3]$ yields a compact orbit, and hence $G(\mathbf{Z})$ is infinite, so that we have infinitely many solutions to $N(x+y^3\sqrt{2}+z^3\sqrt{4}) = x^3+2y^3+4z^3-6xyz = 1$.

Example 3.2.7 (*Division algebras*). Let D be a division algebra, and $\mathscr{O}_D$ an order in D: this is a $\mathbf{Z}$-subalgebra with the same dimension as D. Then $\mathscr{O}_D^*$ is co-compact inside $(D\otimes\mathbf{R})^*$.

The proof is exactly the same as in the case above: we never used commutativity of multiplication in the field F.

To clarify things, let's discuss some examples of division algebras. Let

$$D_{\alpha,\beta} = \left\{a+bi+cj+dk \,|\, a,b,c,d \in \mathbf{Q},\, i^2=\alpha, j^2=\beta, ij=-ji=k\right\}$$

for some $\alpha,\beta \in \mathbf{Q}^*$. This is a division algebra as long as α is not in the image of the Norm map from $\mathbf{Q}(\sqrt{\beta})$ to $\mathbf{Q}$.

Suppose $\alpha,\beta \in \mathbf{Z}$ - this can always be arrange since multiplying α by a square does not change the resulting division algebra, and same for β. Then in this setting the theorem says that taking the order $\mathscr{O}_D = \{a+bi+cj+dk \,|\, a,b,c,d \in \mathbf{Z}\}$ yields

$$\mathscr{O}_D^* = \left\{a+bi+cj+dk \,|\, a^2-\alpha b-\beta c^2+\alpha\beta d^2 = \pm 1\right\}$$

being infinite.

Remark 3.2.8. As mentioned before, the proof via reduction theory is in fact effective, that is to say one can find a solution by working through the proof.

Example 3.2.9. We construct now another example of division algebra. Let $L/\mathbf{Q}$ be a field extension with cyclic Galois group $\mathrm{Gal}(L/\mathbf{Q}) \cong \mathbf{Z}/n\mathbf{Z}$ and fix a generator σ of this Galois group. Take $\beta \in \mathbf{Q}^*$ and set

$$D = L\langle\tau\rangle$$

with relations

$$\tau x\tau^{-1} = \sigma(x) \forall x \in L \text{ and } \tau^n = \beta.$$

It turns out that D is a division algebra exactly when β is not in the norm group $\mathbf{N}(L^*) \subset \mathbf{Q}^*$.

Remark 3.2.10. Notice that this generalized the previous construction, which was obtained for $n=2$ by taking $L = \mathbf{Q}(\sqrt{\alpha})$.

By the way, if n is not prime, it could happen that the center of the division algebra D defined as above is larger than expected - this corresponds to $[D] \in \mathrm{Br}(\mathbf{Q})$ having order smaller than expected.

Theorem 3.2.11 (Mostow-Tamagawa theorem)**.** *Let $G/\mathbf{Q}$ be a reductive algebraic group. Then $G(\mathbf{R})/G(\mathbf{Z})$ is compact (equivalently, $G(\mathbf{A_Q})/G(\mathbf{Q})$ is compact) if and only if G is anisotropic.*

Remark 3.2.12. For general number fields F and a reductive algebraic group G/F, a similar statement can be deduced by using Weil restriction.

Let's recall the definition of anisotropic. All the examples discussed so far, e.g. SO_Q for Q an indefinite quadratic form and the Norm-1 units $D^{(1)}$ of a division algebra D are anisotropic.

Definition 3.2.13 (Anisotropic group). For our purpose, consider an embedding $G \hookrightarrow \mathrm{GL}_n$. Then G is *anisotropic* if it satisfies any of the equivalent conditions.

(1) No element $g \in G(\mathbf{Q})$ is unipotent except for the identity. Here an element $g \in G \subset \mathrm{GL}_n$ is unipotent if 1 is its only eigenvalue.
(2) No element of $\mathrm{Lie}(G)$ is nilpotent, except for 0.
(3) G contains no nontrivial split tori.

Proof of Mostow-Tamagawa theorem. We will sketch a proof of the "‘anisotropic to compact" direction.

In the example mentioned before we had a quadratic form $Q(x_1,\dots,x_n)$ and we considered the orbit of $[\mathbf{Z}^n]$ under the $\mathrm{SO}_Q(\mathbf{R})$-action on the space of lattices in $\mathbf{R}^n$. This time, we consider instead the action of G on {lattices in $\mathrm{Lie}(G)$}, after we have dealt with Z_G in a similar way as for the Dirichlet unit theorem.

Suppose $Z_G = 1$, and pick a fixed lattice $L^0 \subset \mathrm{Lie}(G)$; consider its G-orbit. The key fact is the following: for each nonzero $X \in \mathrm{Lie}(G)$, anisotropicity guarantees that the orbit of $g \in G(\mathbf{R})$ under conjugation is bounded away from 0, by the same version of the well-known statement

$$\text{If } X \in \mathrm{Mat}_{n\times n}, \text{ then } 0 \in \overline{\{gXg^{-1}\}}_{g\in\mathrm{GL}_n} \text{ if and only if } X \text{ is nilpotent.}$$

□

4. Diophantine inequalities

4.1. Margulis's Theorem.

Theorem 4.1.1 (Margulis)**.** *Let Q be an indefinite quadratic form in $n \geq 3$ variables which is irrational (that is to say, it's not a multiple of a rational form). Then $Q(\mathbf{Z}^n)$ is dense in* $\mathbf{R}$.

Before sketching the proof, we remark that this is false for $n = 2$!

Example 4.1.2. Let $Q(x,y) = (x-\sqrt{2}y)(x-\sqrt{3}y)$, we claim that the values of Q on $\mathbf{Z}^2$ are bounded below. Indeed, if $Q(x,y)$ were to be small for integers x,y, one of the two factors have to be small (but they cannot both be small since taking the difference yields $\left(\sqrt{2}-\sqrt{3}\right)y$ and y is in $\mathbf{Z}$).

For instance, suppose $x-\sqrt{2}y \approx 0$. Then rewriting

$$Q(x,y) = \frac{x^2-2y^2}{x+\sqrt{2}y}(x-\sqrt{3}y)$$

yields that

$$\frac{x-\sqrt{3}y}{x+\sqrt{2}y} \approx \frac{(\sqrt{2}-\sqrt{3})y}{2\sqrt{2}y} = \frac{\sqrt{2}-\sqrt{3}}{2\sqrt{2}}$$

and $Q(x,y)$ is approximately an integer multiple of it, which thus cannot be too small.

Proof. Recall that in the proof of infinitude of solutions to Pell's equation we showed that the $\mathrm{SO}_Q(\mathbf{R})$-orbit of $[\mathbf{Z}^2]$ was closed in the space of all lattices. Here the opposite happens: Margulis shows that

for $n \geq 3$, the orbit $\mathrm{SO}_Q(\mathbf{R})[\mathbf{Z}^n]$ is dense in $\{n\text{-dimensional lattices with volume }1\}$.

Assuming this, for every lattice L we can find $g \in \mathrm{SO}_Q(\mathbf{R})$ with $g\mathbf{Z}^n \approx L$. Choosing L to contain a vector v having $Q(v)$ as wanted, we can approximate it very closely with a vector $w \in g\mathbf{Z}^n$, but then $Q(w) \in Q(g\mathbf{Z}^n) = Q(\mathbf{Z}^n)$, proving the theorem.

To prove that the $\mathrm{SO}_Q(\mathbf{R})$-orbit of $[\mathbf{Z}^n]$ is dense when $n \geq 3$, Margulis uses crucially that for $n \geq 3$, the group $\mathrm{SO}_Q(\mathbf{R})$ contains unipotent elements. Fix then $0 \neq N \in \mathrm{Lie}\left(\mathrm{SO}_Q\right)$ a nilpotent element, and study the orbit $e^{tN}[\mathbf{Z}^n]$, which one can think of "orbit in the nilpotent direction". The importance of taking N to be nilpotent is to make sure that e^{tN} grows only polynomially in t. □

Remark 4.1.3. We can see that for $n = 2$ the proof fails since the $\mathrm{SO}_Q(\mathbf{R})$-orbit of $[\mathbf{Z}^2]$ is not dense, even if it may have horrible behaviour. Indeed, for $n = 2$ we have $\mathrm{SO}_Q(\mathbf{R}) \cong \mathbf{R}^*$ so quite evidently there are no unipotent elements besides the identity.

The general idea that we should keep from these examples is that to study quadratic forms on $\mathbf{Z}^n$, we can consider the SO_Q-action on $\mathbf{Z}^n$ inside the space of all lattices, and then study the shape of the orbit.

4.2. **Finiteness theorem for quadratic forms.**

As another application of reduction theory, we start by studying the number of quadratic forms.

Definition 4.2.1 (Discriminant of a quadratic form). Let $Q(x_1, \ldots, x_n) = \sum_{i,j} a_{i,j} x_i x_j$ be an integral quadratic form, so that $a_{i,j} \in \mathbf{Z}$. Equivalently, $Q(\vec{x}) = \vec{x}^T A \vec{x}$ for a symmetric matrix A such that $2A \in \mathrm{Mat}_n(\mathbf{Z})$. We define the *discriminant* of Q to be $\operatorname{disc} Q := \det(2A)$.

Example 4.2.2. For the binary quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ we obtain $A = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$ so that $\operatorname{disc} Q = \det(2A) = 4ac - b^2$.

The following theorem goes as back as Gauss for the cases of binary and ternary quadratic forms.

Theorem 4.2.3. *There are only finitely many integral quadratic forms of discriminant* $\operatorname{disc} Q = D \neq 0$*, up to equivalence (where by equivalence we mean integral change of coordinates, that is to say, up to* $\mathrm{GL}_n(\mathbf{Z})$*-action).*

Remark 4.2.4. Later on we will explicitly count the number of quadratic forms of discriminant D by using the mass formula, but it's nice to know a priori that there are finitely many.

Proof. Suppose first that Q is positive definite: in this case the theorem is a direct consequence of reduction theory.

Applying reduction theory to $(\mathbf{Z}^n, Q)$, find an (A, B)-reduced basis $\{v_1, \ldots, v_n\}$ for $\mathbf{Z}^n$ with the property that

$$\|v_1\| \cdot \ldots \cdot \|v_n\| \asymp_{n,A,B} \mathrm{vol}_Q(\mathbf{Z}^n).$$

The notation $\mathrm{vol}_Q(\mathbf{Z}^n)$ means the volume of the standard lattice $\mathbf{Z}^n$ with respect to the quadratic form Q. In fact, all lengths $\|v\| = \|v\|_Q = \sqrt{Q(v)}$ are computed with respect to Q. For instance if $Q = ax^2 + cy^2$, then $\mathrm{vol}_Q(\mathbf{Z}^2) = \sqrt{ac}$.

In general we have

$$\mathrm{vol}_Q(\mathbf{Z}^n) = \sqrt{\operatorname{disc} Q} \cdot 2^{-n/2}$$

where the power of 2 has been introduced by our scaling (passing from A to $2A$ when defining $\operatorname{disc} Q$), but after all we do not care about constants only depending in n, so we get

$$\|v_1\| \cdot \ldots \cdot \|v_n\| \asymp_{n,A,B} \sqrt{\operatorname{disc} Q}. \tag{4.2.1}$$

Now the $Q(v_i)$'s are nonzero positive integers (by definiteness), so they are bounded below. On the other hand, (4.2.1) shows that they are also bounded above by $C_n\sqrt{\operatorname{disc} Q}$. By Cauchy-Schwarz obtain then that

$$\left|\langle v_i, v_j\rangle\right| \le \|v_i\| \cdot \|v_j\| \le \left(C_n\sqrt{\operatorname{disc} Q}\right)^2 = C_n^2 \operatorname{disc} Q$$

We have then a reduced basis $\{v_i\}$ such that with respect to it, $Q(x) = \sum_{i,j} a_{i,j} x_i x_j$ and $a_{i,J} = \left|\langle v_i, v_j\rangle\right| \le C \operatorname{disc} Q$. Hence there are finitely many possibilities for Q of bounded discriminant.

Remark 4.2.5. We will see later using the mass formula that the number of definite quadratic forms in dimension n of fixed discriminant $\operatorname{disc} Q = D$ grows as n^{n^2}. There was some explanation using a model via $n \times n$ matrices, which explains the n^2 exponent.

Suppose now that Q is indefinite. It turns out that for each fixed signature the number of quadratic form is bounded independently of n! One can see that as a consequence of strong approximation. This uniform bound comes out as a consequence of the fact that for many different quadratic forms $Q(x_1, \ldots, x_n)$ in n variables, adding two more by setting $\widetilde{Q} = Q(x_1, \ldots, x_n) - x_{n+1}^2 - x_{n+2}^2$ makes them become equivalent.

Since the result in the indefinite case is so different, we should not expect the proof of the definite case to go through. Where does it break? Well, we used definiteness crucially in the previous case when we claimed that the $Q(v_i)$ were bounded below. This clearly fails in the indefinite case, so we have to use a new argument.

The following argument is due to Hermite: the idea is to *replace Q by a positive definite quadratic form Q_+ having the same discriminant* and run the previous argument on that. More precisely, in suitable coordinates (after a *real* change of variables) we have

$$Q(x_1, \ldots, x_n) = \sum_{i \le p} x_i^2 - \sum_{i > p} x_i^2,$$

so we take

$$Q_+(x) = \sum_{i \le p} x_i^2 + \sum_{i > p} x_i^2.$$

Obviously $Q_+ \ge |Q|$ and since we only swapped a few signs in the formula, we have $\operatorname{disc} Q_+ = |\operatorname{disc} Q| = |D|$, but now Q_+ is not necessarily integral. At any case, we can run the same argument as in the previous step, and for a reduced (A, B)-basis $\{v_1, \ldots, v_n\}$ for Q_+, certainly $\|v_i\|_{Q_+} \ge |Q(v_i)|^2 \in \mathbf{Z}$.

Suppose now that $Q(v_i) \ne 0$ for each v_i. Then as before we get that $\|v_i\|_{Q_+}$ is bounded below, and that is all that we needed in the previous step to conclude that there were only finitely many forms Q_+ of the given discriminant, hence finitely many Q's.

We run a separate argument in the case that $Q(v) = 0$ for some nonzero $v \in \mathbf{Z}^n$. The general idea in the indefinite case is to find a vector of short length (with respect to the given form) and then break it off, splitting the lattice in two pieces, where we can apply induction.

Define

$$\langle x, y\rangle_Q := Q(x+y) - Q(x) - Q(y)$$

a bilinear form whose matrix is $2A$, where $Q(x) = x^T A x$.

We can then find a vector $a \in \mathbf{Z}^n$ such that $\langle v, a\rangle = \det(2A) = \operatorname{disc} Q$, since $(2A)\mathbf{Z}^n$ has index $\det(2A)$ in $\mathbf{Z}^n$, hence it contains $\det(2A)\mathbf{Z}^n$.

We look at the collection of vectors $a + tv \in \mathbf{Z}^n$ for $t \in \mathbf{Z}$: since

$$Q(a+tv) = Q(a) + t^2 Q(v) + t\langle a, v\rangle = Q(a) + t \cdot \det(2A),$$

for a suitable choice of t we obtain

$$0 < Q(a+tv) \leq |\det(2A)| = |\operatorname{disc} Q|.$$

We obtain then a vector $v' = a + tv$ such that roughly speaking, splitting $\mathbf{Z}^n = \langle v'\rangle \oplus \langle v'\rangle^\perp$ and inducting on the dimension gives the claim.

More precisely, by an integral change of coordinates we can assume that $v' = (1, 0, \dots, 0)$, and then $Q(x_1, \dots, x_n) = \alpha x_1^2 + x_1 l(x_2, \dots, x_n) + \widetilde{Q}(x_2, \dots, x_n)$ where $0 < \alpha \leq |\operatorname{disc} Q|$, and $l(x_2, \dots, x_n)$ is a linear form. Using a change of coordinates of the form

$$\begin{aligned} x_1 &\mapsto x_1 + \widetilde{l}(x_2, \dots, x_n) \\ x_2 &\mapsto x_2 \\ &\vdots \\ x_n &\mapsto x_n \end{aligned}$$

we can assume that the linear form l has all coefficients between 0 and 2α. Multiplying the equation for $\widetilde{Q}$ by $4a$, we find that

$$4aQ = (2ax_1 + L)^2 + Q''(x_2, \dots, x_n).$$

Now we have

$$\operatorname{disc} Q'' = \frac{(4a)^n \operatorname{disc} Q}{4(2a)^2}.$$

By induction there are finitely many possibilities for Q'' up to linear equivalence.

□

Remark 4.2.6. The argument in the indefinite case seems to suggest that there are many indefinite quadratic forms, but we know this is not the case.

5. Volume of the space of lattices

5.1. **Overview.** In this section we discuss measures and volumes on the space of lattices. One of the main theorems is the following.

Theorem 5.1.1. *There exists a unique probability measure on the space*

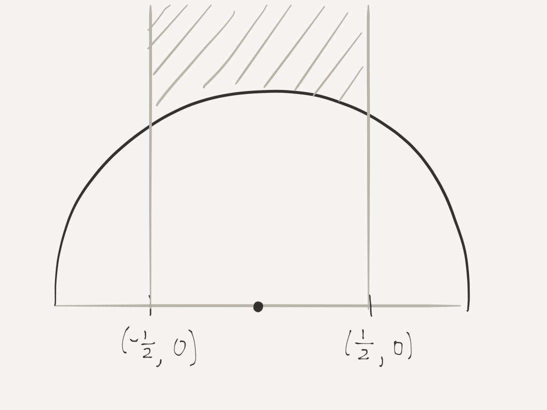
$$\{\text{volume-1 lattices on } \mathbf{R}^n\} = \mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z})$$

that is invariant by $\mathrm{SL}_n(\mathbf{R})$.

In other words, there exists a canonical notion of ’‘random lattice in $\mathbf{R}^n$” as long as we normalize the volume.

Remark 5.1.2. This is remarkable since the space of volume-1 lattices is not compact, yet the existence of an invariant probability measure means that it is “bounded” in some sense.

Before proving this, let us go back to our favorite example. Take $n=2$ so that after rotating and scaling the space $\mathrm{SL}_2(\mathbf{R})/\mathrm{SL}_2(\mathbf{Z})$ thought of the space of lattices $\mathbf{Z}(1,0)+\mathbf{Z}(x,y)$



The probability measure of the theorem turns out to be $\frac{\mathrm{d}x\,\mathrm{d}y}{y^2}\frac{3}{\pi}$, where the last factor is just to normalize the measure to have volume 1.

Recall the situation of Question 1.2.1: given a large prime p, we can choose $1\le\lambda\le p-1$ at random, and then take the volume-1 lattice

$$L_{\lambda,p}=\frac{\{(x,y)\in\mathbf{Z}^2\,|\,x\equiv\lambda y \mod p\}}{\sqrt{p}}.$$

This corresponds to sampling from the probability measure.

Denoting by δ_L the Dirac’s δ at the lattice L (a point in our space of all lattices), we have that

$$\frac{\sum_{\lambda=1}^{p-1}\delta_{L_{\lambda,p}}}{p}\to\mu \qquad \text{as } p\to\infty$$

where μ is the probability measure given by the theorem. In fact, one can verify computationally the above statement by plotting the distribution of the lattices $L_{\lambda,p}$ for large primes p.

The smallest solution to $x\equiv\lambda y$ corresponds to the y-coordinate, so the probability distribution function mentioned on day 1 already tells us that the lattices become scarcer as we increase the y-coordinate, a fact confirmed by the limit measure $\mu=\frac{\mathrm{d}x\,\mathrm{d}y}{y^2}\frac{3}{\pi}$.

5.2. **Haar measure.** By measure on a space X we will always mean a continuous functional on the space of compactly supported continuous functions $C_c(X)$.

Theorem 5.2.1. *On any Lie group G there exists a unique (up to scaling) measure μ which is invariant by left translation: that is to say, for any measure set $S \subset G$, we have $\mu(S) = \mu(gS)$ for any $g \in G$.*

In particular we will be interested in the case $G = \mathrm{SL}_n(\mathbf{R})$.

Example 5.2.2. Before giving the proof, let's make it explicit in the case of $\mathrm{SL}_2(\mathbf{R})$. Write

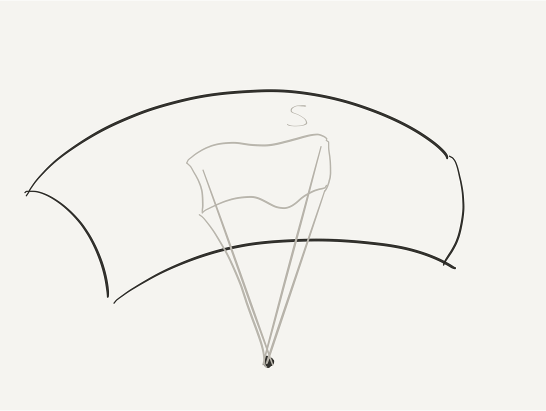
$$g^{-1}\,\mathrm{d}g = \begin{bmatrix} x & y \\ z & w \end{bmatrix}^{-1} \begin{bmatrix} \mathrm{d}x & \mathrm{d}y \\ \mathrm{d}z & \mathrm{d}w \end{bmatrix} = \begin{bmatrix} v_1 & v_2 \\ v_3 & v_4 \end{bmatrix}$$

where v_i are four left-invariant 1-forms on G, hence wedging any three of them will give a left invariant 3-form, i.e. a volume form. For instance $v_1 \wedge v_2 \wedge v_3 \neq 0$ works.

Once we have a (left-invariant) volume form ω, we can get a (left-invariant) measure μ_ω by setting

$$\int f\,\mathrm{d}\mu_\omega := \int f \cdot \omega.$$

Even more explicitly, here's how you compute measures for $\mathrm{SL}_2(\mathbf{R}) = \{A \in \mathrm{Mat}_2(\mathbf{R}) \mid \det A = 1\}$: draw $\mathrm{SL}_2(\mathbf{R})$ as the relevant hypersurface in $\mathbf{R}^4$, and let $S \subset \mathrm{SL}_2(\mathbf{R})$ be a nice set. Draw the cone over S with vertex at the origin: the volume of S with respect to the invariant Haar measure on $\mathrm{SL}_2(\mathbf{R})$ is the volume of that cone.



Recall that the goal is to understand the shape and size of $G(\mathbf{R})/G(\mathbf{Z})$ where G is a semisimple group. Just think $\mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z})$. We want to prove that there is a unique $\mathrm{SL}_n(\mathbf{R})$-invariant probability measure on $\mathrm{SL}_n\mathbf{R}/\mathrm{SL}_n\mathbf{Z}$. One should think of this as a boundedness type statement. In particular, it implies that there is a sensible notion of "random lattice" (by contrast, there is no sensible notion of "random real number").

On a Lie group G, there exists a uinque up to scaling left-invariant measure. For existence, one takes an invariant differential form ω_L; then the associated measure $|\omega_L|$ is invariant. For uniqueness, suppose ν is a left-invariant measure. If

$$\nu = f(g)|\omega_L|$$

for a function f (where we need absolute continuity of ν with respect to $|\omega_L|$ to rule out something like a δ-function), then clearly f needs to be a left-invariant function, hence constant.

Why is ν absolutely continuous with respect to $|\omega_L|$? (i.e. if something has measure 0 for ν then it also does for $|\omega_L|$). This is left as an exercise.

Left vs right Haar measure. For $\mathrm{SL}_n\,\mathbf{R}$, we have $\mu_L = \mu_R$ but not in general.

Example 5.2.3. Consider

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \right\}.$$

Then we have

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix}.$$

The right-invariant measure is $\frac{da}{a}db$, since a was changed by a dilation and b was changed by a translation.

On the other hand, the left-invariant measure is $\frac{1}{a}\frac{da}{a}db$ because the b' is also being scaled, by a.

In general, the left and right Haar measures are related by the formula

$$\mu^R = \mu^L(g \mapsto \det \mathrm{Ad}(g))$$

where $\mathrm{Ad}(g)X = gXg^{-1}$. In the preceding example,

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} x & ay \\ 0 & 0 \end{pmatrix}$$

so the determinant of $\mathrm{Ad}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ is a. This matches up ith what we found.

It is easy to see why this is the case: μ^R comes from a right-invariant differential form, μ^L comes from a left-invariant differential form, and they differ by conjugation. That is, to get from e to g you could left multiply by g and right multiply by g, and these differ by conjugation.

In particular, for the group of upper triangular matrices

$$\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \begin{pmatrix} 1 & & \\ & 1 & \\ n_{ij} & & 1 \end{pmatrix}.$$

the left-invariant measure is

$$\mu^L = \frac{da_1}{a_1} \cdots \frac{da_n}{a_n} \prod_{i>j} n_{ij}$$

and the right-invariant measure is

$$\mu^R = \frac{da_1}{a_1} \cdots \frac{da_n}{a_n} \prod_{i>j} n_{ij} \underbrace{\prod_{i>j} \frac{a_i}{a_j}}_{\det \mathrm{Ad}(g)}.$$

Note that by Gram-Schmidt / Iwasawa Decomposition / QR decomposition, every $\in \mathrm{GL}_n(\mathbf{R})$ is uniquely expressible as

$$kan$$

where $k \in O_n(\mathbf{R})$, a is diagonal, and n is lower triangular unipotent (to make this unique we adopt the convention that by absorbing signs into k, all the entries of a are positive). Write $an = b$. In coordinates $q = kb$, we have that the right Haar measure is

$$\text{right Haar measure} = d^L k \cdot d^R b.$$

This is surprising because the kb decomposition is not a direct product of groups (the k and b factors don't commute). This is surprisingly hard to show directly, but we can argue as follows.

Proof. Let dg be a left (right) Haar measure on G. Then we have

$$\text{right Haar measure} = d^L k \cdot d^R b = f(g)\, dg$$

for some f. Here we are using that the left side is absolutely continuous with respect to dg because the map $K \times B \to G$ is a diffeomorphism. Whatever this measure is, it is left-invariant by K and right-invariant by b. Then $f(kb) = f(1)$ for all k and b, but everything in $\mathrm{GL}_n(\mathbf{R})$ is expressible in this form, so f is constant. □

For $\mathrm{SL}_n(\mathbf{R})$, the story is similar but the product only goes up to a_{n-1} since a_n is determined by the condition that the product be 1:

$$\text{(right Haar measure)} = d^L k \cdot \prod_{i=1}^{n-1} \frac{da_i}{a_i} \cdot \prod dn_{ij} \prod_{i>j} \frac{a_i}{a_j}$$

(the a_i are positive and signs are absorbed into k)

Finally we prove Theorem 5.1.1.

Proof. We will prove that $\mathrm{SL}_n \mathbf{R} / \mathrm{SL}_n \mathbf{Z}$ has a finite measure with respect to the Haar measure on $\mathrm{SL}_n \mathbf{R}$, so there exists a $\mathrm{SL}_n \mathbf{R}$-invariant probability measure.

Recall that we constructed an "approximate fundamental domain" $S_{A,B}$, which had the property that $S_{A,B} \cdot \mathrm{SL}_n \mathbf{Z} = \mathrm{SL}_n \mathbf{R}$ ("$S_{A,B}$ contains a fundamental domain"). We remind you that the construction was

$$S_{A,B} = \mathrm{SO}_n(\mathbf{R}) \cdot \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \begin{pmatrix} 1 & \\ 1 & \\ n_{ij} & 1 \end{pmatrix}$$

with $|a_i/a_{i+1}| \geq A$ and $|n_{ij}| \leq B$. The $\mathrm{SO}_n(\mathbf{R})$ is compact and the unipotent factor is too, so it suffices to study the measure of the center factor, which is

$$\int_{\substack{a_1 \dots a_n = 1 \\ a_i/a_{i+1} \geq A}} \prod_{i=1}^{n-1} \frac{da_i}{a_i} \prod_{i>j} \frac{a_i}{a_j}.$$

Example 5.2.4. For $n=3$, this is explicitly

$$\int_{\substack{a_1/a_2\geq A\\ a_2/a_3\geq A\\ a_1a_2a_3=1}} \frac{da_1}{a_1}\frac{da_2}{a_2}\left(\frac{a_2}{a_1}\right)\left(\frac{a_3}{a_2}\right)\left(\frac{a_3}{a_1}\right)$$

Making the change of coordinates $x=\frac{a_1}{a_2}, y=\frac{a_2}{a_3}$, we can rewrite this as

$$\int_{x\geq A; y\geq A}\frac{dx}{x}\frac{dx}{y}\frac{1}{xy(xy)}$$

which is evidently convergent. This reflects the general behavior; without the modular function the thing is barely divergent, and this pushes it to being convergent.

□

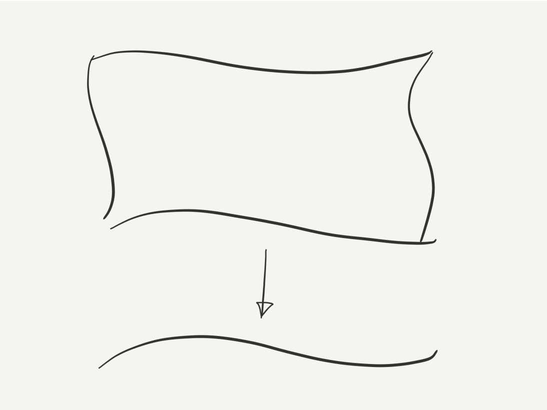
Remark 5.2.5. It might seem like thereis an asymmetry between left and right here. It comes from the fundamental domain. Recall that $S_{A,B}$ was defined by parametrizing the reduced basis as $v_1,\dots,v_n$ and the orthogonalized version as $\overline{v_1},\dots,\overline{v_n}$. These were related

$$\begin{pmatrix} v_1 & \dots & v_n\end{pmatrix} = \begin{pmatrix}\overline{v_1} & \dots & \overline{v_n}\end{pmatrix} \text{(lower triangular)}$$

which is why the order kan was forced upon us.

Remark 5.2.6. In fact, for a natural choice of Haar measure the volume is $\zeta(2)\cdot\zeta(3)\cdot\ldots\cdot\zeta(n)$.

5.3. **Fibral measures.** Suppose $f\colon X\to Y$ is a submersion of manifolds.

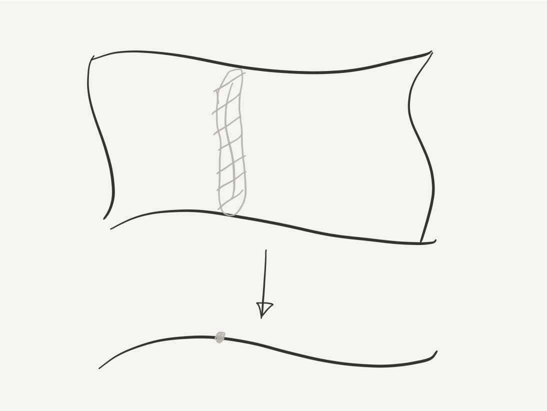


If we have a volume form ω_X on X and a volume form ω_Y on Y, then we can form a "quotient" volume form ω_F on each fiber $F_y := f^{-1}(y)$ which is characterized by the property that for any function G on X,

$$\int G\omega_X = \int_Y\left(\int_{f^{-1}(y)} G\omega_{f^{-1}(y)}\right)\omega_Y.$$

Explicitly, if $S \subset X$ is a nice subset then the fiber measure of $S \cap f^{-1}(y)$ is the limit over small balls $B \ni y$ of

$$\frac{\text{measure}_X \text{ of } S \cap f^{-1}(B)}{\text{measure}_Y \text{ of } B}$$



This means that if v is a differential form of degree X of degree $\dim X - \dim Y$ such that

$$v \wedge f^* \omega_Y = \omega_X$$

then the $\omega_{f^{-1}(y)}$ are obtained by restricting v to $f^{-1}(y)$.

Example 5.3.1. Consider

$$\det \colon X = \mathrm{GL}_n \mathbf{R} \to \mathbf{R}^* =: Y.$$

Then $\det^{-1}(1) = \mathrm{SL}_n \mathbf{R}$. What is the Haar measure on $\mathrm{GL}_n \mathbf{R}$? It is not dM_{ij}, since for insance this is obviously not invariant under multiplication by a scalar matrix; it is $\frac{dM_{ij}}{(\det M)^n}$. The measure on $\mathbf{R}^*$ is dy/y. So what we are saying is that the fiber measure can be obtained by taking any v_{n^2-1} on $\mathrm{GL}_n \mathbf{R}$ such that $v_{n^2-1} \wedge d(\det) = \frac{dM_{ij}}{(\det M)^n}$ (where by $d(\det)$ we mean $\det^* dy/y$). Then $v|_{\mathrm{SL}_n \mathbf{R}}$ gives the "fiber" form.

For instance, on $\mathrm{SL}_2 \mathbf{R}$ we are looking for a 3-form such that

$$v_3 \wedge d(xw - yz) = \frac{dx \wedge dy \wedge dz \wedge dw}{\det^2}.$$

Here $d(xw - yz) = x\,dw + w\,dz - y\,dz - z\,dy$, so such a v_3 is

$$v_3 = \frac{dy \wedge dz \wedge dw}{x}.$$

This defines a Haar measure on $\mathrm{SL}_2 \mathbf{R}$.

Example 5.3.2. Let's go back to the example of Pell's equation

$$x^2 - Dy^2 = 1.$$

Earlier we estimated the number of solutions with $x \leq T$ to be $\approx \frac{\log T}{\sqrt{d}}$. The heuristic for this was that the number of solutions should be the area of the narrow strip around hyperbola $0.5 < x^2 - Dy^2 < 1.5$

This is a little arbitrary though, because of the choice of endpoins 0.5 and 1.5. Really we don't care how the function behaves away from 1, so it would be better to consider

$$\frac{\{1-\epsilon < x^2 - Dy^2 < 1+\epsilon\}}{2\epsilon}$$

as $\epsilon \to 0$. This is the "fibral measure" of $\{x^2 - Dy^2 = 1 \mid 1 \leq x \leq T\}$ for the function $f\colon \mathbf{R}^2 \to \mathbf{R}$ sending $(x,y) \mapsto x^2 - Dy^2$.

How do we find this measure? We look for a 1-form v on $\mathbf{R}^2$ satisfying

$$v \wedge (2x\,dx - 2Dy\,dy) = dx \wedge dy$$

and restrict this to the hyperbola. For instance, we can take $v = \frac{dx}{2Dy}$. (By the way, this form restricted to the hyperpbola $x^2 - dy^2 = 1$ is invariant under $\mathrm{SO}(x^2 - dy^2)$, basically by construction.) So

$$2\int_1^T \frac{dx}{2Dy} = \int_1^T \frac{dx}{Dy} \approx \frac{1}{\sqrt{D}} \int_1^T \frac{dx}{x} = \frac{\log T}{\sqrt{D}}.$$

Remark 5.3.3. The general heuristic is that if you consider polynomial equations $f_1, \dots, f_n$ then the number of solutions to $f_i(x_1, \dots, x_n) = 0$ should be approximated in a similar manner. For spaces with many symmetries, e.g. homogeneous spaces, the formula has a tendency to be *exactly* correct - that is the magic of the *mass formula.*

5.4. **Integral Haar measure.** We computed earlier that for the Haar measure on $\mathrm{SL}_n \mathbf{R}$ the volume of $\mathrm{SL}_n \mathbf{R} / \mathrm{SL}_n \mathbf{Z}$ is finite. Now we will explain that there is a "canonical" choice of measure, and for it we will compute the volume to be

$$\mathrm{vol} = \zeta(2)\zeta(3)\dots\zeta(n)$$

and also heuristically explain why.

Let's go back to $\mathrm{SL}_n \mathbf{R}$ (Example 5.3.1). We wanted a form v such that

$$v \wedge (x\,dw + w\,dx - y\,dz - z\,dy) = dx\,dy\,dz\,dw$$

and one can take for instance

$$\frac{dydzdw}{w} \text{ or } \frac{dydzdx}{z} \text{ or } \dots$$

The general formula for $\mathrm{SL}_n \mathbf{R}$ is

$$\boxed{\omega = \frac{\prod_{1 \le i \le j} dx_{ij} \text{ (omitting } x_{k\ell})}{(\text{minor})_{k\ell}}.} \tag{5.4.1}$$

We have

$$\det = \sum x_{k\ell} (\text{minor})_{k\ell}$$

so

$$d(\det) = \sum dx_{k\ell} \wedge (\text{minor})_{k\ell} + \dots$$

and after after restricting to the $\mathrm{SL}_n \mathbf{R}$ the extra terms $\dots$ disappear.

Note that ω extends to an invariant differential form on $\mathrm{SL}_n / \operatorname{Spec} \mathbf{Z}$ (this is basically evident from the expression, since the sets with non-vanishing minors cover SL_n). The set of such forms is a free $\mathbf{Z}$-module of rank 1, and this ω is a generator for it. That determines ω up to sign. (If we had multiplied it by 7, then it would vanish modulo 7.)

Let's say this another way. Look at the tangent space $\mathrm{SL}_n \mathbf{R}$, which can be thought of as trace-free matrices in $M_n(\mathbf{R})$. This ω assigns volume 1 to the natural integral structure of trace-free matrices in $M_n(\mathbf{Z})$.

Theorem 5.4.1. *With the measure* $|\omega|$, *we have*

$$\operatorname{vol}(\mathrm{SL}_n \mathbf{R} / \mathrm{SL}_n \mathbf{Z}) = \zeta(2) \cdot \ldots \cdot \zeta(n).$$

Let's first give a heuristic explanation. We have $\mathrm{SL}_n(\mathbf{R}) \subset M_n(\mathbf{R})$ cut out by the equation $\det = 1$. Normalize the volume of $\mathrm{SL}_n \mathbf{R}$ using the volume form $|\omega|$. We want to estimate:

How many elements of $\mathrm{SL}_n \mathbf{Z}$ are there inside some large ball $B \subset \mathrm{SL}_n \mathbf{R}$?

In fact we will derive Theorem 5.4.1 by comparing two heuristics.

Heuristic 1. The answer should be $\frac{\operatorname{vol}(B)}{\operatorname{vol}(\mathrm{SL}_n \mathbf{R} / \mathrm{SL}_n \mathbf{Z})}$ (this is an analogue of the heuristic that the number of lattice points inside a ball $B \subset \mathbf{R}^n$ should be about $\operatorname{vol}(B) = \operatorname{vol}(B) / \operatorname{vol}(\mathbf{R}^n / \mathbf{Z}^n)$).

Heuristic 2. The number of points on the hyperbola is the fibral measure, which is just $\operatorname{vol}(B)$. This is the same reasoning as for Pell's equation. But we need a correction, because the current heuristic takes no account of mod N properties.

Example 5.4.2. Consider 2×2 matrices with $\mathbf{Z}/3$-coefficients. There are $3^4 = 81$ of them. The number with determinant 1 would be 27 if the determinants were uniformly distributed, but this is not quite right. The correct answer is

$$\frac{(3^2 - 1)(3^2 - 3)}{2} = 24.$$

Note that this differs from the "expected" value of 27, so this is telling us that the number of matrices with determinant 1 is "slightly less than expected". So we should correct the heuristic by $\frac{24}{27}$, because modulo 3 there is a slight repulsion away from determinant 1.

Remark 5.4.3. This heuristic goes back at least to Hardy-Littlewood; in analytic number theory it is known as *singular series.*

So let's figure out what the correction factors should be for all p. It should be

$$c_p = \frac{\#\{\text{matrices mod } p \text{ with det } 1\}}{p^{n^2}/p}.$$

The answer turns out to be

$$c_p = \left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^3}\right)\dots\left(1-\frac{1}{p^n}\right).$$

Remark 5.4.4. Strictly speaking, we should do the same with p replaced with p^k and take the limit as $k \to \infty$. This means that we take account of behavior modulo all powers of primes. This limit can be described as the fibral measure of $\mathrm{SL}_n \mathbf{Z}_p$ for the standard measure for $M_n(\mathbf{Z}_p) \xrightarrow{\det} \mathbf{Z}_p$, i.e. the $\mathbf{Z}_p$-analogue of ω. In this case the limits stabilize at $k = 1$, which is why we can get away with this simplified account.

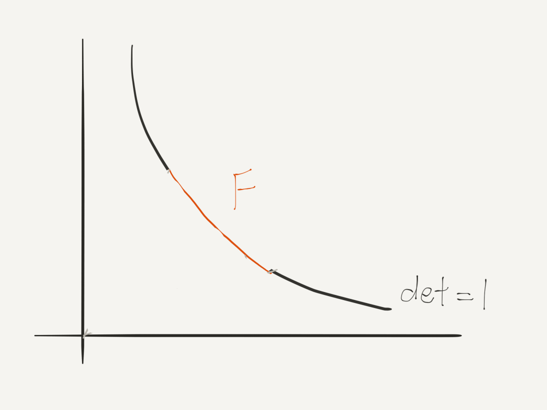
The conclusion is that

$$\begin{aligned}\prod_p c_p &= \prod_p \left(1-\frac{1}{p^2}\right)\prod_p\left(1-\frac{1}{p^3}\right)\dots\prod_p\left(1-\frac{1}{p^n}\right)\\ &= \zeta(2)^{-1}\zeta(3)^{-1}\dots\zeta(n)^{-1}.\end{aligned}$$

Comparing this with Heuristic 1 gives

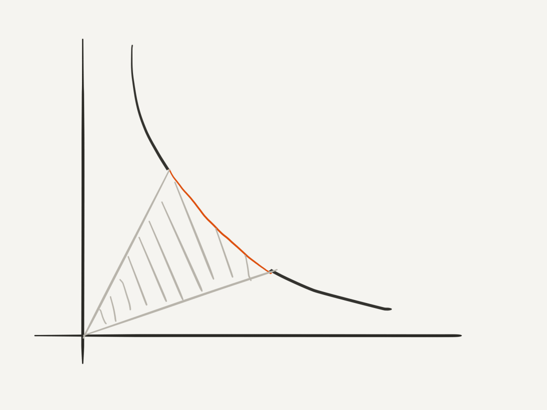
$$\mathrm{vol}(\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}) = \zeta(2)\cdot\zeta(3)\cdot\ldots\cdot\zeta(n).$$

Proof of Theorem 5.4.1. Consider a fundamental domain F for $\mathrm{SL}_n \mathbf{Z}$ (marked in red in the picture).

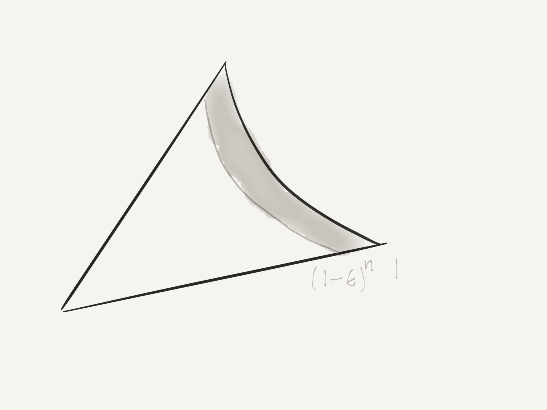


(We're going to pretend that F is compact, although it is not.) We're going to compute the volume of lattice points in F by computing the number of lattice points in an asymptotic scaling of it.

Let cone_F be the cone from the origin over F. As remarked in Example 5.2.2, we can also think of the Haar measure for SL_2 as computing the volume of the cone from the origin. This will be off from our canonical Haar measure by a scalar factor; what scalar is it?



We claim that the scalar is $1/n$, so that the volume of cone_F is $\mu(F)/n$. Why? Imagine the strip obtained by scaling F by the interval $(1-\epsilon, 1)$, which consists of matrices with determinant lying in $((1-\epsilon)^n, 1)$.



So the volume of the shaded region is $\approx \mu(F)(n\epsilon)$. Therefore, if we scale by the interval $(r(1-\epsilon), r)$ then the volume of $(r, r(1-\epsilon))F$ is $r^{n^2}\mu(F)(n\epsilon)$. Now we integrate over r: the volume of the full cone is

$$\text{vol}(\text{cone}_F) = \mu(F)n\int_0^1 r^{n^2}\frac{dr}{r} = \frac{\mu(F)}{n}.$$

So it suffices to show that the volume V of cone_F is $\frac{\zeta(2)\dots\zeta(n)}{n}$. To do this, we count lattices points in $[0,T]\cdot F$; this should closely approximate $\text{vol}([0,T]\cdot F)$. If we scale the cone by a factor of T, then its volume scales by T^{n^2}, so on one hand we have

$$\text{vol}([0,T]\cdot\text{cone}_F) = T^{n^2}V.$$

On the other hand, it should be approximately the number of lattice points $M_n(\mathbf{Z}) \cap [0,T]F$. (In general, for a compact domain the difference between the volume and the number of lattice points is the measure of a 1-neighborhood about the boundary.)

So how can we count the number of lattice points? We can think of $(0,X] \cdot \mathrm{SL}_n \mathbf{R}$ as the set of matrices with determinant in $(0,X^n]$. Then $(0,X] \cdot F$ is a fundamental domain for $\mathrm{SL}_n \mathbf{Z}$ acting on matrices with determinant $\leq X^n$, so $X^{n^2} V$ is approximately the number of matrices in $M_n(\mathbf{Z})$ with $1 \leq \det \leq X^n$ modulo the action of $\mathrm{SL}_n \mathbf{Z}$. We write this as

$$\sum_1^{X^n} A(k), \quad A(k) = \#\{M \in M_n(\mathbf{Z}) \mid \det M = k\}/\mathrm{SL}_n \mathbf{Z}.$$

So

$$V = \lim_{T \to \infty} \frac{\sum_{k=1}^T A(k)}{T^n}.$$

Lemma 5.4.5. *For $n = 2$,*

$$A(k) = \sum_{0<d|k} d$$

In general,

$$A(k) = \sum_{k=a_1 \ldots a_n; a_i \in \mathbf{N}} a_1^{n-1} a_2^{n-2} \ldots a_n^0.$$

Proof. $A(k)$ is the number of subgroups $L \subset \mathbf{Z}^n$ with index k. The reason is that given a matrix M, we can send it to the lattice $M \cdot \mathbf{Z}^n$. Since M has determinant k this has index k, and right translation by $\mathrm{SL}_n(\mathbf{Z})$ doesn't affect it.

For $n = 2$, any sublattice $L \subset \mathbf{Z}^2$ with index k is uniquely the span of $(a,0)$ (just taking the first multiple of $(1,0)$ lying in L) and (ℓ, b) where we can adjust ℓ to be in $[0,a)$ with $a,b > 0$. The index is ab, so the number of such things with index k is

$$\sum_{ab=k} a.$$

This works in general. For instance, how would this start off for $n = 3$? Any sublattice $L \subset \mathbf{Z}^3$ is uniquely the span of $(a,0,0)$, $(\ell,b,0)$, and (m,n,c) where $0 \leq \ell, m < a$ and $0 \leq n < b$.

□

Now we are reduced to computing

$$\frac{\sum_{k<T} A(k)}{T^n}.$$

The nicest way to do this is to write down a generating function. For $n = 2$, $A(k)$ is multiplicative, so it's useful to consider the Dirichlet series.

$$\begin{aligned}\sum \frac{A(k)}{k^s} &= \sum_k \frac{1}{k^s} \sum_{ab=k} a \\ &= \sum_{a,b\geq 1} \frac{a}{a^s b^s} \\ &= \sum \frac{1}{a^{s-1}} \sum \frac{1}{b^s} \\ &= \zeta(s-1)\zeta(s).\end{aligned}$$

In general, the result is

$$\sum \frac{A(k)}{k^s} = \zeta(s)\zeta(s-1)\ldots\zeta(s-n+1).$$

Let's rescale this a bit:

$$\sum \frac{A(k)/k^{n-1}}{k^s} = \zeta(s)\zeta(s+1)\ldots\zeta(s+n-1). \tag{5.4.2}$$

We expect the sum to have a limit, which means that $A(k)$ should be (at least on average) $\approx ck^{n-1}$. Just pretend for the moment that this is right. If so, then we would expect

$$\sum_k \frac{A(k)/k^{n-1}}{k^s} = \sum \frac{c}{k^s} = c\zeta(s).$$

If we slowly decrease the value of s, this becomes singular at $s = 1$ and the residue there is c, so this is nice for $s > 1$ but behaves like $\frac{c}{s-1}$ near $s = 1$. On the other hand, as $s \to 1$ the right hand side of (5.4.2) is

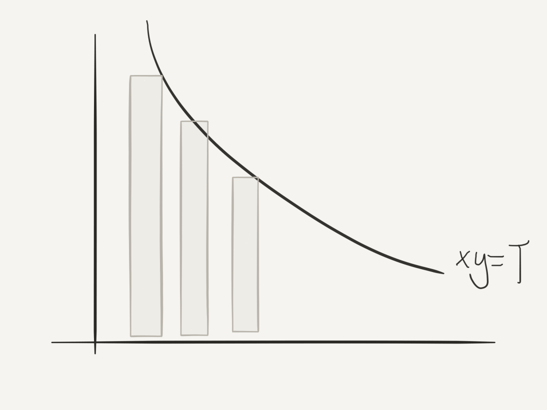
$$\zeta(s)\zeta(s+1)\ldots\zeta(s+n-1) \sim \frac{\zeta(2)\ldots\zeta(n)}{s-1}.$$

So this is telling us that $c = \zeta(2)\cdot\ldots\cdot\zeta(n)$. Of course we didn't prove it, but standard analysis makes this rigorous.

Let's just do this "by hand" for $n = 2$:

$$\sum_{k<T}\left(\sum_{ab=k} a\right).$$

You can think of this as the lattice points below the hyperbola $xy = T$.



We can count this by cutting it up into columns: the number of points with a given x-coordinate is

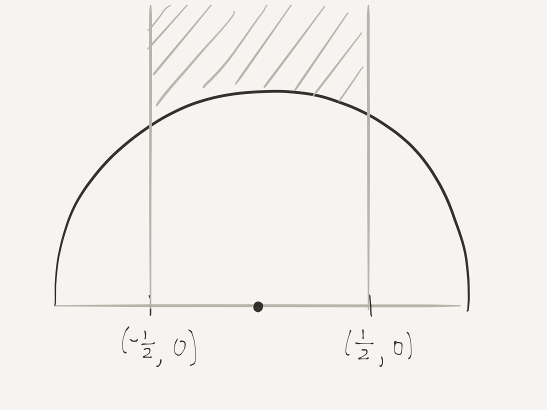
$$\sum_{1\le y\le T/x} y \approx (T/x)^2\frac{1}{2}$$

Adding this up over x yields

$$\approx \frac{1}{2}\sum_x \left(\frac{T}{x}\right)^2 = \frac{1}{2}T^2\cdot\zeta(2).$$

□

Let's do a consistency check for $n=2$. In this case we understand the space $\mathrm{SL}_2\,\mathbf{R}/\,\mathrm{SL}_2\,\mathbf{Z}$ by hand: $\{(x,y)\colon |x|\le 1/2, x^2+y^2\ge 1\}$ is the space of lattices in $\mathbf{R}^2$ up to rotation and scaling. (Compared with $\mathrm{SL}_2\,\mathbf{R}/\,\mathrm{SL}_2\,\mathbf{Z}$, we have collapsed the rotations.)



The point (x,y) corresponds to the lattice $\langle(1,0),(x,y)\rangle$. The fundamental domain (without collapsing rotations) is

$$\mathrm{SO}_2\,\mathbf{R}\times\begin{pmatrix}\sqrt{y} & 0\\ 0 & 1/\sqrt{y}\end{pmatrix}\times\begin{pmatrix}1 & 0\\ x & 1\end{pmatrix}$$

where $\{|x| \leq 1, x^2+y^2 \geq 1\}$. We explicitly parametrize the $\mathrm{SO}_2\,\mathbf{R}$ as

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \times \begin{pmatrix} \sqrt{y} & 0 \\ 0 & 1/\sqrt{y} \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$$

The measure μ in coordinates (θ, y, x) is $\frac{1}{2} d\theta \frac{1}{y} \frac{dy}{y} dx$ (the 1/2 coming from the square root), because the formula is to multiply a left Haar measure for K and a *right* Haar measure for the other thing. So the total measure is

$$\pi \int \frac{dx\,dy}{y^2}.$$

This turns out to be $\pi^2/3 = \zeta(2)/2$.

Exercise 5.4.6. What happened to the 1/2?

Remark 5.4.7. The same method works if we replace M_n by a field extension $K/\mathbf{Q}$. This gives a proof of the class number formula. (This is Dirichlet's original method.) If $(D \otimes \mathbf{R}) = M_n\mathbf{R}$, and $\mathscr{O}$ is an order in D, then the same reasoning (interpreting $\mathrm{SL}_n\,\mathbf{Z}$ as elements of determinant 1 in $M_n\mathbf{Z}$) gives

$$\mu(\mathrm{SL}_n\,\mathbf{R}/\mathscr{O}^{(1)}) = \frac{p}{q}\zeta(2) \cdot \ldots \cdot \zeta(n)$$

where $\mathscr{O}^{(1)}$ is the norm-1 units and $p/q \in \mathbf{Q}$.

5.5. **Application.** (This is in Seungki Kim's Ph.D. thesis.)

Earlier we defined the notion of (A, B)-reduced basis for a lattice L. There is a probability measure on the space of lattices and the number of reduced bases is always finite, so one can ask for instance:

> What is the number of $(A, 1/2)$-reduced bases for L?

The answer should be $\mathrm{vol}(S_{A,1/2})/\mathrm{vol}(\mathrm{SL}_n\,\mathbf{R}/\mathrm{SL}_n\,\mathbf{Z})$. The answer is that this is

$$\frac{2^n}{n!(n-1)!}\left(\frac{1}{A}\right)^{\frac{n^3-n}{6}} \frac{1}{\xi(2)\ldots\xi(n)}$$

where $\xi(s) = (\pi^{-s/2}\Gamma(s/2))\xi(s)$. Note that this grows as c^{n^3}, so the number of reduced bases grows extremely rapidly; they are nearly unique for $n = 2$ but highly non-unique in general.

Where do these factors come from? When computing the volume of $\mathrm{SO}_n\,\mathbf{R}$ with respect to the volume form which at the identity is given by $\prod_{i<j} dx_{ij}$, you get

$$\prod_{i=2}^{n}\left(\frac{2\pi^{i/2}}{\Gamma(i/2)}\right).$$

The factor $\left(\frac{2\pi^{i/2}}{\Gamma(i/2)}\right)$ is the surface area of a unit sphere in $\mathbf{R}^i$. This can be proved by successive fibering: SO_n acts on S^{n-1}, with stabilizer isomorphic to SO_{n-1}:

$$\begin{tikzcd}
\mathrm{SO}_{n-1} \arrow[r] & \mathrm{SO}_n\,\mathbf{R} \arrow[d] \\
 & S^{n-1}
\end{tikzcd}$$

The product has the formal structure of something like $\zeta(2)\ldots\zeta(n)$. This coincidence happens in all cases, up to powers of 2 which vary irregularly from case to case.

6. Sphere packing

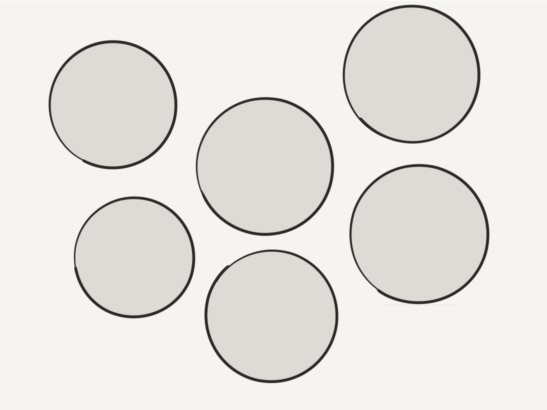
The question we want to consider is:

What is the largest density of packing of spheres of equal radius in $\mathbf{R}^n$*?*

Let's call this number ρ_n.

Lemma 6.0.1. *We have* $\rho_n \geq 2^{-n}$.

Proof. This is the "greedy bound": simply pack the spheres arbitrarily until no more fit.



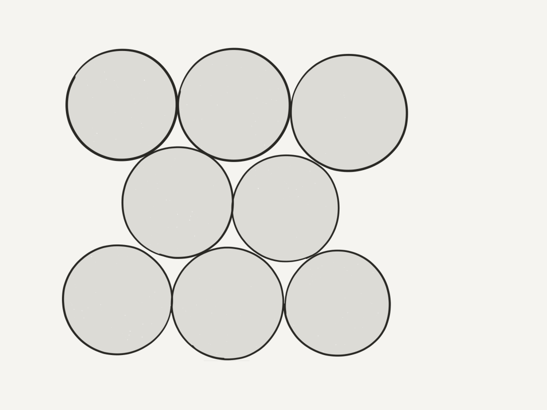
If the centers of the spheres are at x_i, then there does not exist y such that $|y - x_i| \geq 2$ for all i, or else we could fit a sphere centered at y. Therefore,

$$\bigcup B(x_i, 2)$$

cover $\mathbf{R}^n$. So if we shrink them by a factor of $1/2$, then their density is at least $1/2^n$. □

This is very crude; it is just to normalize our expectations. In large dimensions it is hard to pack spheres! We won't be able to do much better.

6.1. **Low-dimensional packings.** In 2 dimensions, the best packing is



(This is the lattice packing for the lattice A_2.) It has density

$$\rho_2 = \frac{\pi}{2\sqrt{3}} > 0.9.$$

This is a *lattice packing*, which is a packing whose centers form a lattice.

The packing associated to a lattice $L \subset \mathbf{R}^n$ is described as follows. The balls with radius R centered at the lattice points are disjoint if and only if $L \cap B_{2R} = \{0\}$. The sphere packing associated to L is obtained by taking the largest possible value of R (which is the half the length of the shortest vector).

Example 6.1.1. If $L = \mathbf{Z}^n$ then $2R = 1 \implies R = 1/2$, so the sphere packing is

$$\bigcup_{v \in \mathbf{Z}^n} (V + B_{1/2}),$$

so the density is

$$\text{vol}(B_{1/2}) = \frac{\pi^{n/2}}{(n/2)!} \left(\frac{1}{2}\right)^n.$$

Note that this is asymptotically terrible because $\frac{\pi^{n/2}}{(n/2)!}$ scales like n^{-n}. (A "typical" lattice is much better.)

Example 6.1.2. The D_n lattice is $\{(x_i) \in \mathbf{Z}^n \mid \sum x_i \text{ even }\}$. Let's compute the density of D_n relative to that of $\mathbf{Z}^n$. The point is to eliminate the vectors of length 1, so $2R = \sqrt{2}$ and $R = 1/\sqrt{2}$. The precise we pay is that we have only half as many balls, so the density is $(\sqrt{2})^n/2$ times that of $\mathbf{Z}^n$.

Example 6.1.3. $A_n = \{(x_i) \in \mathbf{Z}^{n+1} \mid \sum x_i = 0\}$.

Example 6.1.4. $E_8 = D_8 \cup \left(D_8 \cup (\frac{1}{2}, \ldots, \frac{1}{2})\right)$.

Lattice	Density
$\mathbf{Z}^n$	$\frac{\pi^{n/2}}{(n/2)!}\left(\frac{1}{2}\right)^n$
D_n	$\frac{\pi^{n/2}}{(n/2)!}\frac{1}{2}\left(\frac{1}{2}\right)^{n/2}$
A_n	
E_8	$\frac{\pi^4}{4!}\frac{1}{2^4}$

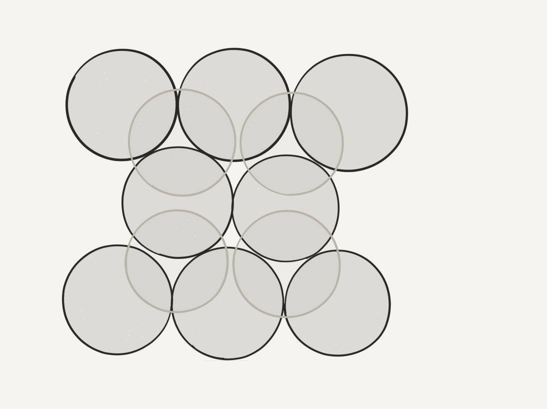
In low dimensions, all the best sphere packings that we know about come from lattices.

dimension	densest packing known	density
2	A_2	>0.9
3	$A_3 = D_3$	≈ 0.74
4	D_4	
5	D_5	
6	E_6	
7	E_7	
8	E_8	$\frac{\pi^4}{4!}\frac{1}{2^4} \approx 0.25$

You can try to do this trick in general: take two lattices and try to slide them together. In dimension 8 you can slide in a complete copy without reducing the size of the spheres, so the density *doubles.*

These are almost surely the densest packings in their dimensions, but the densest packing is only provably found in dimensions $1,2,3$ (huge computational work of Tom Hales), 8, 24 (Maryna Viazovska). In dimension 24 it is the packing associated to the Leech lattice. For the Leech lattice, the answer is $\frac{\pi^{12}}{12!} \approx 0.002$. (This is very respectable! Compare with $1/2^{24}$.)

An interesting phenomenon in dimensions 8, 24 is that there is one lattice which is *much* better than the others. In dimension 3, the lattice is obtained by stacking on top of the 2D solutions



but there are many ways of doing this.

Theorem 6.1.5 (Minkowski)**.** *We have*

$$\rho_n \geq 2 \cdot 2^{-n}.$$

In fact, this can be achieved with a lattice packing.

Remark 6.1.6. The best known result is

$$\rho_n \geq c n 2^{-n}.$$

We need a tool called *Siegel's integration formula.* Let $\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}$ have an invariant measure of mass 1.

Let $C \subset \mathbf{R}^n$ be a measurable set not containing 0 (think of it as a ball). Then, when L is chosen randomly from $\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}$ (the space of lattices of volume 1 in $\mathbf{R}^n$) the average size of $C \cap L$ should be about $\mathrm{vol}(C)$. Siegel's Theorem says that this is true on average:

$$\boxed{\int_{g \in \mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}} \#(C \cap \mathbf{Z}^n g) = \mathrm{vol}(C)}.$$

We'll prove this next time.

Exercise 6.1.7. We can do it by pure thought. Think about this.

Corollary 6.1.8. *If* $\mathrm{vol}(C) < 1$ *then there is a lattice disjoint from it.*

Proof of Minkowski's Theorem. Let $B = \{||x|| \leq R\}$ be a ball of volume 2 and C to be a hemisphere of B minus $\{0\}$. By the Corollary 6.1.8 L doesn't contain an element of C, hence also no element of B because L is symmetric under inversion. Then $\{v + \frac{1}{2}B \colon v \in L\}$ are disjoint, so the density is at least $\geq 2^{1-n}$. □

Example 6.1.9. In $\mathbf{R}^n$, the ball of volume 1 has radius $\approx C\sqrt{n}$ (the diagonal of a hypercube). So Siegel's formula says that a typical lattice of volume 1 has 1 vector on average in $\{||x|| \leq C\sqrt{n}\}$. On the other hand, $\mathbf{Z}^n$ has an *exponential* number of such vectors (for instance, any assignment of each coordinate to be 0 or 1 works).

6.2. **Proof of Siegel's Theorem.** We now go back to the proof of Siegel's Theorem. For $f \in L^1(\mathbf{R}^n)$, we define E_f from the space of lattices to $\mathbf{R}$ sending $L \mapsto \sum_{v \in L, v \neq 0} f(v)$. The claim is that

$$\int_{\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}} E_f \cdot d\mu = \int_{\mathbf{R}^n} f(x)\, dx$$

where dx is the Lebesgue measure. We can recover the statement above by taking f to be the characteristic function of C.

Easy proof. The map

$$f \mapsto \int_{\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}} E_f \, d\mu$$

defines a continuous functional $C_c(\mathbf{R}^n) \to \mathbf{R}$. The coninuity is not obvious; it amounts to the statement that for a compact subset $K \subset \mathbf{R}^n$, if $\mathrm{supp}(f) \subset K$ then

$$\int_{\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}} E_f \ll ||f||_\infty.$$

This defines a measure on $\mathbf{R}^n$, *which is* $\mathrm{SL}_n \mathbf{R}$-*invariant.* But the only such measures are of the form $a \cdot \delta_0 + b \cdot$ (Lebesgue). Why? Let ν be an $\mathrm{SL}_n \mathbf{R}$-invariant measure on $\mathbf{R}^n$. It is enough to show that $\nu(f) \propto \int f\, dx$ for $f \in C_c(\mathbf{R}^n - 0)$. If we knew that ν were absolutely continuous with respect to Lebesgue, then implies Radon-Nikodym would imply that $\nu = \varphi(x)\,dx$ for some $\mathrm{SL}_n\,\mathbf{R}$-invariant function φ, which is necessarily consant.

So why is the absolute continuity true? Choose $H \in C_c(\mathrm{SL}_n\,\mathbf{R})$ with

$$\int_{\mathrm{SL}_n\,\mathbf{R}/\,\mathrm{SL}_n\,\mathbf{Z}} H = 1.$$

Then $\nu = g\nu$ for all $g \in \mathrm{SL}_n\,\mathbf{R}$ implies that

$$\nu = \int_g H(g)(g\cdot\nu)\,dg = H * \nu.$$

This "smooths out" ν away from 0.

Now that we know

$$f \mapsto \int_{\mathrm{SL}_n\,\mathbf{R}/\,\mathrm{SL}_n\,\mathbf{Z}} = a\delta_0 + b\,dx$$

e need to compute the constants a and b. Let $f = \frac{\chi_{\mathrm{Ball}(R)}}{\mathrm{vol}(\mathrm{Ball}(R))}$, so $\int f(x)\,dx = 1$. Then for each L, $E_f(L)$ is the number of lattice points in $\mathrm{Ball}(R)$, which converges to 1 as $R \to \infty$. Granting the continuity once again, dominated convergence implies that

$$\int E_f(L) \to 1 \text{ as } R \to \infty$$

and the left hand side approaches b as $R \to \infty$ since the contribution of the delta function is overwhelmed. Similarly taking $f = \chi_{B(R)}$ with $R \to 0$, we get that $a = 0$. □

A "harder proof of Siegel's Theorem. We now give another proof.

Definition 6.2.1. We say that f is *primitive* if $v \neq nv'$ for some $n \in \mathbf{Z}$ with $n \geq 2$. Then

$$E_f^* = \sum_{v\in L \text{ primitive}} f(v).$$

We will compute

$$\int_{L\in\mathrm{SL}_n\,\mathbf{R}/\,\mathrm{SL}_n\,\mathbf{Z}} E_f^*(L)\,dg$$

The parametrization is $L = g\cdot\mathbf{Z}^n$, so this is

$$\int_{L\in\mathrm{SL}_n\,\mathbf{R}/\,\mathrm{SL}_n\,\mathbf{Z}} E_f^*(L)\,dg = \int_{\mathrm{SL}_n\,\mathbf{R}/\,\mathrm{SL}_n\,\mathbf{Z}} \sum_{v\in\mathbf{Z}^n \text{ prim.}} f(gv)\,dg.$$

Since $\mathrm{SL}_n\,\mathbf{Z}$ acts transitively on primitive vectors in $\mathbf{Z}^n$, with the stabilizer of

$$e_n := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

being

$$P_n\mathbf{Z} := \begin{pmatrix} * & \dots & * & 0 \\ * & \dots & * & \vdots \\ * & \dots & * & 1 \end{pmatrix} \subset \mathrm{SL}_n \mathbf{Z}.$$

So we can rewrite

$$\int E_f^* = \int_{g \in \mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}} \sum_{\gamma \in \mathrm{SL}_n \mathbf{Z}/P_{\mathbf{Z}}} f(g\gamma e_n) = \int_{g \in \mathrm{SL}_n \mathbf{R}/P_{\mathbf{Z}}} f(ge_n)\, dg.$$

If we change $g \mapsto gp$ with $p \in P_{\mathbf{R}}$ then this is unchanged, so we can take out a factor of $P_{\mathbf{R}}/P_{\mathbf{Z}}$:

$$\int_{g \in \mathrm{SL}_n \mathbf{R}/P_{\mathbf{Z}}} f(ge_n)\, dg = \mathrm{vol}(P_{\mathbf{R}}/P_{\mathbf{Z}}) \int_{\mathrm{SL}_n \mathbf{R}/P_{\mathbf{R}}} f(ge_n) = \mathrm{vol}(P_{\mathbf{R}}/P_{\mathbf{Z}}) \int_{\mathbf{R}^n} f(x)\, dx.$$

(where we have to be careful with the normalization of the volumes and to check that the quotient measure on $\mathrm{SL}_n / P_{\mathbf{R}}$ really is the quotient measure). This shows that

$$\int_{\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}} E_f^* = \mathrm{vol}(P_{\mathbf{R}}/P_{\mathbf{Z}}) \int_{\mathbf{R}^n} f\, dx.$$

Now what is $P_{\mathbf{R}}/P_{\mathbf{Z}}$? It has a block that looks like $\mathrm{SL}_{n-1}\mathbf{R}$ and one that looks like $\mathbf{R}^{n-1}$. So

$$\mathrm{vol}(P_{\mathbf{R}}/P_{\mathbf{Z}}) = \mathrm{vol}(\mathbf{R}^{n-1}/\mathbf{Z}^{n-1}) \cdot \mathrm{vol}(\mathrm{SL}_{n-1}\mathbf{R}/\mathrm{SL}_{n-1}\mathbf{Z}).$$

So we've computed that

$$\int_{\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}} E_f^* = \mathrm{vol}(\mathrm{SL}_{n-1} / \mathrm{SL}_{n-1}\mathbf{Z}) \int_{\mathbf{R}^n} f\, dx.$$

We can use this to inductively compute the volume.

Remark 6.2.2. The abve identity is compatible for the canonical integral measure on $\mathrm{SL}_n \mathbf{R}$ arising from the differential form $\prod \widehat{dx_{kl}}/m_{k,\ell}$ (see (5.4.1)) and the Lebesgue measure.

Now take $f = \chi_{B(R)}$. Letting $R \to \infty$, the number of primitive lattice points in $B(R)$ needs to be normalized by the probability that the coordinates are coprime. The familiar argument for $n = 2$ easily generalizes to:

$$E_f^*(L) \approx \frac{B(R)}{\zeta(n)}.$$

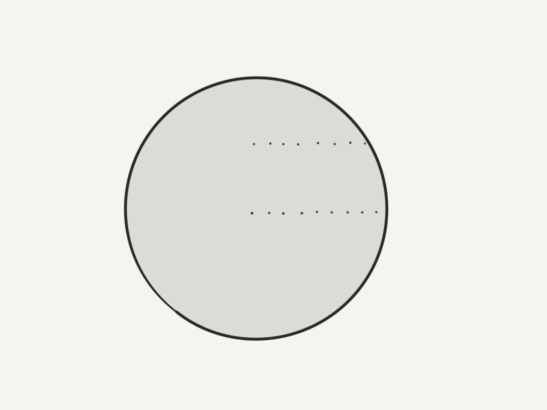
Letting $R \to \infty$, we get

$$\mathrm{vol}(\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}) = \zeta(n)\mathrm{vol}(\mathrm{SL}_{n-1}\mathbf{R}/\mathrm{SL}_{n-1}\mathbf{Z}) = \zeta(n)\zeta(n-1)\dots\zeta(2).$$

Now let's talk about the convergence that have been swept under the rug. We should check that $\int |E_f| < \infty$, and it is enough to show that $\int E_{1_{\mathrm{Ball}(R)}} < \infty$ because we have only used f such that $|f| \le c|1_{\mathrm{Ball}(R)}|$. We have to estimate

$$E_{1_{\mathrm{Ball}(R)}}(L) = \#(L \cap \mathrm{Ball}(R)) - 1.$$

Note that this can go to infinity: imagine a lattice with one really short basis vector.



So this is unbounded; we need some estimates. Suppose L has reduced basis $v_1, \dots, v_n$; we want to estimate

$$\#(L \cap \mathrm{Ball}(R)) = \#\{(m_i) \in \mathbf{Z}^n : ||\sum m_i v_i|| \le R\}.$$

Recall that in terms of reduced bases, the lengths behave as if they were orthogonal, so we need

$$m_i \le c \cdot R/||v_i||.$$

The number of possibilities for (m_i) is then $\le c(R/||v_i|| + 1)$. Then

$$\#(L \cap \mathrm{Ball}(R)) \le C \prod \left(\frac{R}{||v_i||} + 1 \right).$$

So

$$\begin{aligned} \int_{\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}} E_f &\le \int_{L \in S_{A,B}} \#(L \cap \mathrm{Ball}_R) \\ &\le c_{n,A,B} \cdot \int_{\substack{y_1,\dots,y_n \\ \prod y_i = 1 \\ y_i \ge A y_{i+1}}} \frac{dy_1}{y_1} \cdots \frac{dy_{n-1}}{y_{n-1}} \frac{1}{\prod_{i>j} y_i/y_j} \prod \left(\frac{R}{y_i} + 1 \right) \end{aligned}$$

By explicit computation, we can check that this converges.

6.3. **Upper bounds.** We showed the lower bound

$$\rho_n \ge 2 \cdot 2^{-n}.$$

Now we will discuss an upper bound. The asymptotically best bound is

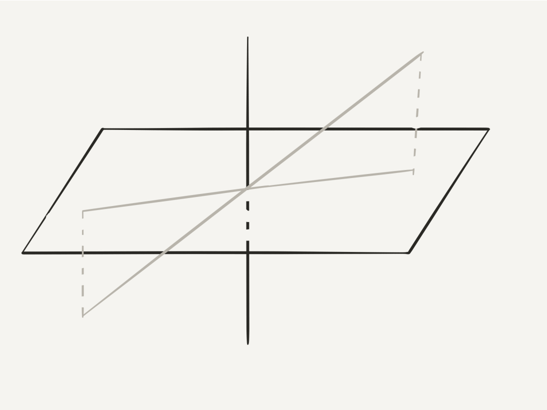
$$\rho_n \le 2^{-\beta n}$$

where $\beta \approx 0.599\dots$. This is due to Kabatiansky-Levenshtein.

As discussed previously, we also know ρ_2, ρ_8, and ρ_{24}. We'll prove that $\rho_n \le 2^{-0.5n}$ and explain the idea of the stronger results.

Lemma 6.3.1. *Suppose we have non-zero vectors $v_1, \dots, v_N \in \mathbf{R}^n$ such that the angle between any v_i, v_j is at least $\pi/2$. Then $N \le 2n$.*

Proof. Project the remaining vectors onto the orthogonal complement; the angles can only get further apart. (The dot product is negative; removing one coordinate where the contributions align makes it more negative.)



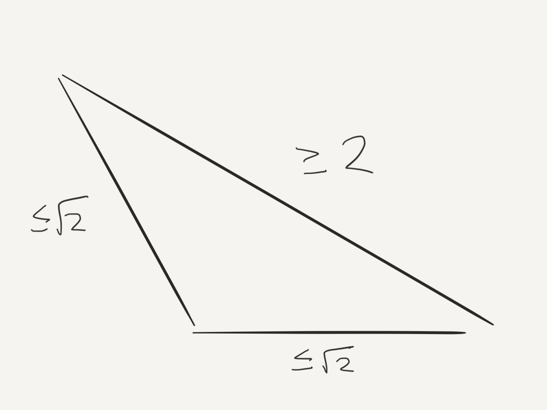
□

Exercise 6.3.2. Show that if we replace $\pi/2$ by $\pi/2+\epsilon$ for any $\epsilon>0$, then we can bound N independently of n. Show that if we replace $\pi/2$ by $\pi/2-\epsilon$, then there are an exponential number of such vectors.

Proposition 6.3.3. *We have* $\rho_n \le 2n \cdot 2^{-0.5n}$.

This is a slight weakening of a result due to Blichtfeld which says that $\rho_n \le 2^{-0.5n}$.

Proof. Imagine a packing of spheres of radius 1 centered at x_i. We know that $|x_i - x_j| \ge 2$. We want to bound the number of spheres that are near. If $|x_i|, |x_j| \le \sqrt{2}$ then the triangle between the origin and x_i, x_j has side lengths $(\le \sqrt{2}, \le \sqrt{2}, \ge 2)$, so must have angle at least $\pi/2$.



The upshot (by the Lemma) is that there are at most $2n$ sphere centers in Ball$(0, \sqrt{2})$. This implies that the density is at most $2n(1/\sqrt{2})^n$. Why? Let χ_i be the characteristic function of a ball of radius $\sqrt{2}$ centered at x_i. Then $\sum \chi_i(x) \le 2n$. Taking the average over x, we get $\rho_n(\sqrt{2})^n \le (2n)$. □

How can we do better? Let $\chi = \chi_{\mathrm{Ball}(0,\sqrt{2})}$. We just showed that $\sum_i \chi(x-x_i) \le 2n$, which is small on the scale of the problem. Can we improve this using another χ?

We want to choose $\chi \in C_c(\mathbf{R}^n)$ such that

$$G(x) := \sum \underbrace{\chi(x-x_i)}_{\tau_{x_i}\chi}$$

is small. We'll try to choose χ so that $\tau_{x_i}\chi, \tau_{x_j}\chi$ don't intersect each other. More precisely, we'll assume that

$$\langle \tau_y \chi, \chi\rangle \le 0 \text{ for all } |y| \ge 2.$$

Fix B to be a large ball in $\mathbf{R}^n$. Then we have

$$\langle G, G\rangle_B = \sum_i \langle \chi, \chi\rangle \#\{\text{spheres in } B\} + (\text{edge effects})$$

since our assumption makes the cross-terms contribute negatively. Letting $N = \#\{\text{spheres in } B\}$, we thus have

$$\langle G, G\rangle_B \approx N\langle \chi, \chi\rangle. \tag{6.3.1}$$

On the other hand, by Cauchy-Schwarz we have

$$\langle G, G\rangle_B \ge \operatorname{vol} B \cdot (\text{average value of } G \text{ on } B)^2. \tag{6.3.2}$$

The average value is

$$\frac{\int \chi \cdot N}{\operatorname{vol}(B)} + (\text{edge effects})$$

Putting together (6.3.1) and (6.3.2) gives

$$\frac{(\int \chi)^2 N^2}{\operatorname{vol}(B)} \le \langle \chi, \chi\rangle N - \text{edge effects}$$

Taking B to ∞, we find that the density of sphere centers, which is $(N/\operatorname{vol} B)$, is at most $\frac{\langle \chi, \chi\rangle}{\langle \chi, 1\rangle^2}$.

Theorem 6.3.4. *Suppose that $\chi \in \mathscr{S}(\mathbf{R}^n)$ such that $\langle \tau_y \chi, \chi\rangle \le 0$ for $|y| \ge 2R$. Then*

$$\rho_n \le \frac{\langle \chi, \chi\rangle}{\langle \chi, 1\rangle^2} \cdot \textit{(volume of a sphere of radius R)}.$$

We can linearize this problem. If we write $F(y) = \langle \tau_y \chi, \chi\rangle$, so $F(y) \le 0$ for $|y| \ge 2R$, then

$$\rho_n \le \frac{F(0)}{\int F}$$

because $\int F = (\int \chi)^2$. On $\mathbf{R}^n$, we have

$$\widehat{g}(k) = \int g(x) e^{ikx}\, dx.$$

Then

$$\widehat{F} = |\widehat{\chi}(k)|^2.$$

This reasoning suggests:

Theorem 6.3.5 (Cohn-Elkies)**.** *Given a Schwartz function F such that $F(y) \leq 0$ for $|y| \geq 2R$ and $\widehat{F} \geq 0$, then*

$$\rho_n \leq \text{(volume of sphere of radius } R\text{)} \frac{F(0)}{\widehat{F}(0)}.$$

To prove this carefully one should rephrase the original argument on the Fourier transform side.

For suitable F, this gives $\rho_n \leq 2^{-0.599n}$.

Example 6.3.6. Let's try to cook up an F that beats the trivial bound for $n = 2$. We choose $R = 1/2$. We want a function $F \colon \mathbf{R}^2 \to \mathbf{R}$ satisfying$F(\vec{x}) \leq 0$ for $|\vec{x}| \geq 1$ and $\widehat{F} \geq 0$. We could try to enforce the first condition by putting

$$F(x,y) = (1 - \vec{x} \cdot \vec{x}) e^{-\frac{c}{2} \vec{x} \cdot \vec{x}}.$$

Then

$$\rho_2 \leq \frac{\pi}{4} \frac{1}{\widehat{F}(0)}.$$

What is $\widehat{F}$? Recall that

$$\widehat{e^{-x^2/2}} = \sqrt{2\pi} e^{-k^2/2}.$$

and $\widehat{xg} = -i \partial_k \widehat{g}$. So

$$\widehat{e^{-\frac{c}{2}(x^2+y^2)}} = \frac{2\pi}{c} e^{-\frac{1}{2c}(k_1^2+k_2^2)}.$$

Then

$$\widehat{F} = \frac{2\pi}{c}(1 + \partial_{k_1}^2 + \partial_{k_2}^2) e^{-\frac{1}{2c}(k_1^2+k_2^2)}.$$

So

$$\begin{aligned} \partial_k e^{\alpha k^2/2} &= -\alpha k e^{-\alpha k^2/2} \\ \partial_k^2 &= (-\alpha + \alpha^2 k^2) e^{-\alpha k^2/2}. \end{aligned}$$

Then

$$\widehat{F} = \frac{2\pi}{c} \left(1 - 2/c + \frac{k_1^2 + k_2^2}{c^2} \right) e^{-(k_1^2+k_2^2)/2c}$$

which is positive if $c > 2$. This is positive for $c > 2$, and for such c we get

$$\rho_2 \leq \frac{1}{8} \frac{c}{1 - 2/c} \leq 1.$$

It's now clear by pure thought that you can perturb this to do better than 1, by perturbing this example. Suppose we replace $f \leftarrow f + \epsilon h$. We can assume that $f(0)$ is unchanged by choosing $h(0) = 0$. We take h to be some $P(r^2)(1 - r^2)e^{-2r^2}$. If this is going to satisfy the conditions for ϵ small enough, then

- the Fourier transform $\hat{h}(k)$ should be ≥ 0 for large $|k|$, because $\hat{f}(0) > 0$,
- $P(t) \geq 0$ for large enough t.

These conditions are satisfies as long as the highest degree term of $P(t)$ is $a_k t^k$ where $a_k > 0$, and the Fourier transform is positive. That latter thing basically amounts to $k \in 2\mathbf{Z}$: the Fourier transform is the Laplace transform applied k times... Clearly it's possible to satisfy these conditions and have $h(0) = 0$, $\hat{h}(0) > 0$.

I tried doing this with $h(r) = (Ar^8 + Br^6)(1 - r^2)e^{-2r^2}$. Optimizing for A and B, we get a density bound $\rho_2 \leq 0.96$.

Cohn-Elkies used functions of the form $f = (\text{poly}) \cdot \text{Gaussian}$. Doing this in dimensions $2, 8, 24$, they found that the functions and resulting bounds both converged. The upper bounds for ρ_n were very close to the known packings. On the basis of this, they conjectured:

Conjecture 6.3.7. *In dimensions $n = 2, 8, 24$ there exists a Schwarz function f_n satisfying the conditions above, such that* vol *(R-ball)*$\cdot \frac{f_n(0)}{\hat{f}_n(0)}$ *is the density of the $A_2/E_8/$Leech packing.*

For $n = 8$ this was recently proved by Maryna Viazovska, and shortly thereafter it was done in $n = 24$ by Viazovska and collaborators. The functions are obtained as transforms of modular forms. In $n = 2$ it is still open.

7. The Leech lattice

7.1. **Even unimodular lattices.**

Recall the definition of the E_8 lattice. You start with

$$D_8 = \{(x_1, \ldots, x_8) \in \mathbf{Z}^8 \mid \sum x_i \equiv 0 \pmod 2\}.$$

We then take

$$E_8 = D_8 \cup \left(D_8 \cup \frac{1}{2}(1, \ldots, 1) \right).$$

How might we have discovered this lattice? Notice that D_8 has the property that $\langle x, x \rangle \in 2\mathbf{Z}$ for all x and $\langle x, y \rangle \in \mathbf{Z}$ for all x, y. (The second is implied by the first.)

Definition 7.1.1. We say that a lattice $L \subset \mathbf{R}^n$ is *integral* if $\langle x, y \rangle \in \mathbf{Z}$ for all $x, y \in L$ and *even* if $\langle x, x \rangle \in 2\mathbf{Z}$. We say that L is *unimodular* if $\text{vol}(L) = 1$.

Even unimodular lattices exist only when $8 \mid n$.

Example 7.1.2. For $n = 8$, the only unimodular lattice is E_8.

For $n = 16$, we have $E_8 \oplus E_8$ and "E_{16}" (the same consruction with respect to D_{16}).

For $n = 24$, there are 24 even unimodular lattices. Among them there is a unique one such that no $x \in L$ has length $\langle x, x, \rangle = 2$. This is the *Leech lattice*. The others are the *Niemeier lattices*. We know 3 of them: $E_8 \oplus E_8 \oplus E_8$, $E_8 \oplus E_{16}$, and E_{24}.

For $n = 32$, there are at least 10^9 such lattices.

Given D_8, how might we have discovered E_8? i.e. how can I extend D_8 to an even unimodular lattice L?

We know that L must be of the form $D_8 + \mathbf{Z}x$ where $2x \in D_8$. We need $\langle D_8, x \rangle \in \mathbf{Z}$ for the pairing on L to be integral. This means that $x \in D_8^* = \mathbf{Z}^8 + \mathbf{Z} \cdot \frac{1}{2}(1, \ldots, 1)$. Let $e = \frac{1}{2}(1, \ldots, 1)$.

So x corresponds to an element of $D_8^*/D_8 \cong \mathbf{Z}/2\times\mathbf{Z}/2$, with explicit representatives

$$\begin{aligned} e &= (\frac{1}{2},\dots,\frac{1}{2}) \\ f &= (1,\dots,0) \\ e+f &= (\frac{3}{2},\frac{1}{2},\dots,\frac{1}{2}) \end{aligned}$$

Each such x gives $D_8+\mathbf{Z}x$ on which the inner product is integral. To check evenness, we have to check $\langle x,x\rangle \in 2\mathbf{Z}$.

$$\begin{aligned} \langle e,e\rangle &= 2 \\ \langle f,f,\rangle &= 1 \\ \langle e+f,e+f\rangle &= 4. \end{aligned}$$

In fact $x=e,e+f$ both work.

7.2. **The Golay code.** A *perfect code* in $\mathbf{F}_2^D$ is a subset S such that for some integer ℓ, the balls of radius ℓ around $s\in S$ tile $\mathbf{F}_2^D$, i.e. $\coprod_{s\in S}\text{Ball}(s,\ell)=\mathbf{F}_2^D$ (where distance is the Hamming distance). This is only possible if

$$|S|\cdot\underbrace{\left(\binom{D}{0}+\ldots+\binom{D}{\ell}\right)}_{\text{size of ball}}=2^D.$$

Golay showed that there exists a perfect code $S\subset\mathbf{F}_2^{23}$ with $\#S=2^{12}$ and $\ell=3$. (Note that $1+\binom{23}{1}+\binom{23}{2}+\binom{23}{3}=2048$.) In fact S is a vector space.

Let's call this code $\mathscr{G}_{23}\subset\mathbf{F}_2^{23}$. It can be chosen to be a *vector subspace.* It is "symmetric" in the sense that the automorphism group $M_{23}:=\{\sigma\in S_{23}\colon\sigma(\mathscr{G}_{23})=\mathscr{G}_{23}\}$ acts transitively on the 23 coordinates. (In fact it even acts *four-transitively.*)

Remark 7.2.1. This automorphism group is the exceptional simple group, the *Mathieu group* M_{23}. (Incidentally, we don't know any field extension $K\supset\mathbf{Q}$ with $\text{Gal}(K/\mathbf{Q})=M_{23}$.)

The fact that $\mathscr{G}_{23}$ is so symmetric nearly pins it down. Necessarily M_{23} has a 23-cycle (since it acts transitively on a set with a prime number of elements), so we can identify the 23 coordinates with $\mathbf{Z}/23$ and assume that translation by $\mathbf{Z}/23$ preserves $\mathscr{G}_{23}$. We can think of $\mathscr{G}_{23}$ as a 12-dimensional subspace of $\mathbf{F}_2[\mathbf{Z}/23]$, and it is invariant by $\mathbf{Z}/23$. Writing x for a generator of $\mathbf{Z}/23$, we can write

$$\mathbf{F}_2[\mathbf{Z}/23]=\mathbf{F}_2[x]/(x^{23}-1).$$

Over $\mathbf{F}_2$ we can factor

$$x^{23}-1=(x-1)fg$$

where $\deg f=\deg g=11$. If ζ is a primitive 23rd root of unity in $\overline{\mathbf{F}}_2$, then the roots of $x^{23}-1$ are ζ^i for $0\le i\le 22$ and the irreducible factors correspond to orbits of Frobenius $y\mapsto y^2$ on these roots. What are the orbits of squaring? The order of 2 in $(\mathbf{Z}/23)^*$

is 11, and $\langle 2\rangle$ is the set of quadratic residues. So the orbits of Frobenius are $\{1\}$, $Q :=$ {quadratic residues}, and $N :=$ {quadratic non-residues}. So we can write

$$f(x) = \prod_{q\in Q}(x-\xi^q) \qquad g(x) = \prod_{n\in N}(x-\xi^n).$$

Then

$$\mathbf{F}_2[x]/(x^{23}-1) = \mathbf{F}_2[x]/f \times \mathbf{F}_2[x]/(x-1) \times \mathbf{F}_2[x]/g.$$

Since $\mathscr{G}_{23}$ is $\mathbf{Z}/23$-invariant, it must be an ideal in $\mathbf{F}_2[\mathbf{Z}/23]$. The only such ideals are sums of these factors, so there are only two possibilities for $\mathscr{G}_{23}$:

$$\mathscr{G}_{23} = \mathbf{F}_2[x]/f \qquad \text{or} \qquad \mathscr{G}_{23} = \mathbf{F}_2[x]/g.$$

In fact applying $t \mapsto -t$ on $\mathbf{Z}/23$ switches the two, so they are indistinguishable.

We can think of $\mathscr{G}_{23}$ are the set of all multiples of g in $\mathbf{F}_2[x]/(x^{23}-1)$. Alternatively, it is the set of all $h \in \mathbf{F}_2[x]/(x^{23}-1)$ such that $h(\zeta^n) = 0$ for all $n \in N$. (Note that this imposes 11 conditions on a 23-dimensional space.)

Key point. Every non-zero $h \in \mathscr{G}_{23}$ has $|h| \geq 7$.

This implies that if $h, h' \in \mathscr{G}_{23}$ then $\text{Ball}(h,3)\cap\text{Ball}(h',3) = \emptyset$, since otherwise their difference would have size at most 6.

Of course one can check the key point by hand, but here is one trick.

Lemma 7.2.2. *For all $h \in \mathscr{G}_{23}$, we have $|h| \equiv 0$ or $3 \mod 4$.*

Proof. Let $\mathscr{G}_{23}^0 \subset$ be the set of all $y \in \mathscr{G}_{23}$ such that $|y|$ is even. This is $\mathbf{F}_2[x]/g$, since the map to $\mathbf{F}_2[x]/(x-1)$ is adding up all the coordinates. So

$$\mathscr{G}_{23} = \mathscr{G}_{23}^0 \oplus \mathbf{F}_2(1,1,\dots,1).$$

it is enough to show that for $h \in \mathscr{G}_{23}^0$ we have $|h| \equiv 0 \mod 4$, since changing by $(1,1,\dots,1)$ changes the number of non-zero elements by $3 \mod 4$.

For $h, h' \in \mathscr{G}_{23}^0$ we can consider

$$h \cdot h' = \sum_i h_i h_i'.$$

We claim that this is necessarily 0. Why? We have $Q = -N$, so $\mathbf{F}_2[x]/f$ and $\mathbf{F}_2[x]/g$ are dual to each other as $\mathbf{Z}/23$-representations (duality replaces the characteristic polynomial with the one having the inverse roots). Therefore we cannot have a non-trivial pairing on $\mathbf{F}_2[x]/f$.

So

$$|h+h'| = |h| + |h'| - 2|h \cap h'|.$$

Since the last term is divisible by 4, we get that

$$h \mapsto |h|$$

is a homomorphism from $\mathscr{G}_{23}^0$ to $2\mathbf{Z}/4\mathbf{Z}$. Again for representation-theoretic reasons this must be 0. □

Remark 7.2.3. The element $\sum_{n\in N} x^n$ (i.e. the vector with 1s only in N position) belongs to $\mathscr{G}_{23}$ and its translates under $\mathbf{Z}/23$ generate $\mathscr{G}_{23}$. This is left as an exercise.

We can extend to $\mathscr{G}_{24} \subset \mathbf{F}_2^{24}$ by forcing the bits to sum to 0 (this is called adding a "parity bit"):

$$\mathscr{G}_{24} := \{(\vec{x}, x_{24}) \in \mathscr{G}_{23} \times \mathbf{F}_2 \colon \sum x_i \neq 0\}$$

It follows from the preceding result that for all $h \in \mathscr{G}_{24}$, we have $|h| \equiv 0 \mod 4$ and $|h| \geq 8$.

Remark 7.2.4. Another combinatorial coincidence is that for every set $S \subset \{1, \dots, 24\}$ of size 5 is contained in a *unique* code word of $\mathscr{G}_{24}$ of length 8.

The automorphism group of $\mathscr{G}_{24}$ is the (simple) Mathieu group M_{24}. This is 5-transitive, which is as good as one a finite simple group can get without being symmetric or alternating (by the classification of finite simple groups).

We have $\mathscr{G}_{23} \subset \mathbf{F}_2^{\mathbf{Z}/23}$, and we can consider $\mathscr{G}_{24} \subset \mathbf{F}_2^{\mathbf{Z}/3\cup\{\infty\}}$. In this perspective $M_{24} \supset \mathrm{PSL}_2(\mathbf{Z}/23)$.

7.3. **Construction of the Leech lattice.** It's very natural to use codes to impose congruence conditions on integral lattices. (We want to eliminate short vectors, so we can try to eliminate them mod 2, and $\mathscr{G}_{24}$ has no short vectors.) Define

$$L_0 := \{x \in \mathbf{Z}^{24} \mid x \mod 2 \in \mathscr{G}_{24}\}.$$

This obviously isn't unimodular. Since $\dim_{\mathbf{F}_2} \mathscr{G}_{24} = 12$, this has index 2^{12} in $\mathbf{Z}^{24}$. Therefore, $L := \frac{1}{\sqrt{2}} \cdot L_0$ has volume 1, i.e. is unimodular. For $\vec{x} \in L_0$, we have

$$\langle \vec{x}, \vec{x} \rangle \equiv 0 \mod 4.$$

Therefore, $\mathrm{vol}(L) = 1$ and $\langle x, x \rangle \in 2\mathbf{Z}$ for $x \in L$; that is, L is even.

However, this is still not the Leech lattice.

We need to kill more short vectors. Now we started with $\mathbf{Z}^{24}$, which has many short vectors, like the coordinate vectors. The construction L kills off the short vectors $e_1, e_1 + e_2, e_1 + e_2 + e_3, \dots$ but doesn't kill off $2e_1, 2e_2$, etc. So the shortest vectors left are twice the coordinate vectors; we want to kill these off now. Set

$$L_* = \frac{1}{\sqrt{2}} \{\vec{x} \in \mathbf{Z}^{24} \mid \vec{x} \in \mathscr{G}_{24} \mod 2, \sum x_i \equiv 0 \mod 4\}.$$

Now the shortest vectors are $\frac{1}{\sqrt{2}}(e_1 + \ldots + e_8)$ or $\frac{1}{\sqrt{2}}(2e_1 + 2e_2)$.

Now (just as for D_8) we can extend L_* by 2. Consider the dual lattice $L_*^\vee$, and consider $(L_*)^\vee / L_* \cong \mathbf{Z}/2 \times \mathbf{Z}/2$. We just need to find an element v such that $\langle v, v \rangle \in 2\mathbf{Z}$. Coset representatives are

$$\frac{1}{\sqrt{2}}(1, 0, \dots, 0)$$

$$\frac{1}{\sqrt{2}}(1/2, 1/2, \dots, 1/2)$$

$$\frac{1}{\sqrt{2}}(3/2, 1/2, \dots, 1/2)$$

which have lengths $1/2, 3, 4$, so the last vector works. (Perhaps there is an error? Two of them should have worked.)

8. Quadratic forms

A *quadratic form* over a ring R is a formal expression

$$Q(x_1, \dots, x_n) = \sum_{i \geq j} a_{ij} x_i x_j, \quad a_{ij} \in R.$$

(We're mostly interested in $R = \mathbf{Z}$, but this compels us to consider also $\mathbf{Q}, \mathbf{R}, \mathbf{Q}_p, \mathbf{Z}_p, \mathbf{Z}/N\mathbf{Z}$.) We can write this as

$$\vec{x}^T A \vec{x}$$

where

$$A = \begin{pmatrix} a_{11} & \frac{1}{2}a_{12} \\ \frac{1}{2}a_{12} & a_{22} \end{pmatrix}$$

We say that

$$Q \sim Q'$$

if we can obtain Q' from Q using an invertible change of coordinates, i.e.

$$A' = B^T A B \text{ for some } B \in \mathrm{GL}_n(R)$$

We define the *discriminant* of a quadratic form Q to be

$$\operatorname{disc} Q := \det(2A).$$

If $Q' \sim Q$ then $(\operatorname{disc} Q') = (\operatorname{disc} Q)u^2$ for some $u \in R^*$.

8.1. Genus of a quadratic form.

Over $\mathbf{Z}$, we say that Q and Q' are in the same *genus* if they are equivalent in $\mathbf{Z}/N$ for all N and $Q \sim_{\mathbf{R}} Q'$. Equivalently, $Q \sim_{\mathbf{Z}_p} Q'$ for all p and $Q \sim_{\mathbf{R}} Q'$.

Lemma 8.1.1. *If Q, Q' are in the same genus, we have* $\operatorname{disc} Q = \operatorname{disc} Q'$. *In particular, there are only finitely many* $\mathbf{Z}$*-equivalence classes in a genus.*

Proof. If Q, Q' are in the same genus thatn $\operatorname{disc} Q \equiv (\operatorname{disc} Q')u^2 \mod N$ for all N, for some $u \in (\mathbf{Z}/N\mathbf{Z})^*$. □

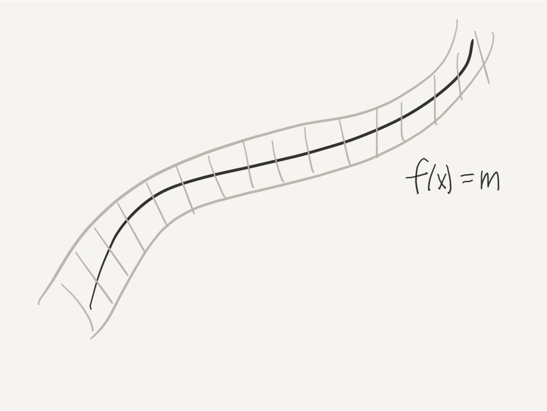
So we have

$$\{\text{genus of } Q\} \subset \{\text{forms of the same discriminant as } Q\}.$$

In practice one should think of this as being almost an equality.

Example 8.1.2. Even unimodular lattices form a single genus.

8.2. **Hardy-Littlewood heuristic.** Recall that a heuristic for the number of solutions to $f(x_1,\dots,x_n)=m$ with $(x_1,\dots,x_n)\in B$ for $f\in\mathbf{Z}[x_1,\dots,x_n]$ is as follows. Consider a small neighborhood of the equation $f=m$.



Then the *Hardy-Littlewood heuristic* predicts that number of solutions is

$$\#\{f(x_1,\dots,x_n)=m\}\approx\lim_{\epsilon\to 0}\frac{\mathrm{vol}(B\cap f^{-1}(m-\frac{\epsilon}{2},m+\frac{\epsilon}{2}))}{\epsilon}\cdot\prod_p \mathrm{density}_p.$$

Here

$$\mathrm{density}_p=\lim_{N\to\infty}\frac{\#\{\text{solutions modulo } p^N\}}{p^{N(n-1)}}.$$

8.3. **The Mass formula.** Now suppose that Q is a positive-definite quadratic form over $\mathbf{Z}$. Define

$$r_Q(m)=\#\{(x_1,\dots,x_n)\in\mathbf{Z}^n \mid Q(x_1,\dots,x_n)=m\}.$$

(In the indefinite case this number might be infinite, but one can make a good definition by modding out by equivalence of forms.) The *expectation* is that

$$r_q(m)=\text{HL heuristic}(Q,m). \tag{8.3.1}$$

If Q,Q' are in the same genus then the right side is for Q and Q' are equivalent. (The density forms are exactly the same by definition, and the volume term is basically the discriminant.) However, the left hand sides may not be, so there is one obvious obstruction to the expectation being reality. The mass formula says that (8.3.1) is exact *when averaged over the genus.*

Theorem 8.3.1 (Mass formula version 1)**.** *We have*

$$\frac{\sum_{Q\in\mathrm{genus}(Q_0)} r_Q(m)\cdot w_Q}{\sum_Q w_Q}=\textit{HL heuristic}(Q_0,m)$$

where $w_Q:=\frac{1}{|\mathrm{Aut}(Q)|}$, *and* $\mathrm{Aut}(Q):=\{\gamma\in\mathrm{GL}_n\mathbf{Z}\colon Q(\gamma x)=Q(x)\}$.

This is a miracle; even the fact that the right hand side (a priori an infinite product) is a rational number is surprising in any given case.

Example 8.3.2. If $Q_0 = x^2 + y^2 + z^2$, then $\text{genus}(Q_0) = \{Q_0\}$. So this tells us a formula for the number of ways of writing m as a sum of three squares. Basically all cases when such a formula is known comes from the Mass formula.

Theorem 8.3.3 (Mass formula version 2)**.** *We have*

$$\sum_{Q \in \text{genus}(Q_0)} w_Q = \textit{explicit function}(Q_0).$$

Some parallels. Before going into the proofs, we discuss some parallels. For a nice function f on $\mathbf{R}^n$, we defined a function E_f on the space of lattices $\mathrm{SL}_n \mathbf{R} / \mathrm{SL}_n \mathbf{Z}$ by the rule

$$E_f(L) = \sum_{v \in L - \{0\}} f(v).$$

Then we argued that

$$\int E_f = \int f \tag{8.3.2}$$

From this we deduced by an inductive argument the measure of $\mathrm{SL}_n \mathbf{R} / \mathrm{SL}_n \mathbf{Z}$. The equality (8.3.2) is parallel to Version 1 of the Mass formula, and the measure calculation is parallel to Version 2.

Outline of proof. Roughly, we'll show "Version 2 in dimension $n-1$ implies Version 1 in dimension n implies Version 2 in dimension n". (In the parallel story, the only idea for (8.3.2) was to take f to be the characteristic function of a large ball; this corresponds to averaging over m. But there are also some new ideas here.)

8.4. **Review of quadratic forms.**

A quadratic form q over a field K can always be diagonalized:

$$q \sim a_1 x_1^2 + \ldots + a_n x_n^2.$$

The argument is to choosing v with $q(v) \neq 0$, and then split the space as $\langle v \rangle \oplus \langle v \rangle^{\perp}$. Then $q \sim a_1 x_1^2 + q'(x_2, \ldots, x_n)$ where $a_1 = q(v)$, and then applies induction.

We're going to consider *non-degenerate* quadratic forms (i.e. $\text{disc} \neq 0$).

8.4.1. *Quadratic forms over* $\mathbf{C}$.

We have

$$q(x_1, \ldots, x_n) \sim x_1^2 + \ldots + x_n^2.$$

There are are no invariants at all except for the dimension n.

8.4.2. *Quadratic forms over* $\mathbf{Z}/p\mathbf{Z}$*, for* $p > 2$.

We can always make a change of variables to pu

$$q(x_1, \ldots, x_n) \sim x_1^2 + \ldots + x_{n-1}^2 + \alpha x_n^2.$$

To get this, we just need to show that if $n > 1$ then q takes the value 1. This follows from counting.

In our normalization, $\text{disc}\, q = (2^n)\alpha$ so q is classified by n and $\text{disc}\, q \in (\mathbf{Z}/p)^* / \square$.

8.5. **Quadratic forms over $\mathbf{Q}_p$.** A quadratic form q is classified by $n, \operatorname{disc} q$, and the *Hasse-Minkowski invariant*, which is in $\{\pm 1\}$. We have to explain what this is.

Remark 8.5.1. But first we give an aside for context. Over any field we can form the *Witt ring* W of quadratic forms modulo the hyperbolic plane. There is a map $W \to \mathbf{Z}/2$ giving the dimension mod 2; let I be the kernel. Then $I/I^2 \xrightarrow{\sim} K^*/(K^*)^2$, and this is the discriminant map.

Next, there is a map

$$I^2/I^3 \xrightarrow{\sim} H^2(K, \mathbf{Z}/2)$$

and this is the Hasse-Minkowski invariant.

Continuing, one can construct maps

$$I^n/I^{n+1} \to H^n(K, \mathbf{Z}/2).$$

Milnor conjectured that this is an isomorphism for all n, which was eventually proved by Orlov-Vishik-Voevodsky.

If we write $q \sim \sum_{i=1}^n a_i x_i^2$, then the *Hasse-Minkowski invariant* is

$$\prod_{i<j} (a_i, a_j)_p \in \{\pm 1\}$$

where $(a_i, a_j)_p$ is the Hilbert symbol. (It is not a priori obvious that this is well-defined, but it is.)

Remark 8.5.2. This invariant can be thought of as a class in the Brauer group. It is probably the associated Clifford algebra.

Hilbert symbol. For $a, b \in \mathbf{Q}_p^*$ we define

$$(a,b)_p = \begin{cases} 1 & z^2 = ax^2 - by^2 \text{ has a non-zero solution } (x,y,z) \\ -1 & \text{otherwise.} \end{cases}$$

Remark 8.5.3. This makes sense over $\mathbf{R}$ as well. It is

$$(a,b)_\infty = \begin{cases} -1 & a, b < 0 \\ 1. & \text{otherwise} \end{cases}$$

Properties.

- (BILINEAR) We have
$$(a, bb') = (a,b)(a,b')$$
and
$$(aa', b) = (a,b)(a', b).$$
- (SYMMETRIC) We have $(a,b)_p = (b,a)_p$.
- (SYMBOL) In addition to the bilinearity, $(x, 1-x)_p = 1$ for all $x \in F^* \setminus \{1\}$. This also implies that $(x, -x)_p = 1$.

- For $p > 2$, if a, b are p-units then
$$(a,b)_p = 1.$$
If a is a p-unit, then $(a,p) = \left(\frac{a}{p}\right) = \begin{cases} 1 & a = QR \\ -1 & a = NQR \end{cases}.$
- (PRODUCT FORMULA) For $a, b \in \mathbf{Q}^*$ we have
$$(a,b)_\infty \prod_p (a,b)_p = 1.$$
This is basically a reformulation of quadratic reciprocity.

8.6. **Quadratic forms over Q.**

Example 8.6.1. Are the forms $2x^2+3y^2$ and x^2+6y^2 equivalent over $\mathbf{Q}$? The corresponding matrices are
$$\begin{pmatrix} 2 & \\ & 3 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & \\ & 6 \end{pmatrix}.$$
We only need to check the Hasse-Minkowski invariants:
$$(2,3)_p \overset{?}{=} (1,6)_p.$$
The right hand side is 1 for all p, since the HM invariant is a symbol. The left side is 1 if $p > 3$. For $p = 3$, it is -1. At ∞ it is also 1, so the product formula says that it is -1 at $p = 2$.

Example 8.6.2. Are the forms $2x^2 + 7y^2$ and $x^2 + 14y^2$ equivalent over $\mathbf{Q}$? We have to compare $(2,7)_p$ and $(1,14)_p$. By the same reasoning, this is okay except at $p = 2, 7, \infty$. At 7 we get $(2,7)_p = 1$, so the same thing at all places.

For two quadratic forms q, q' over $\mathbf{Q}$, we have
$$q \sim_{\mathbf{Q}} q' \iff q \sim_{\mathbf{Q}_p} q' \text{ for all } p \text{ and } q \sim_{\mathbf{R}} q'$$
which is equivalent to having the same dimension, discriminant, signature, and Hasse-Minkowski invariants at all primes p.

8.7. **Quadratic forms over $\mathbf{Z}_p$ ($p > 2$).** For $p > 2$, all quadratic forms over $\mathbf{Z}_p$ can still be diagonalized! That is, we have after change of variables
$$q \sim \sum a_i x_i^2.$$
Why? Choose $\vec{x} = (x_1, \ldots, x_n) \in \mathbf{Z}_p^n$ so that $v_p(q(x_1, \ldots, x_n))$ is minimal (here v_p is the p-valuation). By a change of variables, we can assume that $\vec{x} = (1, 0, \ldots, 0)$, so then
$$q(\vec{x}) = a_{11}x_1^2 + x_1 \text{Linear}(x_1, \ldots, x_n) + q'(x_2, \ldots, x_n).$$
Now we claim that the coefficient a_{11} divides all the other coefficients. Indeed, since $q(\vec{x}) = a_{11}x_1^2 + a_{12}x_1x_2 + \ldots$ we can write
$$a_{12} = \frac{q(e_1+e_2) - q(e_1) - q(e_2)}{2},$$

so a_{11} divides a_{12}, and similarly all the other a_{ij}. So

$$q(\vec{x}) = a_{11}(x_1^2 + \dots)$$

and we can now complete the square.

Uniqueness. For $p > 2$, a quadratic form $q = \sum a_i x_i^2$ over $\mathbf{Z}_p$ group the terms by their p-valuations:

$$q = p^0(a_1 x_1^2 + \dots + a_k x_k^2) + p^1(b_1 y_1^2 + \dots b_\ell y_\ell^2) + \dots$$

Write this as $p^0 q_0 + p^1 q_1 + \dots$. Then the dimensions $q_0, q_1, \dots$ and the discriminants of the q_i (valued in $\mathbf{Z}_p^*/\square \cong \{\pm 1\}$) form a complete set of invariants.

8.8. **Quadratic forms over $\mathbf{Z}_2$.** Any quadratic form q is a direct sum of diagonal terms or 2×2 blocks axy or $a(x^2 + xy + y^2)$. The argument is similar, except that you can't complete the square, but you can break off a 2×2 block.

8.9. **Application.** Let's prove that an even unimodular lattice $L \subset \mathbf{R}^n$ must have $8 \mid n$.

Since $\langle x, x \rangle \in 2\mathbf{Z}$ for all x, we have an integral quadratic form $q(x) = \frac{\langle x,x \rangle}{2}$. Let A be the matrix for q, so

$$q(x) = x^T A x.$$

Then $\det(2A) = 1$ because L is unimodular.

We know that

$$HM(q)_\infty \prod HM(q)_p = 1$$

by the product rule applied termwise.

We'll show that $HM(q)_p = 1$ for $p \neq 2$. Over $\mathbf{Z}_p$, we can diagonalize $q = \sum a_i x_i^2$, and $\prod 2a_i = 1$ so all the a_i are p-units, so $(a_i, a_j)_p = 1$ for all i, j. This shows that $HM(q)_p = 1$.

Over $\mathbf{R}$, we can diagonalize

$$q \sim \sum a_i x_i^2, \quad a_i > 0$$

so the Hasse-Minkowski invariant is $\prod (1,1)_\infty = 1$.

It only remains to figure out what happens at 2. There it turns out that we can always write write

$$q = \sum a_i x_i^2 + \sum b_i xy + \sum c_i (x^2 + xy + y^2)$$

(with the b_i, c_i being powers of 2). Corresponding, the matrix A is a sum of blocks

$$(a_i) \oplus b_i \begin{pmatrix} & 1/2 \\ 1/2 & \end{pmatrix} \oplus c_i \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix}.$$

Since

$$1 = \det 2A = \prod (2a_i) \prod b_i^2 (-1) \prod c_i^2 \det \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

there are no a_i's, and all $b_i = c_i = 1$. So q is a sum of r copies of xy and s copies of $x^2 + xy + y^2$ over $\mathbf{Z}_2$. Then

$$1 = \det(2A) = (-1)^r 3^s.$$

Even in $\mathbf{Z}/8$, an equality $3^r(-1)^s = 1 \implies r, s$ are both even. So the product formula implies $HM(q)_2 = (-1)^{r(r-1)/2+s(s-1)/2}$, which forces $(r+s)/2$ to be even. Then the dimension, which is $2(r+s)$, is divisible by 8.

9. The mass formula: examples

9.1. **Binary quadratic forms.** Recall Minkowski's theorem: given a lattice $L \subset \mathbf{R}^n$, if the volume of the ball of radius $r/2$ is bigger than the volume of L, then there exists a non-zero $x \in L$ with $||x|| \leq R$.

Example 9.1.1. Consider $Q = x^2 + y^2$, and suppose $Q' \in \text{genus}(x^2+y^2)$. Consider $(\mathbf{Z}^2, Q')$, a lattice of volume 1. By Minkowski's theorem, there exists $v \in \mathbf{Z}^2 - \{0\}$ with $Q'(v) \leq R^2$ as soon as $\pi R^2/4 > 1$, i.e. $R^2 > 4/\pi$. $Q(v')$ is a non-zero integer, so for R sufficiently close to $4/\pi$ the resulting vector v' must satisfy $Q(v') = 1$.

Choose coordinates on $\mathbf{Z}^2$ so that $v' = (1,0)$. Then

$$Q'(x,y) = x^2 + bxy + cy^2.$$

Note that $\text{disc}(ax^2 + bxy + c^2) = \det \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} = 4ac - b^2$. So $\text{disc}(Q') = 4c - b^2 = \text{disc}(x^2+y^2) = 4$.

Replacing x by $x+y$ changes b to $b+2$. Therefore we can assume that $b = 0$ or 1, which forces $b = 0, c = 1$ hence $Q' = x^2 + y^2 = Q$.

What are the automorphisms of Q? Note that any such must permute the vectors of length 1, which are $\{(\pm 1, 0), (0, \pm 1)\}$. Therefore the automorphisms are $(x,y) \mapsto (\pm x, \pm y)$ and $(x,y) \mapsto (\pm y, \pm x)$.

Example 9.1.2. Let $Q_0 = x^2 + xy + 6y^2$ (which has discriminant 23). Suppose $Q' \in \text{genus}(Q_0)$. This has volume $\sqrt{23/4}$. (We can diagonalize it to $ax^2 + by^2$. This lattice has volume $\sqrt{ab}$ and discriminant $4ab$, so the volume is $\sqrt{\text{disc}/4}$.) Then by Minkowski's Theorem we have a vector of length $\leq \frac{2\sqrt{23}}{\pi}$, so there exists $v' \in \mathbf{Z}^2$ with $Q'(v') \in \{1,2,3\}$.

Case 1: $Q'(v') = 3$. Again you can assume that $v' = (1,0)$ and $Q' = 3x^2 + bxy + cy^2$. If we adjust x to $x+y$, then b goes to $b+6$. Then we can assume that $-2 \leq b \leq 3$. If we replace y by $-y$, then b is negated, so we only need to check $b \in \{0,1,2,3\}$.

We have $\text{disc}\, Q' = 12c - b^2 = 23$. The only solution is $b = 1$ and $c = 2$. This leads to the form $Q' = 3x^2 + xy + 2y^2$.

We leave the other cases as an exercise. The answer is that there is nothing new: the forms are equivalent to $Q_0 = x^2 + xy + 6y^2$ or $Q_1 = 3x^2 + xy + 2y^2$. We still have to check that $Q_0 \sim_{\mathbf{Z}_p} Q_1$ for all primes p.

Exercise 9.1.3. Repeat this analysis for $x^2 + 6y^2$. A similar analysis leads to $Q_1 = 2x^2 + 3y^2$. These two are *not* equivalent over $\mathbf{Q}_3$.

You can check $Q_0 \sim_{\mathbf{Z}_p} Q_1$ by the classification theory we discussed before, and the following lemma.

Lemma 9.1.4. *Let Q, Q' be quadratic forms over $\mathbf{Z}^2$. If $v_p(\operatorname{disc} Q), v_p(\operatorname{disc} Q') \leq 1$ (for $p = 2$, demand that $v_p(\dots) \leq 3$) then $Q \sim_{\mathbf{Z}_p} Q'$ if and only if* $\operatorname{disc} Q = \operatorname{disc} Q'$ *and $HM(Q)_p = HM(Q')_p$, i.e. if and only if $Q \sim_{\mathbf{Q}_p} Q'$.*

Finally we record the automorphisms:

- $\operatorname{Aut}(Q_1) = \{(x, y) \mapsto (-x, -y), \operatorname{Id}\}$,
- $\operatorname{Aut}(Q_0) = \{(x, y) \mapsto (x + y, -y), (-x - y, -y), (-x, -y), (x, y)\}$.

So $|\operatorname{Aut}(Q_0)| = 4$ and $|\operatorname{Aut}(Q_1)| = 2$.

Remark 9.1.5. Gauss considers binary Q up to equivalence by $\mathrm{SL}_2 \mathbf{Z}$. Then $2x^2 + xy + 3y^2 \not\sim 3x^2 + xy + 2y^2$, because it requires a matrix with determinant -1. For this all the automorphism groups have the same size. With this notion, the set of binary quadratic forms of discriminant D has a group structure, and that makes it isomorphic to the ideal class group of the order with discriminant $-D$.

9.2. **The mass formula for binary quadratic forms.** We'll work through the statements of the mass formula for binary quadratic forms:

$$\frac{\sum_{Q \in \operatorname{genus}(Q_0)} r_Q(m) \cdot w_Q}{\sum_Q w_Q} = \text{HL heuristic}(Q_0, m)$$

and

$$\sum_{Q \in \operatorname{genus}(Q_0)} w_Q = \text{explicit function}(Q_0).$$

We want to prove a version of this, where we average not just over the genus but all forms of discriminant D.

We want to compute

$$\sum_{\substack{Q \colon ax^2 + bxy + c^2/\sim \\ \operatorname{disc} Q = d}} \frac{\#\{\text{vectors } v \in \mathbf{Z}^2 \mid Q(v) = m\}}{|\operatorname{Aut}(Q)|}.$$

For simplicity assume that m is squarefree, so that v is automatically primitive. In other words, we are counting

$$\begin{aligned} &= \frac{\#\{Q(x, y), v \in \mathbf{Z}^2 \mid Q(v) = m; \operatorname{disc} Q = d\}}{\mathrm{GL}_2 \mathbf{Z}} \\ &= \frac{\#\{Q(x, y) \colon Q(1, 0) = m; \operatorname{disc} Q = d\}}{\text{stabilizer of } (1, 0) \text{ in } \mathrm{GL}_2 \mathbf{Z}} \\ &= \frac{\#\{mx^2 + bxy + cy^2 \colon 4mc - b^2 = d\}}{\text{stabilizer}} \end{aligned}$$

This is very analogous to the unfolding process we used in the second proof of Siegel's formula, $\int E_f = \int f$. Note that the stabilizer is generated by $(x, y) \mapsto (x + y, y)$ and $(x, y) \mapsto (-x, -y)$. Using the stabilizer we can assume that $0 \leq b \leq m$, because by applying $(x, y) \mapsto (x + y, y)$ we can assume that $-(m - 1) \leq b \leq m$, and then we can apply $x \mapsto (-x, -y)$. The endpoints (i.e. forms with $b = 0$ or $b = m$) are counted with weight $1/2$, because there is only one pre-image.

So what we have found is

$$\sum_{Q \operatorname{disc} D} \frac{r_Q(m)}{|\operatorname{Aut}(Q)|} = \sum_{b=0}^{m}{}' \{\#c \mid 4mc - b^2 = D\}$$

where the $\sum'$means the endpoints are counted with weight 1/2. Thanks to our limitations on b, there is exactly one solution if D is a square modulo $4m$, so this is

$$= \sum_{b=0}^{m}{}' \begin{cases} 1 & b^2 \equiv -D \mod 4m \\ 0 & \text{otherwise} \end{cases}$$

which is "the number of square roots $\sqrt{-D}$, modulo $4m$". It's important that we not only have this formula, but that there is a nice interpretation of the right hand side.

Review of the HL heuristic. We're expecting to find the output from the Hardy-Littlewood heuristic on the right hand side. The heuristic says that

$$\#\{Q = m\} \approx \operatorname{vol}(Q = m) \cdot \prod v_p$$

where

$$v_p = \lim_{\ell \to \infty} \frac{\#\{Q = m \pmod{p^\ell}\}}{p^{(n-1)\ell}}.$$

Example 9.2.1. Let's check version 1 of the mass formula for $Q = x^2 + xy + 6y^2$. For simplicity we take $m \neq 23$ to be a prime. Last time we found that the genus of $x^2 + xy + 6y^2$ consists of $Q_0 = x^2 + xy + 6y^2$, which has automorphism size 4, and $Q_1 = 2x^2 + xy + 3y^2$, which has automorphism size 2.

The answer should be the number of solutions to $b^2 \equiv -23 \mod 4m$ in $0 \le b \le m$. This is 0 if -23 is not a square mod m; otherwise there are two square roots, an even one and an odd one, but only the odd one works mod 4 so we get 1.

In other words, if $-23 = \square \mod m$ then

$$\frac{r_{Q_0}(m)}{4} + \frac{r_{Q_1}(m)}{2} = 1.$$

In fact either $r_{Q_0}(m) = 4$ or $r_{Q_1}(m) = 2$, since as soon we have one solution we get more by acting an automorphism.

We need to check that HL heuristic $(Q_0, m) = 1$. This is

$$\lim_{\epsilon \to 0} \frac{\operatorname{vol}(Q^{-1}(m - \epsilon/2, m + \epsilon/2)}{\epsilon} \prod \lim_{\ell \to \infty} \frac{\#\{Q = m \pmod{p^\ell}\}}{p^{(n-1)\ell}}.$$

First, let's consider the volume of $\{Q = m\}$. The volume of $Q \le R$ is $\pi R / \sqrt{23/4}$. So the volume of the shell is $\pi\epsilon / \sqrt{23/4} = 2\pi/\sqrt{23}$.

Now what about the factors

$$v_p = \frac{\lim \#\{Q = m \mod p^\ell\}}{p^\ell}?$$

If $p \neq 23, m, 2$ then by the theory of quadratic forms over $\mathbf{Z}_p$ (namely that they can be diagonalized) we have $Q \sim x^2 - uy^2$ where u is a unit. If u is a square, then

$$x^2 - uy^2 = (x - \sqrt{u}y)(x + \sqrt{u}y) \sim xy.$$

Thus the number of solutions to $xy \equiv m \mod p^\ell$ is the number of units in $\mathbf{Z}/p^\ell$, which is $p^\ell(1-1/p)$. If u is not a square, then the number of solutions mod p^ℓ is $p^\ell(1+1/p)$, which you check by reducing to $\mathbf{Z}/p$ and checking that it's $p+1$ in that case. Therefore,

$$\nu_\ell = 1 \pm 1/p$$

but $\operatorname{disc} Q = -4u$, so $u = -23/4$ up to squares. Therefore,

$$\nu_p = \begin{cases} 1+1/p & -23 \neq \square \mod p \\ 1-1/p & -23 = \square \mod p \\ 2 & p = 23 \\ 1/2 & p = 2 \\ 2(1-1/p) & p = m, -23 = \square \mod m \\ 0 & p = m, -23 \neq \square \mod m \end{cases}$$

So the HL heuristic is

$$\frac{2\pi}{\sqrt{23}} 2^2 \prod_p (1 - \chi(p)/p)$$

where

$$\chi(p) = \begin{cases} 1 & -23 = \square \mod p \\ 0 & p = 23 \\ -1 & -23 \neq \square \mod p \end{cases}$$

The product is

$$\prod_p (1 - \chi(p)/p) = \sqrt{23}/3\pi.$$

How do you derive this? Inverting the left hand side gives

$$\prod_p \frac{1}{(1-\chi(p)/p)^{-1}} = \sum \frac{\chi(n)}{n}$$

where $\chi(n)$ is defined multiplicatively. This is periodic with period 23. So we can rewrite this as a sum of terms $\sum \zeta^n/n$, where ζ varies over 23rd roots of unity. So the HL heuristic gives

$$\frac{8\pi}{\sqrt{23}} \frac{\sqrt{23}}{3\pi} = \frac{8}{3}.$$

We should have gotten $1/(3/4) = 4/3$. Actually, the Mass formula is off by a factor of 2 when $n = 2$.

The mass formula version 1 is

$$\operatorname{vol}(Q = m) \prod_p \frac{\#\{Q = m \mod p^\ell\}}{p^*} = \frac{\sum \frac{r_Q(m)}{|\mathrm{Aut}(Q)|}}{\sum \frac{1}{|\mathrm{Aut}(Q)|}}.$$

We can refromulate the mass formula version 2 is

$$\frac{\mathrm{vol}(O_Q)}{2}\prod_p \frac{\frac{1}{2}\#O_Q(\mathbf{Z}/p^\ell)}{p^*} = \frac{2}{\sum 1/|\mathrm{Aut}(Q)|}$$

which makes the similarity between the formulas clearer. Here O_Q is the set of linear transformations preserving Q, so $O_{\mathbf{Q}}(\mathbf{Z}) = \mathbf{Z}$, and $O_Q(\mathbf{Z}/p^\ell)$ is the set of linear transformations mod p^ℓ preserving Q. Also, by volume we mean $\mathrm{vol}(O_Q) = \mathrm{vol}(O_Q(\mathbf{R}))$ for the "fiber" volume form of $Q\colon \mathbf{R}^n \to \mathbf{R}$. We do the same thing here where the "fiber" form is where we think of $O_Q(\mathbf{R})$ as the fiber of the map $M_n(\mathbf{R})$ to the quadratic forms over $\mathbf{R}$ sending $M \mapsto Q(Mx)$.

9.3. **The Kneser neighbour method.** The main new idea in the general case is a good way of parametrizing the genus. To explain the rough idea, recall that E_8 was constructed by going down to D_8 and then squeezing in another copy. The construction of the Leech lattice was similar: start with the sublattice of $\mathbf{Z}^{24}$ mapping to the Golay code, pass to some intermediate thing, then extend to the Leech lattice.

This idea lets you generate new elements in a genus. Namely, for a general quadratic form you perform an analogue of going down and back up. This is the "Kneser neighbour method".

To talk about this propertly we need a slight change of perspective, shifting the emphasis from quadratic forms to *lattices*. If q is a quadratic form on $\mathbf{Q}^n$ and $L \subset \mathbf{Q}^n$ is a lattice, such that $q(L) \subset \mathbf{Z}$, then (q, L) defines a quadratic form over $\mathbf{Z}$.

Properties.

- If $L, L' \subset \mathbf{Q}^n$ are lattices, then $(q, L) \sim (q, L') \iff$ there exists $g \in O_q(\mathbf{Q})$ such that $gL = L'$.

  The argument is that $(q, L) \sim (q, L')$ when there exists $\lambda\colon L \to L'$ with $q(\lambda(v)) = q(v)$. Then you take g to be an extension of λ to $\mathbf{Q}^n$.
- (q, L) and (q, L') are in the same genus if and only if for all primes p, there exists $g \in O_q(\mathbf{Q}_p)$ such that $gL_p = L'_p$. Here L_p is the closure of L in $\mathbf{Q}_p^n$, which you can think of concretely as taking a basis $v_1, \ldots, v_n$ for L and setting $L_p := \mathbf{Z}_p v_1 + \ldots + \mathbf{Z}_p v_n$.

Now we come to the Kneser neighbour method. The is a generalization of our construction of the Leech lattice:

$$\begin{tikzcd}
\{x \in \mathbf{Z}^{24} \mid x \in \mathscr{G}_{24}\} & & \text{Leech} \\
& L_1 \arrow[ul, dash, "2"] \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

Let q be a quadratic form on $\mathbf{Q}^n$ and L a lattice in $\mathbf{Q}^n$ with $q(L) \subset \mathbf{Z}$. Let p be a prime not dividing $\mathrm{disc}(q)$.

Definition 9.3.1. A *p-neighbour* of L is a lattice $L' \subset \mathbf{Q}^n$ fitting into a diagram

$$\begin{tikzcd}
L \arrow[dr, dash, "p"'] & & L' \arrow[dl, "p"] \\
& L \cap L' &
\end{tikzcd}$$

with $q(L') \subset \mathbf{Z}$ (and $L' \neq L$).

Theorem 9.3.2. *For all p-neighbours L', (q, L') and (q, L) are in the same genus. Also, there is a bijection*

$$\{p\text{-neighbours } L'\} \longleftrightarrow \{\text{lines } \ell \subset L/pL \mid q \mod p \text{ is } 0 \text{ on } \ell\}.$$

Remark 9.3.3. If you join (q, L) and (q, L') whenever L and L' are neighbours, you get a graph structure on the genus. (This may be called the "Kneser graph".)

Proof. Let A be the matrix for q, so that

$$\langle x, y\rangle = x^T(2A)y = q(x+y) - q(x) - q(y).$$

Choose $v' \in L' - L \cap L'$. Let $v = pv' \in L \cap L'$. Let $\overline{v}$ be the image of v in L/pL. We're basically going to show that we can reconstruct everything from this $\overline{v}$. Then $\overline{v}$ determines $L \cap L'$ in the following sense. Note that

$$\langle L \cap L', v\rangle \in p\mathbf{Z}$$

so $L \cap L' \subset \{\lambda \in L \mid \lambda(v) \equiv 0 \mod p\}$, but this must be an equality since both sides have index p in L (this uses that the discriminant is not divisible by p).

This means that we can describe (this is where we use $v' \notin L$)

$$L \cap L' = \{x \in L \colon \langle x \mod p, \overline{v}\rangle \equiv 0 \mod p\}.$$

Next, $\overline{v}$ determines v up to translation by p^2L. The reason is that $q(v) = p^2 q(v') \in p^2\mathbf{Z}$, so we can find v by lifting $\overline{v}$ arbitrarily to $v_0 \in L$ and then adjusting $v = v_0 + pt$. We want

$$q(v) = q(v_0) + p\langle v_0, t\rangle + p^2 q(t)$$

to be divisible by p^2. So among the lifts of $\overline{v}$ in L, this condition determines v modulo p^2: we need to solve for t (unique up to pL) such that $p\langle v_0, t\rangle + q(v_0) \equiv 0 \mod p^2$.

Therefore, $\overline{v}$ determines L' by the following recipe:

$$L' = L \cap L' + \mathbf{Z}\frac{v}{p}$$

where $L \cap L' = \{x \in L \colon \langle x, \overline{v}\rangle = 0 \mod p\}$ and v is a lift of $\overline{v}$ to L such that $q(v) \equiv 0 \mod p^2$.

This rule gives a bijection between neighbours L' and $[\overline{v}] \mod p$ with $q(\overline{v}) = 0$. □

Example 9.3.4. Let $q = x^2 + xy + 6y^2$, $L = \mathbf{Z}^2$. Take $p = 3$. Start with $\overline{v} \in (\mathbf{Z}/3\mathbf{Z})^2$ with $q(\overline{v}) = 0$. For instance, we could take $\overline{v} = (0,1)$. Then

$$L \cap L' = \{x \in \mathbf{Z}^2 \colon \langle x, \overline{v}\rangle \equiv 0 \mod 3\} = \{(m,n) \in \mathbf{Z}^2 \colon 3 \mid m\}.$$

To find L', lift $\overline{v}$ to $v \in \mathbf{Z}^2$ such that $q(v) \equiv 0 \mod 9$. For instance, we can take $v = (3,1)$. Now we adjoin $\frac{1}{3}v = (1, 1/3)$, obtaining

$$\{(m,n) \colon 3 \mid m\} + \mathbf{Z}(1, \frac{1}{3}) = \mathbf{Z}(1, \frac{1}{3}) + \mathbf{Z}(0,1).$$

Let $e=(1,\frac{1}{3})$ and $f=(0,1)$. Then

$$q(xe+yf)=x^2+\left(\frac{x^2}{3}+xy\right)+6\left(\frac{x}{3}+y\right)^2=2x^2+5xy+6y^2.$$

The substitution $x\mapsto x-y$ turns this form into $2x^2+xy+3y^2$, which is the other form we found earlier in this genus.

Remark 9.3.5. The number of neighbors is the number of isotropic lines in L/pL. We can put the quadratic form into

$$x_1^2+\ldots+x_{n-1}^2+ux^2.$$

There is some formula for the number of isotropic lines, roughly p^{n-2} since there are p^{n-1} lines and one in p is isotropic.

Finally, we have to show that if L,L' are neighbors then (q,L) and (q,L') are in the same genus. Here is the sketch of the argument. We use the classification of forms over $\mathbf{Z}_p$. At $\ell\neq p$ we have $L=L'=L\cap L'$, so we can take $g=1$. You can change coordinates so that

$$\begin{aligned}L_p&=\mathbf{Z}_p^n\\ q&=x_1x_2+q(x_3,\ldots,x_n)\\ \overline{v}&=(1,0,\ldots,0)\\ L_p\cap L_p'&=\{(x_1,\ldots,x_n)\colon x_2\in p\mathbf{Z}_p, x_i\in\mathbf{Z}_p \text{ for } i\neq 2\}\\ L_p'&=\{(x_1,\ldots,x_n)\colon x_1\in\frac{1}{p}\mathbf{Z}_p, x_2\in p\mathbf{Z}_p, x_i\in\mathbf{Z}_p\}.\end{aligned}$$

At $\ell=p$, we can take $g(x_1,\ldots,x_n)=(\frac{x_1}{p},px_2,x_3,\ldots,x_n)$ and this $g\in O_q$.

9.4. **Parametrization of genus.** We reiterate that we are now adopting the perspective of a quadratic form q on $\mathbf{Q}^n$. A lattice L is a subset of $\mathbf{Q}^n$ such that $q(L)\subset\mathbf{Z}$. Then

- $(q,L)\sim_{\mathbf{Z}}(q,L)$ if and only if there exists $g\in O_q(\mathbf{Q})$ with $gL=L'$.
- $(q,L)\sim_{\mathbf{Z}_p}(q,L)$ if and only if there exists $g\in O_q(\mathbf{Q}_p)$ with $gL_p=L_p'$.

Lemma 9.4.1. *The map sending $L\mapsto(L_p)_p$ gives a bijection*

$$\{\textit{lattices in }\mathbf{Q}^n\}\longleftrightarrow\left\{\begin{smallmatrix}\{L_p\subset\mathbf{Q}_p^n\}\\ \textit{for almost all } p,\ L_p=\mathbf{Z}_p^n\end{smallmatrix}\right\}$$

Proof. If $L\subset\mathbf{Q}^n$ is a lattice, then $L_p=\mathbf{Z}_p^n$ for almost all p because we can choose N,M such that

$$\frac{1}{N}\mathbf{Z}^n\supset L\supset M\mathbf{Z}^n.$$

To show that this is a bijection, write down the inverse

$$\{L_p\}\to\text{“intersection of } L_p\text{”}=\{x\in\mathbf{Q}^n\mid x\in L_p \text{ for every } p\}.$$

□

The group $\mathrm{GL}_n\,\mathbf{Q}_p$ acts on lattices in $\mathbf{Q}^n$ in the following way. Given $g\in\mathrm{GL}_n\,\mathbf{Q}_p$, we send $L\longleftrightarrow(L_2,L_3,\ldots)$ to the lattice $(L_2,L_3,\ldots,gL_p,\ldots)$.

Example 9.4.2. Let $g = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Q}_3)$. How does g act on $\mathbf{Z}^2$? It only focuses on the "3-adic" aspect, so

$$g \cdot \mathbf{Z}^2 = \{x \in \mathbf{Z}^2 \mid x \in \begin{pmatrix} 2 & \\ & 3 \end{pmatrix} \mathbf{Z}_3^2\} = \{(m,n) \in \mathbf{Z}^2 : 3 \mid n\}.$$

Putting these actions together, we get an action of

$$\prod_p{}' \mathrm{GL}_n \mathbf{Q}_p$$

on lattices in $\mathbf{Q}^m$ (the restricted product means that for almost all p, $g_p \in \mathrm{GL}_n \mathbf{Z}_p$). Note that if we embed $\mathrm{GL}_n \mathbf{Q} \hookrightarrow \prod_p' \mathrm{GL}_n \mathbf{Q}_p$ then the action restricts to the natural action of $\mathrm{GL}_n \mathbf{Q}$.

Now we introduce a convenient packaging of this structure, namely the *adeles*.

Definition 9.4.3. Define the *finite adeles* to be

$$\mathbf{A}_f = \prod_p{}' \mathbf{Q}_p$$

(so $x_p \in \mathbf{Z}_p$ for almost all p). The full ring of *adeles* is

$$\mathbf{A} = \mathbf{R} \times \prod_p{}' \mathbf{Q}_p.$$

The topology is the natural one induced by the presentation

$$\mathbf{A}_f = \bigcup_{\text{finite set } S} \left(\prod_{p \in S} \mathbf{Q}_p \times \prod_{p \notin S} \mathbf{Z}_p \right)$$

where we take the product topology on $\prod_{p \in S} \mathbf{Q}_p \times \prod_{p \notin S} \mathbf{Z}_p$. This makes the adeles into a locally compact topological ring.

So we've shown that $\mathrm{GL}_n \mathbf{A}_f$ acts on lattices in $\mathbf{Q}^n$.

Theorem 9.4.4 (Parametrization of the Genus)**.** *Let Q be an integral quadratic form on $\mathbf{Z}^n$. There is a bijection*

$$\mathrm{genus}(Q) \longleftrightarrow \mathrm{SO}_Q(\mathbf{Q}) \backslash \mathrm{SO}_{\mathbf{Q}}(\mathbf{A}_f) / \prod_p \mathrm{SO}_Q(\mathbf{Z}_p)$$

(the right hand side is the set of orbits of $\mathrm{SO}_Q(\mathbf{Q})$ *on* $\mathrm{SO}_{\mathbf{Q}}(\mathbf{A}_f)/\prod_p \mathrm{SO}_Q(\mathbf{Z}_p)$*).*

How should we think of this? We should think of $\mathbf{Q} \hookrightarrow \mathbf{A}$ as a "thick" version of $\mathbf{Z} \hookrightarrow \mathbf{R}$. Therefore we should think of

$$\mathrm{SO}_{\mathbf{Q}}(\mathbf{A}_f) / \prod_p \mathrm{SO}_Q(\mathbf{Z}_p)$$

as similar to the orbits of $\mathrm{SO}_Q(\mathbf{Z})$ on $\mathrm{SO}_Q(\mathbf{R})$, so this "behaves like"

$$\mathrm{SL}_n \mathbf{R} / \mathrm{SL}_n \mathbf{Z}.$$

We will be able to rephrase version 2 of the mass formula: for a natural measure on $\mathrm{SO}_Q(\mathbf{A})$, the volume of the right hand side is 2. This was discovered by Weil ["Adeles and Algebraic Groups"].

Proof. Let q be the quadratic form induced by Q on $\mathbf{Q}^n$, i.e. "Q considered over $\mathbf{Q}$". So $Q = (q, \mathbf{Z}^n)$. Let $\mathscr{L}$ be the set of lattices $L \subset \mathbf{Q}^N$ such that (q, L) is in the same genus as $(q, \mathbf{Z}^n)$. There is a natural map

$$\mathscr{L} \to \mathrm{genus}(Q).$$

We claim that it is surjective. This has some content, as follows. If $Q' \sim Q$ then $Q' \sim_{\mathbf{Z}_p} Q$ and $Q' \sim_{\mathbf{R}} Q$. The nontrivial content is that this implies that $Q' \sim_{\mathbf{Q}} Q$, i.e. there exists a map $\lambda\colon \mathbf{Q}^n \to \mathbf{Q}^n$ such that $Q(\lambda(v)) = Q'(v)$. Then $Q' = (q, \lambda(\mathbf{Z}^n))$.

So genus(Q) is the set of orbits of $O_q(\mathbf{Q})$ on $\mathscr{L}$.

Since $(q, L) \sim_{\mathbf{Z}_p} (q, L') \iff L = gL'$ for some $g \in O_q(\mathbf{Q}_p)$, if $(q, L) \in \mathscr{L}$ then for all p we have $L_p = g_p \mathbf{Z}_p^n$ for some $g_p \in O_q(\mathbf{Q}_p)$. In other words, L is in the $O_q(\mathbf{A}_f)$-orbit of $\mathbf{Z}^n$. So $\mathscr{L}$ is the orbit of $\mathbf{Z}^n$ under $O_q(\mathbf{A}_f)$, which is

$$\mathscr{L} = O_q(\mathbf{A}_f)/\prod_p \text{stabilizer of } \mathbf{Z}_p^n$$

and the latter is $\prod_p O_q(\mathbf{Z}_p)$. So the genus of Q is the set of $O_q(\mathbf{Q})$-orbits on $O_q(\mathbf{A}_f)/\prod_p O_q(\mathbf{Z}_p)$.

We can replace O_q by SO_q using that:

(1) $O_q(\mathbf{Q})$ contains an element of determinant -1,

(2) for all p, $O_q(\mathbf{Z}_p)$ contains an element of determinant -1. This is not trivial; one way to see it is to choose $v \in \mathbf{Z}_p^n$ such that $q(v)$ is divisible by p, i.e. $v_p(q(v))$ is minimal. Then reflection through v (i.e. reflection through its orthogonal hyperplane) sends

$$x \mapsto x - \frac{q(x+v) - q(x) - q(v)}{q(v)} v$$

and we can see from the choice of v that $\frac{q(x+v)-q(x)-q(v)}{q(v)}$ is integral.

□

Remark 9.4.5. Actually there was a mistake. The map

$$O_q(\mathbf{A}_f)/U \to \mathrm{genus}(Q)$$

sending $L \in O_q(\mathbf{A}_f) \cdot \mathbf{Z}^n$ to (q, L). This descends to give the bijection between $\mathrm{SO}_q(\mathbf{Q})$-orbits and the genus. Replacing O by SO, one gets that the map is still surjective by the argument with reflections. But it may not be injective.

The upshot is that the SO_q thing is only the genus of Q up to *strict* equivalence.

Example 9.4.6. The genus of $x^2 + xy + 6y^2$ is $\{x^2 + xy + 6y^2, 2x^2 + xy + 3y^2\}$. However, up to strict equivalent we have $\{x^2 + xy + 6y^2, 2x^2 + xy + 3y^2, 3x^2 + xy + 2y^2\}$. Note that $\#\mathrm{Aut}(x^2 + xy + 6y^2) = 4$ and $\#\mathrm{Aut}(2x^2 + xy + 3y^2) = 2$, so the total mass is $1/4 + 1/2 = 3/4$.

If we do the computation for "strict" version of genus, we only look at automorphisms of determinant 1. So we get $\#\mathrm{Aut}^+(x^2 + xy + 6y^2) = 2$, $\#\mathrm{Aut}^+(2x^2 + xy + 3y^2) = 2$, and $\#\mathrm{Aut}^+(3x^2 + xy + 2y^2) = 2$. So the total mass is $1/2 + 1/2 + 1/2 = 3/2$.

In fact it is always the case that the mass of the strict genus is always exactly twice the mass of the genus. Either you have a determinant -1 self-map, in which case it doesn't divide, or it does divide into two copies.

10. Proof of the mass formula

10.1. Measures and the volume of $\mathrm{SL}_n \mathbf{A}/\mathrm{SL}_n \mathbf{Q}$.

If X is a smooth algebraic variety over $\mathbf{Q}$ and ω is an algebraic differential form of degree $= \dim X$ then we get a measure $|\omega|$ on $X(\mathbf{R})$.

Properties:

- $|f\omega| = |f| \cdot |\omega|$ for f an algebraic function.
- the measure of $Y(\mathbf{R})$ if $Y \hookrightarrow X$ is a lower-dimensional subvariety is always 0.
- If $\pi\colon X \to Y$ is algebraic and smooth, choose ω_X on X and some non-vanishing ω_Y on Y and let $\omega_{\pi^{-1}(y)}$ on each fiber $\pi^{-1}(y)$. Then for F continuous and compactly supported,
$$\int_{X(\mathbf{R})} F|\omega_X| = \int_{Y(\mathbf{R})} |\omega_Y| \int_{\pi^{-1}y(\mathbf{R})} |\omega_{\pi^{-1}(y)}| F.$$
- This is compatible with restriction to an open subset.
- If $\omega = dx_1 \wedge \ldots \wedge dx_n$ on $\mathbf{A}^n$, then $|\omega|$ is the Lebesgue measure.

Similarly, we get a measure $|\omega|_p$ on $X(\mathbf{Q}_p)$ with normalization that $|dx_1 \wedge \ldots \wedge dx_n|$ is the Haar measure with $|\mathbf{Z}_p^n| = 1$ on $\mathbf{Q}_p^n$. In particular, for $\pi\colon X \to Y$ as above (smooth in the algebraic sense) and $F \in C_c(X(\mathbf{Q}_p))$, we have an induced fibral form $\omega_{\pi^{-1}y}$ such that
$$\int_{X(\mathbf{Q}_p)} F|\omega_X|_{\mathbf{Q}_p} = \int_{y \in Y(\mathbf{Q}_p)} |\omega_Y|_{\mathbf{Q}_p} \int_{\pi^{-1}y} F|\omega_{\pi^{-1}y}|_{\mathbf{Q}_p}$$
and the inner integral is continuous in $y \in Y(\mathbf{Q}_p)$.

Example 10.1.1. Suppose $X \subset \mathbf{A}^n$ is defined by
$$f_1 = f_2 = \ldots = f_r = 0.$$
Suppose that the map
$$F\colon \mathbf{A}^n \xrightarrow{(f_1,\ldots,f_r)} \mathbf{A}^r$$
is smooth above 0 (i.e. its derivative is of full rank). On $\mathbf{A}^n$ put the form $dx_1 \wedge \ldots \wedge dx_n$ and on $\mathbf{A}^r$ put $dx_1 \wedge \ldots \wedge dx_r$. On X we put the "fiber" differential form, which is any ω_X such that
$$\omega_X \wedge df_1 \wedge \ldots \wedge df_r = dx_1 \wedge \ldots \wedge dx_n.$$
What is $|\omega_X|_{\mathbf{Q}_p}(X(\mathbf{Z}_p))$? (The answer has to do with counting points modulo powers of p.)

Let $F_K = 1_{\mathbf{Z}_p^n \cap \pi^{-1}B}$, where $B = p^K \mathbf{Z}_p^r$ (thought of as a small ball around 0), where we'll consider $K \to \infty$ (so that B shrinks to 0). Then

$$\begin{aligned}\int_{\mathbf{A}^n(\mathbf{Q}_p)} F_K &= \text{measure}\{x \in \mathbf{Z}_p^n \mid \pi(x) \in B\} \\ &= \text{measure}\{x \in \mathbf{Z}_p^n \mid f_1(x) \equiv \ldots \equiv f_r(x) \equiv 0 \mod p^K\}\end{aligned}$$

Assuming that the f_i have integral coefficients, this is

$$= \frac{\#\{x \in (\mathbf{Z}/p^k)^n : f_1(x) = f_2(x) = \ldots = f_r(x) = 0\}}{p^{Kn}}.$$

(When the f_i don't have integral coefficients, you have to adjust slightly.) Now,

$$\lim_{K \to \infty} \int_{\mathbf{A}^n(\mathbf{Q}_p)} F$$

computes the integral over $y \in B$ of the volume of the fiber, which as we take $K \to \infty$ the left side is just the volume of $X(\mathbf{Z}_p)$, so we find that

$$\text{vol}(X(\mathbf{Z}_p)) = \lim_{K \to \infty} \frac{1}{\text{vol}(B) = p^{-Kr}} \cdot \frac{\#\{x \in (\mathbf{Z}/p^k)^n : f_1(x) = f_2(x) = \ldots = f_r(x) = 0\}}{p^{Kn}}.$$

Therefore, we have found that

$$|\omega_X| X(\mathbf{Z}_p) = \lim_{K \to \infty} \frac{\#\{x \in (\mathbf{Z}/p^k)^n : f_1(x) = f_2(x) = \ldots = f_r(x) = 0\}}{p^{K(n-r)}}.$$

Here one can think of $p^{K(n-r)}$ is the expected number of solutions (since there are n variables and r equations). This gives an interpretation of the factors showing up in the Hardy-Littlewood heuristic.

Remark 10.1.2. Here is an aside. Let X, Y be projective smooth Calabi-Yau varieties over $\mathbf{C}$ (so there are volume forms). Suppose X and Y are birational. Batyrev showed that $b_i(X) = b_i(Y)$ for all i, by using p-adic integration.

First he reduced to the case where X, Y are defined over $\mathbf{Q}$. Then he showed that $\#X(\mathbf{F}_p) = \#Y(\mathbf{F}_p)$ for almost all p; this implies equaliy of Betti numbers by a standard argument. The proof is that

$$\int_{X(\mathbf{Q}_p)} |\omega_X| = \int_{Y(\mathbf{Q}_p)} |\omega_Y|$$

because birationality implies modification on a set of measure 0.

Example 10.1.3. Let's consider SL_n, with the same ω as before:h

$$\omega := \prod_{(i,j) \neq (1,1)} \frac{dx_{ij}}{\text{minor}(1,1)}.$$

This ω was the "fiber" volume form for

$$\det\colon \text{Mat}_{n \times n} \to \mathbf{A}^1.$$

Then

$$|\omega|(\mathrm{SL}_n \mathbf{Z}_p) = \lim_{K\to\infty} \frac{\#\mathrm{SL}_n(\mathbf{Z}/p^K)}{p^{K(k^2-1)}} = \left(1-\frac{1}{p^2}\right)\left(1-\frac{1}{p^3}\right)\dots\left(1-\frac{1}{p^n}\right).$$

In particular, the measure of $\prod_p \mathrm{SL}_n \mathbf{Z}_p$ is $\frac{1}{\zeta(2)\zeta(3)\dots\zeta(n)}$. We showed earlier that $|\omega|_R(\mathrm{SL}_n \mathbf{R}/\mathrm{SL}_n \mathbf{Z}) = \zeta(2)\zeta(3)\dots\zeta(n)$. This implies that if F is a fundamental domain for $\mathrm{SL}_n \mathbf{Z}$ acting on $\mathrm{SL}_n \mathbf{R}$, then the product volume of $F \times \prod_p \mathrm{SL}_n \mathbf{Z}_p$ is 1.

Lemma 10.1.4. *This set $F \times \prod_p \mathrm{SL}_n \mathbf{Z}_p$ is a fundamental domain for $\mathrm{SL}_n \mathbf{Q}$ acting on $\mathrm{SL}_n \mathbf{A}$*

Proof. We have $\mathrm{SL}_n \mathbf{A} = \mathrm{SL}_n \mathbf{R} \times \mathrm{SL}_n \mathbf{A}_f$. The key fact is that each element $g \in \mathrm{SL}_n \mathbf{A}_f$ can be written as γu for $\gamma \in \mathrm{SL}_n \mathbf{Q}$ and $u \in \prod_p \mathrm{SL}_n \mathbf{Z}_p$. Moreover, this is unique up to replacing γ by $\gamma\delta^{-1}$ and u by δu, where $\delta \in \mathrm{SL}_n \mathbf{Z}$.

The main way to understand an adelic group like $\mathrm{GL}_n \mathbf{A}_f$ is to understand its action on lattice. For $g \in \mathrm{GL}_n \mathbf{A}_f$, the action is by applying g to $\mathbf{Z}^n$. This is some in the ambient $\mathbf{Q}^n$, so you can get to it by some element in $\mathrm{GL}_n \mathbf{Q}$, and you can further fiddle to get to it with $\mathrm{SL}_n \mathbf{Q}$. So $g \cdot \mathbf{Z}^n = \gamma \cdot \mathbf{Z}^n$ for some $\gamma \in \mathrm{SL}_n \mathbf{Q}$, so $\gamma^{-1} g$ stabilizes $\mathbf{Z}^n$, hence belongs to $\prod \mathrm{SL}_n \mathbf{Z}_p$.

□

As an upshot, we get the following more uniform statement:

Corollary 10.1.5. *We have*

$$\mathrm{vol}(\mathrm{SL}_n \mathbf{A}/\mathrm{SL}_n \mathbf{Q}) = 1.$$

For SL_n replaced by any semisimple algebraic group, one gets a rational number, and we know what this rational number is.

10.2. The volume of $\mathrm{SO}_q \mathbf{A}/\mathrm{SO}_q \mathbf{Q}$.

We will see that Version 2 of the mass formula looks like the statement

$$\mathrm{vol}(\mathrm{SO}_q \mathbf{A}/\mathrm{SO}_q \mathbf{Q}) = 2.$$

We can phrase things in terms of an *adelic* measure coming from a differential form ω on SL_n coming from det: $M_n \to \mathbf{A}$. As we have seen, the volume of $\mathrm{SL}_n \mathbf{A}/\mathrm{SL}_n \mathbf{Q}$ is 1 (this is the volume with respect to $|\omega|_{\mathbf{R}} \times \prod_p |\omega|_p$. This measure is unchanged by scaling by $\lambda \in \mathbf{Q}^*$, by the product rule, so this is canonical and independent of the choice of ω.

Let Q be a positive-definite integral quadratic form. Let $q = Q$ considered as a $\mathbf{Q}$-form. Fix ω to be a left-invariant algebraic differential form on SO_q. We can "construct" this explicitly as a fibral measure by viewing O_q as the fiber of

$$\mathrm{Mat}_{n\times n} \to \{\text{quadratic forms in } n \text{ variables}\},$$

sending $A \mapsto q(Ax)$, with the measure on M_n being $\prod da_{ij}$ and the measure on quadratic forms is $\prod db_{ij}$, if they are parametrized by $q = \sum b_{ij} x_i x_j$.

We'll prove that with respect to the form $|\omega|_{\mathbf{R}} \prod_p |\omega_p|$,

$$\boxed{\mathrm{vol}(\mathrm{SO}_q(\mathbf{A})/\mathrm{SO}_q(\mathbf{Q})) = 2}$$

and then show that this is equivalent to version 2 of the mass formula.

Proof. Let $g_1, \dots, g_k$ be representatives for $\mathrm{SO}_q\,\mathbf{Q}$-orbits on $\mathrm{SO}_q\,\mathbf{A}_f/\prod_p \mathrm{SO}_q\,\mathbf{Z}_p$. We saw earlier that the set $\{g_i\}$ is in bijection with the genus of Q for the relation of *strict* equivalence, under the map

$$g_i \mapsto (q, g_i\mathbf{Z}^n) =: Q_i.$$

Therefore, we have the partition

$$\mathrm{SO}_q\,\mathbf{A} = \coprod_{i=1}^{k} \mathrm{SO}_q\,\mathbf{Q} \cdot g_i(\mathrm{SO}_q\,\mathbf{R} \cdot U).$$

This gives a good "fundamental domain" for $\mathrm{SO}_q\,\mathbf{Q} \backslash \mathrm{SO}_q\,\mathbf{A}$, but one has to be careful because there is some "folding", due to stabilizers:

$$\mathrm{measure}(\mathrm{SO}_q\,\mathbf{Q} \backslash \mathrm{SO}_q\,\mathbf{A}) = \sum_{i=1}^{k} \frac{\mathrm{measure}(\mathrm{SO}_q\,\mathbf{R} \cdot U)}{\#(SO_q\mathbf{Q} \cap g_i(\mathrm{SO}_q\,\mathbf{R} \cdot U)g_i^{-1})}$$

where $\#(SO_q\mathbf{Q} \cap g_i(\mathrm{SO}_q\,\mathbf{R} \cdot U)g_i^{-1})$ is the number of automorphisms of Q_i. For instance, taking $g_1 = 1$ and we see $\mathrm{SO}_q\,\mathbf{Q} \cap \mathrm{SO}_q\,\mathbf{R} \cdot U$ which is $\mathrm{SO}_q\,\mathbf{Q}$.

Therefore,

$$\mathrm{measure}(\mathrm{SO}_q\,\mathbf{Q} \backslash \mathrm{SO}_q\,\mathbf{A}) = \mathrm{measure}(\mathrm{SO}_q\,\mathbf{R} \cdot U) \sum_{\substack{Q_i \in \mathrm{genus}(Q_1) \\ \mathrm{strict}\sim}} \frac{1}{|\mathrm{Aut}^+ Q_i|}.$$

Recall that the "mass" of the genus up to strict equivalence is always twice the mass of the genus up to equivalence:

$$\sum_{\mathrm{genus}(Q_1)/\mathrm{strict}\sim} \frac{1}{|\mathrm{Aut}^+ Q_i|} = 2 \sum_{\mathrm{genus}(Q)/\sim} \frac{1}{|\mathrm{Aut}(Q)|}.$$

So to show $\mathrm{measure}(\mathrm{SO}_q\,\mathbf{Q} \backslash \mathrm{SO}_q\,\mathbf{A}) = 2$ is equivalent to showing

$$\sum \frac{1}{|\mathrm{Aut}(Q)|} = \frac{1}{\mathrm{measure}(\mathrm{SO}_q\,\mathbf{R} \cdot U)} = \left(\mathrm{measure}(\mathrm{SO}_q\,\mathbf{R}) \prod_p \mathrm{measure}(\mathrm{SO}_q\,\mathbf{Z}_p)\right)^{-1}. \tag{10.2.1}$$

Recall that

$$\mathrm{measure}(\mathrm{SO}_q\,\mathbf{Z}_p) = \lim_{k\to\infty} \frac{\#\frac{1}{2}O_q(\mathbf{Z}/p^k)}{p^{k\dim O_q}}$$

and there is a similar expression for $\mathrm{SO}_q\,\mathbf{R}$.

Example 10.2.1. For $Q = x^2 + y^2$, we have $\mathrm{Aut}(Q) = 8$.

We now calculate the volumes to show that this matches the right side of (10.2.1). For $p \neq 2$,

$$\mathrm{SO}_q(\mathbf{Z}/p^k) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^2 + b^2 = 1 \right\}$$

and the number of solutions is $p^k(1 \pm \frac{1}{p})$, with $+$ when $p \equiv 3 \pmod 4$ and $-$ when $p \equiv 1$ (mod 4).

For $p=2$, we have $\#O_q(\mathbf{Z}/8)=128$ and $\#O_q(\mathbf{Z}/16)=256$, and for all large k,

$$\frac{1}{2}\frac{\#O_q(\mathbf{Z}/2^k)}{2^k}=8.$$

Finally, computing the measure at $p=\infty$ is just a matter of understanding the right normalization of the mesaure. We realize $O_q(\mathbf{R})$ as the fiber of

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\mapsto(\alpha x+\beta y)^2+(\gamma x+\delta y)^2=(\alpha^2+\gamma^2)x^2+2(\alpha\beta+\gamma\delta)xy+(\beta^2+\delta^2)y^2$$

Differentiating this at the identity, we get

$$\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\mapsto(2a_{11},2a_{12}+2a_{21},2a_{22}).$$

Therefore, we can take the fibral invariant form on $O_q\mathbf{R}$ to be $da_{12}/8$ (at the identity), which in terms of the parametrization

$$\mathrm{SO}_2\,\mathbf{R}=\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}$$

is $d\theta/8$. Then $|\omega|_{\mathbf{R}}(\mathrm{SO}_2\,\mathbf{R})=\frac{2\pi}{8}=\frac{\pi}{4}$.

In summary, the right hand side of (10.2.1) is in this case

$$\left(\underbrace{\frac{\pi}{4}}_{\mathbf{R}}\cdot\underbrace{8}_{2}\cdot\prod_p\underbrace{(1\pm 1/p)}_{p>2}\right)^{-1}.$$

Note that

$$\prod_p(1\pm 1/p)^{-1}=(1-1/3+1/5-1/7+1/9+\ldots)^{-1}=\frac{4}{\pi}$$

so the right side of (10.2.1) is 8^{-1}, as desired.

10.3. **The inductive step.** We'll now give an inductive argument showing that Version 2 of the mass formula in dimension $n-1$ implies versions 1 and 2 in dimension n. The idea is the same as the computation of $\sum_{Q,\mathrm{disc}\,Q=D}r_Q(n)$ that we did earlier.

Let Q be the n-dimensional integral quadratic form. Let L_i be representatives for $\mathrm{SO}_q\,\mathbf{Q}$ acting on $\mathrm{SO}_q\,\mathbf{A}_f\cdot\mathbf{Z}^n$. So $L_i\subset\mathbf{Q}^n$ are lattices and $\{(q,L_i)\}$ comprise the genus of Q modulo strict equivalence. We want to show:

$$\text{average of } r_{Q_i}(m)=\frac{\sum_i\frac{r_{Q_i}(m)}{|\mathrm{Aut}^+Q_i|}}{\sum_i\frac{1}{|\mathrm{Aut}^+Q_i|}}$$

or the analogous version with Aut instead of Aut^+ for the genus modulo the usual equivalence (as opposed to strict). The denominator is (by definition) the "total mass". The numerator is

$$\sum_i \frac{r_{Q_i}(m)}{|\mathrm{Aut}^+ Q_i|} = \sum_i \frac{\#\{(v, L_i) \colon q(v) = m\}}{|\mathrm{Aut}(q, L_i)|}$$
$$= \#\left\{ \mathrm{SO}_q\,\mathbf{Q} - \text{orbits on pairs } (v, L) \colon \substack{L \in \mathrm{SO}_q \mathbf{A}_f \cdot \mathbf{Z}^n \\ v \in L \\ q(v) = m} \right\}$$

where if (v, L) has stabilizer $H \subset \mathrm{SO}_q\,\mathbf{Q}$ then it is counted with weight $1/|G|$.

Now we unfold this by moving v to standard position. Fix $v_0 \in \mathbf{Q}^n$ with $q(v_0) = m$. Then all $v' \in \mathbf{Q}^n$ with $q(v') = m$ are in the orbit of v_0 under $\mathrm{SO}_q\,\mathbf{Q}$ (by Witt's Theorem.) Let $H = \mathrm{Stab}(v_0) \subset \mathrm{SO}_q$. This is an orthogonal group in $n-1$ dimensions.

Remark 10.3.1. Gauss showed that the number of representations $x^2 + y^2 + z^2 = n$ has to do with a class number for binary quadratic forms. This seems to be the earliest recognition of the principle that representation numbers in dimension n have to do with class numbers in dimension $n-1$.

So the count is

$$\sum_i \frac{r_{Q_i}(m)}{|\mathrm{Aut}^+ Q_i|} = \sum_i \frac{\#\{(v, L_i) \colon q(v) = m\}}{|\mathrm{Aut}(q, L_i)|}$$
$$= \#\left\{ \mathrm{SO}_q\,\mathbf{Q} - \text{orbits on pairs } (v, L) \right\}$$
$$= \#\{H(\mathbf{Q}) - \text{orbits on } L \in \mathrm{SO}_q \mathbf{A}_f \cdot \mathbf{Z}^n \colon L \ni v_0\}.$$

Let $\mathscr{L} := \{H(\mathbf{Q}) - \text{orbits on } L \in \mathrm{SO}_q \mathbf{A}_f \cdot \mathbf{Z}^n \colon L \ni v_0\}$. We're going to break up the set of lattices L into orbits of $H(\mathbf{A}_f)$. Indeed, the condition of containing v_0 is preserved by $H(\mathbf{A}_f)$, so $H(\mathbf{A}_f)$ acts on $\mathscr{L}$. Choose representatives $L_1, \ldots, L_g$ for these orbits. (If m is not divisible by high powers of primes, then g will usually be 1, so large g has to do with high divisibility of m). Then we write

$$\sum_i \frac{r_{Q_i}(m)}{|\mathrm{Aut}^+ Q_i|} = \sum_i \frac{\#\{(v, L_i) \colon q(v) = m\}}{|\mathrm{Aut}(q, L_i)|}$$
$$= \#\left\{ \mathrm{SO}_q\,\mathbf{Q} - \text{orbits on pairs } (v, L) \right\}$$
$$= \#\{H(\mathbf{Q}) - \text{orbits on } L \in \mathrm{SO}_q \mathbf{A}_f \cdot \mathbf{Z}^n \colon L \ni v_0\}$$
$$= \sum_{j=1}^{g} \#\{H(\mathbf{Q}) - \text{ orbits on } H(\mathbf{A}_f) L_j\}.$$

By the same reasoning as before, $\{H(\mathbf{Q})-$ orbits on $H(\mathbf{A}_f)L_j\}$ are the same as $H(\mathbf{Q})$-orbits on $H(\mathbf{A}_f)/U_j$ where U_j is the stabilizer of L_j in $H(\mathbf{A}_f)$.

Recall that we calculated the total mass to be

$$\mathrm{vol}(\mathrm{SO}_q(\mathbf{A})/\,\mathrm{SO}_q(\mathbf{A})) \cdot \mathrm{vol}(\mathrm{SO}_q\,\mathbf{R} \cdot \prod_p \mathrm{SO}_q\,\mathbf{Z}_p)^{-1}$$

by unfolding the orbits of $\mathrm{SO}_q\,\mathbf{Q}$ on $\mathrm{SO}_q\,\mathbf{A}$. We can apply the same reasoning in this case to the numerator to conclude that

$$\sum_i \frac{r_{Q_i}(m)}{|\mathrm{Aut}^+ Q_i|} = \sum_j \mathrm{vol}(H(\mathbf{A})/H(\mathbf{Q})) \cdot (\mathrm{vol}\, H(\mathbf{R}) \mathrm{vol}(U_j))^{-1}.$$

To summarize, we have chosen some fixed vector v_0 with $Q(v_0) = m$. Let $G = \mathrm{SO}_q(\cong \mathrm{SO}_n)$ and $H = \mathrm{Stab}(v_0)(\cong SO_{n-1})$. We have found

$$\frac{\sum_{Q' \in \mathrm{genus}(Q)} \frac{r_{Q'}(m)}{|\mathrm{Aut}(Q')|}}{\sum_{Q' \in \mathrm{genus}(Q)} \frac{1}{|\mathrm{Aut}\, Q'|}} = \left(\frac{\mathrm{vol}(H(\mathbf{A})/H(\mathbf{Q}))}{\mathrm{vol}(G(\mathbf{A})/G(\mathbf{Q}))}\right) \cdot \sum_{j=1}^{g} \frac{\mathrm{vol}(G(\mathbf{R})) \prod_p \mathrm{vol}\, G(\mathbf{Z}_p)}{\mathrm{vol}(H(\mathbf{R}))\mathrm{vol}(U_j)} \tag{10.3.1}$$

where $L_1, \dots, L_g$ is a set of representatives for $H(\mathbf{A}_f)$ acting on $\mathscr{L} = \{L \in G(\mathbf{A}_f)\mathbf{Z}^n : v_0 \in L\}$.

Note that we can identify $\mathscr{L} = \prod_p \mathscr{L}_p$ where

$$\mathscr{L}_p = \{\text{lattices } L_p \subset \mathbf{Q}_p^n \text{ of form } G(\mathbf{Q}_p) \cdot \mathbf{Z}_p^n : v_0 \in L_p\}$$

The orbits of $H(\mathbf{A}_f)$ on $\mathscr{L}$ correspond to the product over p of $H(\mathbf{Q}_p)$-orbits on $\mathscr{L}_p$. That is a singleton for almost all p.

The Hardy-Littlewood heuristic. Let X be the variety $Q^{-1}(m)$. Note that G acts on X, and the stabilizer of v_0 is H. Define a volume form ω_X on X as the fibral form by regarding X as the fiber of

$$Q : \mathbf{A}^n \to \mathbf{A}^1.$$

According to the Hardy-Littlewood heuristic, the number of solutions to $Q = m$ is approximately

$$\mathrm{vol}(X(\mathbf{R})) \prod_p \mathrm{vol}(X(\mathbf{Z}_p))$$

with volumes with respect to ω_X.

Instead of ω_X we can use the "quotient form" ω_G/ω_H. These are both algebraic differential forms on $X/\mathbf{Q}$, so they are proportional (being both G-invariant). The product formula implies that they give the same answer.

Now G acts transitively on X, but this doesn't necessarily mean that $G(\mathbf{Z}_p)$ acts transitively on $X(\mathbf{Z}_p)$. If that were true, then we would have

$$\mathrm{vol}(X(\mathbf{Z}_p)) = \frac{\mathrm{vol}(G(\mathbf{Z}_p))}{\mathrm{vol}(H(\mathbf{Z}_p))}.$$

In general, there are several orbits of $G(\mathbf{Z}_p)$ acting on $X(\mathbf{Z}_p)$.

Lemma 10.3.2. *The $G(\mathbf{Z}_p)$-orbits on $X(\mathbf{Z}_p)$ are in bijection with $H(\mathbf{Q}_p)$-orbits on $\mathscr{L}_p$.*

Proof. Using that $G(\mathbf{Q}_p)$ acts transitively on $X(\mathbf{Q}_p)$, we have a bijection between $G(\mathbf{Z}_p)$-orbits on $X(\mathbf{Z}_p)$ and $G(\mathbf{Z}_p)$-orbits on vectors $g v_0 \in \mathbf{Z}_p^n$ for $g \in G(\mathbf{Q}_p)$.

$$\begin{tikzcd}
G(\mathbf{Z}_p)\backslash X(\mathbf{Z}_p) \arrow[d, equal] & \\
G(\mathbf{Z}_p)\backslash\{g v_0 \in \mathbf{Z}_p^n : g \in G(\mathbf{Q}_p)\} \arrow[r, equal] & G(\mathbf{Z}_p)\backslash\{g H(\mathbf{Q}_p) : v_0 \in g^{-1}\mathbf{Z}_p^n\}
\end{tikzcd}$$

But

$$G(\mathbf{Z}_p)\backslash\{gH(\mathbf{Q}_p)\colon v_0\in g^{-1}\mathbf{Z}_p^n\}=G(\mathbf{Z}_p)\backslash\{G(\mathbf{Z}_p)g^{-1}H(\mathbf{Q}_p)\colon g^{-1}\mathbf{Z}_p^n\in\mathscr{L}_p\}.$$

Finally, the right side is equal to $H(\mathbf{Q}_p)$-orbits on $\mathscr{L}_p$ by sending the orbit of g to the lattice $g^{-1}\mathbf{Z}_p^n$. □

For $L\in\mathscr{L}_p$, let H_L be the stabilizer of L in $H(\mathbf{Q}_p)$. The Lemma shows that

$$X(\mathbf{Z}_p)=\coprod_{H(\mathbf{Q}_p)-\text{orbits on }\mathscr{L}_p}G(\mathbf{Z}_p)/U_L.$$

At the level of measures this says that

$$\operatorname{vol}(X(\mathbf{Z}_p))=\sum\frac{\operatorname{vol}(G(\mathbf{Z}_p))}{\operatorname{vol}(H_L)}.$$

Also, $\operatorname{vol}(X(\mathbf{R}))=\frac{\operatorname{vol}(G(\mathbf{R}))}{\operatorname{vol}(H(\mathbf{R}))}$ and so taking the product gives

$$\operatorname{vol}(X(\mathbf{R}))\prod_p\operatorname{vol}(X(\mathbf{Z}_p))=\sum\frac{\operatorname{vol}(G(\mathbf{R}))}{\operatorname{vol}(H(\mathbf{R}))}\cdot\prod_p\frac{\operatorname{vol}G(\mathbf{Z}_p)}{\operatorname{vol}(H_L)}.$$

Comparing this with the right side of (10.3.1), we see that we have shown

$$\text{average of } r_Q(m)=\left(\frac{\operatorname{vol}(H(\mathbf{A})/H(\mathbf{Q}))}{\operatorname{vol}(G(\mathbf{A})/G(\mathbf{Q}))}\right)\cdot(\text{HL heuristic}).$$

We would like to show that the multiplying factor $\left(\frac{\operatorname{vol}(H(\mathbf{A})/H(\mathbf{Q}))}{\operatorname{vol}(G(\mathbf{A})/G(\mathbf{Q}))}\right)$ is 1. We will do this by averaging over m.

Remark 10.3.3. This argument is showing that there is a correspondence between

$$\text{solutions to } Q(x)=m\longleftrightarrow\text{genus of a quadratic form in dimension } n-1$$

and there is even a map from left to right, by taking the orthogonal complement.

10.4. **The averaging step.** We now show that

$$\frac{\operatorname{vol}(H(\mathbf{A})/H(\mathbf{Q}))}{\operatorname{vol}(G(\mathbf{A})/G(\mathbf{Q}))}=1$$

by averaging over m, assuming $m\geq 5$. More precisely, the argument works by assuming

$$\operatorname{vol}(\mathrm{SO}_q(\mathbf{A})/\mathrm{SO}_q(\mathbf{Q}))=2$$

for all forms q in dimension $n-1$, and then showing that it is also true in dimension n (i.e. Version 2 in dimension $n-1$ implies Version 1 in dimension n and Version 2 in dimension n).

We can write the Hardy-Littlewood heuristic as

$$\text{HL heuristic}=\nu_\infty(m)\prod_p\nu_p(m)$$

where $\nu_\infty(m)=\operatorname{vol}(X(\mathbf{R}))$ and $\nu_p(m)=\operatorname{vol}(X(\mathbf{Z}_p))$. We have shown that

$$\frac{\sum_{Q_i}\frac{r_{Q_i}(m)}{|\mathrm{Aut}|}}{\sum_{Q_i}\frac{1}{|\mathrm{Aut}|}}=\left(\frac{\operatorname{vol}(H(\mathbf{A})/H(\mathbf{Q}))}{\operatorname{vol}(G(\mathbf{A})/G(\mathbf{Q}))}\right)\cdot\left(\nu_\infty(m)\prod_p\nu_p(m)\right)\tag{10.4.1}$$

We are going to "average" both sides over m.

Letting LHS denote the left hand side of (10.4.1), we clearly have

$$\sum_{m<M} LHS(m) \approx \sum_{m<M} \nu_\infty(m).$$

Theefore, it suffices to show that the average of $\prod_p \nu_p(m)$ over m equals 1. This follows from three ingredients:

(1) For $n \geq 5$, there exists $C = C_q$ such that

$$1 - C/p\sqrt{p} \leq \nu_p(m) \leq 1 + \frac{C}{p\sqrt{p}}.$$

(2) The map $m \mapsto \nu_p(m)$ is continuous as a function of $m \in \mathbf{Z}_p$. (We need $n \geq 3$ for this.)

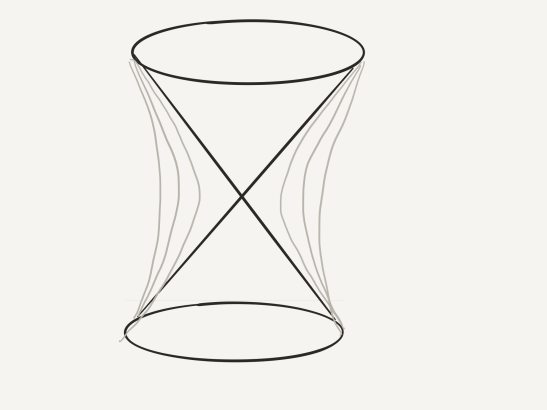
(3) We have

$$\int_{\mathbf{Z}_p} \nu_p(m) = 1$$

This is easy: ν_p is the pushforward of the usual measure on $\mathbf{Z}_p^n$ by the form q, so the measure is the volume of $\mathbf{Z}_p^n$, which is 1.

Why do these imply what we want? (1) means that we can restrict the infinite product to a finite one. (2) says that the sum is approximated by an integral, and (3) says that the integral is 1.

To prove (1) and (2), we use the Fourier transform. Think about the quadratic form $Q := x^2 + y^2 - z^2$.



We're asking about the measure of these fibers. It's infinite, so we cut off by some compact set.

$$\nu_\infty(m) = \text{measure of } K \cap Q^{-1}(m).$$

Something bad happens at the singular point, but the measure of the fiber is still coninuous there. This is non-trivial - it's not true for the similar example $Q' = x^2 - y^2$ in the plane! In fact, the fiber measures blow up if and only if the fibral singularities are *rational* in the sense of algebraic geomery.

Let ψ be a character of $\mathbf{Z}_p$, i.e. a continous homomorphism

$$(\mathbf{Z}_p,+)\to\mathbf{C}^*.$$

By continuity has to factor through $\mathbf{Z}/p^k$ for some k. Let the *level* of ψ be the smallest k such that ψ factors through $\mathbf{Z}/p^k$. For simplicity, suppose $Q=\sum_{i=1}^n x_i^2$ and $p>2$. (There is 1 character of level 0, $p-1$ of level 1, p^2-p of level 2, etc.) Then the Fourier transform of ν_p is

$$\mathscr{F}(\nu_p)=\int\psi(m)\nu_p(m).$$

The measure ν_p is (by definition) the pushforward of the standard one on $\mathbf{Z}_p^n$ by sum of squares, so this

$$\mathscr{F}\nu_p(\psi)=\int_{\mathbf{Z}_p^n}\psi(x_1^2+\ldots+x_n^2)=\left(\int_{\mathbf{Z}_p}\psi(x^2)\right)^n.$$

By the same reasoning as for the Gauss sum, one can check that

$$\left|\int\psi(x^2)\right|^2=p^{-\mathrm{level}(\psi)}.$$

(Think of this as a p-adic Gaussian.) So

$$|\mathscr{F}(\nu_p)|(\psi)=p^{-\mathrm{level}(\psi)n/2}.$$

So if $n\geq 3$, then this is integrable ($\mathscr{F}(\nu_p)\in L^1$)). That's enough to make it continuous. You also get (1) from an explicit estimate.

10.5. **The base case.** We set up the following induction. Let Q be a quadratic form in n variables. Then we showed that

$$\text{Average over genus of } r_Q(m)=\frac{\mathrm{vol}(H(\mathbf{A})/H(\mathbf{Q}))}{\mathrm{vol}(G(\mathbf{A})/G(\mathbf{Q}))}\cdot(\text{HL heuristic}).$$

This was basically an elementary computation. Let's call the left side $LHS(m)$ and the Hardy-Littlewood heuristic $HL(m)$. We also showed that for $m\geq 5$,

$$\sum_{m<M}LHS(m)\sim\sum_{m<M}HL(m). \tag{10.5.1}$$

In particular, if we know that $\mathrm{vol}(H(\mathbf{A})/H(\mathbf{Q}))=2$ for all forms in dimension $n-1$, then we get the result also in dimension n.

Therefore it only remains to establish the base case. There are several options of attack:

(1) Very carefully extend (10.5.1) to all $n\geq 2$. (There has to be something different for $n=2$!)

(2) Weil used the exceptional isomorphisms:
- $\mathrm{SO}_3\sim\mathrm{SL}_2$,
- $\mathrm{SO}_4\sim\mathrm{SL}_2\times\mathrm{SL}_2$.

to handle $n=3,4$.

(3) The Hardy-Littlewood circle method implies that for $n \geq 5$, *without averaging*

$$LHS(m) \sim HL(m) \text{ as } m \to \infty.$$

Also, the group H is evidently unchanged by $m \mapsto k^2 m$. Taking k to be large and using the above, we deduce that

$$\mathrm{vol}(H(\mathbf{A})/H(\mathbf{Q})) = \mathrm{vol}(G(\mathbf{A})/G(\mathbf{Q}))$$

for *all* H. So by checking the volume for *one* H in dimension 4, we get $\mathrm{vol}(H(\mathbf{A})/H(\mathbf{Q})) = 2$ for all $n \geq 4$.

(4) Directly show (in some other way) that

$$LHS(m) = HL(m) \text{ for all } n \geq 3.$$

We will do this with θ-functions (at least in the even unimodular case).

Dimension 2. When $n = 2$, we have in fact

$$LHS(m) = \frac{1}{2} HL(m)$$

i.e. the Hardy-Littlewood prediction is *off* by a factor of 2!

Why? Recall that $HL(m) = \nu_\infty(m) \prod_p \nu_p(m)$. The point of these factors were to "correct" $\nu_\infty(m)$ by a factor $\nu_p(m)$ for each p. The underlying idea is to correct as if different primes impose "independent" conditions. However, in $n = 2$ "the $\nu_p(m)$ are not independent", which causes the overcounting by a factor of 2.

The point is that if a binay form Q has discriminant D, then $\nu_p(m) \neq 0$ implies that $Q(x) - m = 0$ has a solution, so $(-D, m)_p = 1$. But thanks to the product formula, we know that

$$\prod_p (-D, m)_p = 1.$$

10.6. **Examples of version 2 for even unimodular lattices.** If Q arises from an even unimodular lattice, the mass formula gives (noting that all even unimodular lattices lie comprise a single genus)

$$\left(\sum \frac{1}{|\mathrm{Aut}(Q)|} \right)^{-1} = \prod_{i=2}^{n} S_i \prod_p \left(1 - \frac{1}{p^2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p^{n-2}}\right)$$

where

$$S_i := \frac{2\pi^{i/2}}{\Gamma(i/2)}$$

is the volume of a high-dimensional sphere. Therefore, the archimedean term is the volume of $\mathrm{SO}_n \mathbf{R}$, and the factoring coming from p is the volume of $\mathrm{vol}(\mathrm{SO}_q \mathbf{Z}_p)$. Actually, in this product the middle term has exponent 2, e.g. for $n = 8$ it is

$$\prod_{i=2}^{8} S_i^{-1} \zeta(2)\zeta(4)^2\zeta(6).$$

You can make this nicer by using the functional equation, which absorbs the real volume terms.

- For $n = 8$, the formula gives
$$1/|\mathrm{Aut}\, E_8| \approx 1.4 \times 10^{-9}.$$
- In dimension 16, the right side is 2.4×10^{-18}.
- In dimension 24, the right side is 7.9×10^{-15}.
- In dimension 32, you get about 40×10^6. So there are at least 80 million even unimodular lattices, since $\mathrm{Aut}\, Q \geq 2$.

The Gamma is like a factorial, so this is asymptotically n^{Cn^2}. The Gram matrix has n^2 entries, with size about n. From this you can deduce a lower bound for $b_i(\mathrm{SL}_n \mathbf{Z})$. The reason is that you can construct an involution of the locally symmetric space (Rohlfs) with fixed points the unimodular lattices, and use Lefschetz fixed point formula.

11. Theta series

11.1. **Modular forms from theta series.** Let L be an even unimodular lattice of dimension n and $Q(x) = \frac{\langle x,x\rangle}{2}$. We define the theta series
$$\theta_Q = \sum_{x \in \mathbf{Z}^n} e^{2\pi i z Q(x)} = \sum_{m \geq 0} r_Q(m) q^m$$
for $q = e^{2\pi i z}$. This is convergent for $\mathrm{Im}\, z > 0$, i.e. $|q| < 1$.

Theorem 11.1.1. *Suppose that* $2Q$ *arises from an even unimodular lattice (so* Q *itself can take odd values). Then*

(1) θ_Q *is a modular form for* $\mathrm{SL}_2 \mathbf{Z}$ *of weight* $n/2$.

(2) The average of θ_Q *over the genus of* Q*, meaning*
$$\frac{\sum \frac{\theta_{Q_i}}{|\mathrm{Aut}\, Q_i|}}{\sum \frac{1}{|\mathrm{Aut}\, Q_i|}}$$
is the Eisenstein series of weight $n/2$*, normalized with constant term* 1.

Remark 11.1.2. This second statement is an instance of a more general phenomenon observed by Siegel-Weil: the "average of θ-series over a genus = an Eisenstein series".

In particular, (2) gives a computation of the average of $r_Q(m)$ and you can check that this equals $HL(m)$. So you can think of (2) as a different incarnation of the mass formula (version 1).

11.2. **Proof of Theorem 11.1.1.** It is enough to check that it transforms as
$$\theta_Q\left(\frac{az+b}{cz+d}\right) = (cz+d)^{n/2}\theta_Q(z)$$
for
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
since they generate $\mathrm{SL}_2 \mathbf{Z}$. The first is obvious: it is built into the periodicity. The second corresponds to $z \mapsto -1/z$. It follows from Poisson summation.

To explain: we can think of Q as arising from the standard quadratic form $\sum x_i^2$ on $\mathbf{R}^n$, restricted to some lattice $L \subset \mathbf{R}^n$. Unimodularity means that the dual lattice

$$L^\vee := \{v \in \mathbf{R}^n : \langle v, L\rangle \in \mathbf{Z}\} = L.$$

The Fourier transform is

$$\hat{f}(k) = \int_v f(x) e^{2\pi i \langle k,x\rangle}\, dx$$

where dx is "Lebesgue measure", obtained by choosing an orthonormal basis. Poisson summation says that

$$\sum_{v \in L} f(v) = \sum_{\xi \in L^\vee} \hat{f}(\xi)$$

(using that L is unimodular), where

$$\hat{f}(\xi) = \int f(x) e^{2\pi i \langle x, \xi\rangle}\, dx.$$

We apply this to $f(x) := e^{-\pi t \langle x,x\rangle}$, which has the important property that

$$(\mathscr{F} e^{-\pi\langle x,x\rangle})(\xi) = e^{-\frac{\pi}{t}\langle \xi,\xi\rangle}.$$

Now using that L is even unimodular,s we find that

$$\hat{f}(x) = e^{-\frac{\pi}{t}\langle x,x\rangle} t^{-n/2}.$$

This implies that

$$\sum_{x \in L} e^{-\pi t\langle x,x\rangle} = t^{-n/2} \sum_L e^{-\frac{\pi}{t}\langle x,x\rangle}$$

using that $L = L^*$, so putting $t = iz$ gives

$$\theta_Q(z) = z^{-n/2}\theta_Q(-1/z).$$

Eisenstein series. Now we come to the second part. First, we give a digression on what Eisenstein series actually are. Modular forms of weight k correspond to functions on lattices in $\mathbf{C}$, which are homogeneous:

$$f(\lambda\Lambda) = \lambda^{-k} f(\Lambda).$$

In particular, E_k corresponds to

$$f(\Lambda) := \sum_{z \in \Lambda} z^{-k}.$$

The graded ring of (level one) modular forms is generated by the Eisenstein series E_4 and E_6:

$$\bigoplus_k \mathscr{M}_k = \mathbf{C}[E_4, E_6].$$

Now, the Fourier expansion of Eisenstein series is

$$E_k \sim (\text{constant term}) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

How can you remember the constant term? If you look back at the definition of Eisenstein series, you see that it should be formally 0 when $q=1$. Formally we also have

$$\sum \frac{\sigma_{k-1}(n)}{n^s} = \zeta(0)\zeta(1-k)$$

so the constant term is $-\zeta(0)\zeta(1-k)$.

Example 11.2.1. When $n=8$, we have $\mathscr{M}_4 = \mathbf{C}E_4$. Since $\theta_{\mathbb{E}_8}$ is in here, it must be propotional to E_4:

$$E_4 \sim \theta_{\mathbb{E}_8} = 1 + \dots.$$

Comparing constant terms, we find

$$\theta_{\mathbb{E}_8} = 1 + \frac{-1}{\zeta(0)\zeta(-3)} \sum \sigma_3(n) q^n$$

and the constant $\frac{-1}{\zeta(0)\zeta(-3)}$ is 240, so the number of vectors in E_8 of length $2m$ is $240\sigma_3(m)$.

Example 11.2.2. When $n=16$ we have lattices $\mathbb{E}_8 \oplus \mathbb{E}_8$ and $\mathbb{E}_{16}$, so

$$\theta_{\mathbb{E}_8 \oplus \mathbb{E}_8} = \theta_{\mathbb{E}_{16}}.$$

This was used by Milnor to give an example of two non-isomorphic Riemannian manifolds with the same spectrum (of the Laplacian). The point was to consider $\mathbf{R}^{16}$ modulo the respective lattices; the fact that the associated theta functions coincide implies that that the quotients have the same spectrum.

Example 11.2.3. For $n=24$, $\mathscr{M}_{12}$ is the span of E_{12} and $\Delta = E_4^3 - E_6^2$. For every even unimodular L,

$$\theta_Q = \alpha E_{12} + \beta \Delta.$$

The constant α is determined by the fact that the first coefficient is 1, and the second constant is determined by knowing the number of vectors of length 2.

For the Leech lattice, we have

$$\theta = 1 + \frac{65520}{691} \sum \sigma_n(m) q^m + ?$$

Recall that for the Leech lattice $r_Q(1) = 0$ (arranging this to be the case was one of the motivations for the construction), so we must have

$$\theta = 1 + \frac{65520}{691} \sum \sigma_n(m) q^m - \frac{65520}{691}\Delta.$$

Note that this implies that

$$\tau(m) \equiv \sigma_{11}(m) \mod 691$$

because θ is clearly integral.

Example 11.2.4. For $n=32$, $\mathscr{M}_{16}$ is still two-dimensional. So by the same reasoning the theta series are determined by one parameter, namely the number of vectors of shortest length. There aren't so many vectors, so many of them give the same theta series.

Finally, we discuss part (2) of Theorem 11.1.1. To prove it, we use Hecke operators. Recall that

$$T_m f(\Lambda) = \frac{1}{m} \sum_{\Lambda' \subset_m \Lambda} f(\Lambda').$$

Lemma 11.2.5. *Fix $m \geq 2$. The Eisenstein series E_k is an eigenfunction of T_m with eigenvalue $\sigma_{k-1}(m)$ and this space is 1-dimensional.*

Proof. It's enough to show that all eigenvalues of T_m on $\mathscr{S}_k$ are smaller. We'll show by a maximum modulus argument that any eigenvalue of T_m is at most $(\deg T_m) m^{k/2-1}$. For instance, if m is prime then this is $\leq (m+1)m^{k/2-1}$.

Namely, we homogenize f by multiplying it by a power of the area: more precisely, $\widetilde{f}(\Lambda) := f(\Lambda) \cdot \text{Area}(\Lambda)^{-k/2}$. This makes it so that $\widetilde{f}$ depends only on the class of the lattice modulo homothety, so it descends to a function on the usual fundamental domain. The cuspidality assumption implies that f extends continuously to the point at infinity, hence is bounded. Then by the maximum modulus principle applied at a point where $\widetilde{f}$ is maximized shows that $T\widetilde{f}$ expands it by at most the degree.

□

Therefore, it's enough to show that the average of θ_Q is a T_m-eigenfunction. Fix p and let the neighbors of Q be $Q_1, \dots, Q_g$. Let g be the number of isotropic lines in $(\mathbf{Z}/p\mathbf{Z})^n$. We claim that

$$\sum \theta_{Q_i} = (a + bT_{p^2})\theta_Q$$

for a and b which are explicit polynomials in p. (In fact we'll see that $b = 1$.)

To see why this claim finishes off the proof, note that summing this equation over Q in a genus, we obtain

$$g(\text{Average of } \theta_Q) = (a + bT_{p^2})(\text{Average of } \theta_Q),$$

because g is the number of neighbors.

To see the claim, we remind you what the neighbor operation is.

(1) Start with (L, Q) and take $0 \neq v \in L/pL$ with $Q(v) = 0$.
(2) Lift v to $\widetilde{v} \in L$ such that $Q(\widetilde{v}) \equiv 0 \pmod{p^2}$.
(3) Set $L' = \{y \in L \colon \langle y, v \rangle \equiv 0 \pmod{p}\} + \mathbf{Z}\frac{\widetilde{v}}{p}$.

Now, by definition

$$\sum_{i=1}^{g} \theta_{Q_i} = \sum_{i=1}^{g} \sum_{v \in L_i} q^{Q(v)}.$$

All the possible neighbors L_i are in $p^{-1}L$. We count for each $v \in p^{-1}L$ how many L_i contain it. So we rewrite the above as

$$\sum_{w \in p^{-1}L} \#\{L_i \ni w\} \cdot q^{Q(w)}.$$

There are several cases; we just sketch how they go.

- If $w \in pL$, then $\#\{L_i \ni w\} = g$. (All neighbors contains pL.)

- If $w \in L - pL$, then a neighbor L_i formed from $v \in L/pL$ contains w exactly when $\langle w, v\rangle \equiv 0 \pmod{p}$. So we need to figure out the number of isotropic vectors orthogonal to w. That is, we are looking for the number of isotropic lines in $w^{\perp} \subset (\mathbf{Z}/p\mathbf{Z})^n$. There are two subcases, depending on whether or not w is itself isotropic.
- If $w \in p^{-}L - L$, then $w \in L_i$ if and only if $Q(w) \in \mathbf{Z}$ (and w can only be contained in one L_i).

♠♠♠ TONY: [this still needs to be finished]

11.3. **Theta functions from general lattices.** Let Q be an integral quadratic form on L. Then there is an associated bilinear form

$$\langle x, y\rangle = Q(x+y) - Q(x) - Q(y).$$

To be clear, if $Q(x) = x^T A x$ then $\langle x, y\rangle = x^T(2A)y$.

Let $D = \text{disc} = \det(\langle \cdot, \cdot \rangle) = \#(L^*/L)$ where L^* is the dual of L with respect to $\langle \cdot, \cdot\rangle$. Note that $L^* \supset L$ because the pairing is integral on L.

Let $\theta_Q(z) = \sum_{x \in L} e^{2\pi i z Q(n)}$. This is evidently still periodic, but if we apply Poisson summation then we obtain

$$\theta_Q(z) = \left(\sum_{x \in L^*} e^{2\pi i(-1/z)Q(n)} \right)(\ldots).$$

This is problematic because it relates θ_Q not to itself but to a theta function attached to a *different* lattice. The way out will be to analyze the package of several theta functions at once. That is, we'll analyze not only θ_Q but the sums over every coset of L in L^*:

$$\sum_{L+\lambda} e^{2\pi i z Q(n)}.$$

Fourier analysis on groups. For any $\psi \in \mathbf{C}[L^*/L]$, define

$$\theta_\psi = \sum_{n \in L^*/L} \psi(n) \sum_{x \in n+L} e^{2\pi i Q(x) z} = \sum_{x \in L^*} \psi(x) e^{2\pi i Q(x) z}.$$

(In this framework, the theta function attached to L is the special case with ψ equal to the characteristic function of the identity.) Call $G := L^*/L$. The form $\langle \cdot, \cdot \rangle$ descends to a pairing

$$G \times G \to \mathbf{Q}/\mathbf{Z}$$

and also Q descends to a function

$$Q \colon G \to \mathbf{Q}/\mathbf{Z}.$$

If we change z to $z+1$, we find

$$\theta_\psi(z+1) = \theta_{e^{2\pi i Q}\psi}(z)$$

where $e^{2\pi i Q}$ is viewed as a function on G.

The Fourier transform on G is

$$(\mathscr{F}\psi)(\ell) := \frac{1}{\sqrt{D}}\sum_{G}\psi(x)e^{2\pi i\langle x,\ell\rangle}$$

(noramlized to make it unitary). An exercise in Poisson summation shows that

$$\left(\frac{i}{z}\right)^{n/2}\theta_{\psi}(-1/z) = \theta_{\mathscr{F}\psi}(z).$$

The Weil representation. Define operators $S, T \colon \mathbf{C}[G] \to \mathbf{C}[G]$ by

$$T\psi = \psi \cdot e^{-2\pi i Q}$$
$$S\psi = (\mathscr{F}\psi)\gamma_q$$

Here $\gamma_q \in \mu_8$, and in fact $\gamma_q \in \mu_4$ if n is even. However, just ignore it for now.

These satisfy the relations

$$(S^2) = (ST)^3 = \gamma_Q^2 w \tag{11.3.1}$$

where $w\psi(x) = \psi(-x)$. These relations look a lot like the ones for the standard generators S, T of $\mathrm{SL}_2\mathbf{Z}$. In particular, the map

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \mapsto S$$
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto T$$

extends (for n even) to a map $\rho\colon \mathrm{SL}_2\mathbf{Z} \to \mathrm{Aut}(\mathbf{C}[G])$. For n even, then, we have an action of $\gamma \in \mathrm{SL}_2\mathbf{Z}$ on the theta functions:

$$\theta_{\psi}\,|_{\gamma^{-1}} = \theta_{\gamma\psi}.$$

where the slash operator is

$$(f\,|_{\gamma})(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

and for n odd this is similar, but with a 2-fold cover of $\mathrm{SL}_2\mathbf{Z}$.

Now we go back to explain what γ_Q is. A formula for it is

$$\gamma_Q = \frac{1}{\sqrt{D}}\sum_{x\in G} e^{2\pi i Q(x)} = i^{n/2}.$$

(Note that this implies that the dimension of an even unimodularlattice is divisible by 8, since we have seen that in that case $\gamma_Q = 1$.)

Example 11.3.1. For $L = \mathbf{Z}$ and $Q(x) = x^2$, the pairing is $2xy$ and $L^* = 1/2\mathbf{Z}$, so

$$\gamma = \frac{1}{\sqrt{2}}(1 + e^{\pi i/2}) = \sqrt{i}.$$

Why does this help? It's a fact that for n even, the representation ρ factors through $\mathrm{SL}_2(\mathbf{Z}/D)$, so θ_{ψ} is a modular form of weight $n/2$ for $\Gamma(D)$.

Let's discuss how to check the relations

$$(S^2) = (ST)^3 = \gamma_Q^2 w.$$

Let $\delta_x \in \mathbf{C}[G]$ be the characteristic function of x and $e_x = \mathscr{F}\delta_x$, so $e_x(y) = e^{2\pi i \langle x,y\rangle}$. Write $e(Q)$ for $e^{2\pi i Q}\colon G \to \mathbf{C}^*$.

You can just compute that

$$\mathscr{F}(e(Q)e_x) = \gamma_Q e^{-2\pi i Q(x)} e(-Q)e_{-x}.$$

etc.

Extra symmetries. The representation ρ is closely related to a natural projective representation $\rho_{G\times G}$ of $G \times G$ on $\mathbf{C}[G]$. This come from two different natural actions of G on $\mathbf{C}[G]$. We take $(g,1)$ to act by translation ($\delta_x \mapsto \delta_{x+g}$), and $(1,g)$ acts by translation in Fourier space, which comes out to

$$e_x \mapsto e_{x-g}.$$

These don't commute, but they commute up to scalar, hence descend to an action on the projectivization.

The representation ρ_{SL_2} is compatible with $\rho_{G\times G}$ in the following sense. We have an action of SL_2 on $G \times G$. The $(g,1)$ and $(1,g)$ are switched by Fourier transform. This means that for $\gamma \in \mathrm{SL}_2\mathbf{Z}$,

$$\rho_{G\times G}(\gamma(g,h)\gamma^{-1}) = \rho_{\mathrm{SL}_2}(\gamma)\rho_{G\times G}(g,h)\rho_{\mathrm{SL}_2}(\gamma^{-1})$$

(equality up to scalar). You can check this on the generators. This property actually almost characterizes ρ_{SL_2}. The reason this doesn't characterize is because of issues with projective representations (there is a centralizer, even for PGL_2).

11.4. **Moduli interpretation.** The slogan of the moduli interpretation is:

> Theta series come from sections of line bundles over the universal abelian variety.

To explicate, a modular form is a section of a line bundle on a modular curve. Theta series extend to sections on the universal abelian variety.

The more precise way to say this is as follows. Consider the moduli space $\mathscr{M}$ parametrizing abelian varieties equipped with a symmetric theta divisor (the zero locus of section of degree 1 ample symmetric line bundle, i.e. $[-1]^*\mathscr{L} \cong \mathscr{L}$). This has a universal abelian variety $\mathscr{A}$ with universal theta divisor $\mathscr{O}(\Theta)$.

$$\begin{tikzcd} \mathscr{A} \arrow[d] \\ \mathscr{M} \arrow[u, bend left=60, "e"] \end{tikzcd}$$

From this we get a divisor $e^*\mathscr{O}(\Theta)$ on $\mathscr{M}$.

Theorem 11.4.1 (Mumford)**.** *We have*

$$(e^*\mathscr{O}(\Theta))^{\otimes 2} = e^*(\det \Omega^1_{\mathscr{A}/\mathscr{M}})^\vee \textit{ in } \mathrm{Pic}(\mathscr{M}) \otimes \mathbf{Q}.$$

Remark 11.4.2. The need to tensor with $\mathbf{Q}$ comes from the horrible mess of 8th roots of unity that we saw earlier.

We get classical θ-series by pulling back a section of $\mathscr{O}(\Theta)$ along the identity section. (This accounts for the extra symmetries.)

Example 11.4.3. Consider $\sum q^{n^2}$. We want to see how this is a specialization of a section on $\mathscr{A}$ along the identity section. Consider

$$\theta(q,z) = \sum_{n \in \mathbf{Z}} z^{2n} q^{n^2}$$

for $z \in \mathbf{C}^*$. Then we can regard $\theta(q,z)$ as a section of a line bundle over the eliptic curve $\mathbf{C}^*/q^{\mathbf{Z}}$. It satisfies

$$\theta(q,zq) = q^{-1} z^{-2} \theta(q,z).$$

So $\theta(q,z)$ is a section of the corresponding line bundle on $\mathbf{C}^*/q^{\mathbf{Z}}$.

Which line bundle is this? (For instance what is it's degree?) When $z^2 = -q$, the theta function become

$$\sum_{n \in \mathbf{Z}} q^{n^2 - n}$$

which vanishes formally after grouping in pairs. So θ vanishes along the divisor cut out by $z^2 = -q$, i.e. the line bundle is $\mathscr{O}(P_1 + P_2)$ where P_1, P_2 are the nontrivial 4-torsion points.

Now that we know what the line bundle is, we can write down another section as

$$\prod_{m \in \mathbf{Z}} \left(1 - \left(\frac{z^2}{-q} \right) q^m \right)$$

This doesn't make sense because of all the negative terms, so we rewrite it:

$$\theta' := \prod_{m \geq 0} \left(1 - \left(\frac{z^2}{-q} \right) q^{2m} \right) \prod_{m > 0} \left(1 - \left(\frac{z^2}{-q} \right)^{-1} q^{2m} \right)$$

This θ' has the same transformation law:

$$\theta'(qz,q) = (z^{-2} q^{-1}) \Theta'(z,q)$$

and the ratio θ'/θ is basically $\prod_{n \geq 0} (1 - q^{2n})$. Unwinding the precise relation gives the Jacobi triple product formula.