Lecture 1: Geometry of Numbers

F. Oggier

Journées Algébriques du Gabon, Libreville, Mars 2025

Overview

These lectures are about lattices, a bit of their geometry, how they relate to:

- number theory (Lecture 1),
- "classical" coding theory (Lecture 2),
- algebraic number theory (Lecture 3),
- quaternion algebras (Lecture 4).

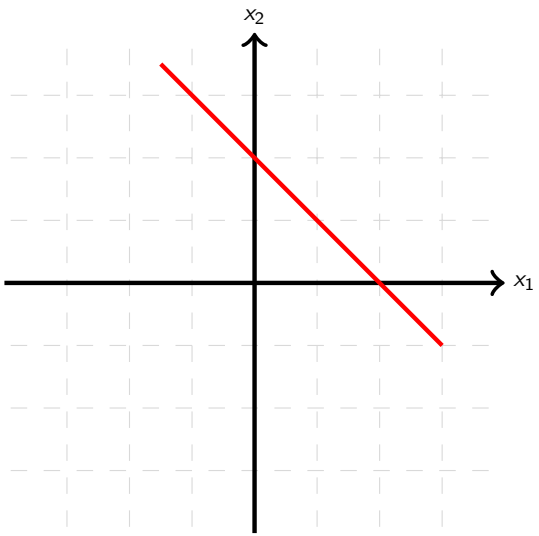
All lectures also discuss some connection to either coding theory or cryptography.

- Hermann Minkowski (1864-1909): number theory, mathematical physics, theory of relativity.
- Geometric tools to study number theoretic problems.

- The volume $v(X)$ of a subset $X \subset \mathbb{R}^n$ is defined as

$$v(X) = \int_X dx_1 \cdots dx_n.$$

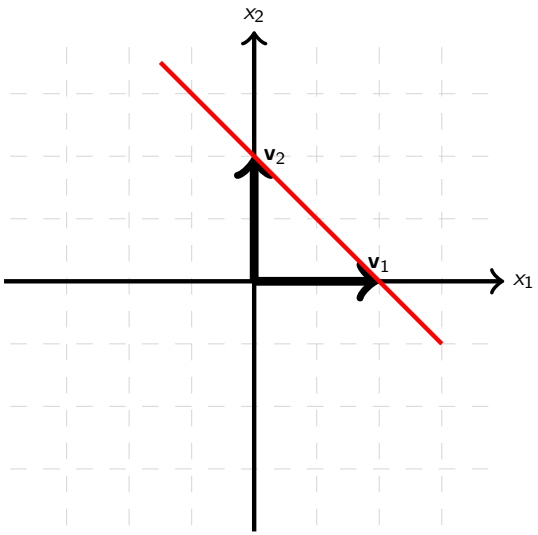
$$\begin{aligned} v(X) &= \int_0^{b/a_2} \left(\int_0^{\frac{b}{a_1} - \frac{a_2 x_2}{a_1}} dx_1 \right) dx_2 \\ &= \int_0^{b/a_2} \frac{b - a_2 x_2}{a_1} dx_2 \\ &= \frac{b^2}{2a_1 a_2}. \end{aligned}$$

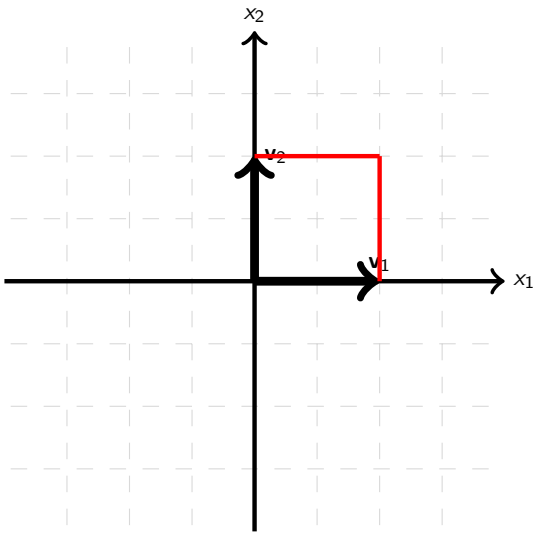


$a_1 x_1 + a_2 x_2 \leq b,\ x_1, x_2 \geq 0$
$\left(x_1 = \frac{b}{a_1} - \frac{a_2 x_2}{a_1},\ a_1 \neq 0,\ a_2 \neq 0\right)$

- The volume $v(X)$ of a subset $X \subset \mathbb{R}^n$ is defined as

$$v(X) = \int_X dx_1 \cdots dx_n.$$





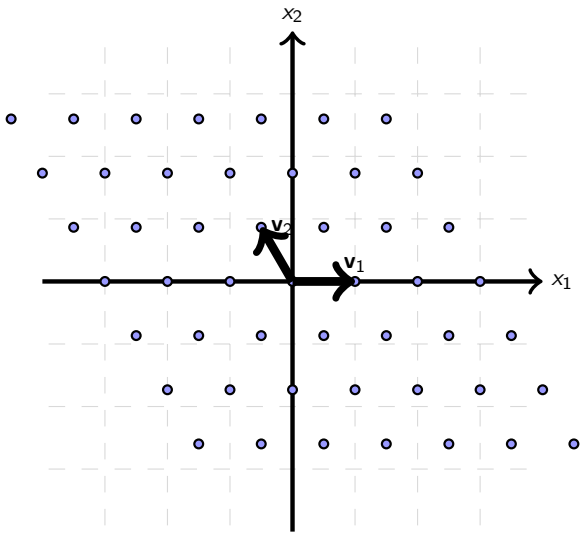
$$\begin{aligned} v(X) &= \int_0^{b/a_2} \left(\int_0^{\frac{b}{a_1} - \frac{a_2 x_2}{a_1}} dx_1 \right) dx_2 \\ &= \frac{b^2}{2a_1 a_2} \end{aligned}$$

$$\begin{aligned} v(X) &= \int_0^{b/a_2} \int_0^{b/a_1} dx_1 dx_2 \\ &= \det\left(\begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{bmatrix} \right) = \frac{b^2}{a_1 a_2} \end{aligned}$$

Suppose $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent vectors in $\mathbb{R}^n$ $(m \leq n)$.

- A lattice $L \subset \mathbb{R}^n$, generated by $\mathbf{v}_1, \ldots, \mathbf{v}_m$, is the additive subgroup of $\mathbb{R}^n$ generated by $\mathbf{v}_1, \ldots, \mathbf{v}_m$:

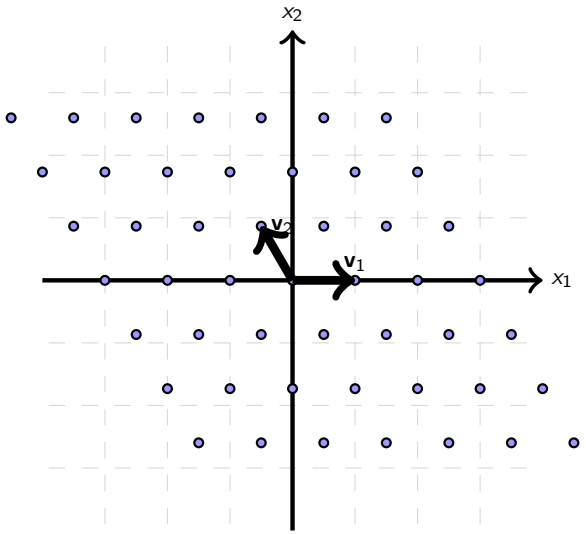
$$L = \{\mathbf{u}M,\ \mathbf{u} \in \mathbb{Z}^m\},\ M = \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_m \end{bmatrix},\ G = MM^T.$$



$$M = \begin{bmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix},\ G = \begin{bmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{bmatrix}.$$

We will consider $m = n$.

The matrix M containing the basis vectors is called a generator matrix, the matrix $G = MM^T$ is called a Gram matrix (it contains the "geometry" of the lattice, that is the norms of the basis vectors on its diagonal, and their inner product or angle elsewhere).

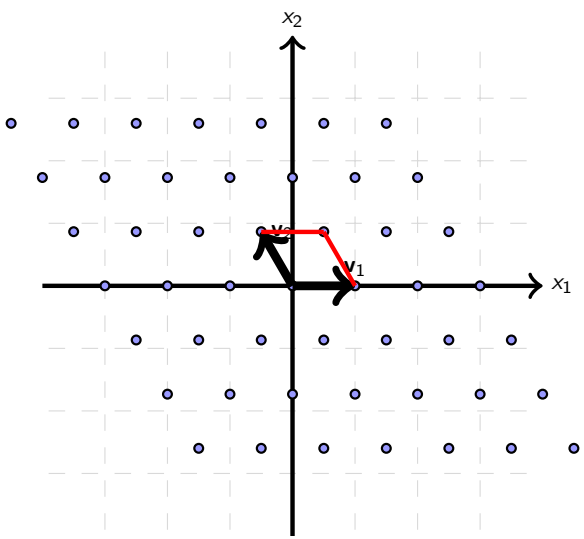


$$M = \begin{bmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}, \; G = \begin{bmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{bmatrix}.$$

A lattice has many generator matrices and Gram matrices.

- Lattices are defined up to a change of basis by a unimodular matrix (with integer coefficients and determinant ± 1).
- Multiplication by an orthogonal matrix rotates the lattice.
- Scaling changes the matrices by a scale factor but does not change the geometry.

- A fundamental domain T for a lattice L is the set consisting of all elements $\sum_{i=1}^{m} a_i \mathbf{v}_i$, where $a_i \in [0,1) \subset \mathbb{R}$.
- The determinant of a lattice L, denoted by $\det(L)$, is the square of the volume of the fundamental domain of L, or the determinant of its Gram matrix $G = MM^T$.



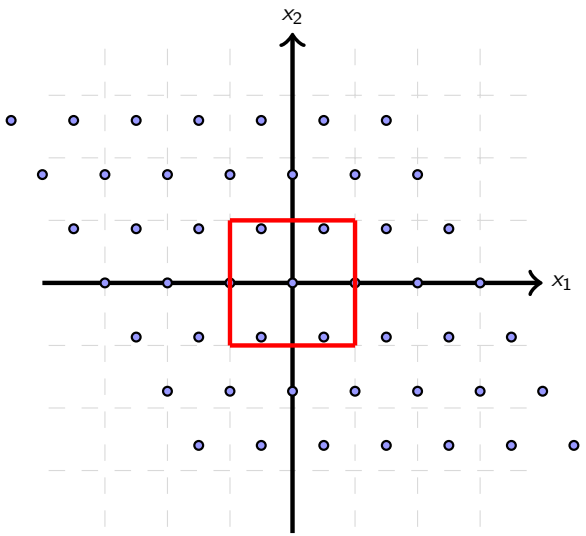
$$\begin{aligned} \det(L) &= v(T)^2 \\ &= \left(\int\int dx_1 dx_2\right)^2 \\ &= \det\left(\begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{bmatrix}\right)^2 = \frac{3}{4}. \end{aligned}$$

$$M = \begin{bmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}, \; G = \begin{bmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{bmatrix}.$$

- A subset $X \subset \mathbb{R}^n$ is convex if whenever $x, y \in X$, the point $\lambda x + (1-\lambda)y \in X$ for all real λ, $0 \leq \lambda \leq 1$. Geometrically, all points on the straight line segment joining x to y also lie in X, whenever $x, y \in X$.
- A subset $X \subset \mathbb{R}^n$ is symmetric if $x \in X$ implies $-x \in X$. Geometrically, X is invariant under reflection in the origin.

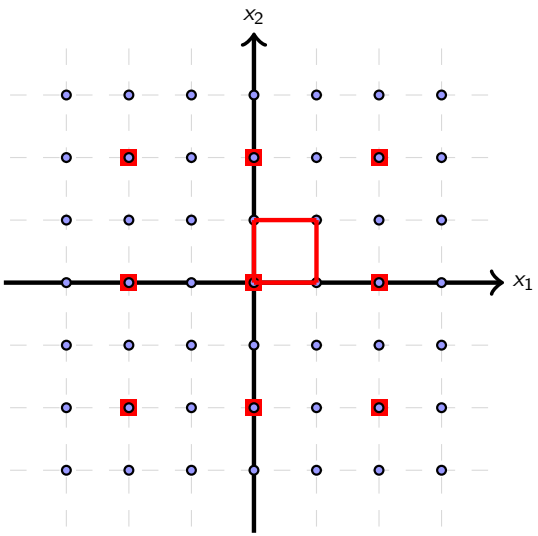
Minkowski's Theorem.

Let L be an n-dimensional lattice in $\mathbb{R}^n$ with fundamental domain T, and let X be a bounded symmetric convex subset of $\mathbb{R}^n$. If $v(X) > 2^n v(T)$, then X contains a non-zero point of L.



$$v(X) > 2^2 \frac{\sqrt{3}}{2} = 2\sqrt{3} \approx 3.4641$$

Proof. Scale L by a factor of 2, to get the lattice $2L$ with fundamental domain $2T$ of volume $2^n v(T)$.



Consider the torus

$$\mathbb{T}^n = \mathbb{R}^n/2L,$$

whose volume by definition is

$$v(\mathbb{T}^n) = v(2T) = 2^n v(T).$$

Now the natural map $\pi : \mathbb{R}^n \to \mathbb{T}^n$ cannot preserve the volume of X, since

1. by assumption

$$v(X) > 2^n v(T) = v(\mathbb{T}^n),$$

2. and since $\pi(X) \subseteq \mathbb{T}^n$, we have

$$v(\pi(X)) \leq v(\mathbb{T}^n) = 2^n v(T) < v(X).$$

Thus $v(X) \neq v(\pi(X))$, i.e., π does not preserve the volume of X.
Claim. It follows that $\pi|_X$ is not injective.
Hence there exist $x_1, x_2 \in X$, $x_1 \neq x_2$ such that

$$\pi(x_1) = \pi(x_2) \iff x_1 - x_2 \in 2L.$$

Since $x_2 \in X$, then by symmetry of X, $-x_2 \in X$. Since $x_1, -x_2 \in X$, then by convexity of X, $\frac{1}{2}(x_1 - x_2) \in X$.
Thus, since $x_1 - x_2 \in 2L$, $\frac{1}{2}(x_1 - x_2)$ is a non-zero point of L contained in X. $\square$

Claim. If X is a bounded subset of $\mathbb{R}^n$ and $v(X)$ exists, and if $v(\pi(X)) \neq v(X)$, then $\pi|_X$ is not injective.

Proof. Assume $\pi|_X$ is injective. Since X is bounded, it intersects only a finite number of $T + l$ for T a fundamental domain of L and $l \in L$. Set $X_l = X \cap (T + l)$ so we have

$$X = X_{l_1} \cup \ldots \cup X_{l_n}.$$

Set $Y_{l_i} = X_{l_i} - l_i$, so $Y_{l_i} \subseteq T$. Since $\pi(x - l_i) = \pi(x)$ for all $x \in \mathbb{R}^n$, the Y_{l_i} are disjoint as a consequence of $\pi|_X$ being injective.

$$\begin{aligned} v(\pi(X)) &= v(\pi(\cup X_{l_i})) \\ &= v(\cup Y_{l_i}) \text{ since } \pi(X_{l_i}) = \phi(Y_{l_i}) \text{ for } \phi : T \simeq \mathbb{T}^n \\ &= \sum v(Y_{l_i}) \text{ since } Y_{l_i} \text{ are disjoint} \\ &= \sum v(X_{l_i}) \text{ since translation preserves the volume} \\ &= v(X), \text{ a contradiction.} \square \end{aligned}$$

A locally volume-preserving map that does not preserve volume globally cannot be injective.

Two-Squares Theorem. If p is a prime of the form $4k+1$, then p is a sum of two integer squares.

Proof. The multiplicative group of invertible integers modulo p has order $p-1=4k$, so it contains an element u of order 4. Then $u^2 \equiv -1 \pmod{p}$ since -1 is the only element of order 2.

- Let $L \subseteq \mathbb{Z}^2$ be the lattice in $\mathbb{R}^2$ consisting of all pairs (a,b) such that $b \equiv ua \pmod{p}$.
- Then $(a,b) = a(1,u) + k(0,p)$ for $k \in \mathbb{Z}$, and the volume of a fundamental domain T for L is p.

By Minkowski's Theorem, any circle with its centre at the origin and radius r which has area

$$\pi r^2 > 4p$$

contains a non-zero point of L.

- Choose $r^2 = \frac{3p}{2}$, so $\pi r^2 = \frac{3\pi}{2} p > 4p$.
- Hence, there exists a non-zero point (a, b) of L for which

$$0 \neq a^2 + b^2 \leq r^2 = \frac{3}{2} p < 2p.$$

- From $b \equiv ua \pmod{p}$ and $u^2 \equiv -1 \pmod{p}$, we have

$$a^2 + b^2 \equiv a^2 + u^2 a^2 \equiv 0 \pmod{p}.$$

Since $a^2 + b^2$ is a multiple of p that strictly lies between 0 and $2p$, it must be equal to p. $\square$

Four-Squares Theorem. Every positive integer is a sum of four integer squares.

Proof. We first prove that the theorem holds for all prime p.

- If $p = 2$, $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Suppose p is odd. The congruence equation

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}$$

has a solution with $u, v \in \mathbb{Z}$. Indeed, u^2 takes $(p+1)/2$ distinct values, and so does $-1 - v^2$, for a total of $p+1$ values, so they must intersect.

- Consider the lattice $L \subset \mathbb{Z}^4$ consisting of points (a, b, c, d) such that

$$c \equiv ua + vb \pmod{p}, \; d \equiv ub - va \pmod{p}.$$

- Then $(a, b, c, d) =$
  $a(1, 0, u, -v) + b(0, 1, v, u) + k(0, 0, p, 0) + l(0, 0, 0, p)$,
  $k, l \in \mathbb{Z}$, and the volume of a fundamental domain T for L is p^2.

By Minkowski's Theorem, any 4-dimensional sphere with its centre at the origin and radius r such that its volume is greater than $16p^2$ contains a non-zero point of L.

- Choose $r^2 = 1.9p$, then the volume of the sphere is $\frac{\pi^2 r^4}{2} = \frac{(1.9p\pi)^2}{2} > 16p^2$.
- Then there exists a non-zero lattice point (a, b, c, d) of L such that (a, b, c, d) lies within the sphere with radius r:

$$0 \neq a^2 + b^2 + c^2 + d^2 \leq r^2 = 1.9p < 2p.$$

- The lattice point (a, b, c, d) satisfies $c \equiv ua + vb \pmod{p}$ and $d \equiv ub - va \pmod{p}$, so

$$\begin{aligned} c^2 + d^2 &\equiv (ua + vb)^2 + (ub - va)^2 \pmod{p} \\ &\equiv u^2a^2 + v^2b^2 + u^2b^2 + v^2a^2 \pmod{p} \\ &\equiv (u^2 + v^2)(a^2 + b^2) \\ &\equiv -a^2 - b^2 \text{ since } u^2 + v^2 \equiv -1 \pmod{p} \end{aligned}$$

and $a^2 + b^2 + c^2 + d^2$ is a multiple of p.

Since $a^2 + b^2 + c^2 + d^2$ is a multiple of p that lies strictly between 0 and $2p$, it must be equal to p. This shows that the theorem holds for all primes.
Note that

$$\begin{aligned}&(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2)\\ =&(aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 +\\ &(aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2\end{aligned}$$

Therefore the theorem holds for any integer n by factorising n into primes and applying the identity above recursively. $\square$

We recall that a lattice $L \subset \mathbb{R}^n$, generated by $\mathbf{v}_1, \ldots, \mathbf{v}_m$, is the additive subgroup of $\mathbb{R}^n$ generated by $\mathbf{v}_1, \ldots, \mathbf{v}_m$:

$$L = \{\mathbf{u}M,\ \mathbf{u} \in \mathbb{Z}^m\},\ M = \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_m \end{bmatrix},\ G = MM^T.$$

We consider $m = n$.

- The dual lattice L^* is by definition

$$L^* = \{\mathbf{y} \in \mathbb{R}^n,\ \mathbf{y} \cdot \mathbf{x} \in \mathbb{Z} \text{ for all } \mathbf{x} \in L\}.$$

- For a basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$, define the dual basis $\mathbf{d}_1, \ldots, \mathbf{d}_n$ as the unique basis satisfying

$$\mathbf{v}_i \cdot \mathbf{d}_j = \delta_{ij}, \ 1 \leq i, j \leq n.$$

- Let $L(M)$ and $L(M')$ be two lattices, generated respectively by the generator matrices

$$M = \begin{bmatrix} \mathbf{v}_1 \\ \vdots \\ \mathbf{v}_n \end{bmatrix}, \ M' = \begin{bmatrix} \mathbf{d}_1 \\ \vdots \\ \mathbf{d}_n \end{bmatrix}.$$

Claim. $L(M)^* = L(M')$. We first prove $L(M)^* \supseteq L(M')$.

- Write $\mathbf{x} \in L(M)$ as $\sum a_i \mathbf{v}_i$, $a_i \in \mathbb{Z}$, so

$$\mathbf{x} \cdot \mathbf{d}_j = \sum a_i (\mathbf{v}_i \cdot \mathbf{d}_j) = a_i \in \mathbb{Z}$$

  and the vectors in the dual basis are in $L(M)^*$.
- It follows that $L(M') \subseteq L(M)^*$.

Claim. $L(M)^* = L(M')$. We first prove $L(M)^* \subseteq L(M')$.

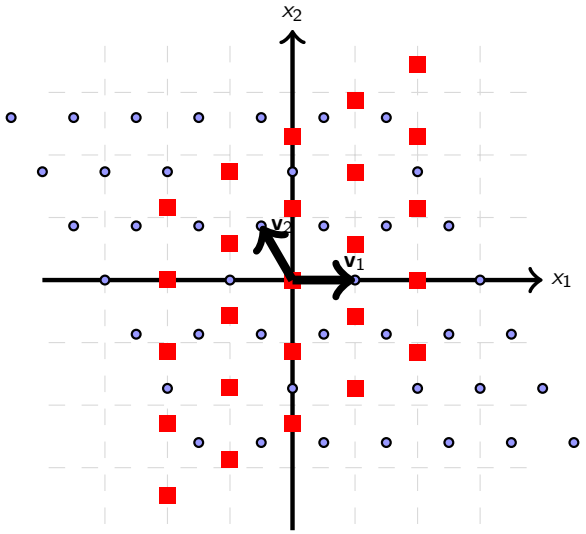
- Take $\mathbf{y} \in L(M)^*$, then write $\mathbf{y} = \sum a_i \mathbf{d}_i$, $a_i \in \mathbb{R}$.
- Then $\mathbf{y} \cdot \mathbf{v}_j \in \mathbb{Z}$ and

$$\mathbf{y} \cdot \mathbf{v}_j = \sum a_i (\mathbf{d}_i \cdot \mathbf{v}_j) = a_i$$

so $a_i \in \mathbb{Z}$ and $\mathbf{y} \in L(M')$. $\square$

Consequently:

- For L a lattice with M as a generator matrix, its dual lattice L^* will have $(M^T)^{-1}$ as a generator matrix.
- For any lattice L, $(L^*)^* = L$.
- For any lattice L, $\det(L^*) = \frac{1}{\det(L)}$.
- A lattice is called unimodular if $L = L^*$.



$$M = \begin{bmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$$

$$M^T = \begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix}, \ (M^T)^{-1} = \frac{2}{\sqrt{3}} \begin{bmatrix} \frac{\sqrt{3}}{2} & \frac{1}{2} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \frac{1}{\sqrt{3}} \\ 0 & \frac{2}{\sqrt{3}} \end{bmatrix}$$

- Charles Hermite (1822-1901): quadratic forms, elliptic functions, algebra.

Let L be a lattice. Suppose d is the smallest distance between any two distinct points of L, the vectors in L with length d are the shortest vectors of L.

- The minimum norm of L, or the norm of L or the minimum of L, is the length of a shortest nonzero lattice vector of L:

$$N(L) = \min(L) = \inf_{\mathbf{x} \in L, \mathbf{x} \neq 0} N(\mathbf{x}),$$

  where the norm of $\mathbf{x}$ is $N(\mathbf{x}) = \mathbf{x} \cdot \mathbf{x} = (||\mathbf{x}||_2)^2$.

For $L = \mathbb{Z}^n$, $N(L) = 1$.

Let L be a lattice of dimension n, then

$$\gamma(L) = \frac{N(L)}{\sqrt[n]{\det(L)}}.$$

Hermite's constant is defined by

$$\gamma_n = \sup_{\dim(L)=n} \gamma(L) = \sup_{\dim(L)=n} \frac{N(L)}{\sqrt[n]{\det(L)}}.$$

An n-dimensional lattice L is a critical lattice if $\gamma(L) = \gamma_n$.

Consider the lattice L with generator and Gram matrices

$$M = \begin{bmatrix} 2 & 0 \\ 1 & \sqrt{3} \end{bmatrix}, \; G = MM^T = \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}.$$

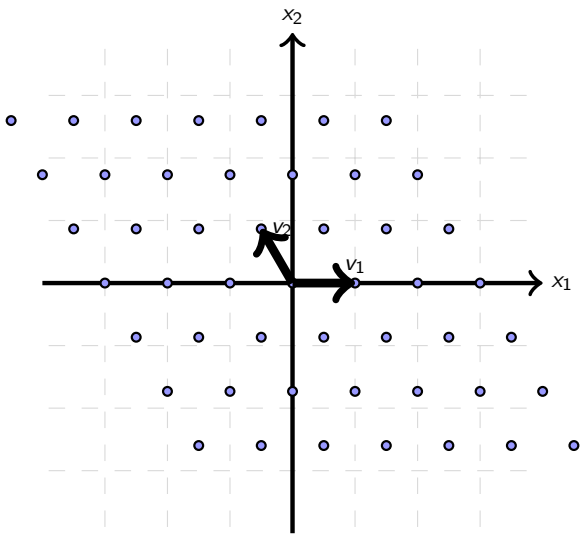
Then $\det(L) = \det(G) = 12$.
The norm of $\mathbf{x} = \mathbf{u}M$ for $u = (u_1, u_2) \in \mathbb{Z}^2$ is

$$\begin{aligned} N(\mathbf{x}) &= \mathbf{u}M(\mathbf{u}M)^T \\ &= \mathbf{u}G\mathbf{u}^T \\ &= 4(u_1^2 + u_1u_2 + u_2^2). \end{aligned}$$

Therefore, $N(\mathbf{x}) \geq 4$ for $\mathbf{x} \neq 0$ in L and $N(L) = 4$ (both basis vectors have norm 4).
Consequently

$$\gamma(L) = \frac{N(L)}{\sqrt{det(L)}} = \frac{4}{\sqrt{12}} = \frac{2}{\sqrt{3}}.$$

$\gamma(L)$ is normalized so it is invariant under scaling.



$$M = \begin{bmatrix} 2 & 0 \\ 1 & \sqrt{3} \end{bmatrix}, \; G = \begin{bmatrix} 4 & 2 \\ 2 & 4 \end{bmatrix}.$$

$$M = \begin{bmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}, \; G = \begin{bmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{bmatrix}.$$

Known values of Hermite's constant:

n	1	2	3	4	5	6	7	8	24
γ_n	1	$\frac{2}{\sqrt{3}}$	$\sqrt[3]{2}$	$\sqrt{2}$	$\sqrt[5]{8}$	$\sqrt[6]{\frac{64}{3}}$	$\sqrt[7]{64}$	2	4

- For L a lattice generated by n basis vectors, we say that L is of rank n.
- A sublattice $L' \leq L$ of rank l is a lattice included in L, generated by l basis vectors.
- Set

$$d_l(L) = \min_{\substack{L' \leq L, \\ rank(L')=l}} \det(L'),\ 1 \leq l \leq n.$$

We define

$$\begin{aligned} \gamma_{n,l}(L) &= d_l(L)\det(L)^{-l/n} \\ \gamma_{n,l} &= \sup_{rank(L)=n} \gamma_{n,l}(L) \end{aligned}$$

for

$$d_l(L) = \min_{\substack{L' \leq L, \\ rank(L')=l}} \det(L'),\ 1 \leq l \leq n.$$

The constant $\gamma_{n,l}$ is called the Rankin constant, and when $l = 1$, it translates into the Hermite constant: $\gamma_{n,1} = \gamma_n$.

We define

$$\begin{aligned} \gamma'_{n,l}(L) &= \sqrt{d_l(L)d_l(L^*)} \\ \gamma'_{n,l} &= \sup_{rank(L)=n} \gamma'_{n,l}(L), \end{aligned}$$

where L^* denotes the dual lattice of L and

$$d_l(L) = \min_{\substack{L' \leq L, \\ rank(L')=l}} \det(L'),\ 1 \leq l \leq n.$$

The constant $\gamma'_{n,l}$ is sometimes called the Bergé-Martinet constant.

Some inequalities are known, for example, for L a lattice and for $0 < l < n$, we have:

1. $\gamma'_{n,l} \leq \gamma_{n,l} \leq (\gamma_n)^l$.
2. For $0 \leq l \leq h \leq n$, we have $\gamma_{n,l} \leq \gamma_{h,l}(\gamma_{n,h})^{l/h}$.
3. For $0 \leq l \leq n/2$, we have $(\gamma_{n,l})^n \leq (\gamma_{n-l,l})^{n-l}(\gamma'_{n,l})^{2l}$ and $\gamma'_{n,2l} \leq (\gamma'_{n-l,l})^2$.
4. If n is even, then $\gamma'_{n,n/2} = \gamma_{n,n/2}$.
5. For $0 \leq l \leq n$, we have $(\gamma_{n,l})^{n-2l} \leq (\gamma_{n-l,l})^{n-l}$.
6. For a positive l, $\gamma'_{2l+1} \leq (\gamma'_{l+1})^2$.
7. $\gamma_{n,l} = \gamma_{n,n-l}$, $\gamma'_{n,l} = \gamma'_{n,n-l}$.

We keep in mind the last property for next slide.

Determining $\gamma_{n,l}$ and $\gamma'_{n,l}$ also remains mostly open. [K. Sawatani, T. Watanabe, K. Okuda, "A note on the Hermite-Rankin constant"]

n	l	$\gamma_{n,l}$	L	$\gamma'_{n,l}$	L
2	1	$\frac{2}{\sqrt{3}}$	A_2	$\frac{2}{\sqrt{3}}$	
3	1	$\sqrt[3]{2}$	$A_3 \simeq D_3$	$\sqrt{3/2}$	D_3
4	1	$\sqrt{2}$	D_4	$\sqrt{2}$	D_4
4	2	$3/2$	D_4	$3/2$	D_4
5	1	$\sqrt[5]{8}$	D_5	$\sqrt{2}$	D_5
5	2				
6	1	$(\frac{64}{3})^{1/6}$	E_6	$\sqrt{8/3}$	
6	2	$3^{2/3}$	E_6	2	E_6
6	3				
7	1	$\sqrt[7]{64}$	E_7	$\sqrt{3}$	
7	2				
7	3				
8	1	2	E_8	2	E_8
8	2	3	E_8	3	E_8
8	3	4	E_8	4	E_8
8	4	4	E_8	4	E_8

As for bounds:

- It is known [N. Gama, N. Howgrave-Graham, H. Koy, P.Q. Nguyen, "Rankin's constant and blockwise lattice reduction"] that

$$\left(\frac{k}{12}\right)^{k/2} \leq \gamma_{2k,k} \leq \left(1+\frac{k}{2}\right)^{k\ln 2+1/2}, \ k \geq 2,$$

- This result was improved, for $k \geq 5$, to

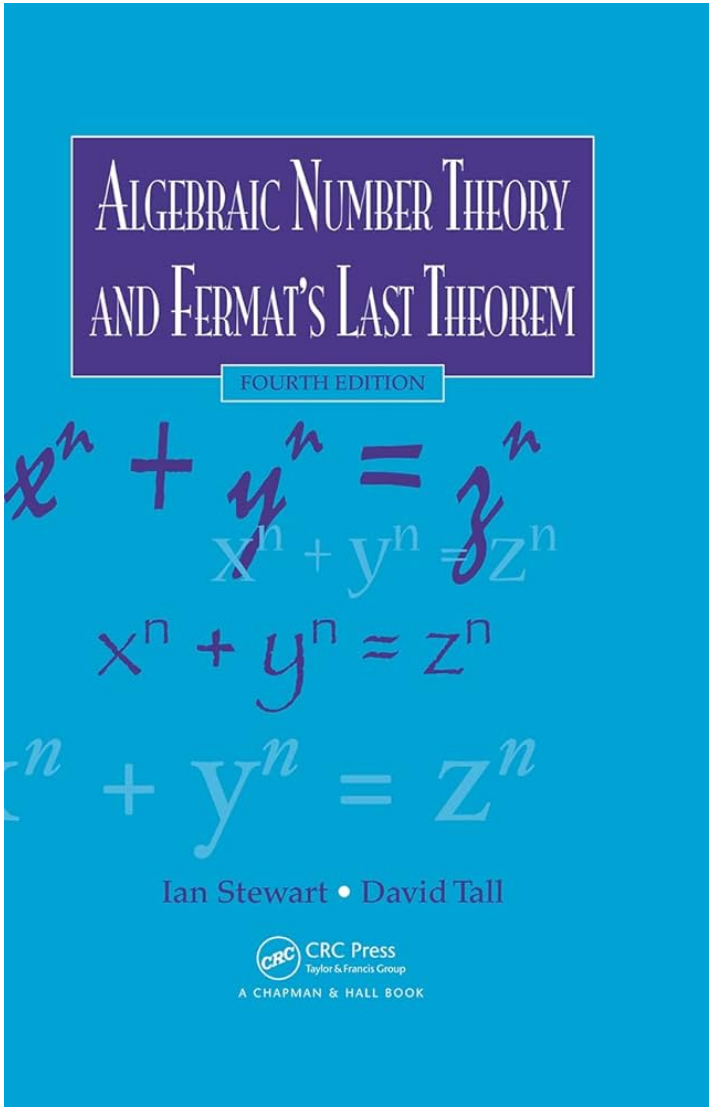
$$\frac{4}{\pi^2\sqrt{k}}\left(\frac{2k}{\pi e^{3/2}}\right)^{k/2} \leq \gamma_{2k,k} \leq e^9(0.0833)^{k/2}\left(\frac{4k-1}{17}\right)^{\frac{k}{4k-2}}(k-0.5)^{k\ln 2}$$

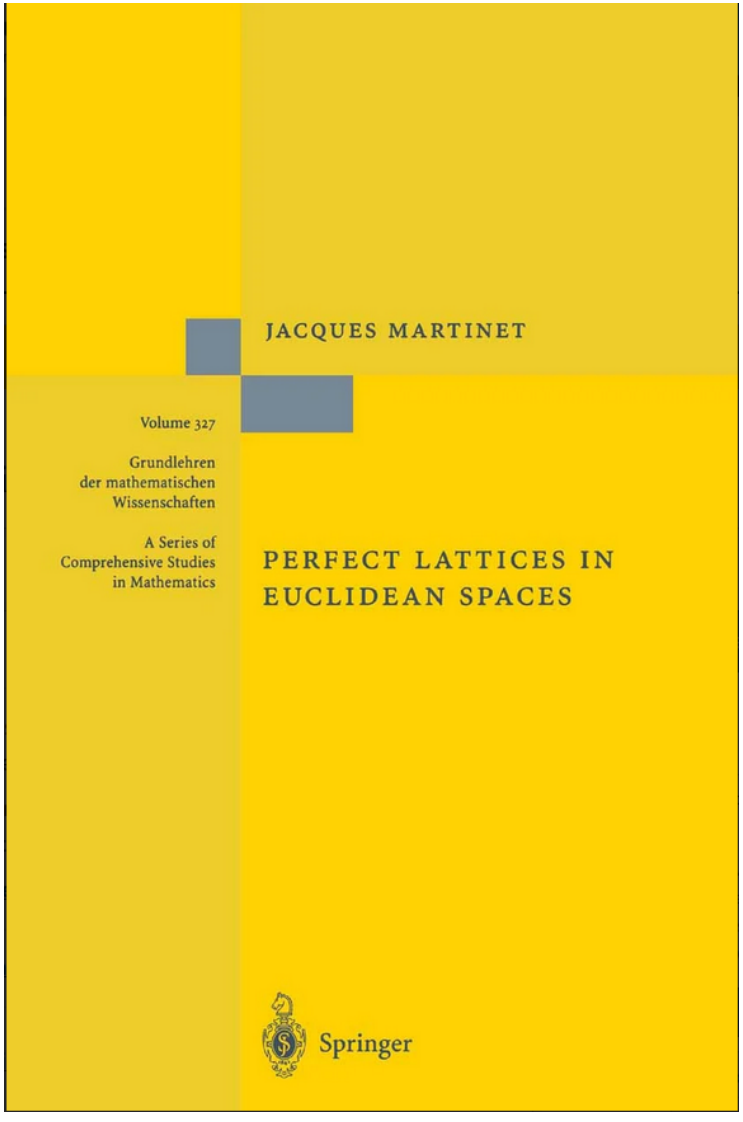
  in [J. Wen, X.W. Chang, "Sharper bounds on four lattice constants"].

- Bounds for arbitrarily large dimensions are of interest for lattice reductions, a topic that attracted a renewed interest in the context of lattice-based cryptography.

Hermite's constant and its generalizations still are of interest:

- Open conjecture for mathematicians.
  - A concrete open question: determine $\gamma_{5,2}$.
- Renewed interest from cryptographers.
- Used by coding theorists (Hermite's constant).


ALGEBRAIC NUMBER THEORY
AND FERMAT'S LAST THEOREM
FOURTH EDITION
$x^n + y^n = z^n$
$x^n + y^n = z^n$
$x^n + y^n = z^n$
Ian Stewart • David Tall
CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK


JACQUES MARTINET
Volume 327
Grundlehren
der mathematischen
Wissenschaften
A Series of
Comprehensive Studies
in Mathematics
PERFECT LATTICES IN
EUCLIDEAN SPACES
Springer