Notes for Math 669

Yiwei Fu, Instructor: Alexander Barvinok

WN 2023

Contents

Office hours:

Chapter 1

Introduction to Lattices

1.1 Definition

Definition 1.1.1. A lattice $\Lambda \subset V$ has the following properties:

1. $\operatorname{span}(\Lambda) = V$.
2. Λ is an additive subgroup.
3. Λ is discrete: for any $r > 0$, let $B_r = \{x \in \mathbb{R}^n, \|x\| \le r\}$, $\Lambda \cap B_r$ is finite.

1.2 Lattice and Its Basis

Last time: $L \in V$ is a subspace if $L = \operatorname{span}(L \cap \Lambda)$

Theorem 1.2.1. *If L is a lattice subspace, $L \ne V$, then $\exists u \in L \setminus \Lambda$ such that $d(u, L) \le d(x, L)$ for all $x \in L \setminus \Lambda$.*

Say $L \in \operatorname{span}\{u_1, \ldots, u_m\}$ linearly independent vectors, $\Pi = \{\}$ There is $u \in \Lambda \setminus L$ such that $\operatorname{dist}(u, \Pi) \le \operatorname{dist}(x, \Pi)$ for all $x \in \Lambda \setminus L$.

Proof. Take $\rho > 0$ large enough. Consider $\Pi_\rho = \{y, d(y, \Pi) \le \rho\}$. It contains points from $\Lambda \setminus L$, choose the one in $\Pi_\rho \cap (\Lambda \setminus L)$ closet to Π. ■

<u>CLAIM</u> $u \in \Lambda \setminus L$ is what we need. Why? Pick any $x \in \Lambda \setminus L$. Let $y \in L$ be the closest to x.

$$\operatorname{dist}(x, L) = \|x - y\| = \|(x - w) - (y - w)\|.$$

$$y = \sum_{i=1}^{m} d_i u_i$$

Let $w = \sum_{i=1}^{m} \lfloor \alpha_i \rfloor u_i \in \Lambda \setminus L, y - w = \sum_{i=1}^{m} \{\alpha_i\} u_i \in \Pi$.

Theorem 1.2.2. *Every lattice has a basis.*

Proof. By induction on $n = \dim V$.

Base case: for $n = 1$, we have $V = \mathbb{R}$.

Let $u > 0$ be the lattice vector closet to 0, among all positive vectors in Λ.

Then u is a basis of Λ. Pick any $v \in \Lambda$. Assume $v > 0$ WLOG. Then $v = \alpha u$ for $\alpha > 0$. If $\alpha \in \mathbb{Z}$ then we are done. If not, consider $w = \alpha u - \lfloor \alpha \rfloor u = \{\alpha\} u$, this is closer to 0 than u, a contradiction.

Induction hypothesis: suppose any lattice of dimension $n - 1$ has a basis.

Induction step: pick a lattice hyperplane H (lattice subspace with $\dim = n - 1$). Then $\Lambda_1 = H \cap \Lambda$ has a basis $u_1, \dots, u_{n-1}$. Pick u_n such that $u_n \notin H$ and $\operatorname{dist}(u_n, H)$ is the smallest. We claim that $u_1, \dots, u_{n-1}, u_n$ is a basis of Λ.

Let $u \in \Lambda$, $u = \sum_{i=1}^{n} \alpha_i u_i$ with $\alpha_i \in \mathbb{R}$. If $\alpha_n = 0$ then $u \in \Lambda_1$, then $\alpha_1, \dots, \alpha_{n-1} \in \mathbb{Z}$. Suppose $\alpha_n \neq 0$. Consider $w = u - \lfloor \alpha_n \rfloor u_n$. $w \in \Lambda$ and $w = \{\alpha_n\} u_n + \sum_{i=1}^{n-1} \alpha_i u_i$. So

$$\operatorname{dist}(w, H) = \operatorname{dist}(\{\alpha_n\} u_n, H) = \{\alpha_n\} \operatorname{dist}(u_n, H)$$

If $\{\alpha_n\} > 0$ then $0 < \operatorname{dist}(w, H) < \operatorname{dist}(u_n, H)$, a contradiction.

So $\{\alpha_n\} = 0 \implies \alpha_n \in \mathbb{Z}$. Then $w = \sum_{i=1}^{n-1} \alpha_i u_i \implies \alpha_1, \dots, \alpha_{n-1} \in \mathbb{Z}$.

So we have constructed a basis for lattice of dimension n, thus finishing the proof. ∎

This is called A.N.Korkin(e)-Zolotarev(öff) basis.

<u>EXERCISE</u> Suppose $u_1, \dots, u_n \in V$ is a basis of subspace. The integer combinations form a lattice.

<u>EXERCISE</u> Suppose a 2-dimensional lattice. Then there exists a lattice basis u, v such that the angle α between u, v satisfies $\frac{\pi}{3} \leq \alpha \leq \frac{\pi}{2}$.

<u>EXERCISE</u> If Λ is a lattice and L is a lattice subspace. The orthogonal projection $\mathrm{PR} : V \to L^{\perp}$. Then $\mathrm{PR}(\Lambda) \subset L^{\perp}$ is a lattice.

Definition 1.2.1. Suppose $u_1, \ldots, u_n$ be a basis of Λ.

$$\Pi = \left\{ \sum_{i=1}^{n} \alpha_i u_i : 0 \leq \alpha_i < 1, i = 1, \ldots, n \right\}$$

is the *fundamental parallelepiped* of a fundamental parallelepiped of Λ.

Theorem 1.2.3. *The volume of a fundamental parallelepiped Π doesn't depend on Π. The volume is called the determinant of Λ. Furthermore, if $B_r = \{x : \|x\| \leq r\}$, then*

$$\lim_{r \to \infty} = \frac{|B_r \cap \Lambda|}{\operatorname{vol} B_r} = \frac{1}{\det \Lambda}.$$

We start with a lemma:

Lemma 1.2.1. *Let Π be a fundamental parallelepiped of $\Lambda \subset V$. Then every vector $x \in V$ is uniquely written as $x = u + y$ where $u \in \Lambda, y \in \Pi$.*

Proof. Existence: Π is the fundamental parallelepiped for $u_1, \ldots, u_n$. If $x = \sum_{i=1}^{n} \alpha_i u_i$ then $u = \sum_{i=1}^{n} \lfloor \alpha_i \rfloor u_i$ and $y = \sum_{i=1}^{n} \{\alpha_i\} u_i$

Uniqueness: suppose $x = u_1 + y_1 = u_2 + y_2$ then $u_1 - u_2 = y_2 - y_1$. Since $u_1 - u_2 \in \Lambda$ we have $y_2 - y_1 = \sum_{i=1}^{n} (\alpha_i - \beta_i) \mathbf{u}_i$. We have $(\alpha_i - \beta_i) \in \mathbb{Z}$. Since $-1 < \alpha_i - \beta_i < 1$, it has to be 0. ∎

A geometry interpretation is that we can cover the whole space with fundamental parallelepipeds without overlaps.

Proof of theorem. Let

$$X_r = \bigcup_{u \in B_r \cap \Lambda} (\Pi + u)$$

Then $\operatorname{vol} X_r = |B_r \cap \Lambda| \operatorname{vol} \Pi$.

Say, $\Pi \subset B_a$ for some $a > 0$. Then $X_r \subset B_{r+a}$. Look at B_{r-a}. It is covered by $\Pi + u : u \in \Lambda$. We should have $\|u\| \leq r$. Hence $B_{r-a} \subset X_r$.

So we have

$$\left(\frac{r-a}{a} \right)^n = \frac{\operatorname{vol} B_{r-a}}{\operatorname{vol} B_r} \leq \frac{\operatorname{vol} X_r}{\operatorname{vol} B_r} \leq \frac{\operatorname{vol} B_{r+a}}{B_r} = \left(\frac{r+a}{a} \right)^n$$

This goes to 1 when $r \to \infty$. ∎

<u>REMARK/EXERCISE</u> The same holds for balls not centered in the origin:

$$B_r(x_0) = \{x : \|x - x_0\| \leq r\}.$$

<u>EXERCISE</u> Suppose a lattice $\Lambda \subset V$ and $u \in \Lambda$. The Voronoi (G.F. Voronoi, 1868-1908) region is defined by

$$\Phi_u = \{x \in V : \|x - u\| \leq \|x - v\|, \forall v \in \Lambda\}.$$

Show that Φ is convex (bounded by at most 2^n affine hyperplanes) and $\operatorname{vol}\Phi = \det\Lambda$.

<u>EXERCISE</u> $(\det\Lambda)(\det\Lambda^*) = 1$

1.3 Sublattice

Definition 1.3.1. Suppose $\Lambda \subset V$ is a lattice, and $\Lambda_0 \subset \Lambda, \Lambda_0 \subset V$ is also a lattice. Λ_0 is then called a sublattice of Λ.

Remark. We have $\operatorname{rank}\Lambda_0 = \operatorname{rank}\Lambda$.

Example 1.3.1. $D_n \subset \mathbb{Z}^n$.

Λ is an Abelian group and $\Lambda_0 \subset \Lambda$ is a subgroup. Look at the quotient Λ/Λ_0 and cosets $\{u + \Lambda_0\}$. The index of Λ_0 in $\Lambda |\Lambda/\Lambda_0|$ = the number of cosets.

Theorem 1.3.1. 1. *Let Π be a fundamental parallelepiped of Λ_0 Then $|\Lambda/\Lambda_0| = |\Pi \cap \Lambda|$.*

2. $|\Lambda/\Lambda_0| = \dfrac{\det\Lambda_0}{\det\Lambda}$.

Proof. 1. By Lemma 1.2.1, every coset has a unique representation in Π.

2. Let $B_r = \{x : \|x\| \leq r\}$. Then

$$\lim_{r\to\infty} = \frac{|B_r \cap \Lambda|}{\operatorname{vol} B_r} = \frac{1}{\det\Lambda}.$$

Let $S \subset \Lambda$ be the set of coset representatives. Then $|S| = |\Lambda/\Lambda_0|$. Then $\Lambda = \bigcup_{u\in S}(u + \Lambda_0)$. Hence

$$\lim_{r\to\infty} \frac{|B_r \cap (u + \Lambda_0)|}{\operatorname{vol} B_r} = \frac{1}{\det\Lambda_0}. \implies \frac{1}{\det\Lambda} = |S|\frac{1}{\Lambda_0}$$ ■

<u>EXERCISE</u>

1. $\det\mathbb{Z}^n = 1$

2. $\det D_n = 2$.
3. $\det D_n^+ = 1$. (n even)
4. $\det A_n = \sqrt{n+1}$. $\det E_8 = 1, \det E_7 = \sqrt{2}, \det E_6 = \sqrt{3}$.
5. If $a_1, \dots, a_n$ are coprime integers not all 0.

$$\Lambda = \{(x_1, \dots, x_n) \in \mathbb{Z}^n : a_1x_1 + \ldots + a_nx_n = 0\} \text{ has } \det \Lambda = \sqrt{a_1^2 + \ldots + a_n^2}.$$

Corollary 1.3.1. *If $u_1, \dots, u_n \in \Lambda$ are linearly independent and*

$$\operatorname{vol}\left\{\sum_{i+1}^{n} \alpha_i u_i : 0 \le \alpha_i < 1\right\} = \det \Lambda$$

then $u-1, \dots, u_n$ is a basis.

Proof. Look at

$$\Lambda_0 = \left\{\sum_{i=1}^{n} m_i u_i : m_i \in \mathbb{Z}\right\}, |\Lambda/\Lambda_0| = 1 \implies \Lambda = \Lambda_0 \qquad \blacksquare$$

Counting integer points. Suppose $\Lambda = \mathbb{Z}^n$.

Pick n linearly independent vectors $u_1, \dots, u_n \in \Lambda$. Consider

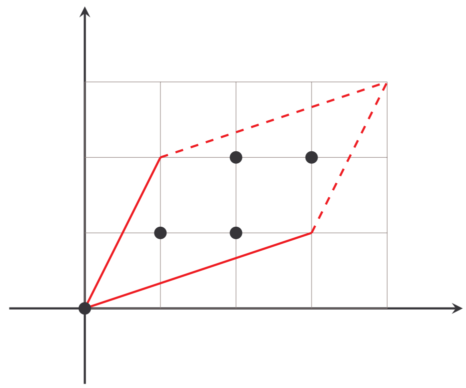
$$\Pi = \left\{\sum_{i=1}^{n} \alpha_i u_i : 0 \le \alpha_i < 1\right\}.$$

Then

$$|\Pi \cap \mathbb{Z}^n| = ?$$

Suppose $\Lambda_0 = \{\sum_{i=1}^n m_i u_i : m_i \in \mathbb{Z}\}$. Then $\det \Lambda_0 = \operatorname{vol} \Pi$.

Suppose $n = 2$, $u_1 = (3, 1), u_2 = (1, 2)$. Then $\operatorname{vol} \Pi = 5$. We can see that the parallelogram contains 5 integer points.



The case for $n = 2$ is special.

Theorem 1.3.2 (Pick Formula (G.A. Pick, 1859-1942))**.** *If $P \subset \mathbb{R}^2$ is a convex polygon with integer vertices and non-empty interior. Then*

$$|P \cap \mathbb{Z}^2| = \textit{ area of } P + \frac{1}{2}|\partial P \cap \mathbb{Z}^2| + 1$$

Proof. Left as exercise. Hint: do it for parallelograms (in any dimension) first, then do it for triangles (special case for $n = 2$), and then all polygons with integer vertices. ∎

<u>EXERCISE</u> For $n = 2$, linearly independent vectors of $u, v \in \mathbb{Z}^2$ form a basis $\iff$ the triangle with vertices $0, u, v$ has no other integer points.

<u>EXERCISE</u> For $n = 3$, construct an example of linearly independent $u, v, w \in \mathbb{Z}^3$ such that the tetrahedron with vertices $0, u, v, w$ has no other integer points but $\{u, v, w\}$ is not a basis of $\mathbb{Z}^3$. In fact, you can have $|\mathbb{Z}^n/\Lambda|$ arbitrarily large.

<u>EXERCISE</u> Suppose $u_1, \ldots, u_k \in \mathbb{Z}^n$ are linearly independent vectors and $\Lambda = \mathbb{Z}^n \cap \operatorname{span}(u_1, \ldots, u_k)$. The $\{u_1, \ldots, u_k\}$ is a basis of Λ if and only if the great common divisor of all $k \times k$ minors of $\begin{bmatrix} u_1^T \\ u_2^T \\ \cdots \\ u_k^T \end{bmatrix}$ is 1.

Linear algebra (Smith normal form, will not use)

If $\Lambda_0 \subset \Lambda$ is a sublattice, then there is a basis $u_1, \ldots, u_n$ of Λ and a basis $v_1, \ldots, v_n$ of Λ_0 such that $v_i = m_i u_i$ for positive integer m_i and such that m_1 divides m_2 which divides $m_3, \ldots$.

1.4 Minkowski Theorem

The goal today is to prove Minkowski Theorem (H. Minkowski, 1864-1909) for convex body.

Definition 1.4.1. Suppose V a Euclidean space, then a set $A \subset V$ is convex if $\forall x, y \in A, [x, y] \in A$ where $\{[x, y] = \alpha x + (1 - \alpha)y : 0 \leq \alpha \leq 1\}$.

Definition 1.4.2. A set A is symmetric if $A = -A = \{-x : x \in A\}$.

Theorem 1.4.1. *Suppose $\Lambda \subset V$ a lattice and $A \subset V$ a convex symmetric set with $\operatorname{vol} A > 2^{\dim V} \det \Lambda$. Then there is $u \subset \Lambda \setminus \{0\}$ such that $u \in A$.s*

$\underline{2^{\dim V} \text{ IS SHARP}}$: Pick $\mathbb{Z}^n \subset \mathbb{R}^n, \det \mathbb{Z}^n = 1$. Let $A = \{-1 < x_i < 1, i = 1, \dots, n\}$ convex and symmetric. Then $\operatorname{vol} A = 2^n$ and $A \cap Z^n = \{0\}$. And from geometric intuition we see that convex and symmetric is needed.

It is a result from Blichfeldt's theorem.

Theorem 1.4.2 (H. F. Blichfeldt, 1873 - 1945)**.** *Let measurable $X \subset V$, $\operatorname{vol} X > \det \Lambda$, then there are $x, y \in X$ such that $x - y \in \Lambda \setminus \{0\}$.*

<u>INTUITION</u> $\det \Lambda$ describes the volume per lattice point. Consider $\{X + u\}$ the translations of X by lattice points. Some of them must overlap i.e. $(X + u_1) \cap (X + u_2) \neq \emptyset$. Then $x + u_1 = y + u_2 \implies x - y = u_2 - u_1 \in \Lambda \setminus \{0\}$.

Proof. Choose a fundamental parallelepiped Π of lattice Λ. Then $\det \Lambda = \operatorname{vol} \Pi$. Then $\{\Pi + u, u \in \Lambda\}$ cover V without overlap. In particular, they cover X.

Let $X_u := ((\Pi + u) \cap X) - u$. $\sum_{u \in \Lambda} \operatorname{vol} X_u = \operatorname{vol} X > \operatorname{vol} \Pi$. And $X_u \subset \Pi$. Then $\exists u_1 \neq u_2$ *s.t.* $X_{u_1} \cap X_{u_2} \neq \emptyset$. Then $\exists x, y \in X$ *s.t.* $x - u_1 = y - u_2 \implies x - y = u_1 - u_2 \in \Lambda \setminus \{0\}$. ∎

Proof of Minkowski's Theorem. Let $X = \frac{1}{2}A = \left\{\frac{1}{2}x, x \in A\right\}$. Then $\operatorname{vol} X = 2^{-\dim v} \operatorname{vol} A > \det \Lambda$. By Blichfeldt, there are $x, y \in X$ such that $x - y \in \Lambda \setminus \{0\}$. Write

$$u = x - y = \frac{1}{2}(2x) + \frac{1}{2}(-2y)$$

Since A is convex and symmetric, $2x, -2y \in A$ and $x - y \in A \implies u \in A$. ∎

<u>EXERCISE</u> Suppose $\Lambda \subset V$ a lattice. Let $X = \{x \in V : \|x\| < \|x - u\|, \forall u \in \Lambda \setminus \{0\}\}$. Let $A = 2X$. Show that A is convex, symmetric, $A = 2^{\dim V} \det \Lambda$ and $A \cap \Lambda = \{0\}$.

Corollary 1.4.1. *If, in addition, A is compact, then it is enough to have $\operatorname{vol} A \geq 2^{\dim V} \det \Lambda$.*

We can apply the proof for $(1 + \varepsilon)A$ and let $\varepsilon \to 0$.

Corollary 1.4.2. *Let $V = \mathbb{R}^n$, and $\|x\|_\infty = \max_{i=1,\dots,n} |x_i|$. Then there is a $u \in \Lambda \setminus \{0\}$ with $\|u\|_\infty \le (\det \Lambda)^{\frac{1}{n}}$.*

Consider $A = \left\{x, |x_i| \le (\det \Lambda)^{\frac{1}{n}}\right\}$.

Corollary 1.4.3. *Suppose $\Lambda \subset V$. Then there is $u \subset \Lambda \setminus \{0\}$ with $\|u\| \le \sqrt{\dim V} (\det \Lambda)^{\frac{1}{n}}$.*

<u>Exercise</u> If $X \subset V$ is measurable and $\operatorname{vol} X > m \det \Lambda$ with $m \in \mathbb{Z}^+$. Then there are $x_1, \dots, x_{m+1} \in X$ such that $x_i - x_j \in \Lambda$ for all pairs i, j.

If A is convex, symmetric, and $\operatorname{vol} A > m \cdot 2^{\dim V} \det \Lambda$. Then A contains m distinct pairs $\pm u_1, \dots, \pm u_m$ of nonzero lattice points.

<u>Exercise (Important)</u> If $X \subset \Lambda$ is a set such that $|X| > 2^{\dim V}$ then there are distinct $x, y \in X$ such that $\frac{x+y}{2} \in \Lambda$.

<u>Exercise</u> Suppose $f : V \to \mathbb{R}_+$ is integrable and $\Lambda \subset V$ a lattice. Then there are $z_1, z_2 \in V$ such that

$$\sum_{u \in \Lambda} f(u + z_1) \ge \frac{1}{\det \Lambda} \int_V f(x)\, \mathrm{d}x \ge \sum_{u \in \Lambda} f(u + z_2).$$

We need the column of the unit ball in $\mathbb{R}^n$.

$$\Gamma(x) = \int_0^\infty t^{x-1} e^{-t}\, \mathrm{d}t$$

$$\Gamma(x+1) = x\Gamma(x)$$

$$B = \{x : \|x\| = 1\}, B \subset \mathbb{R}^n, \operatorname{vol} B = \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2} + 1\right)}$$

We start with integral:

$$\int_{-\infty}^\infty e^{-x^2}\, \mathrm{d}x = \sqrt{\pi}, \int_{\mathbb{R}^n} e^{-\|x\|^2}\, \mathrm{d}x = \left(\sqrt{\pi}\right)^n$$

Let $S(r) = \{x \in \mathbb{R}^n : \|x\| = r\}$ and κ be the surface area of $S(1)$.

$$\begin{aligned} \left(\sqrt{\pi}\right)^n &= \int_0^\infty \left(\int_{S(r)} e^{-\|x\|^2}\, \mathrm{d}x \right) \mathrm{d}r \\ &= \int_0^\infty r^n \kappa e^{-r^2}\, \mathrm{d}r \\ &= \frac{1}{2} \int_0^\infty t^{\frac{n-2}{2}} \kappa e^{-t}\, \mathrm{d}t \\ &= \kappa \frac{1}{2} \int_0^\infty t^{\frac{n-2}{2}} \kappa e^{-t}\, \mathrm{d}t = \frac{1}{2} \kappa \gamma \left(\frac{n}{2}\right) \end{aligned}$$

So we have $\kappa = \frac{2(\sqrt{\pi})^n}{\Gamma\left(\frac{n}{2}\right)}$.

Then

$$\operatorname{vol} B = \int_0^1 \kappa t^{n-1} \, \mathrm{d}r = \frac{\kappa}{n} = \frac{\pi^{n/2}}{\Gamma\left(\frac{n}{2}+1\right)}.$$

1.5 Applications of Minkowski's Theorem

First application:

Theorem 1.5.1 (Lagrange's four squares theorem (J-L Lagrange, 1736-1813)). *If $n \geq 0$ is a non-negative integer, then $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ for some integer x_1, x_2, x_3, x_4.*

Proof. Start as Lagrange did: first, prove assuming that n is prime, then there are $a, b \in \mathbb{Z}$ such that $a^2 + b^2 + 1 \equiv 0 \pmod{n}$.

$n = 2$ is clear. Consider values of $a^2 \pmod{n}$ for $n > 2$ and $a = 0, 1, \ldots, \frac{n-1}{2}$. They are all distinct. Otherwise $a_1^2 \equiv a_2^2 \equiv \pmod{n} \implies (a_1 - a_2)(a_1 + a_2) \pmod{n}$.

Consider values $-1 - b^2 \pmod{n}$ for $b = 0, 1, \ldots, \frac{n-1}{2}$. They are all different values.

There are a total of $n + 1$ values, so there exists $a^2 \equiv -1 - b^2 \pmod{n}$ by pigeonhole principle.

We introduce one generally useful lemma:

Lemma 1.5.1. *Suppose $a_1, \ldots, a_k \in \mathbb{Z}^n$ and $m_1, \ldots, m_k$ positive integers and*

$$\Lambda = \{x \in \mathbb{Z}^n : \langle x, a_i \rangle \equiv 0 \pmod{m_i}\}.$$

Then Λ is a lattice and $\det \Lambda \leq m_1 \cdots m_k$.

Consider their cosets: pick $0 \leq b_i \leq m_i$, and the coset is

$$\{x \in \mathbb{Z}^n : \langle x, a_i \rangle \equiv b_i \pmod{m_i}\}$$

if the set is non-empty. Then $|\mathbb{Z}^n / \Lambda| = \frac{\det \Lambda}{\det \mathbb{Z}^n}$.

The rest is from Davenport: Suppose a lattice

$$\Lambda = \left\{ x \in \mathbb{Z}^4 : \begin{array}{l} x_1 \equiv a x_3 + b x_4 \\ x_2 \equiv a x_4 - b x_3 \end{array} \pmod{n} \right\}.$$

If $(x_1, x_2, x_3, x_4) \in \Lambda$ then

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv (ax_3 + bx_4)^2 + (ax_4 - bx_3)^2 + x_3^2 + x_4^2 \pmod{n}$$
$$a^2x_3^2 + b^2x_4^2 + 2abx_3x_4 +$$
$$a^2x_4^2 + b^2x_3^2 - 2abx_3x_4 + x_3^2 + x_4^2 \equiv (a^2 + b^2 + 1)x_3^2 + (b^2 + a^2 + 1)x_4^2 \equiv 0 \pmod{n}$$

So we have $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{n}$ for all $(x_1, x_2, x_3, x_4) \in \Lambda$. So $\det \Lambda \leq n^2$. Consider the ball B with radius $\sqrt{2n}$. The volume of the ball $\operatorname{vol} B = 2n^2\pi^2 \geq 2^4 n^2 \geq 2^4 \det \Pi$. So there exists $(x_1, x_2, x_3, x_4) \in \Lambda \setminus \{0\}$ such that $x_1^2 + x_2^2 + x_3^2 + x_4^2 < 2n$ and $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{n}$.

So we conclude that such $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$.

Now suppose n is not prime, write $n = \prod p_i$ where p_i's are prime numbers.

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

where

$$\begin{cases} z_1 = x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 \\ z_2 = x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 = x_1y_3 + x_2y_4 + x_3y_1 + x_4y_2 \\ z_4 = x_1y_4 - x_2y_3 - x_3y_3 + x_4y_1 \end{cases}$$

Remember through quaternions. $x_1 + ix_2 + jx_3 + kx_4$. ■

Jacobi's Formula (C.G.J Jacobi, 1804-1851) The number of integer solutions (not necessarily positive) of the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$$

is $8 \cdot \sum_{d | n, 4 \nmid d} d$.

<u>EXERCISE</u> Deduce the Jacobi's Formula from the identity

$$\left(\sum_{k=-\infty}^{\infty} q^k \right)^4 = 1 + 8 \sum_{k=1}^{\infty} \frac{q^k}{(1 + (-q)^k)^2}, \text{ for } |q| < 1.$$

Gauss Circle Problem (C.-F Gauss, 1777, 1855) $B_r = \left\{ x \in \mathbb{R}^2 : \|x\| \leq r \right\}$. As $r \to \infty$, $|B(r) \cap \mathbb{Z}^2| \approx \pi r^2 + O(r^{1/2+\varepsilon})$ for any $\varepsilon > 0$? Best known is $O(r^{0.63})$ for $\varepsilon = 0.13$.

<u>EXERCISE</u> If n is prime, $n \equiv 1 \pmod 4$. Then $n = x_1^2 + x_2^2$ for some $x_1, x_2 \in \mathbb{Z}$.

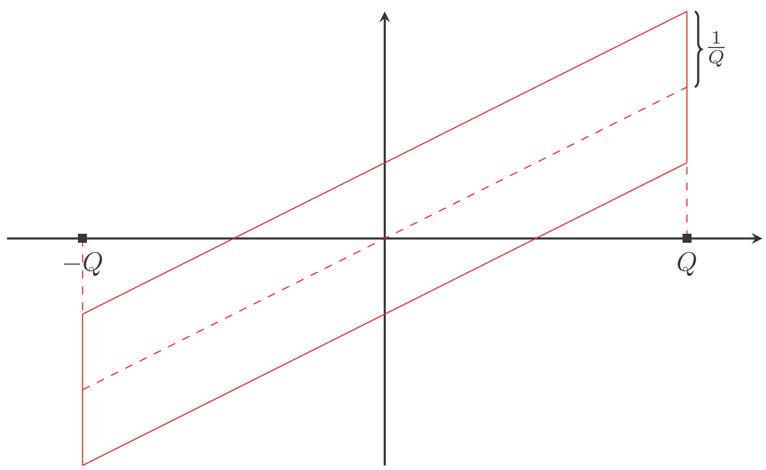
How well can we approximate a real number for rational numbers?

If $\alpha \in \mathbb{R}$ and $q \geq 1$ is an integer, then for some integer p we have $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q}$.

Theorem 1.5.2. *For any $\alpha \in \mathbb{R}$ and $M > 0$, there exists $q \geq M$ and an integer p such that $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$.*

It shows that this holds for infinitely many q.

Proof. Assume WLOG that α is irrational. Pick $Q \geq 1$ an integer. Consider the parallelogram in $\mathbb{R}^2 : \left\{|x| \leq Q, |\alpha x - y| \leq \frac{1}{Q}\right\}$.



Π is convex, symmetric, compact, with area $\Pi = 4 = 2^2$.

By Minkowski, there exists $(q,p) \in \mathbb{Z}^2 \setminus \{0\}, (q,p) \in \Pi$ such that $|\alpha q - p| \leq \frac{1}{Q}, |p| \leq \frac{1}{Q} \implies p = 0$. Assume that $q > 0$.

We have $q \leq Q$, and

$$|\alpha q - p| \leq \frac{1}{Q} \implies \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{Qq} \leq \frac{1}{q^2}$$

It remains to show that for any M we can choose $q \geq M$.

Why? α is irrational. Choose Q so large that we cannot have $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{Q}$ for $q \leq M$. ∎