Minkowski's theorem and applications

Abhiram Kumar

17th April, 2023

Outline

- Lattices and examples
- Minkowski's lattice point theorem
- Some applications
- Lagrange's four squares theorem

Lattices

A (full) lattice Λ in $\mathbb{R}^n$ is a $\mathbb{Z}$-span of n linearly independent vectors in $\mathbb{R}^n$. The covolume of Λ is defined to be the volume of $\mathbb{R}^n/\Lambda$.

A (full) lattice Λ in $\mathbb{R}^n$ is a $\mathbb{Z}$-span of n linearly independent vectors in $\mathbb{R}^n$. The covolume of Λ is defined to be the volume of $\mathbb{R}^n/\Lambda$.

- $\mathbb{Z}^2$ in $\mathbb{R}^2$ has covolume 1.

A (full) lattice Λ in $\mathbb{R}^n$ is a $\mathbb{Z}$-span of n linearly independent vectors in $\mathbb{R}^n$. The covolume of Λ is defined to be the volume of $\mathbb{R}^n/\Lambda$.

- $\mathbb{Z}^2$ in $\mathbb{R}^2$ has covolume 1.
- $\mathcal{O}_K$ in $\mathbb{R}^{r+2s}$ has covolume $\frac{1}{2^s}\sqrt{|disc(K)|}$.

How big can a set which avoids all the lattice points be?

Lattice point theorem

How big can a set which avoids all the lattice points be?

Theorem

Let Λ be a lattice in $\mathbb{R}^n$ and K be a convex, symmetric and bounded subset of $\mathbb{R}^n$ with volume greater than $2^n covol(\Lambda)$. Then K contains a non-zero lattice point.

Lattice point theorem

Proof.

Let F be a fundamental domain for Λ. Then $\mathbb{R}^n$ is a disjoint union of translates $x + F$ where $x \in \Lambda$

Lattice point theorem

Proof.

Let F be a fundamental domain for Λ. Then $\mathbb{R}^n$ is a disjoint union of translates $x + F$ where $x \in \Lambda$

$$\frac{1}{2}K = \bigcup_{x \in \Lambda} \left(\left(\frac{1}{2}K \right) \cap (x + F) \right)$$

Lattice point theorem

Proof.

Let F be a fundamental domain for Λ. Then $\mathbb{R}^n$ is a disjoint union of translates $x + F$ where $x \in \Lambda$

$$\frac{1}{2}K = \bigcup_{x\in\Lambda} \left(\left(\frac{1}{2}K \right) \cap (x + F) \right)$$

$$vol(F) < vol\left(\frac{1}{2}K\right) = \sum_{x\in\Lambda} vol\left(\left(\frac{1}{2}K \right) \cap (x + F) \right)$$

Proof.

Let F be a fundamental domain for Λ. Then $\mathbb{R}^n$ is a disjoint union of translates $x + F$ where $x \in \Lambda$

$$\frac{1}{2}K = \bigcup_{x \in \Lambda} \left(\left(\frac{1}{2}K \right) \cap (x + F) \right)$$

$$vol(F) < vol\left(\frac{1}{2}K\right) = \sum_{x \in \Lambda} vol\left(\left(\frac{1}{2}K \right) \cap (x + F) \right)$$

$$= \sum_{x \in \Lambda} vol\left(\left(\frac{1}{2}K - x \right) \cap F \right)$$

Lattice point theorem

Proof.

Let F be a fundamental domain for Λ. Then $\mathbb{R}^n$ is a disjoint union of translates $x + F$ where $x \in \Lambda$

$$\frac{1}{2}K = \bigcup_{x \in \Lambda} \left(\left(\frac{1}{2}K \right) \cap (x + F) \right)$$

$$vol(F) < vol\left(\frac{1}{2}K\right) = \sum_{x \in \Lambda} vol\left(\left(\frac{1}{2}K \right) \cap (x + F) \right)$$

$$= \sum_{x \in \Lambda} vol\left(\left(\frac{1}{2}K - x \right) \cap F \right)$$

Therefore, for some $x_1 \neq x_2 \in \Lambda$

$$\left(\frac{1}{2}K - x_1 \right) \cap \left(\frac{1}{2}K - x_2 \right) \neq \phi$$

Proof.

Therefore, for some $k_1, k_2 \in K$,

$$\frac{1}{2}k_1 - x_1 = \frac{1}{2}k_2 - x_2$$

Lattice point theorem

Proof.

Therefore, for some $k_1, k_2 \in K$,

$$\frac{1}{2}k_1 - x_1 = \frac{1}{2}k_2 - x_2$$

Therefore, $0 \neq (x_1 - x_2) = \frac{1}{2}k_1 + \frac{1}{2}(-k_2) \in K \cap \Lambda$ □

Applications

Applications

- Finiteness of class groups with the Minkowski bound

Applications

- Finiteness of class groups with the Minkowski bound
- Dirichlet's unit theorem

Applications

- Finiteness of class groups with the Minkowski bound
- Dirichlet's unit theorem
- Dirichlet's approximation

- Finiteness of class groups with the Minkowski bound
- Dirichlet's unit theorem
- Dirichlet's approximation
- Lagrange's four squares theorem

Sum of four squares

Can every positive integer be written as a sum of four perfect squares?

Sum of four squares

Can every positive integer be written as a sum of four perfect squares?
Yes! It was proved by Lagrange in 1770, using the principle of infinite descent.

Sum of four squares

Can every positive integer be written as a sum of four perfect squares?
Yes! It was proved by Lagrange in 1770, using the principle of infinite descent.
We give a proof using Minkowski's lattice point theorem! This proof is borrowed from the exercises of *Lectures on Discrete Geometry* by Jiri Matousek

Sum of four squares

Theorem

Every natural number is a sum of four squares

Theorem

Every natural number is a sum of four squares

Proof.

It is enough to prove the statement for odd primes p

Sum of four squares

Theorem

Every natural number is a sum of four squares

Proof.

It is enough to prove the statement for odd primes p

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2)$$

$$= (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_2)^2$$

$$+(a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2$$

□

Sum of four squares

Proof.

The first step is to show existence of integers a, b such that $a^2 + b^2 \equiv -1 \mod p$

Proof.

The first step is to show existence of integers a, b such that
$a^2 + b^2 \equiv -1 \mod p$
If -1 is a quadratic residue $\mod p$, then we are done.

Sum of four squares

Proof.

The first step is to show existence of integers a, b such that $a^2 + b^2 \equiv -1 \mod p$

If -1 is a quadratic residue $\mod p$, then we are done.

If not, consider the pairs $(0, p-1), (1, p-2), \cdot(\frac{p-1}{2}, \frac{p-1}{2})$

Sum of four squares

Proof.

The first step is to show existence of integers a, b such that
$a^2 + b^2 \equiv -1 \mod p$
If -1 is a quadratic residue $\mod p$, then we are done.
If not, consider the pairs $(0, p-1), (1, p-2), \cdot(\frac{p-1}{2}, \frac{p-1}{2})$
There exits a pair $(k, p-k-1)$, such that both k and $p-k-1$ are quadratic residues $\mod p$, so we are done since
$k + (p-k-1) \equiv -1 \mod p$ □

Sum of four squares

Proof.

Next we consider the following lattice

$$\Lambda = \{(x, y, z, t) \in \mathbb{Z}^4 : z \equiv ax + by \mod p, t \equiv bx - ay \mod p\}$$

Proof.

Next we consider the following lattice

$$\Lambda = \{(x, y, z, t) \in \mathbb{Z}^4 : z \equiv ax + by \mod p, t \equiv bx - ay \mod p\}$$

This has a $\mathbb{Z}$-basis given by

$$\{(1, 0, a, b), (0, 1, b, -a), (0, 0, p, 0), (0, 0, 0, p)\}$$

Sum of four squares

Proof.

Next we consider the following lattice

$$\Lambda = \{(x, y, z, t) \in \mathbb{Z}^4 : z \equiv ax + by \mod p, t \equiv bx - ay \mod p\}$$

This has a $\mathbb{Z}$-basis given by

$$\{(1, 0, a, b), (0, 1, b, -a), (0, 0, p, 0), (0, 0, 0, p)\}$$

and hence the covolume of Λ is p^2

Proof.

Next we consider the following lattice

$$\Lambda = \{(x, y, z, t) \in \mathbb{Z}^4 : z \equiv ax + by \mod p, t \equiv bx - ay \mod p\}$$

This has a $\mathbb{Z}$-basis given by

$$\{(1, 0, a, b), (0, 1, b, -a), (0, 0, p, 0), (0, 0, 0, p)\}$$

and hence the covolume of Λ is p^2
Let $K = \{x^2 + y^2 + z^2 + t^2 < 2p\}$ be a ball in $\mathbb{R}^4$

Sum of four squares

Proof.

Next we consider the following lattice

$$\Lambda = \{(x, y, z, t) \in \mathbb{Z}^4 : z \equiv ax + by \mod p, t \equiv bx - ay \mod p\}$$

This has a $\mathbb{Z}$-basis given by

$$\{(1, 0, a, b), (0, 1, b, -a), (0, 0, p, 0), (0, 0, 0, p)\}$$

and hence the covolume of Λ is p^2
Let $K = \{x^2 + y^2 + z^2 + t^2 < 2p\}$ be a ball in $\mathbb{R}^4$
K is bounded, convex and symmetric with volume $2\pi^2 p^2$

$$vol(K) = 2\pi^2 p^2 > 2^4 covol(\Lambda)$$

Proof.

Next we consider the following lattice

$$\Lambda = \{(x, y, z, t) \in \mathbb{Z}^4 : z \equiv ax + by \mod p, t \equiv bx - ay \mod p\}$$

This has a $\mathbb{Z}$-basis given by

$$\{(1, 0, a, b), (0, 1, b, -a), (0, 0, p, 0), (0, 0, 0, p)\}$$

and hence the covolume of Λ is p^2
Let $K = \{x^2 + y^2 + z^2 + t^2 < 2p\}$ be a ball in $\mathbb{R}^4$
K is bounded, convex and symmetric with volume $2\pi^2 p^2$

$$vol(K) = 2\pi^2 p^2 > 2^4 covol(\Lambda)$$

Therefore, by Minkowski's theorem, we get a non-zero point $(x, y, z, t) \in K \cap \Lambda$

□

Sum of squares

Proof.

$$x^2 + y^2 + z^2 + t^2 \equiv x^2 + y^2 + (ax + by)^2 + (bx - ay)^2 \mod p$$

Sum of squares

Proof.

$$x^2 + y^2 + z^2 + t^2 \equiv x^2 + y^2 + (ax + by)^2 + (bx - ay)^2 \mod p$$

$$\equiv x^2 + y^2 + a^2x^2 + b^2y^2 + b^2x^2 + a^2y^2 \mod p$$

Sum of squares

Proof.

$$x^2 + y^2 + z^2 + t^2 \equiv x^2 + y^2 + (ax + by)^2 + (bx - ay)^2 \mod p$$

$$\equiv x^2 + y^2 + a^2x^2 + b^2y^2 + b^2x^2 + a^2y^2 \mod p$$

$$\equiv (x^2 + y^2)(1 + a^2 + b^2) \equiv 0 \mod p$$

Proof.

$$x^2 + y^2 + z^2 + t^2 \equiv x^2 + y^2 + (ax + by)^2 + (bx - ay)^2 \mod p$$

$$\equiv x^2 + y^2 + a^2x^2 + b^2y^2 + b^2x^2 + a^2y^2 \mod p$$

$$\equiv (x^2 + y^2)(1 + a^2 + b^2) \equiv 0 \mod p$$

Therefore, we have a non-zero point $(x, y, z, t) \in \mathbb{Z}^4$ satisfying,

$$x^2 + y^2 + z^2 + t^2 \equiv 0 \mod p$$

and

$$0 < x^2 + y^2 + z^2 + t^2 < 2p$$

Sum of squares

Proof.

$$x^2 + y^2 + z^2 + t^2 \equiv x^2 + y^2 + (ax + by)^2 + (bx - ay)^2 \mod p$$

$$\equiv x^2 + y^2 + a^2x^2 + b^2y^2 + b^2x^2 + a^2y^2 \mod p$$

$$\equiv (x^2 + y^2)(1 + a^2 + b^2) \equiv 0 \mod p$$

Therefore, we have a non-zero point $(x, y, z, t) \in \mathbb{Z}^4$ satisfying,

$$x^2 + y^2 + z^2 + t^2 \equiv 0 \mod p$$

and

$$0 < x^2 + y^2 + z^2 + t^2 < 2p$$

Therefore, we get $p = x^2 + y^2 + z^2 + t^2$ □

Thank you!