Geometry of Numbers

Our goal: What numbers are a sum of two squares?

In Lecture: Descent method

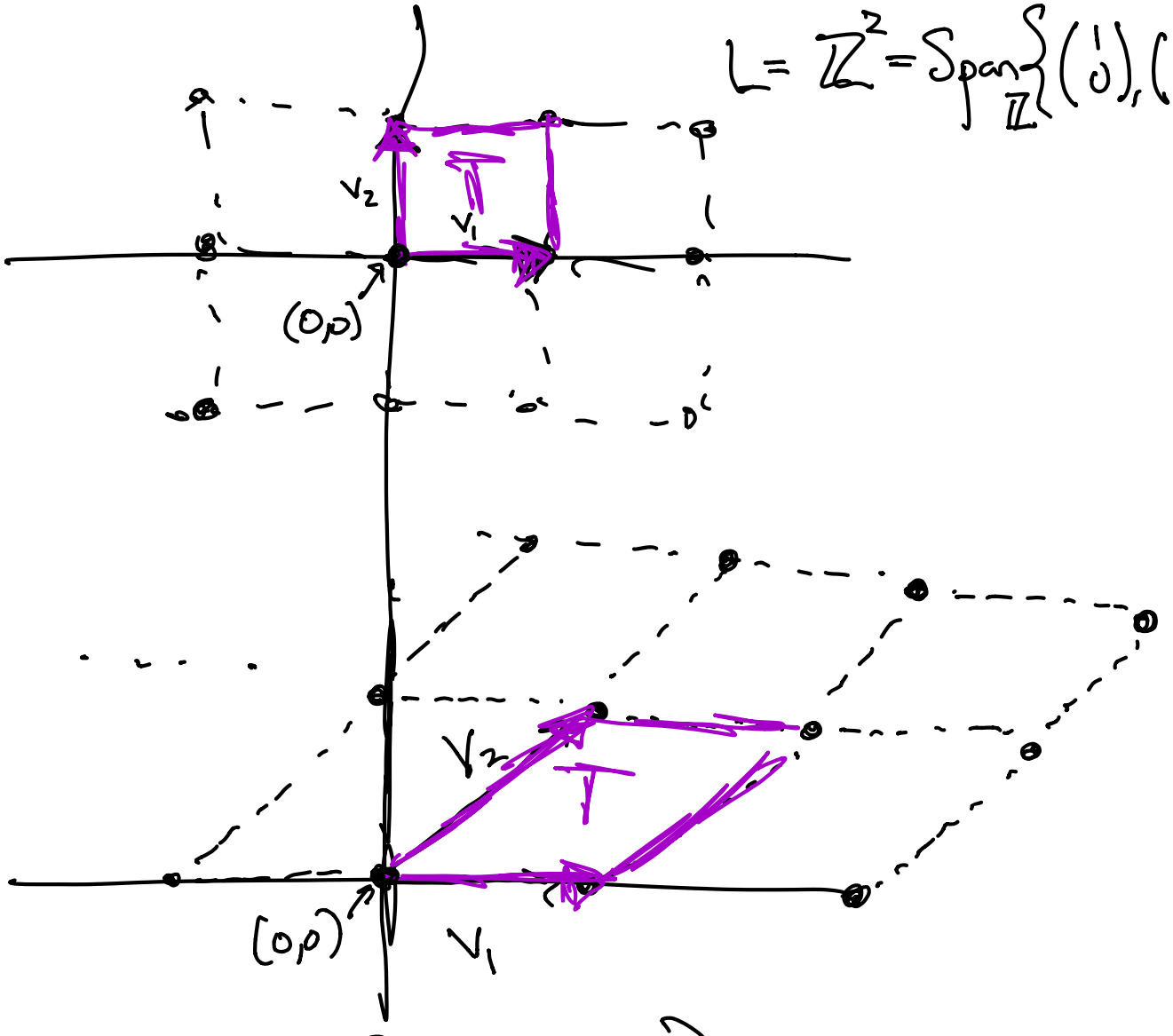
Discussion: Lattice points

Handout (?): Algebra

Some definitions:

- A lattice in $\mathbb{R}^2$ is defined as $L = \text{Span}_{\mathbb{Z}}\{v_1, v_2\}$ for two linearly independent vectors v_1, v_2.

$L = \mathbb{Z}^2 = \text{Span}_{\mathbb{Z}}\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$



$$L = \text{Span}_{\mathbb{Z}}\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right\}$$

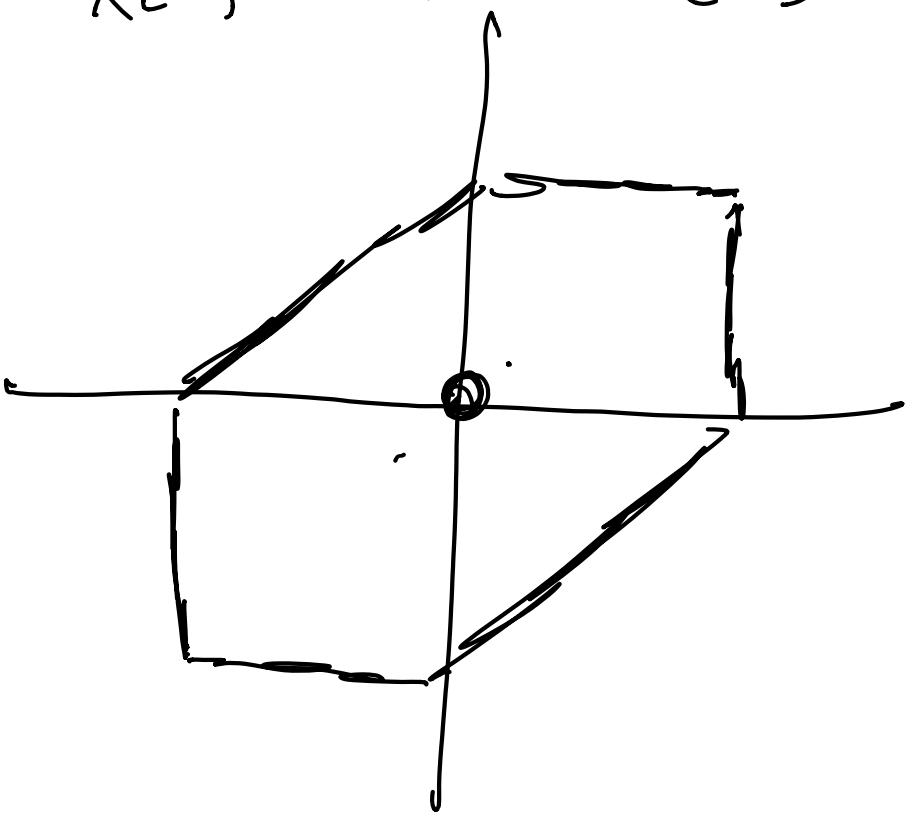
T

- The fundamental Parallelogram of a lattice L is defined as

$$\left\{\lambda_1 v_1 + \lambda_2 v_2 : 0 \le \lambda_i < 1\right\}$$

- A set S is called <u>convex</u> if for any $x, y \in S$ we have $\lambda x + (1-\lambda) y \in S$ for $\lambda \in [0,1]$. i.e, the line connecting x and y is contained in S.

- S is called <u>0-Symmetric</u> if $x \in S \Rightarrow -x \in S$



Convex, 0-Symmetric

Our proof will use two theorems about lattices:

Minkowski's Thm: Let $S \subseteq \mathbb{R}^2$ be convex, 0-symmetric region, and L be a lattice. If $\text{Area}(S) > 4\,\text{Area}(T)$ then S contains a non-zero lattice point of L.

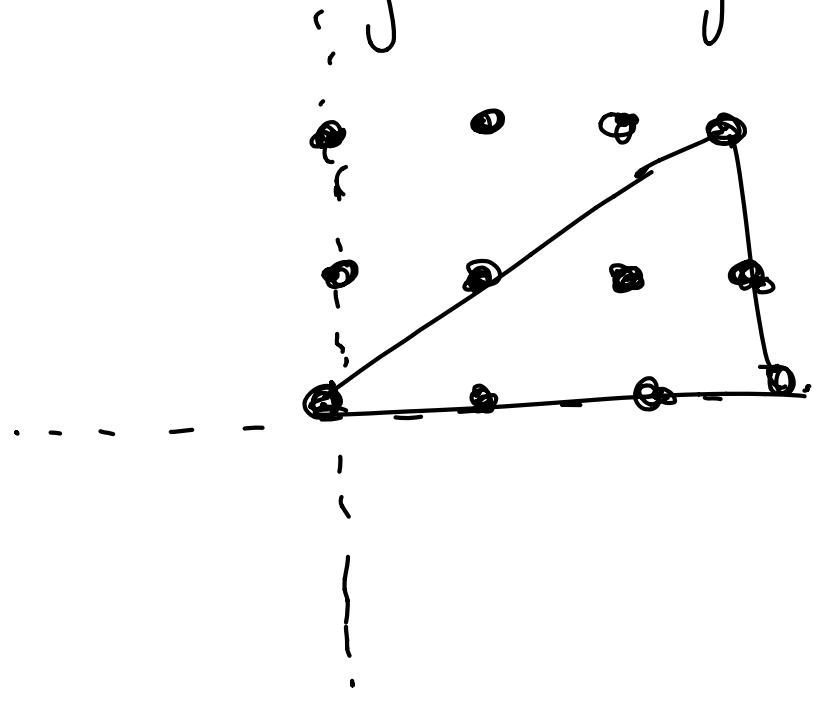
Pick's Thm: Let L be a lattice in $\mathbb{R}^2$. Let P be a convex polygon with vertices on L.

$$\text{Area}(P) = \left(I + \frac{1}{2}B - 1\right)\text{Area}(T)$$

I = # lattice pts inside P

B = # lattice pts on boundary of P

Special case done on HW 8. for $L = \mathbb{Z}^2$ and P a right triangle.



Thm: (Fermat)

$p \equiv 1 \bmod 4 \iff p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Moreover, this representation is unique, up to order of x, y and up to sign.

Proof:

$\Longleftarrow$ Suppose $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Note that $xy \neq 0$.

$\Longrightarrow x^2 + y^2 \equiv 0 \bmod p$

$\Longrightarrow x^2 \equiv -y^2 \bmod p$

$$\Rightarrow \left(\frac{x}{y}\right)^2 \equiv -1 \mod p$$

$$\Rightarrow \left(\frac{-1}{p}\right) = 1$$

$$\Rightarrow p \equiv 1 \mod 4.$$

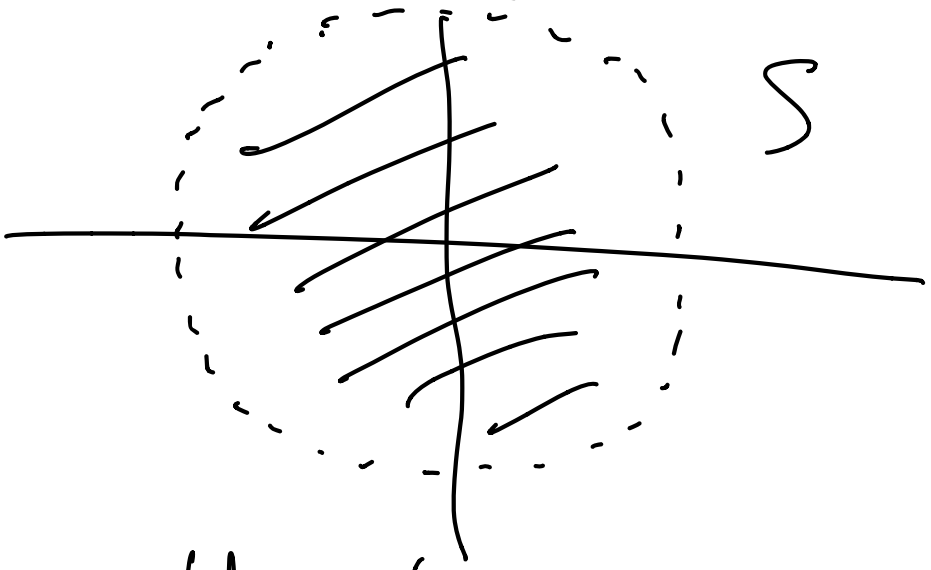
Now for the hard part:

$\Leftarrow$ Assume $p \equiv 1 \mod 4$.

Then $\left(\frac{-1}{p}\right) = 1$. Choose

$1 \leq k \leq p-1$ s.t. $k^2 \equiv -1 \mod p$

Let $S = \{(x,y) : x^2 + y^2 < 2p\}$.



We will choose a special lattice L, and show S contains a lattice point of L. Define

$$L = \{(x,y) : y \equiv kx \bmod p\}$$

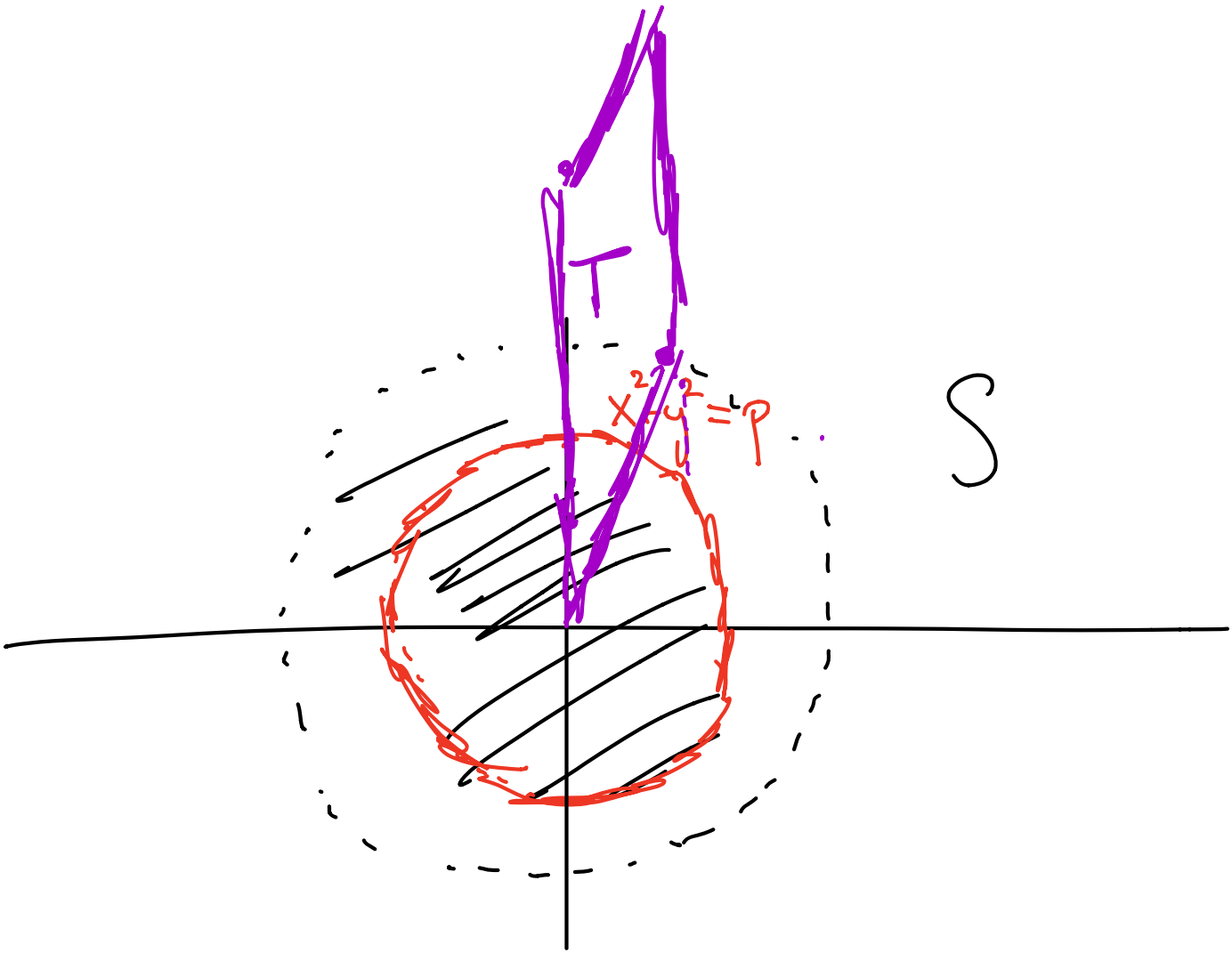
$$= \mathrm{Span}_{\mathbb{Z}}\left\{\begin{pmatrix}1\\k\end{pmatrix}, \begin{pmatrix}0\\p\end{pmatrix}\right\}$$

What's special about L?

every point on L satisfies

$$\left(\frac{x}{y}\right)^2 \equiv -1 \mod p, \text{ i.e.}$$

$$x^2 + y^2 \equiv 0 \mod p.$$



$$\text{Area}(S) = 2\pi p$$

$$\text{Area}(T) = \det\begin{pmatrix} 1 & 0 \\ k & p \end{pmatrix} = p$$

Since $2\pi p > 4p$, by Minkowski S contains a lattice point of L.

Let's say (a,b) is such a lattice point.

$$a^2+b^2 < 2p$$

$$a^2+b^2 \equiv 0 \bmod p$$

$$\Rightarrow \boxed{a^2+b^2 = p.}$$

Now we just need to show uniqueness.

This amounts to showing there are 8 integer points on the circle

$$x^2+y^2 = p : z \longleftarrow \mathbb{C}$$

$(a,b), (a,-b), (-a,b), (-a,-b)$

$(b,a), (b,-a), (-b,a), (-b,-a)$

For any $(x,y) \in C$, note that one of (x,y) and $(x,-y)$ must lie on $C \cap L$:

$$x^2+y^2=p \implies x^2+y^2 \equiv 0 \bmod p$$

$$\implies x \equiv \pm ky \bmod p \text{ - WLOG,}$$

say $x \equiv ky \bmod p$.

If both (x,y) and $(x,-y) \in C \cap L$

$$\implies y \equiv -y \bmod p$$

$$\implies y \equiv 0 \bmod p \quad \longrightarrow \Leftarrow$$

So showing 4 integer pts is the same as showing 4 lattice points.

Construct a convex polygon P

out of the lattice points in $\mathbb{Z}^2$.

By Pick's theorem,

$$\text{Area}(P) = \left(I + \frac{B}{2} - 1\right) \text{Area}(\square)$$

By def^n of L, the only interior lattice pt is origin, because all lattice pts satisfy $x^2 + y^2 \equiv 0 \bmod p$.

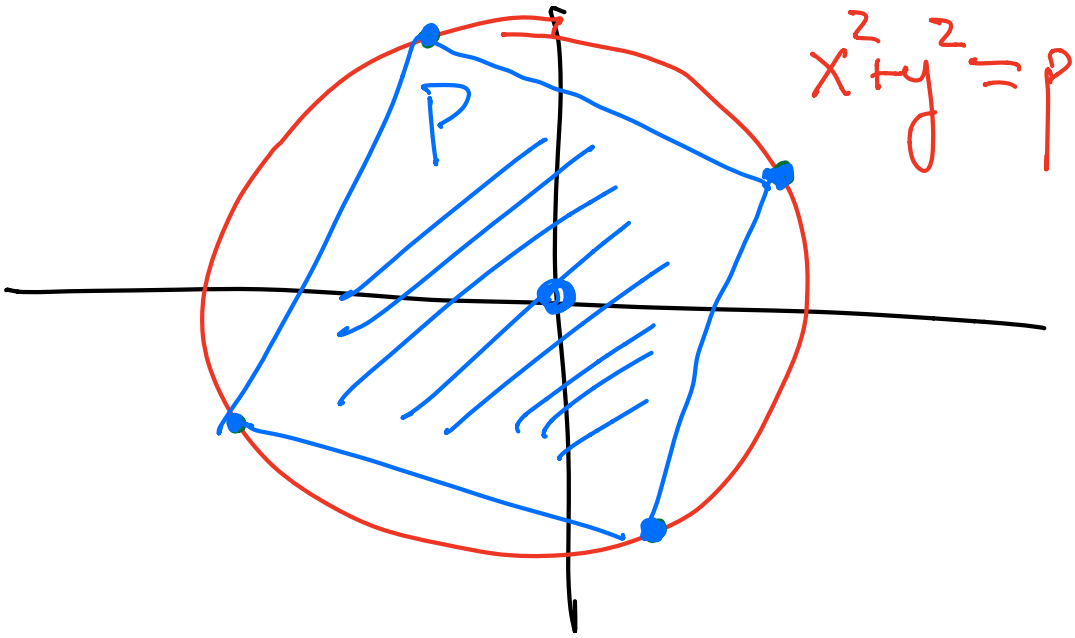
So $\boxed{I = 1}$

non-zero

This means that all lattice pts are on boundary of P.

$$\text{Area}(P) = \frac{\#\text{lattice pts}}{2} \cdot p$$

$$(\#\text{lattice pts}) \cdot p = 2 \cdot \text{Area}(P)$$



$$\text{Area}(P) < \text{Area}(C) = \pi p$$

$$p \cdot (\#\text{lattice pts}) < 2\pi p$$

$$\Rightarrow \boxed{\#\text{lattice pts} < 2\pi.}$$

Final observation:

if $(a,b) \in C \cap L$

then $a \equiv kb \bmod p$

$\Rightarrow$ $ka \equiv -b \bmod p$, so

$(a,b) \in C \cap L \Rightarrow (-b,a) \in C \cap L$

Also, note $(-a,-b) \in C \cap L$

so that $(b,-a) \in C \cap L$

So **# lattice pts divisible by 4**

$\Rightarrow$ # lattice pts $= 4$ $\blacksquare$

Challenge: Modify this argument to prove

$p = x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$

$\iff p \equiv 1, 3 \mod 8.$

Can you do the same for

$p = x^2 + 3y^2$?