BMC **Lattice points and number theory** **April 2023**

Paul Zeitz, zeitzp@usfca.edu

We will explore various topics in number theory, mostly related to representations of integers as sums of squares and other powers, and will use visual, geometric tools to analyze the problems. The way that we get geometry to play with number theory is by pondering *lattice points* and applying *linear algebra*.

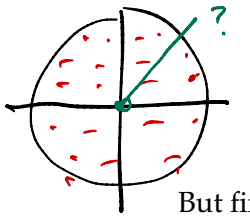
Our goal will be to prove two important theorems.

THE "CHRISTMAS" THEOREM.

Let p be an odd prime. There exist integers x, y such that

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

if and only if $p \equiv 1 \pmod 4$.



LAGRANGE'S 4-SQUARES THEOREM.

Every integer can be written as a sum of at most four squares.

But first, a teaser problem.

THE DARK FOREST.

Imagine a circle centered at the origin, with radius 12, and at every lattice point other than the origin on or inside this circle, grow a perfectly cylindrical tree centered at the lattice point, with radius of 0.1. If you stand at the origin, can you see outside the forest?

1 Number theory review

Recall the following concepts that we discussed in the fall.

- A number a is called a *quadratic residue* modulo n if it is a "square" mod n; i.e., if there exists x such that $x^2 \equiv a \pmod n$. We will use the abbreviation QR for quadratic residue.
- Let p be a prime. If $a \perp p$ (i.e., a and p are relatively prime), define the *Legendre symbol* $\left(\frac{a}{p}\right)$ to equal 1 if a is a QR and $= -1$ if a is not a QR $\pmod p$. Thus, for example, $\left(\frac{2}{7}\right) = 1$, since $3^2 \equiv 2 \pmod 7$, but $\left(\frac{3}{7}\right) = -1$, because there are no x satisfying $x^2 \equiv 3 \pmod 7$.
- We compute $(p-1)/2$ so frequently that we will denote it by h_p, where h means "half." If the prime is understood in context, we will just write h.

Assume that p is an odd prime and that $a \perp p$.

Problem 1 ***The Sudoku priniciple.*** *Then the sets*

$$\{a, 2a, 3a, \ldots, (p-1)a\} \quad \text{and} \quad \{1, 2, 3, \ldots p-1\}$$

are equal $\pmod p$.

Problem 2 *The equation* $x^2 \equiv a \pmod p$ *either has no solutions or exactly 2 solutions; consequently there are* h_p *QRs among the residues* $\{1, 2, 3, \ldots p-1\}$.

Problem 3 ***Wilson's theorem.*** *Prove that* $(p-1)! \equiv -1 \pmod p$.

Problem 4 ***Euler's criterion and the square root of*** -1. *You proved Wilson's theorem by pairing, if able, terms in the product* $1 \cdot 2 \cdot 3 \cdots (p-1)$ *whose product was 1. Modify this so that the product is* -1 *to conclude that*

$$\left(\frac{-1}{p}\right) \equiv (-1)^h \pmod p,.$$

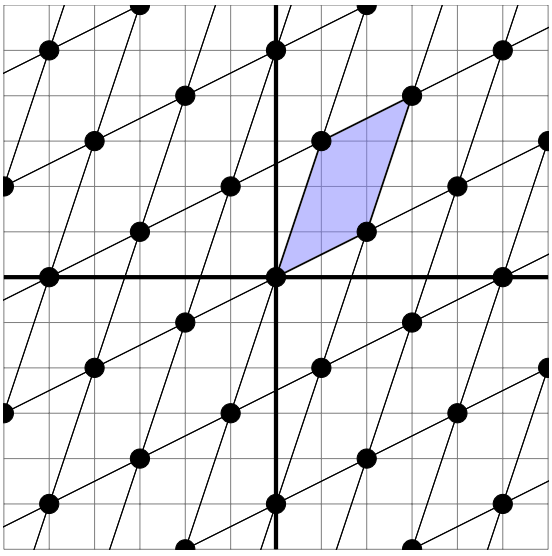
and conclude that there exists a "square root of -1*" modulo* p *if and only if* $p \equiv 1 \pmod 4$.

2 Geometric theorems

The following simple results about lattice points have very powerful applications. A *lattice point* is just a point with integer coordinates. More generally, a *lattice* is the set of points generated by "integer linear combinations" of a set of basis vectors. For example, let $\mathbf{v} = (2, 1)$ and $\mathbf{w} = (1, 3)$ be vectors in $\mathbb{R}^2$. Define the lattice Λ to be the set of points

$$\Lambda = \{a\mathbf{v} + b\mathbf{w} : a, b \in \mathbb{Z}\}.$$

The parallelogram with vertices $(0, 0), \mathbf{v}, \mathbf{w}, \mathbf{V} + \mathbf{w}$ is called the fundamental parallelogram of Λ. In the figure below, the Λ-points are dark circles and the fundamental parallelogram is shaded.



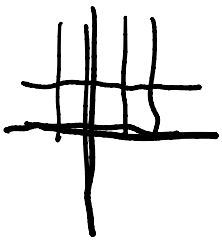
Clearly the notion of lattice and fundamental parallelogram (parallelepiped) can be extended to higher dimensions.

Problem 5 *Blichfeldt's Lemma. Let F be a figure in the plane with area greater than the integer n. Then F can be translated so that it covers $n+1$ lattice points.*

For the next theorem, we need to define an M-*set*. This is a set that is convex, contains the origin, and is symmetric about the origin.

Problem 6 *Minkowski's theorem, vanilla version. An M-set in $\mathbb{R}^d$ with d-dimensional volume greater than 2^d must contain at least one more lattice point besides the origin.*

For example, a 2-dimensional M-set with area greater than 4 must contain at least one more lattice point besides $(0,0)$.



Problem 7 *Minkowski's theorem, general lattice version. Let Λ be a lattice in $\mathbb{R}^d$ and let the d-dimensional volume of its fundamental parallelepiped be V. Then any M-set in $\mathbb{R}^d$ whose d-dimensional volume is greater than $2^d A$ must contain at least one more Λ-point besides the origin.*

Problem 8 *Determinants and volume. Let $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_n}$ be n linearly independent vectors in $\mathbb{R}^n$. Let M be the matrix whose ith column is $\mathbf{v_i}$ (written as a column vector). The volume of the fundamental region of the lattice generated by these n vectors is equal to the absolute value of the determinant of M.*

3 Miscellaneous problems

Problem 9 *Show that every multiple of 6 can be written as a sum of at most four cubes.*

Problem 10 *Show that any integer can be written as a sum of at most five cubes.*

Problem 11 *Show that for any prime p, there exist integers a, b such that $a^2+b^2 \equiv -1 \pmod{p}$.*

Problem 12 *Let $S = \{0, 1, 2, 4, 5, 8, 9, 10, \ldots\}$ be the set of integers that can be written as the sum of two squares. Show that S is multiplicative; i.e., if $a \in S$ and $b \in S$, then $ab \in S$.*

Problem 13 *Prove that the set of integers that can be written as a sum of four squares is multiplicative (without using Lagrange's theorem which says that this set is the natural numbers). Is this assertion true for the set of integers than can be written as a sum of three squares?*

Problem 14 *Pick's theorem. Pick's theorem states that the area of a lattice polygon (one whose vertices are lattice points) is equal to $I + \frac{1}{2}B - 1$, where I and B equal the number of interior and boundary lattice points, respectively. Use Minkowski's theorem to prove Pick's theorem.*

Supp $\exists\, t$ s.t.
$t^2 \equiv a \pmod p$. Then $(-t)^2$ also works

$(-t)^2 \equiv t^2 \equiv a$

- Could $t \equiv -t$?

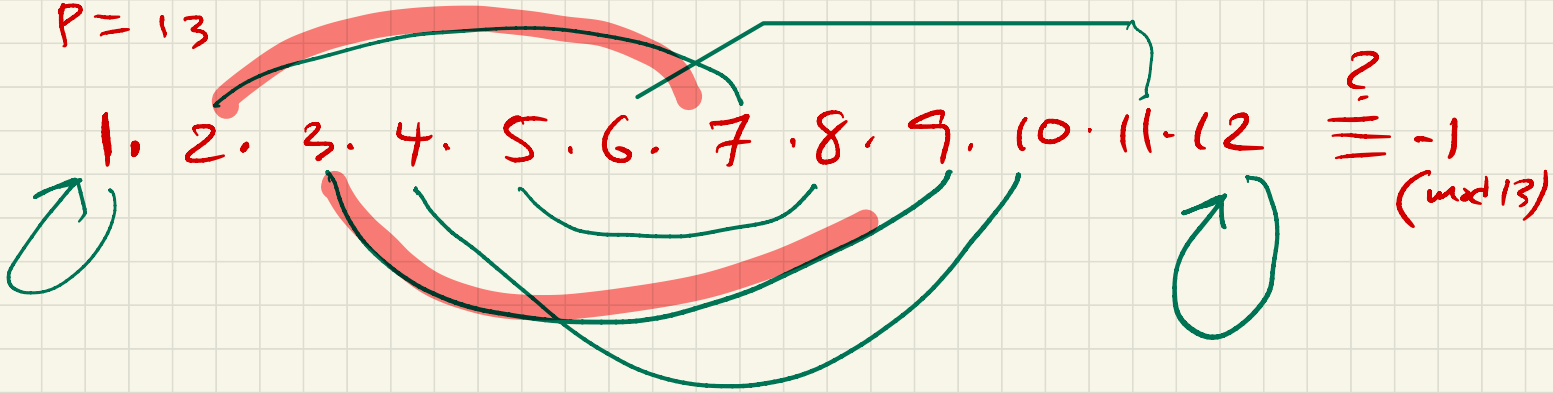
NO p is ODD

- Suppose $\exists\, s$ s.t. $s^2 \equiv a$
$t^2 \equiv a$

$s^2 - t^2 \equiv 0$

$(s-t)(s+t) \equiv 0$

$s-t \equiv 0$ OR $s+t \equiv 0$



$$x^2 \equiv 1 \bmod 13$$

$$x \equiv \pm 1$$

Which primes have "i"

For which primes p $\exists\, u$ s.t. $u^2 \equiv -1 \bmod p$

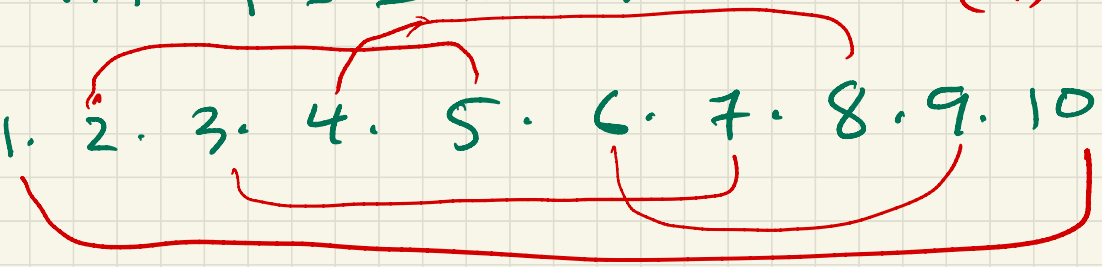
$$\left(\frac{-1}{p}\right) = 1$$

$\frac{11-1}{2} = 5$ pairs

$(-1)^5 = -1$

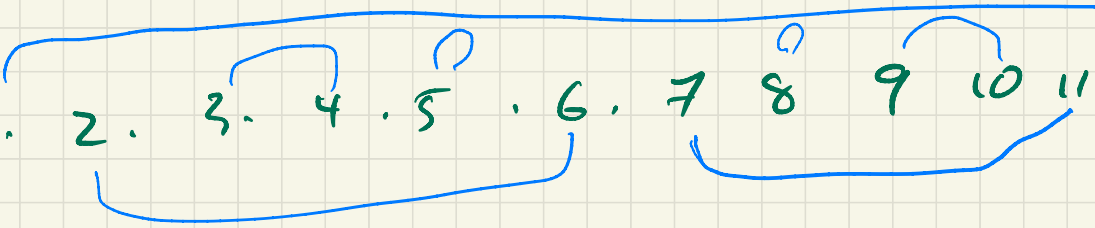
ans: iff $p \equiv 1 \bmod 4$

$p = 11$ $\quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv -1 \bmod 11$

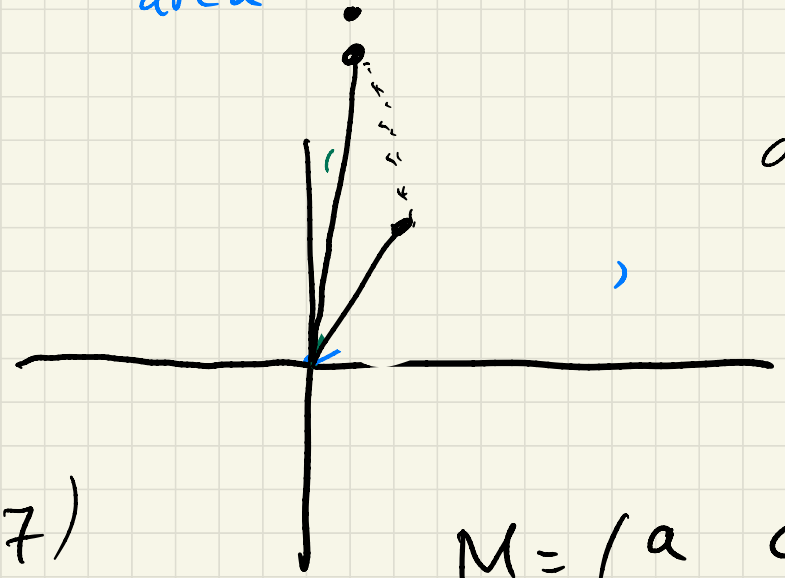


$\frac{13-1}{2} = 6$ pairs

$p = 13$ $\quad 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \equiv -1 \bmod 13$



area

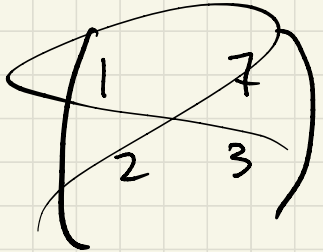


area $= |ad - bc|$

$\vec{v} = (1, 7)$

$\vec{w} = (2, 3)$

$M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$



$(2, 1)$

$(3, 7)$

$\det \begin{pmatrix} 1 & 2 \\ 7 & 3 \end{pmatrix} = 1 \cdot 3 - 2 \cdot 7 = -11$

let $M := ad - bc$

$\det \begin{pmatrix} 2 & 1 \\ 3 & 7 \end{pmatrix} = 11$

$$M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} \vec{v} & \vec{w} \end{pmatrix}$$

column vectors

$\det : \text{Matrices} \longrightarrow \mathbb{R}$

$\det(\vec{v}, \vec{w}) = -\det(\vec{w}, \vec{v})$

det is linear in each variable

$\det(a\vec{v}_1 + b\vec{v}_2, \vec{w}) =$

$\det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$ ☺

$\det(\vec{v}, \vec{w}) = 3$

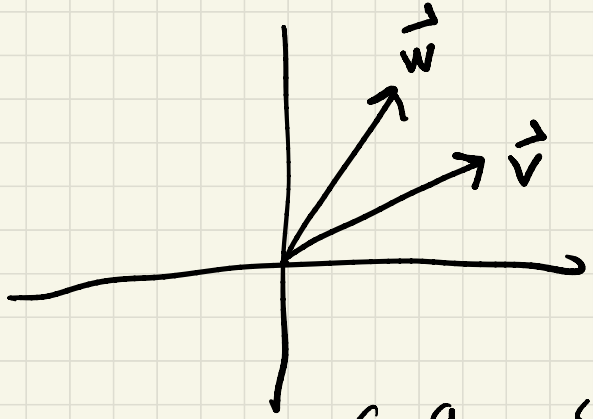
$\det(2\vec{v}, \vec{w}) = 6$

$\det(\vec{u}, \vec{w}) = 11$

$\det(\vec{v}+\vec{u}, \vec{w}) = 14$

$\det(4\vec{v}, 4\vec{w}) = 48$

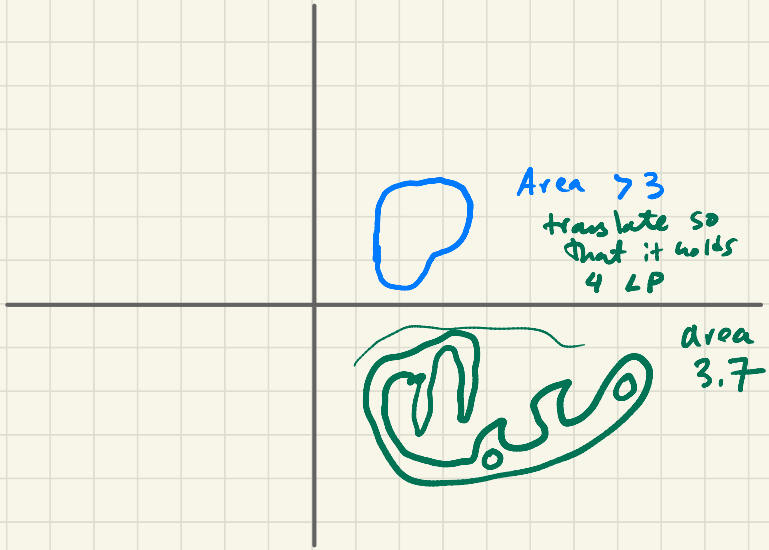
Claim: the "det" function so defined outputs the "signed area" of the fund parall made by the colum vectors



$\det(\vec{v}, \vec{w}) = \text{pos}$

$\det(\vec{w}, \vec{v}) = \text{neg}$

and $\det\begin{pmatrix} a & c \\ b & d \end{pmatrix} = ad - bc$


Area > 3
translate so
that it holds
4 LP
area
3.7

Minkowski Theorem

M-set (bounded)

- Contain origin
- Symmetric wrt orig
- Convex