In this lecture, we study: for what primes p,

$$p = n^2 + m^2$$

with n, m being integers.

Example: $5 = 2^2 + 1^2$ ✓

$13 = 2^2 + 3^2$ ✓

19 ✗

Theorem: Let p be a prime. Then p is a sum of two squares exactly when:

$$p \equiv 1 \pmod 4 \quad \text{or} \quad p = 2.$$

Remark: (1) $p=2$, $2 = 1^2 + 1^2$ ✓

(2) We can use the Theorem to check the numbers in the example

(3) In the proof, we will give an algorithm to find n, m such that $p = n^2 + m^2$ (when $p \equiv 1 \pmod 4$).

Proof: By Remark (1), we only need to focus on odd primes.

We need to prove the following two statements to complete the proof:

Statement I: If p (odd prime) is a sum of two squares, then

$$p \equiv 1 \pmod 4$$

Statement II: If $p \equiv 1 \pmod 4$, p is a sum of two squares.

Proof of statement I: Let p be an odd prime and

$$p = n^2 + m^2 \quad \text{with } m, n \in \mathbb{Z}.$$

Then $-m^2 \equiv n^2 \pmod p \Rightarrow -m^2$ is a QR $\pmod p$

That is: $\left(\frac{-m^2}{p}\right) = 1.$

On the other hand,

$$\left(\frac{-m^2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{m}{p}\right)\left(\frac{m}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{m}{p}\right)^2$$

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

Therefore, $\left(\frac{-1}{p}\right) = 1$ and $p \equiv 1 \pmod 4$. $\triangle$

Proof of Statement II: (Method of Descent)

Idea: suppose that we find $A^2 + B^2 = Mp$ with $M \geq 1$

then we can always find $A_1^2 + B_1^2 = M_1 p$ with $1 \leq M_1 < M$

then we can find $A_2^2 + B_2^2 = M_2 p$ with $1 \leq M_2 < M_1 < M$

....

we continue this process and we finally get:

$$n^2 + m^2 = p$$

Step I.

Since $p \equiv 1 \pmod 4$, $\left(\frac{-1}{p}\right) = 1$. We can find A, $1 \le A \le p-1$

such that $$A^2 \equiv -1 \pmod p$$

We can assume $M \neq 1$. Otherwise, the proof is finished.

This gives. $A^2 + 1^2 = Mp$.

Claim: $M < p$ since $M = \frac{A^2+1}{p} \le \frac{(p-1)^2+1}{p} < p$.

For some reason, we write this as:

$$A^2 + B^2 = Mp \quad \text{with} \quad M < p$$

Step II: find u, v between $-\frac{M}{2}$ and $\frac{M}{2}$ such that

$u \equiv A \pmod M$ $\qquad$ $v \equiv B \pmod M$.

Then $u^2 + v^2 \equiv A^2 + B^2 \pmod M \equiv 0 \pmod M$

We write $u^2 + v^2 = Mr$.

We can show $1 \le r < M$.

- $r = \frac{u^2+v^2}{M} \le \frac{\left(\frac{M}{2}\right)^2 + \left(\frac{M}{2}\right)^2}{M} \le \frac{M}{2} < M$.
- We know $r \ge 0$. It suffices to show $r \neq 0$.

(Proof by contradiction) If $r=0$, then $u^2+v^2=0$ and $u=v=0$.

By definition of u, v, $A \equiv 0 \pmod{M}$ and $B \equiv 0 \pmod{M}$

Then $M^2 \mid A^2+B^2 = Mp$.

This will force $M=1$.

However, we assumed $M>1$.

Step III: Set $A_1 = uA + vB$ $\quad B_1 = vA - uB$

Claim: (1) $M \mid A_1$ and $M \mid B$

(2) $\left(\frac{A_1}{M}\right)^2 + \left(\frac{B_1}{M}\right)^2 = rp$

Since $1 \leq r < M$, we finish the "descent" part.

Proof of Claims: (1) By definition of u, v

$uA + vB \equiv A^2 + B^2 \pmod{M} \equiv 0 \pmod{M}$

$M \mid uA + vB = A_1$

$vA - uB \equiv BA - AB \pmod{M} \equiv 0 \pmod{M}$

$M \mid vA - uB = B_1$

(2) We showed:

$A^2 + B^2 = Mp$

$u^2 + v^2 = Mr$

$$\Rightarrow \quad (u^2+v^2)(A^2+B^2) = M^2 pr.$$

An identity: $\underbrace{(uA+vB)}_{A_1}{}^2 + \underbrace{(vA-uB)}_{B_1}{}^2 = (u^2+v^2)(A^2+B^2)$

$$\Rightarrow \quad A_1^2 + B_1^2 = M^2 pr.$$

By (1) $(M \mid A_1,\ M \mid B_1)$, $\quad \left(\frac{A_1}{M}\right)^2 + \left(\frac{B_1}{M}\right)^2 = rp.$

Step IV: If $r>1$, we repeat the steps.

and finally we find: $\quad n^2 + m^2 = p. \qquad \square$

Example: $\quad p = 881$

Step I: $\quad 387^2 + 1^2 = 170 \cdot 881 \qquad A = 387,\ B = 1,\ M = 170 < 881$

Step II: $\quad 387 \equiv 47 \pmod{170} \qquad u = 47$

$1 \equiv 1 \pmod{170} \qquad v = 1$

$47^2 + 1^2 = 13 \cdot 170 \qquad r = 13.$

Step III: $\quad A_1 = uA + vB = 18190$

$B_1 = vA - uB = 340$

$$(18190)^2 + (340)^2 = 170 \cdot 13 \cdot 170 \cdot 881$$

Divide $M^2 = 170^2$ and:

$$\Rightarrow \left(\frac{18190}{170}\right)^2 + \left(\frac{340}{170}\right)^2 = 13 \cdot 881$$

$$(107)^2 + 2^2 = 13 \cdot 881$$

$13 > 1$, we need to repeat the steps.

Step I' $\quad (107)^2 + 2^2 = 13 \cdot 881$ $\quad A = 107$, $B = 2$, $M = 13 < 881$

Step II' $\quad 107 \equiv 3 \pmod{13}$ $\quad u = 3$

$2 \equiv 2 \pmod{13}$ $\quad v = 2$

$u^2 + v^2 = 13 \cdot 1$ $\quad r = 1.$

Step III' $\quad A_2 = uA + vB = 325$

$B_2 = vA - uB = 208.$

$$(325)^2 + (208)^2 = 13 \cdot 1 \cdot 13 \cdot 881$$

Divide $M^2 = 13^2$ and we get:

$$(25)^2 + (16)^2 = 881$$