QUADRATIC RESIDUES

We have seen how to solve linear congruences and system of linear congruences (Chinese Remainder Theorem)

Today : Discuss quadratic congruences

Example: $$5x^2 \equiv 7 \pmod{13}$$

Studied by Gauss, "Quadratic Reciprocity"

$$x^2 \equiv a \pmod{p}$$

Also studied by Euler and Legendre

Let p be an odd prime.

For numbers between 1 & $p-1$ half are squares mod p & half are non-squares

$x \pmod p \qquad p-x \pmod p$

$x^2 \pmod p$

If $x^2 \equiv y^2 \pmod p$

then $(x-y)(x+y) \equiv 0 \pmod p$

So $x \equiv y \pmod p$

or $x \equiv -y \pmod p$

3	$\underline{1}$, 2 (square)
5	$\underline{1}$, 2, 3, $\underline{4}$
7	$\underline{1}$, $\underline{2}$, 3, $\underline{4}$, 5, 6
11	$\underline{1}$, 2, $\underline{3}$, $\underline{4}$, $\underline{5}$, 6, 7, 8, $\underline{9}$, 10

Euler's Criterion for squareness mod p

<u>Thm:</u> Let p be an odd prime number and let a be an integer coprime to p. Then

a) a is square mod $p \iff a^{(p-1)/2} \equiv 1 \bmod p$

(b) a is non square mod $p \iff (a)^{(p-1)/2} \equiv -1 \bmod p$

<u>Pf:</u> a is square mod p

$\iff x^2 \equiv a \pmod{p}$ has a soln.

$$\Rightarrow \left(x^2\right)^{(p-1)/2} \equiv a^{(p-1)/2} \pmod{p}$$

$$\Rightarrow (a)^{(p-1)/2} \equiv 1 \pmod{p}$$

Suppose $(a)^{(p-1)/2} \equiv 1 \pmod{p}$

Let g be a primitive root mod p

Then $a = g^y$ for some y

Claim: y should be even.

$$a^{(p-1)/2} \equiv g^{y/2(p-1)} \equiv 1 \pmod p$$

$$(p-1) \mid y/2\,(p-1) \implies y \text{ is even.}$$

Take $x = g^{y/2}$

Then, $x^2 \equiv a \pmod p$

(b) follows because

$$a^{p-1} \equiv 1 \pmod p$$

$$\implies (a)^{p-1/2} \equiv \pm 1 \pmod p$$

Corollary: -1 is square mod p

$\iff (-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$

$\iff \frac{p-1}{2}$ is even

$\iff p = 4k+1$ for some $k \in \mathbb{Z}$

But what is the solution to

$$x^2 \equiv -1 \pmod p \;?$$

WILSON'S THEOREM

$$\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & \cdots & \cdots & \cdots & \cdots & p-1 \\ \downarrow & \downarrow & \downarrow & & \cdots & & \cdots & & \cdots & \downarrow \\ 1 & 2^{-1} & 3^{-1} & & & & & & & p-1 \end{array}$$

$$(p-1)! = 1 \times 2 \times 3 \times 4 \times 5 \times \cdots \times (p-1)$$

$$\equiv (p-1) \pmod p$$

$$\equiv -1 \mod p$$

$p = 7$

$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6$

$1 \times 2 \times 3 \times 4 \times 5 \times 6 \equiv 6$

$\equiv -1 \pmod 7$

Let's find square root of -1.

$1 \quad 2 \quad 3 \quad \cdots \quad p-1$

$$E = 2 \times 4 \times 6 \times 8 \times \cdots \times p-1$$

$$O = 1 \times 3 \times 5 \times 7 \times \cdots \times p-2$$

$$(-1)^{\frac{(p-1)}{2}} \times E = (-2) \times (-4) \times \cdots \times -(p-1)$$

$$\equiv O \pmod p$$

$$E \times O \equiv E^2 \times (-1)^{(p-1)/2} \pmod p$$

$$\boxed{(-1) \equiv E^2 \pmod p}$$

<u>Theorem:</u> (Fermat's 2 square thm)

Let p be a prime.

$$p = x^2 + y^2 \iff p = 2 \quad \text{or} \quad p \equiv 1 \pmod 4$$

<u>Pf:</u> ($\Rightarrow$) $p = x^2 + y^2$ Suppose $p \neq 2$

$$p \equiv \underbrace{x^2}_{0 \text{ or } 1} + \underbrace{y^2}_{0 \text{ or } 1} \pmod 4$$

$$p \equiv 1 \pmod 4$$

($\Leftarrow$) If $p=2$ then

$$p = 1^2 + 1^2$$

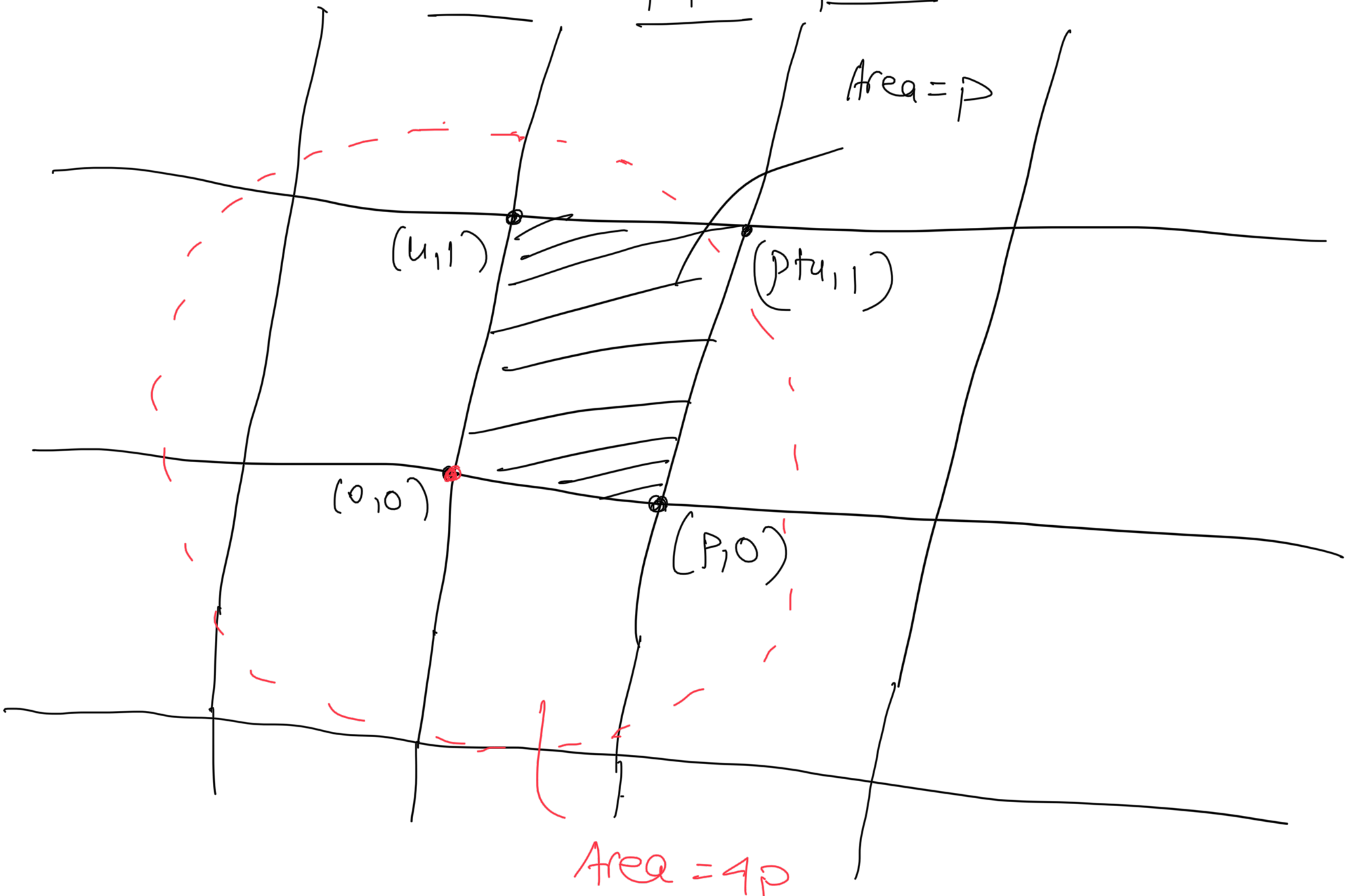
Suppose $p \equiv 1 \pmod 4$ Then

$\exists\, u$ s.t $u^2 \equiv -1 \pmod p$

Take the set of all points

(x, y) such that $x \equiv uy \pmod p$

Minkowski's proof



$$x^2+y^2 \le \frac{4p}{\pi} \quad \& \quad x \equiv uy \pmod p$$

$$u^2 \equiv -1 \Rightarrow x^2+y^2 \equiv 0 \pmod p$$

$\Rightarrow$ x^2+y^2 is a multiple of p

$$x^2+y^2 \neq 0$$

$$x^2+y^2 = p,\ 2p,\ 3p,\ \dots$$

$$\Rightarrow x^2+y^2 = p.$$