Quadratic Congruence

$$\boxed{ax^2+bx+c \equiv 0 \mod n}$$

Just like linear congruences, quadratic congruences may not have solutions!

Ex: $3x \equiv 1 \mod 9$ $\gcd(3,9)=3 \nmid 1$. !!

no solutions!

$$\boxed{\text{Theorem: } ax \equiv b \mod n \text{ has a solution} \iff \gcd(a,n) \mid b}$$

Ex: $0x^2+3x-1 \equiv 0 \mod 9$

Ex: $\phi(4)=2$ $x^2 = \begin{cases} 1, & 2\nmid x \\ 0, & 2 \mid x \end{cases}$ mod 4

$x^2-2 \equiv 0 \mod 4$ NO SOLUTIONS!

We focus on a special case:

$$\boxed{ax^2+bx+c \equiv 0 \mod p}$$

where p odd prime and $\gcd(a,p)=1$

Since $\gcd(a,p)=1$, a has a multiplicative inverse

multiplicative inverse $a^*a \equiv 1 \mod p$

$$ax^2+bx+c \equiv 0 \mod p$$

$$\Downarrow$$

$$x^2+a^*bx+a^*c \equiv 0 \mod p$$

Since p is odd, $\gcd(2,p)=1$.
So there's a number 2^* with $22^*=1$.

$$x^2+a^*bx+a^*c \equiv 0 \mod p$$

Complete the square!

$$(x+?)^2+? \equiv 0 \mod p$$

$$x^2+\beta x+\gamma \longrightarrow \left(x+\frac{\beta}{2}\right)^2-\frac{\beta^2}{4}+\gamma$$

$$(x+2^*a^*b)^2-(2^*a^*b)^2+a^*c \equiv 0 \mod p$$

$$(x+2^*a^*b)^2-4^*(a^*)^2b^2+a^*c \equiv 0 \mod p$$

$$(x+2^*a^*b)^2-4^*(a^*)^2(b^2-4ac) \equiv 0 \mod p$$

$$\underbrace{(x+2^*a^*b)^2}_{\text{perfect squares}} \equiv \underbrace{4^*(a^*)^2}(b^2-4ac) \mod p$$

perfect squares $\Rightarrow$ must be a perfect square!

Theorem: Let p be odd prime and $\gcd(a,p)=1$.
Then

$$ax^2+bx+c \equiv 0 \mod p$$

has a solution $\Leftrightarrow$ b^2-4ac is equivalent to a perfect square mod p.

When it is, the solutions are easy!

$$(x+2^*a^*b)^2 \equiv 4^*(a^*)^2\underbrace{(b^2-4ac)}_{\equiv k^2} \mod p$$

$$(x+2^*a^*b)^2 \equiv 4^*(a^*)^2 k^2 \mod p$$

$$x+2^*a^*b \equiv \pm(2^*a^*k) \mod p$$

$$x = (-b \pm k)2^*a^*$$ quadratic formula!

$k^2 = b^2-4ac$

Ex: $6x^2+5x+1 \equiv 0 \mod 17$

Does it have solutions?

$5^2-4\cdot 6\cdot 1 = 25-24=1$

Solutions are $(-b\pm k)2^*a^*$

$b=5$, $k^2=1 \rightsquigarrow k=1$, $2^* = \frac{17+1}{2} = \frac{18}{2} = 9$

David's Lemma:

$$2^* = \frac{p+1}{2}$$

Proof: $\left(\frac{p+1}{2}\right)2 = p+1 \equiv 1 \mod p$ ✓ $\square$

$a^* = 6^*$: $6^*\cdot 6 \equiv 1 \mod 17$

$6^* = 3$

$$x = (-5 \pm 1)9\cdot 3 = -4\cdot 9\cdot 3, \; -6\cdot 9\cdot 3$$

$$\qquad\qquad 11 \qquad\qquad 8$$

$9\cdot 3 = 27 \equiv 10 \qquad -4\cdot 9\cdot 3 \equiv -40 + \underline{3\cdot 17} \equiv -40+51 = 11$

<u>Definition</u>: Let p be an odd prime.
A number n is called a <u>quadratic residue modulo p</u> if n is equivalent to a perfect square mod p ($\exists\, k$ w/ $n \equiv k^2 \bmod p$). A number is otherwise called a <u>quadratic nonresidue</u>.

<u>Theorem (Euler's Criterion)</u>: Let p be an odd prime and a be an integer w/ $\gcd(a,p)=1$.
Then a is a quadratic residue if and only if

$$\boxed{a^{(p-1)/2} \equiv 1 \mod p}$$

<u>Proof</u>: S'pose a is a quadratic residue.
Then $a \equiv k^2 \bmod p$ for some integer k

$\gcd(a,p)=1 \Rightarrow \gcd(k,p)=1$

FLT: $k^{p-1} \equiv 1 \mod p$

So

$$a^{\frac{p-1}{2}} \equiv (k^2)^{\frac{p-1}{2}} = k^{p-1} \equiv 1 \mod p.$$

Thus

$$a \text{ quad. res} \Rightarrow a^{\frac{p-1}{2}} \equiv 1 \mod p.$$

Conversely, s'pose $a^{\frac{p-1}{2}} \equiv 1 \mod p$.
Since p prime, $\exists$ primitive root of p, ie. b with order $p-1$.

$\Rightarrow b^0, b^1, b^2, b^3, \ldots, b^{p-1}$ are all incongruent mod p

$\therefore a = b^k$ for some k.

Therefore since $a^{\frac{p-1}{2}} \equiv 1 \mod p$,

$$(b^k)^{\frac{p-1}{2}} \equiv 1 \mod p.$$

$$b^{\frac{k(p-1)}{2}} \equiv 1 \mod p$$

The order of b is p-1

$$\frac{k\cancel{(p-1)}}{2} = j\cancel{(p-1)} \quad \text{for some } j \in \mathbb{Z}.$$

$$\therefore \quad k = 2j \qquad \text{and} \qquad \underline{a} \equiv b^k = b^{2j} = (b^j)^2$$

Thus a is a quadratic residue! $\square$

Fact: $a^{\frac{p-1}{2}} \equiv 1 \iff a$ q.r.

Ex: $x^2 \equiv 1 \mod p$, $x = 1$, $x = -1$

$$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \qquad \therefore a^{\frac{p-1}{2}} \text{ solves } x^2 \equiv 1$$

> Corollary: Let p be an odd prime and $\gcd(a,p)=1$.
> $$a^{\frac{p-1}{2}} \equiv \begin{cases} 1, & a \text{ is a quad. residue} \\ -1, & a \text{ is a quad. nonresidue.} \end{cases}$$