Lecture 1

We talked about linear congruence equations & their solutions.

Ex: 1) $2x \equiv 7 \mod 11$

2) $x \equiv 3 \mod 5$
$x \equiv 5 \mod 7$
$x \equiv 1 \mod 17$

Today: We start with quadratic congruences.

$$x^2 \equiv a \mod p$$

Rmk If $p \mid a$ then $x = 0$ is a trivial solution. So we focus on $p \nmid a$.

Def: Let p be an odd prime and $a \in \mathbb{Z}$ s.t. $p \nmid a$. We call a to be a quadratic residue mod p if $\exists\, z$ s.t. $z^2 \equiv a \mod p$.
Otherwise, we say z is a quadratic non-residue.

Rmk: Clearly, if $a \equiv b \bmod p$ then b is also quadratic (non) residue if a is.

So we may restrict $a \in \{1, \dots, p-1\}$

Example: $p = 5$

x	$x^2 \bmod 5$	
1	1	
2	4	← Symmetry
3	4	
4	1	

So 1, 4 are quadratic residues mod 5
2, 3 — — non — —

Example $p = 7$

x	$x^2 \bmod 7$	
1	1	
2	4	
3	2	← symmetry
4	2	
5	4	
6	1	

So $\{1, 2, 4\}$ are quad-residues and $\{3, 5, 6\}$ are non —.

Rmk: As $a^2 \equiv (-a)^2 \equiv (p-a)^2 \bmod p$

We need to check only up to $\frac{p}{2}$.

Recall from last week

1) z is a primitive root mod p if order of z mod p is $p-1$.

2) $\exists$ a primitive root. Infact $\exists\ \varphi(p-1)$ many primitive roots. This is the main theorem of the afternoon lecture last week.

Proof: a is q/rad. res. mod p $\Uparrow\Downarrow$ $a = z^j$ where z is a primitive root & j is even.

p odd prime

Proof: "$\Uparrow$" Obvious if j = even, say $j = 2i$

then $a = z^{2i} = (z^i)^2$. Thus $x = z^i$ is a sol^n of $x^2 \equiv a \bmod p$.

"$\Downarrow$" First, (like many times before)

Consider $\{1, z, \ldots, z^{p-2}\}$.

All elements are <u>distinct mod p</u>.

So they must form the same set as $\{1, \ldots, p-1\}$ mod p.

Now let $\exists\, x$ s.t. $x^2 \equiv a \bmod p$

As $1 \le a \le p-1$ (our assumption)

$a \equiv z^j \bmod p$ for some

$\|$ $0 \le j \le p-2$

x^2

As $p \nmid x$ so $x \in \{1, \ldots, p-1\}$ mod p.

So $x \equiv z^i \bmod p$ for some $0 \le i \le p-2$

Thus $z^{2i} \equiv z^j \bmod p$

$\Rightarrow$ $z^{2i-j} \equiv 1 \bmod p$ (as $z \in \mathbb{Z}/p\mathbb{Z}^\times$)

$\Rightarrow$ $p-1 \mid 2i-j$

last lecture

$\Rightarrow$ $2 \mid 2i-j \Rightarrow 2 \mid j$. $\square$

As p odd

Example: $p = 7$. Recall 3 is a primitive root mod 7

[$3^6 \equiv 1 \mod 7$ and 6 is the smallest exponent.]

j	$3^j \bmod 7$
0	1
1	3
2	2
3	6
4	4
5	5
6	1

Prob:

$3^0, 3^2, 3^4, 3^6$

$\equiv 4 \quad \equiv 4 \quad \equiv 4 \quad \equiv 4 \pmod 7$

$1 \quad 2 \quad 4 \quad 1$

$\{1, 2, 4\}$ are quadratic residues.

$\{3, 5, 6\}$ are not.

Compare with last example.

Def: **Legendre Symbol**

$\left(\frac{a}{p}\right) = 0$, if $p \mid a$

$= 1$, if $p \nmid a$ and a is a quadratic residue mod p.

$= -1$, if $p \nmid a$ and a is a quadratic non-residue mod p.

Theorem (algebra of Legendre symbol)

1) $a \equiv b \bmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ $\left[\Rightarrow \left(\frac{a}{p}\right)^2 = \left(\frac{a^2}{p}\right) = 1\right]$

3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. $\left[\Rightarrow \begin{matrix} +1, & p \equiv 1 \bmod 4 \\ -1, & p \equiv 3 \bmod 4 \end{matrix}\right]$

4) Gauss' quadratic reciprocity

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

$p \neq q$ primes.

[Proof of 4) Non-examinable]

Example: $\left(\frac{13}{17}\right) = ?$

5) $\left(\frac{13}{17}\right)\left(\frac{17}{13}\right) \underset{4)}{=} (-1)^{\frac{(13-1)(17-1)}{4}} = 1$

$\Rightarrow \left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) \underset{1)}{=} \left(\frac{4}{13}\right) \underset{2)}{=} \left(\frac{2}{13}\right)^2 = 1.$