Tuesday, October 15

Quadratic congruences

We want to count solutions to $aX^2+bX+c\equiv 0 \pmod p$, where p is an odd prime (and $p\nmid a$, so that the congruence really is quadratic).

Completing the square: since $(4a,p)=1$, the congruence is the same as

$$4a^2X^2+4abX+4ac\equiv 0 \pmod p$$

$$(2aX+b)^2-b^2+4ac\equiv 0 \pmod p$$

$$(2aX+b)^2\equiv b^2-4ac \pmod p.$$

Set $\Delta=b^2-4ac$. If we can solve $Y^2\equiv\Delta \pmod p$, then we can simply solve

$$2aX+b\equiv Y \pmod p \iff X\equiv(2a)^{-1}(Y-b) \pmod p.$$

(Yes - quadratic formula)

Takeaway: it suffices to understand $Y^2\equiv\Delta \pmod p$. — related to Euler's criterion, and thus $\Delta^{(p-1)/2}$.

Example: $p=7$, so that $\frac{p-1}{2}=3$.

a	$a^3 \pmod 7$	solutions to $X^2\equiv a \pmod 7$
0	0	0
1	1	1, 6
2	$8\equiv 1$	3, 4
3	$27\equiv -1$	none
4	$-27\equiv 1$	2, 5
5	$-8\equiv -1$	none
6	-1	none

Definition: If $(a,m)=1$, then a is a quadratic residue if $X^2\equiv a \pmod m$ has a solution, and a quadratic nonresidue otherwise.

Example: For $m=7$:

- 1, 2, 4 are quadratic residues
- 3, 5, 6 are quadratic nonresidues
- 0 is neither.

Definition: If p is an odd prime, define the Legendre symbol $\left(\frac{a}{p}\right)$ as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue } (\text{mod } p), \\ -1, & \text{if } a \text{ is a quadratic nonresidue } (\text{mod } p), \\ 0, & \text{if } p \mid a. \end{cases}$$

Remarks:

- If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- The number of solutions of $x^2 \equiv a \pmod{p}$ is always $\left(\frac{a}{p}\right) + 1$.

Theorem: If p is an odd prime, then

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

Corollary: For all $a, b \in \mathbb{Z}$,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Modulo p:

- The product of two quadratic residues is another quadratic residue;
- The product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue;
- The product of two quadratic nonresidues is a quadratic residue.

Analogy:

quadratic residues (mod p) $\longleftrightarrow$ positive real numbers

quadratic nonresidues (mod p) $\longleftrightarrow$ negative real numbers

0 (mod p) $\longleftrightarrow$ $0 \in \mathbb{R}$.