Math 312, Lecture 27

Recently: primitive roots

[Residues $r \ mod \ m \ s.t. \ \sum_{j=0}^{\varphi(m)} j^r \equiv 0 \ (m)]

Used them (e.g., Diffie-Hellman)

Theorem: If there is a primitive root mod m, then congruence $x^k \equiv b \ (m)$ has solutions iff

$b^{(k,\varphi(m))} \equiv 1 \ (m)$

then have $\frac{\varphi(m)}{(k,\varphi(m))}$ solutions.

---

Primitive roots only exist if $m = 2, 4, p^k, 2p^k$ where $p$ is an odd prime

---

Saw proof for $m = p$ is prime.

---

Today: Start last topic of the course, Quadratic Reciprocity

- Define quadratic residues, non-residues, the Legendre symbol
- Examples

- Basic properties

Fix an odd prime $p$.

**Definition:** Let $a \in \mathbb{Z}$ not be a multiple of $p$. Call $a$ a quadratic residue $\pmod{p}$ if there is $x \in \mathbb{Z}$ such that $x^2 = a \pmod{p}$. Otherwise say $a$ is a quadratic non-residue.

Write $\left( \frac{a}{p} \right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \\ 0 & \text{else} \end{cases}$

Call this the Legendre symbol.

By the quadratic formula, can solve

$$ax^2 + bx + c = 0 \pmod{p} \quad (a \neq 0 \pmod{p})$$

iff $b^2 - 4ac$ is a quadratic residue $\pmod{p}$.

Then the number of roots is $1 + \left( \frac{b^2 - 4ac}{p} \right)$

(can also define cubic, quartic, ... residues)
Examples: (1) $\text{Mod 3: } \begin{array}{c} 1^2 \equiv 1, 2^2 \equiv 1 \end{array}$ (3) \\
so $1$ is a quadratic residue mod 3, $2$ is a "non-residue".

(2) $\text{Mod 5: } (\pm 1)^2 \equiv 1, (\pm 2)^2 \equiv 4$ so \\
$\left( \frac{1}{5} \right) = \left( \frac{2}{5} \right) = \left( \frac{3}{5} \right) = 1, \left( \frac{4}{5} \right) = -1$ \\
$-1$ is a square mod 5.

(3) $\text{Mod 7: } (\pm 1)^2 \equiv 1, (\pm 2)^2 \equiv 4, (\pm 3)^2 \equiv 2$ \\
so $\left( \frac{1}{7} \right) = \left( \frac{2}{7} \right) = \left( \frac{3}{7} \right) = 1, \left( \frac{4}{7} \right) = \left( \frac{5}{7} \right) = \left( \frac{6}{7} \right) = -1$ \\
(4) $\text{Mod 11: } (\pm 1)^2 \equiv 1, (\pm 2)^2 \equiv 4, (\pm 3)^2 \equiv 9, (\pm 4)^2 \equiv 5, (\pm 5)^2 \equiv 3$ \\
so $\left( \frac{1}{11} \right) = \left( \frac{2}{11} \right) = \left( \frac{3}{11} \right) = \left( \frac{4}{11} \right) = \left( \frac{5}{11} \right) = \left( \frac{6}{11} \right) = \left( \frac{7}{11} \right) = \left( \frac{8}{11} \right) = \left( \frac{9}{11} \right) = \left( \frac{10}{11} \right) = -1$ \\
we used the representatives $\{-p/2, -p/2, p/2\}$ \\
instead of $\{0, \ldots, p-1\}$.

By the CRT, solving $x^2 \equiv a \pmod{m}$ is the same \\
as solving $x^2 \equiv a \pmod{p^k}$ for each prime divisor $p | m$. 

if \( p \) is odd, this is similar to situation mod \( p \) odd prime (Hensel's Lemma: if \( x^2 \equiv a \pmod{p} \) has a root then \( x^2 \equiv a \) has a root mod \( p^k \) for all \( k \)).

How do we tell if the congruence \( x^2 \equiv a \pmod{p} \) has solutions?

We will discuss different methods so far:

1. Brute force: compute all squares mod \( p \)
2. Euler's criterion (next)
3. Quadratic reciprocity (later)

Proposition: (Euler) \( \left( \frac{a}{p} \right) = a^{\frac{p-1}{2}} \pmod{p} \)

Pf: If \( p \nmid a \), both sides are \( 0 \pmod{p} \). If not, this is the theorem quoted above:

Since if primitive roots mod \( p \), \( x^2 \equiv a \pmod{p} \) has solution iff \( a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \) and \( \phi(p) = p-1 \)
so if $a$ is a quadratic residue,

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

then defn of $\left( \frac{a}{p} \right)$

if $a$ is a non-residue, $(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1 \pmod{p}$

so $a^{\frac{p-1}{2}}$ squares to 1, so its -1 = $\left( \frac{a}{p} \right)$

Eq: $\left( \frac{5}{11} \right) = 5^5 \equiv 3125 \equiv 5-2+1-3 \equiv 1 \pmod{11}$

$\left( \frac{6}{11} \right) = 6^5 \equiv 1296 \cdot 6 \equiv (6-9+2-1)-6 \equiv -2 \cdot 6 \equiv -12 \equiv -1 \pmod{11}$

agrees with brute-force checks above.

Corollary: $\left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}}$

Let $p \equiv \pm 1 \pmod{4}$

$p$ is prime.

division into cases: Let $a$ take values 1, -1

If they are different, their difference is a, which is not divisible by $p$.

So $\left( \frac{-1}{p} \right) = \begin{cases} 1 & \text{if } \frac{p-1}{2} \text{ even} \\ -1 & \text{if } \frac{p-1}{2} \text{ odd} \end{cases}$

$p \equiv 3 \pmod{4}$.
Ex. (check table above) \((\frac{-1}{5}) = 1\) but
\((\frac{-1}{3}) = (\frac{-1}{4}) = (\frac{-1}{11}) = -1\).

(about half the primes fall into each category.)

Remark: PS6 has a different proof of this formula for \((\frac{-1}{p})\)

Lemma. (Basic properties) Let \(a, b, a' \in \mathbb{Z}\),
\(sb \ a = a' \ (p)\) then,
1) \((\frac{a}{p}) = (\frac{a'}{p})\)  
2) \((\frac{b^2}{p}) = 1\) if \(p \nmid b\)
3) \((\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})\).

Proof: (1) \((\frac{a}{p})\) is about \(a \equiv 0 (p)\) or \(x^2 \equiv a (p)\)
\((\frac{a'}{p})\) is about \(a' \equiv 0 (p)\) or \(x^2 \equiv 0' (p)\)
these are same statements

2) If \(p \nmid b\), then \(b\) solves \(x^2 \equiv b^2 (p)\)
and \((\frac{b^2}{p}) = 1\).
(3) \( p \mid ab \iff p \mid a \text{ or } p \mid b \) so either both sides are 0 or neither is. 
\[ \left( \frac{a}{p} \right) = 0 \iff p \nmid a \\ \left( \frac{b}{p} \right) = 0 \iff p \nmid b \\ \left( \frac{ab}{p} \right) = 0 \iff p \mid ab \right] \\
\left[ \text{If } \left( \frac{a}{p} \right) = 1 \text{ or } \left( \frac{b}{p} \right) = 1 \text{ also easy.} \right]