MATH 115, SUMMER 2012
LECTURE 14

JAMES MCIVOR

- We've seen that not all congruences of the form are solvable.
- we've reduced to the case of prime modulus
- we know how to determine whether or not a linear congruence $ax + b \equiv 0 \mod p$ is solvable.
- now we turn to quadratic equations.

1. Quadratic Residues

Definition 1. Let $(a, m) = 1$. Then a is called a **quadratic residue mod** m (QR) if the congruence $x^2 \equiv a \mod m$ has a solution. Otherwise it is a **quadratic nonresidue mod** m (QNR).

The idea behind the terminology is that if there's a solution x, then x^2 is something quadratic, and reducing it mod m gives a "quadratic residue", which is a.

- note there are three cases, really: 1) $(a, m) \neq 1$, or else $(a, m) = 1$, and then 2) a is a QR, or 3) a is a QNR. When m is prime, $(a, m) = 1$ is automatic.

Example 1.1. Q: What are the quadratic residues mod 5?
A: 0,1,2,4

- **Main question**: which integers are quadratic residues mod p, for p prime?

To answer this question, we introduce the following useful tool

Definition 2. Let p be an odd prime. For any integer a, the **Legendre symbol** is the number $\left(\frac{a}{p}\right)$ defined by

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

Thus it is a sort of "detector" of whether or not a is a QR mod p.

Example 1.2. Compute $\left(\frac{2}{3}\right)$, $\left(\frac{3}{5}\right)$, $\left(\frac{12}{3}\right)$, and $\left(\frac{19}{101}\right)$.

- The last one is too hard - we need to develop some properties of the Legendre symbol first, and then we'll know how to compute it.
- key property for computations:

Proposition 1. *If p is an odd prime, then*

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

For the proof, we need a famous result that your book proved in 2.8.

Theorem 1. *(Euler's Criterion)*

If p is an odd prime and $p \not| a$, then the congruence $x^2 \equiv a \mod p$ has two solutions if

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

and no solution if

$$a^{\frac{p-1}{2}} \equiv -1 \mod p.$$

Proof. First of all, note that

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

by FLT, so $a^{\frac{p-1}{2}}$ can only be congruent to $\pm 1 \mod p$.

- a is a unit since $(a, p) = 1$
- if there's a solution at all, it must be a unit, too.
- pick a primitive root g. Then $a = g^i$ for some i.
- Any solution x will then be a power of g, say $x = g^k$.

-Then the congruence we want to solve (think of i as given and k as unknown) is

$$g^{2k} \equiv g^i \mod p,$$

or equivalently

$$g^{2k-i} \equiv 1 \mod p$$

which happens if and only if $2k - i | \phi(p) = p - 1$.

- This is the same as $2k \equiv i \mod p - 1$.
- it's a linear congruence! Solution for k iff $(2, p-1)|i$. But p odd, so $(2, p-1) = 2$
- so solution for k iff $2|i$
- $2|i$ iff $i(p-1)/2 \equiv 0 \mod p - 1$. (maybe explain this)
- $i(p-1)/2 \equiv 0 \mod p - 1$ iff $g^{\frac{1(p-1)}{2}} \equiv 1 \mod p$ (by theorem last time: $g^s \equiv 1 \mod m$ iff $\phi(m)|s$, since g has order $\phi(m)$)
- but $g^{\frac{1(p-1)}{2}} \equiv a^{\frac{p-1}{2}}$
- so soln for k (which means soln for x) iff $a^{\frac{p-1}{2}} \equiv 1 \mod p$.
- note that if there is a sol'n for k, it's unique mod $p - 1/2$, by linear congruence thm. This means two solns k mod $p - 1$, so two solns x mod p.

□

Now we use this to prove the key property of the Legendre symbol:

Proof. - if $p|a$, then $\left(\frac{a}{p}\right) = 0$ and also $a^{\frac{p-1}{2}} \equiv 0 \mod p$.

- Now assume $(a, p) = 1$, so $\left(\frac{a}{p}\right) = \pm 1$.
- $\left(\frac{a}{p}\right) = 1$ iff $x^2 \equiv a \mod p$ has a solution iff $a^{\frac{p-1}{2}} \equiv 1 \mod p$, by Euler's criterion.

□

Other useful properties of Legendre symbol

- p is an odd prime, as usual. Then

(1) $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

(2) (very useful) If $a \equiv b \mod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(3) If $p \not| a$, then $\left(\frac{a^2}{p}\right) = 1$
(4) $\left(\frac{1}{p}\right) = 1$
(5) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$

Proof. Do it for yourself in the problem session! □

- note that the first property means it's only interesting to compute the Legendre symbol when a is prime.
- reason: if $a = p_1 \cdots p_r$, then $\left(\frac{a}{p}\right) = \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_r}{p}\right)$, so it's enough to know what the $\left(\frac{p_i}{p}\right)$ are.

Example 1.3. We use these properties to compute some Legendre symbols.

(1) $\left(\frac{2}{7}\right)$
(2) $\left(\frac{4}{7}\right)$
(3) $\left(\frac{-4}{7}\right)$
(4) $\left(\frac{397}{7}\right)$
(5) $\left(\frac{32}{5}\right)$
(6) $\left(\frac{637}{5}\right)$

Final observation: The list $1^2, 2^2, 3^3, \ldots, (\frac{p-1}{2})^2$ contains all the quadratic residues mod p, while $(\frac{p+1}{2})^2, \ldots, (p-1)^2$ are all the quadratic nonresidues.
- so mod p, there are $\frac{p-1}{2}$ QRs and $\frac{p-1}{2}$ QNRs
- note they're all distinct: if $i^2 \equiv j^2 \mod p$ (where $i \not\equiv j \mod p$), then $p | (i^- j^2) = (i+j)(i-j)$, so ...