Lecture 9
Quadratic Residues, Quadratic Reciprocity

Quadratic Congruence - Consider congruence $ax^2 + bx + c \equiv 0 \mod p$, with $a \neq 0 \mod p$. This can be reduced to $x^2 + ax + b \equiv 0$, if we assume that p is odd (2 is trivial case). We can now complete the square to get

$$\left(x + \frac{a}{2}\right)^2 + b - \frac{a^2}{4} \equiv 0 \mod p$$

So we may as well start with $x^2 \equiv a \mod p$

If $a \equiv 0 \mod p$, then $x \equiv 0$ is the only solution. Otherwise, there are either no solutions, or exactly two solutions (if $b^2 \equiv a \mod p$, then $x = \pm b \mod p$). ($x^2 \equiv a \equiv b^2 \mod p \Rightarrow p | x^2 - b^2 \Rightarrow p | (x - b)(x + b) \Rightarrow x \equiv b$ or $-b \mod p$). We want to know when there are 0 or 2 solutions.

(Definition) Quadratic Residue: Let p be an odd prime, $a \not\equiv 0 \mod p$. We say that a is a **quadratic residue** mod p if a is a square mod p (it is a **quadratic non-residue otherwise**).

Lemma 39. *Let $a \not\equiv 0 \mod p$. Then a is a quadratic residuemod p iff $a^{\frac{p-1}{2}} \equiv 1 \mod p$*

Proof. By FLT, $a^{p-1} \equiv 1 \mod p$ and $p - 1$ is even. This follows from index calculus. Alternatively, let's see it directly

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

Let g be a primitive root mod p. $\{1, g, g^2 \ldots g^{p-2}\} = \{1, 2, \ldots p - 1\} \mod p$. Then $a \equiv g^k \mod p$ for some k. With that $a = g^{k+(p-1)m} \mod p$ so k's only defined mod $p - 1$. In particular, since $p - 1$ is even, so we know k is even or odd doesn't depend on whether we shift by a multiple of $p - 1$. (ie., k is well defined mod 2).

We know that a is quadratic residue mod p iff k is even (if $k = 2l$ then $a \equiv g^{2l} \equiv (g^l)^2 \mod p$). Conversely if $a \equiv b^2 \mod p$ and $b = g^l \mod p$ we get $a \equiv g^{2l} \mod p$, so k is even.

Note: this shows that half of residue class mod p are quadratic residues, and half are quadratic nonresidues. Now look at $a^{\frac{p-1}{2}} \equiv \left(g^k\right)^{\frac{p-1}{2}} \equiv g^{\frac{k(p-1)}{2}} \mod p$. $k \equiv 1 \mod p$ iff $p - 1 = \operatorname{ord}_p g$ divides $\frac{k(p-1)}{2}$ iff $(p-1) | \frac{k(p-1)}{2} \leftrightarrow 2 | k \leftrightarrow a$ is a quadratic residue. ∎

(Definition) Legendre Symbol:

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

Defined for odd prime p, when $(a, p) = 1$. (For convenience and clarity, written $(a|p)$).

We just showed that $(a|p) \equiv a^{\frac{p-1}{2}} \mod p$.
Remark 1. This formula shows us that $(a|p)(b|p) = (ab|p)$.

$$\text{LHS} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \mod p \equiv \text{RHS} \mod p$$

and since both sides are $\pm 1 \mod p$, which is an odd prime, they must be equal
Similarly, $(a^2|p) = (a|p)^2 = 1$

Eg.

$$(-4|79) = (-1 \cdot 2^2|79) = (-1|79)(2|79)^2 = (-1|79) = (-1)^{39} = -1$$

Also, 79 is not $1 \mod 4$ so -1 is quadratic non-residue.

We'll work toward quadratic reciprocity relating $(p|q)$ to $(q|p)$. We'll do Gauss's 3rd proof.

Lemma 40 (Gauss Lemma)**.** *Let p be an odd prime, and $a \not\equiv 0 \mod p$. For any integer x, let x_p be the residue of $x \mod p$ which has the smallest absolute value. (Divide x by p, get some remainder $0 \leq b < p$. If $b > \frac{p}{2}$, let $x_p = b$, if $b > \frac{p}{2}$, let x_p be $b - p$. ie., $-\frac{p}{2} < x_p < \frac{p}{2}$) Let n be the number of integers among $(a)_p, (2a)_p, (3a)_p \ldots ((\frac{p-1}{2})a)_p$ which are negative. Then $(a|p) = (-1)^n$.*

Proof. (Similar to proof of Fermat's little Theorem)

We claim first that if $1 \leq k \neq l \leq \frac{p-1}{2}$ then $(ka)_p \neq \pm(la)_p$. Suppose not true: $(ka)_p = \pm(la)_p$. Then, we'd have

$$ka \equiv \pm la \mod p \Rightarrow (k \mp l)a \equiv 0 \mod p \Rightarrow k \mp l \equiv 0 \mod p$$

This is impossible because $2 \leq k + l \leq p - 1$ and $-\frac{p}{2} < k - l < \frac{p}{2}$ and $k - l \neq 0$ (no multiple of p possible).

So the numbers $|(ka)_p|$ for $k = 1 \ldots \frac{p-1}{2}$ are all distinct mod p (there's $\frac{p-1}{2}$ of them) and so must be the integers $\{1, 3 \dots \frac{p-1}{2}\}$ in some order.

$$
\begin{aligned}
1 \cdot 2 \cdot \dots \cdot \left(\frac{p-1}{2}\right) &\equiv \prod_{k=1}^{\frac{p-1}{2}} |(ka)_p| \mod p \\
&\equiv (-1)^n \prod_{k=1}^{\frac{p-1}{2}} (ka)_p \mod p \\
&\equiv (-1)^n \prod_{k=1}^{\frac{p-1}{2}} ka \mod p \\
&\equiv a^{\frac{p-1}{2}} (-1)^n \left(1 \cdot 2 \cdot \dots \cdot \left(\frac{p-1}{2}\right)\right) \mod p \\
\Rightarrow 1 &\equiv a^{\frac{p-1}{2}} (-1)^n \mod p \\
a^{\frac{p-1}{2}} &\equiv (-1)^n \mod p \\
(a|p) &\equiv (-1)^n \mod p \\
(a|p) &= (-1)^n \text{ since } p > 2
\end{aligned}
$$

where the second step follows from the fact that exactly n of the numbers $(ka)_p$ are < 0. ■

Theorem 41. *If p is an odd prime, and $(a, p) = 1$, then if a is odd, we have $(a|b) = (-1)^t$ where $t = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor$. Also, $(2|p) = (-1)^{(p^2-1)/8}$*

Proof. We'll use the Gauss Lemma. Note that we're only interested in $(-1)^n$. We only care about $n \mod 2$.

We have, for every k between 1 and $\frac{p-1}{2}$

$$
\begin{aligned}
ka &= p \left\lfloor \frac{ka}{p} \right\rfloor + (ka)_p + \begin{cases} 0 & \text{if } (ka)_p > 0 \\ p & \text{if } (ka)_p < 0 \end{cases} \\
&\equiv \left\lfloor \frac{ka}{p} \right\rfloor + |(ka)_p| + \begin{cases} 0 & \text{if } (ka)_p > 0 \\ 1 & \text{if } (ka)_p < 0 \end{cases} \mod 2
\end{aligned}
$$

Sum all of these congruences mod 2

$$\sum_{k=1}^{(p-1)/2} ka \equiv \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{k=1}^{(p-1)/2} |(ka)_p| + n \mod 2$$

$$\begin{aligned}\sum_{k=1}^{(p-1)/2} ka &= a \sum_{k=1}^{(p-1)/2} k \\ &= \frac{1}{2} a \left(\frac{p-1}{2}\right)\left(\frac{p-1}{2} + 1\right) \\ &= \frac{a(p^2-1)}{8}\end{aligned}$$

Now $\sum |(a)_p|$. Since $\{|a|_p, \ldots, |\frac{p-1}{2} a|_p\}$ is just $\{1 \ldots \frac{p-1}{2}\}$,

$$\begin{aligned}\sum_{k=1}^{(p-1)/2} |(ka)_p| &= \sum_{k=1}^{(p-1)/2} k \\ &= \frac{1}{2}\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}\right) \\ &= \frac{p-1}{8}\end{aligned}$$

Plug in to get

$$\begin{aligned}n &\equiv a\left(\frac{p^2-1}{8}\right) - \left(\frac{p^2-1}{8}\right) + \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor \mod 2 \\ &\equiv (a-1)\left(\frac{p^2-1}{8}\right) + \sum_{k=1}^{(p-1)/2} (ka|p) \mod 2\end{aligned}$$

If a is odd, we have $\frac{p^2-1}{8}$ is integer and $a-1$ is even, so product $\equiv 0 \mod 2$, to get

$$\begin{aligned}n &\equiv \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor \mod 2 \\ &\equiv t \mod 2 \\ \text{So } (a|p) &= (-1)^n = (-1)^t\end{aligned}$$

When $a = 2$,

$$n \equiv \frac{p^2-1}{8} + \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2k}{p} \right\rfloor \mod 2$$

So, note that for $k \in \{1 \dots \frac{p-1}{2}\}$

$$2 \leq 2k \leq p-1$$

so

$$0 < \frac{2}{p} \leq \frac{2k}{p} \leq \frac{p-1}{p} < 1$$

so

$$\lfloor \frac{2k}{p} \rfloor = 0$$

so

$$\sum_{k=1}^{(p-1)/2} (2k|p) = 0$$

so

$$n \equiv \frac{p^2-1}{8} \mod 2 \text{ and } (2|p) = (-1)^n = (-1)^{\frac{p^2-1}{8}}$$

So far,

$$(-1|p) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p = 1 \mod 4 \\ -1 & \text{if } p = 3 \mod 4 \end{cases}$$

Check

$$(2|p) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p = 1,7 \mod 8 \\ -1 & \text{if } p = 3,5 \mod 4 \end{cases}$$

■

Theorem 42 (Quadratic Reciprocity Law). *If p, q are distinct odd primes, then*

$$(p|q)(q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1 & \text{if } p \text{ or } q \equiv 1 \mod 4 \\ -1 & \text{otherwise} \end{cases}$$

Proof. Consider the right angled triangle with vertices $(0,0), (\frac{p}{2}, 0), (\frac{p}{2}, \frac{q}{2})$. Note that: no integer points on vertical side, no nonzero integer points on hypotenuse (slope is $\frac{q}{p}$, so if we had integer point (a, b) then $\frac{b}{a} = \frac{q}{p} \Rightarrow pb = qa$, so $p|a, q|b$, and if $(a, b) \neq (0, 0)$, then $a \geq p, b \geq q$). Ignore the ones on horizontal side.

Claim: the number of integer points on interior of triangle is

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor$$

Proof. If we have a point (k, l), then $1 \leq k \leq \frac{p-1}{2}$ and slope $\frac{l}{k} < \frac{q}{p} \Rightarrow l < \frac{qk}{p}$. Number of points on the segment $x = k$ is the number of possible l, which is just $\left\lfloor \frac{qk}{p} \right\rfloor$. □

Add these (take triangle, rotate, add to make rectangle) - adding points in interior of rectangle is

$$\sum_{l=1}^{(p-1)/2} \left\lfloor \frac{pl}{q} \right\rfloor + \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$$

$$\begin{aligned} (q|p) &= (-1)^{t_1} \text{where } t_1 = \sum \left\lfloor \frac{qk}{p} \right\rfloor \\ (p|q) &= (-1)^{t_2} \text{where } t_2 = \sum \left\lfloor \frac{pl}{q} \right\rfloor \\ (p|q)(q|p) &= (-1)^{t_1+t_2} \text{where } t_1 + t_2 = \text{ total number of points} \end{aligned}$$

■

18.781 Theory of Numbers
Spring 2012