Lecture 10
Jacobi Symbol, Computation, Zolotareff's Definition

p prime, a integer $\not\equiv 0 \mod p$, a is quadratic residue if $a \equiv x^2 \mod p$.

Eg. $p = 5$, $x = \pm 1, \pm 2 \Rightarrow x^2 = 1, 4$

Eg. $p = 7$, $x = \pm 1, \pm 2, \pm 3 \Rightarrow x^2 = 1, 4, 2$

Eg. $p = 11$, $x = \pm 1, \pm 2, \pm 3, \pm 4, \pm 5 \Rightarrow x^2 = 1, 4, -2, 5, 3$

Eg. $p = 13$, $x = \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6 \Rightarrow x^2 = 1, 4, -4, 3, -1, -3$

Legendre Symbol

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

Quadratic Reciprocity (p, q are prime)

$$(q|p)(p|q) = \begin{cases} -1 & \text{if } p \text{ and } q \equiv 3 \mod 4 \\ 1 & \text{else} \end{cases}$$

Eg. $(7|11)(11|7) = -1, (11|7) = (4|7)$

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

$$(2|p) = \begin{cases} -1 & \text{if } p \equiv \pm 3 \mod 8 \\ 1 & \text{if } p \equiv \pm 1 \mod 8 \end{cases}$$

If $a \equiv a' \mod p$ then $(a|p) = (a'|p)$, and $(ab|p) = (a|p)(b|p)$.

Primitive element mod p: integer g and $g, g^2, g^3, \ldots g^{p-1}$ all distinct mod p.

Eg. $p = 7, g = 3 \Rightarrow g^k = 3, 2, 6, 4, 5, 1$

In terms of primitive roots, a is quadratic residue if $a = g^k$, k even, non-residue if k odd

$$(ab|p) = (a|p)(b|p) \begin{cases} \text{(odd)} + \text{(odd)} & \text{power of } g \Rightarrow \text{even} \\ \text{(even)} + \text{(odd)} & \text{power of } g \Rightarrow \text{odd} \\ \text{(even)} + \text{(even)} & \text{power of } g \Rightarrow \text{even} \end{cases}$$

Gauss's Lemma - write $a, 2a \dots \frac{p-1}{2}a \equiv$ integers in the interval $[-\frac{p}{2}, \frac{p}{2}]$. Count the number of negatives γ to get $(a|p) = (-1)^\gamma$. To evaluate $(2|p)$, notice that the set $\{2, 2 \cdot 2, 3 \cdot 2 \dots \frac{p-1}{2} \cdot 2\}$ are in interval $[2, p-1]$ and that the number of even numbers from $\frac{p}{2}$ to p is γ

Eg. $(17|31)$ - 17 $\equiv 1 \mod 4$ so $(17|31)(31|17) = 1$, so $(17|31) = (31|17) = (3|17) = -(17|3) = -(1|3) = -1$.

Eg. $(17|31) = (48|31) = (4^2 \cdot 3|31) = (4|31)^2(3|31) = (3|31) = -(31|3) = -(1|3) = -1$.

Jacobi Symbol - generalizes Legendre to any two numbers $P, Q = q_1, q_2, \dots q_k$ product of primes

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{q_1}\right)\left(\frac{P}{q_2}\right)\cdots\left(\frac{P}{q_k}\right)$$

where Legendre is 0 if P, Q not relatively prime. **Warning:** Jacobi being 1 does NOT imply that P is a square mod Q.

Eg. $(-1|77) = (-1|7)(-1|11) = (-1)(-1) = 1$

Properties:

$(P|QQ') = (P|Q)(P|Q')$, and $(PP'|Q) = (P|Q)(P'|Q)$.

Eg. $(127|233)$ - $127, 233$ are prime, $127 \equiv 3 \mod 4$ and $233 \equiv 1 \mod 4$.
$(127|233) = (233|127) = -(21|127) = -(127|21) = -(1|21) = -(1|7)(1|3) = -1$, so 127 non quadratic residue mod 233

(Definition) Permutation: A **permutation** of set $\{0, 1, \dots n\}$ is a bijection mapping S to S.

Permutations can result in cycles - for example, the mapping of $\{0, 1, 2, 3, 4, 5, 6\}$ to $\{0, 3, 2, 4, 6, 5, 1\}$ in cycle notation is $(1\ 3\ 4\ 6)(0)(2)(5)$.

Zolotarev's Definition - Computing $(P|Q)$ using permutations: take the set $\{0, 1, \dots Q-1\}$ and map using multiplication by $P \mod Q$, which is a permutation if P, Q are relatively prime. Write permutation in cycle notation, then count the number of even length cycles e to get $(P|Q) = (-1)^e$.

Eg.

$$Q = 7, \quad P = 4, \text{ and } \{0, 1, 2, 3, 4, 5, 6\}$$
$$\Rightarrow \{0, 4, 1, 5, 2, 6, 3\}$$
$$\Rightarrow (0)(1\ 4\ 2)(3\ 5\ 6)$$
$$e = 0, (4|7) = (-1)^0 = 1$$

Eg.

$$Q = 7, P = 5, \text{ and } \{0, 1, 2, 3, 4, 5, 6\}$$
$$\Rightarrow \{0, 5, 3, 1, 6, 4, 2\}$$
$$\Rightarrow (0)(1\ 5\ 4\ 6\ 2\ 3)$$
$$e = 1, (5|7) = (-1)^1 = -1$$

18.781 Theory of Numbers
Spring 2012