Lecture 17
Feb. 13th, 2015
Chapter 21
Last time, Legendre symbol:

$\left(\frac{a}{q}\right)=1$ if a QR, $x^2\equiv a \bmod p$ has solution.

$\left(\frac{a}{q}\right)=-1$ if a NR, $x^2\equiv a \bmod p$ has no solution.

If $a_1\equiv a_2 \bmod p$, $\left(\frac{a_1}{p}\right)=\left(\frac{a_2}{p}\right)$, $x^2\equiv a_1\equiv a_2 \bmod p$.

$\left(\frac{a_1a_2}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)$

Quadratic Reciprocity (Part I)
p odd prime

$\left(\frac{-1}{p}\right)=1$ when $p\equiv 1 \bmod 4$

$\left(\frac{-1}{p}\right)=-1$ when $p\equiv 3 \bmod 4$

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

$\left(\frac{-1}{p}\right)=1 \iff$ for which prime p is -1 QR?

$\iff$ for which prime p does $x^2\equiv -1 \bmod p$ have a solution?

p	3	5	7	11	13	17	19	23	...
sol'ns to $x^2\equiv -1 \bmod p$	NR	2,3	NR	NR	5,8	4,13	NR	NR	...

Proof: use Fermat's Little Theorem.

We'll prove $\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}} \bmod p \Rightarrow \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$

Why? $a=\left(\frac{-1}{p}\right)=\pm1$, $b=(-1)^{\frac{p-1}{2}}=\pm1$

$p\mid(a-b)$, $p\geq 3$, $|a-b|\leq 2$, so $a-b=0$

By Fermat's Little Thm:

$a^{p-1}\equiv 1 \bmod p$, $p\nmid a$, let $A=a^{\frac{p-1}{2}}$, $A^2=(a^{\frac{p-1}{2}})^2=a^{p-1}\equiv 1 \bmod p$

$A\equiv 1$ or $-1 \bmod p$

What is $A \bmod p$?

p	11	31	47	97	173	409
a	3	7	10	15	33	78
$a^{\frac{p-1}{2}}\equiv A \bmod p$	1	1	-1	-1	1	-1
$\left(\frac{a}{p}\right)$	1	1	-1	-1	1	-1

Guess: $A\equiv 1 \bmod p \iff \left(\frac{a}{p}\right)=1$

Euler's Criterion: p odd prime, $a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right) \bmod p$ for any a NR, set $a=-1$, $(-1)^{\frac{p-1}{2}}\equiv\left(\frac{-1}{p}\right) \bmod p$

Proof:

First a is a QR $\Rightarrow \left(\frac{a}{p}\right)=1$

$a\equiv b^2 \bmod p$

$a^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \bmod p$

Consider $X^{\frac{p-1}{2}} \equiv 1 \bmod p$. We just proved every QR is a solution to this equation.

There are exactly $\frac{p-1}{2}$ QRs.

Polynomial p theorem $\Longrightarrow$ There are at most $\frac{p-1}{2}$ solutions to this equation.

So {solution to $X^{\frac{p-1}{2}} \bmod p$} = {QRs mod p}

Now let a to be a NR $\Longrightarrow \left(\frac{a}{p}\right) = -1$

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

$0 \equiv a^{p-1} - 1 \equiv (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \Longrightarrow a^{\frac{p-1}{2}} \equiv -1 \bmod p.$

■

Application of quadratic reciprocity.

Prime 1 mod 4 Theorem

There are inf. many prime congruent to 1 mod 4.

[In chapter 12, we showed there are inf. many primes congruent to 3 mod 4.]

Proof: Suppose we are given a list of prime $p_1, \cdots, p_r \equiv 1 \bmod 4$.

We want to find a new prime $\equiv 1 \bmod 4$ not in the list.

Set $A = (2p_1 \cdots p_r)^2 + 1 = q_1 q_2 \cdots q_s$, q_i's are primes, none of q_i's are in our list since $p_i \nmid A$ for any i, $q_i \neq q_j$ for any i, j.

Claim: All q_i's $\equiv 1 \bmod 4$.

$A \equiv 1 \bmod 4 \Longrightarrow q_i$'s are odd, $q_i \mid A$.

For each i, $A = 2p_1 \cdots p_r$ is a solution to $x^2 + 1 \equiv 0 \bmod q_i$.

So -1 is a QR mod $q_i \Longrightarrow \left(\frac{-1}{q_i}\right) = 1 \Longrightarrow q_i \equiv 1 \bmod 4$

e.g. $p_1 = 5$

$A = (2p_1)^2 + 1 = 101$

$p_1 = 5,\ p_2 = 101$

$A = (2p_1 p_2 p_3)^2 + 1 = 1020101$ prime

...