Lecture 18
Feb 23rd, 2015

Last time, we proved the Quadratic Reciprocity (Part I):

p odd prime, $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1 & \text{if } p\equiv 1 \bmod 4\\ -1 & \text{if } p\equiv 3 \bmod 4\end{cases}$

Part (II) p odd prime, $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1 & \text{if } p\equiv 1 \text{ or } 7 \bmod 8\\ -1 & \text{if } p\equiv 3 \text{ or } 5 \bmod 8\end{cases}$

now

$\left(\frac{2}{p}\right)=1 \iff$ when does $x^2\equiv 2 \bmod p$ have a solution?

Fermat's Little Thm : $\{a, 2a, \cdots, (p-1)a\}=\{1, 2, \cdots, p-1\} \bmod p$

Gauss's Idea:

Euler's criterion: $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \bmod p$

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

Consider $\{2, 2\cdot 2, 2\cdot 3, \cdots, 2\cdot\frac{p-1}{2}\}=\{1, 2, 3, \cdots, p-1\}$

e.g. $p=13$, we get $\{1,2,3,4,5,6\}$ and $\{2,4,6,8,10,12\}$

$2\cdot 4\cdot 6\cdot 8\cdot 10\cdot 12=2^{\frac{13-1}{2}}\cdot(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6) \bmod 13$

can reduce $\{2,4,6,8,10,12\}$ these numbers mod 13 to get numbers lying between 6 & -6.

So $2\cdot 4\cdot 6\cdot 8\cdot 10\cdot 12\equiv 2\cdot 4\cdot 6\cdot(-5)\cdot(-3)\cdot(-1) \bmod 13\equiv(-1)^3(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6) \bmod 13$

So $2^6\equiv(-1)^3 \bmod 13\equiv -1$

Generalization:

p odd prime, let $A=\frac{p-1}{2}$, consider $1, 2, \cdots, A=\frac{p-1}{2}$ and multiply by 2, which is $2, 4, \cdots, 2A=p-1$

$2\cdot 4\cdot\cdots 2A=2^{\frac{p-1}{2}}\cdot A!$

Reduce $2\cdot 4\cdots 2A$ mod p so that they lie between A and $-A$.

for $2\cdot 4\cdots$ (each term smaller or equal to A, unchanged!)

but $\cdots\cdot(p-5)\cdot(p-3)\cdot(p-1)$ (each term bigger than $A=\frac{p-1}{2}$ need to subtract p)

$p-i-p\equiv -i \bmod p$, i odd, $1\leq i\leq A$

$\equiv(-1)^{\text{number of minus signs}}\cdot A!$

where number of minus signs = number of integers $2, 4, \cdots, p-1$ that are larger than $\frac{p-1}{2}$

So $(-1)^{\frac{p^2-1}{8}}=\left(\frac{2}{p}\right)\equiv 2^{\frac{p-1}{2}}\equiv(-1)^{\text{number of minus signs}} \bmod p$

$=\begin{cases}1 & \text{if } p\equiv 1 \text{ or } 7 \bmod 8\\ -1 & \text{if } p\equiv 3 \text{ or } 5 \bmod 8\end{cases}$

We would have 4 cases here.

Case by case analysis.

We do only $p\equiv 3$ & $p\equiv 7 \bmod 8$ cases

CASE 1: $p\equiv 3 \bmod 8$

$p=8k+3$

$p-1=8k+2$

$\frac{p-1}{2}=4k+1$

$2, 4, 6, \cdots, 4k, 4k+2, \cdots, 8k+2$

For those bigger than A: $4k+2, \cdots, 8k+2$, how many are they? Answer $=2k+1$ there are $2k+1$ many of them greater than A.

$$2^{\frac{p-1}{2}} \equiv (-1)^{2k+1} = -1 \bmod p$$

CASE 2: $p \equiv 7 \bmod 8$

$p = 8k+7$

$p-1 = 8k+6$

$A = \frac{p-1}{2} = 4k+3$

$2, 4, 6, \cdots, 4k+2, 4k+4, \ldots, 8k+2$

For those bigger than A: how many are there? $2k+2$

$$2^{\frac{p-1}{2}} \equiv (-1)^{2k+2} \equiv 1 \bmod p$$

Chapter 22 Quadratic Reciprocity (Part II)

This Thm will be in final, write the 3 parts of this quadratic reciprocity thm precisely.

p, q distinct odd primes, then $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ or we state in this way

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \bmod 4 \text{ or } q \equiv 3 \bmod 4 \end{cases}$$

a problem: $\left(\frac{a}{p}\right) = \left(\frac{b}{q}\right) \bmod p$ if $a \equiv b \bmod p$

$x^2 \equiv a \bmod p$, $a = \pm q_1 \cdots q_r$, q_i prime

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{q_1}{p}\right) \cdots \left(\frac{q_r}{p}\right)$$

We only need to calculate $\left(\frac{q}{p}\right)$, q, p primes

e.g. $\left(\frac{5}{3593}\right) = \left(\frac{3593}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$