Lecture 21
March 2nd, 2015
Some HW problems
#4 $p>3$, $p=2, 3$

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

If $p\equiv 1 \bmod 4$, $\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)=1$ $\quad$ $\underset{\text{QR}}{\overset{1}{\uparrow}}$ $\quad$ $\underset{\text{NR}}{\overset{2}{\uparrow}}$

$p\equiv 1 \bmod 3$
$p\equiv 1 \bmod 12$

#6 infi. many primes $\equiv 1 \bmod 3$
Let $p_1,\cdots,p_r$ be prime $\equiv 1 \bmod 3$
Consider $A=(2p_1\cdots p_r)^2+3\equiv 3 \bmod 4$
$=q_1\cdots q_s\equiv \boxed{3 \bmod 4} \longrightarrow$ one of $q_i\equiv 3 \bmod 4$
$(2p_1\cdots p_r)^2+3\equiv 0 \bmod q_i$ for each i
$x^2+3\equiv 0 \bmod q_i$ has a sol $\longrightarrow \left(\frac{-3}{q_i}\right)=1$
$\searrow \left(\frac{-1}{q_i}\right)\left(\frac{3}{q_i}\right)=1=(-1)(-1)\left(\frac{q_i}{3}\right)$ $\quad\cdots$

Jacobi symbol $\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)$, $n=p_1\cdots p_r$

Theorem: m,n odd integer. $\gcd(m,n)=1$
(1). $\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$
(2) $\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$
(3) $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{(m-1)(n-1)}{4}}$

$m=q_1\cdots q_s$, $n=p_1\cdots p_t$
(1). $\left(\frac{-1}{n}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_t}\right)=(-1)^{\frac{p_1-1}{2}}\cdots(-1)^{\frac{p_t-1}{2}}=(-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_t-1}{2}}$

Claim: $\frac{n-1}{2}\equiv\frac{p_1-1}{2}+\cdots+\frac{p_t-1}{2} \bmod 2$
First we prove for $t=2$, i.e. $\frac{ab-1}{2}\equiv\frac{a-1}{2}+\frac{b-1}{2} \bmod 2$, a,b odd
Case 1: $a\equiv 1, b\equiv 1 \bmod 4$, $\frac{ab-1}{2}, \frac{a-1}{2}, \frac{b-1}{2}$ all even.
Case 2: $a\equiv 3, b\equiv 3 \bmod 4$, $\frac{a-1}{2}, \frac{b-1}{2}$ odd $\rightsquigarrow \frac{a-1}{2}+\frac{b-1}{2}$ even
$ab\equiv 1 \bmod 4$
Case 3: $a\equiv 1 \bmod 4$ $\quad$ $\frac{a-1}{2}+\frac{b-1}{2}$ odd
$b\equiv 3 \bmod 4$ $\quad$ $\frac{ab-1}{2}$ odd
Use induction on t

(2) $\left(\frac{2}{n}\right)=\left(\frac{2}{p_1}\right)\cdots\left(\frac{2}{p_t}\right)=(-1)^{\frac{p_1^2-1}{8}}\cdots(-1)^{\frac{p_t^2-1}{8}}=(-1)^{\frac{p_1^2-1}{8}+\cdots+\frac{p_t^2-1}{8}}$

Claim: $\frac{n^2-1}{8}\equiv\frac{p_1^2-1}{8}+\cdots+\frac{p_t^2-1}{8} \bmod 2$
We prove it for $t=2$: $\frac{a^2b^2-1}{8}\equiv\frac{a^2-1}{8}+\frac{b^2-1}{8} \bmod 2$, a,b odd

$\pm 1, \pm 5 \bmod 8$

Case 1: $a \equiv \pm 1, b \equiv \pm 1 \mod 8$

$\frac{a^2-1}{8}, \frac{b^2-1}{8}, \frac{(ab)^2-1}{8}$ all even

Case 2: $a \equiv \pm 5, b \equiv \pm 5 \mod 8$

$\frac{a^2-1}{8}, \frac{b^2-1}{8}$ odd $\longrightarrow \frac{a^2-1}{8} + \frac{b^2-1}{8}$ even

$\frac{(ab)^2-1}{8}$ even

Case 3: $a \not\equiv \pm b \mod 8 \longrightarrow \frac{a^2-1}{8} + \frac{b^2-1}{8}$ odd

$\frac{(ab)^2-1}{8}$ odd

(3). $$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right) \cdots \left(\frac{m}{p_t}\right)$$
$$= \left(\frac{q_1}{p_1}\right) \cdots \left(\frac{q_s}{p_1}\right) \cdots \left(\frac{q_1}{p_t}\right) \cdots \left(\frac{q_s}{p_t}\right)$$
$$= \prod_{i=1}^{t} \prod_{j=1}^{s} \left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{t} \prod_{j=1}^{s} \left(\frac{p_i}{q_j}\right) (-1)^{\frac{(p_i-1)(q_j-1)}{4}} = \prod_{i=1}^{t} \left(\frac{p_i}{m}\right) \cdot (-1)^{\frac{p_i-1}{4}\left(\sum_{j=1}^{s}(q_j-1)\right)}$$

$$= \left(\frac{n}{m}\right)(-1)^{\frac{1}{4}\left[\sum_{i=1}^{t}(p_i-1)\right]\left[\sum_{j=1}^{s}(q_j-1)\right]}$$

$$\prod_{j=1}^{s} \left(\frac{p_i}{q_j}\right)(-1)^{\frac{(p_i-1)(q_j-1)}{4}} = \left(\frac{p_i}{m}\right)(-1)^{\left(\frac{p_i-1}{4}\right)(q_1-1+\cdots+q_s-1)}$$

Claim: $\frac{1}{4}\left(\sum_{i=1}^{t}(p_i-1)\right)\left(\sum_{j=1}^{s}(q_j-1)\right) \equiv \frac{1}{4}(m-1)(n-1) \mod 2$

$$\left\| \right. \quad \left(\sum_{i=1}^{t} \frac{p_i-1}{2}\right)\left(\sum_{j=1}^{s} \frac{q_j-1}{2}\right)$$

From (1):

$$\equiv \frac{n-1}{2} \cdot \frac{m-1}{2} \mod 2$$

e.g. Determine whether $x^2-3x-1 \equiv 0 \mod \underbrace{31957}_{\text{prime}}$ has a sol.

$x = \frac{3 \pm \sqrt{9+4}}{2}$

$4x^2 - 12x - 4 \equiv 0$

$\Downarrow$

$(2x-3)^2 \equiv 13 \mod 31957 \implies \left(\frac{13}{31957}\right) = \left(\frac{31957}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$ so there is a sol.

$y^2 \equiv 13$

$2x-3 \equiv y \mod 31957$

Find a prime p s.t. $x^2-3x-1 \equiv 0 \mod p$ has a solution.

$p > 13$. $\left(\frac{13}{p}\right) = 1$

$\rightarrow p \equiv \cdots \mod 13$

$x^2+1 \equiv 0 \mod p$. Solvability criterion is given by <u>congruence</u>.

$p > 2$, solvable iff $p \equiv 1 \mod 4$

But in higher degree equation, finding criterion for solvability is one of the most important open problems.

e.g. $f(x) = 4x^3 - 4x^2 + 1 \equiv 0 \mod p$.

Find prime p st. $f(x) \equiv 0 \mod p$ has 3 sols. (if raise to 5th degree, don't know a pattern!)

$\Leftrightarrow \left(\frac{-11}{p}\right) = 1$ and $p = x^2 + 11y^2$

$\Leftrightarrow c(p) = 2$, $p \neq 2, 11$

where $\underbrace{\eta(2\tau)\,\eta(22\tau)}_{\text{modular form of weight one}} = q \prod_{n=1}^{\infty} (1-q^{2n})(1-q^{22n}) = \sum_{n=1}^{\infty} c(n)\, q^n$

Next lecture: sum of 2 squares.