Lecture 19
Feb. 25th, 2015

problem 4 in assignment 4: n is a perfect product, if n = product of its divisors other than itself.

$$6=1\cdot 2\cdot 3$$

classify perfect product.

Suppose n has at least two distinct factors $p\neq q$, n is perfect product.

$\frac{n}{p}, \frac{n}{q}$ are divisors of n.

$n=$ product of divisor $\geq \frac{n}{p}\cdot\frac{n}{q}=\frac{n^2}{pq}$

$pq\geq n\geq pq$, so $n=pq$

Sps n has only one prime factor p.

$n=p^k$, $p^k=n=1\cdot p\cdot p^2\cdots p^{k-1}=p^{1+2+\cdots+k-1}=p^{\frac{k(k-1)}{2}}$

$k=\frac{k(k-1)}{2}\Rightarrow k=3$

Law of quadratic reciprocity: p, q are odd primes $p\neq q$. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=-1^{\frac{(p-1)(q-1)}{4}}$

Gauss's original proof:

Gauss's Lemma: p is an odd prime, $p\nmid a$

list $a, 2a, \cdots, \left(\frac{p-1}{2}\right)a$ mod p.

So that they are all reduced between $-\left(\frac{p-1}{2}\right)$ and $\frac{p-1}{2}$

let n denote the number of negative integers in that list, then $\left(\frac{a}{p}\right)=(-1)^n$.

$a=2, p=13$.

$\frac{p-1}{2}=6$

$2=2, 2\times2=4, 2\times3=6, 2\times4=8\equiv-5, 2\times5=10\equiv-3$

$2\times6=12\equiv-1\Rightarrow n=3$, $\left(\frac{2}{13}\right)=(-1)^{\frac{13^2-1}{8}}=-1$

e.g. $\left(\frac{3}{17}\right)$, $\frac{p-1}{2}=8$

$3=3, 3\times2=6, 3\times3\equiv-8, 3\times4\equiv-5, 3\times5\equiv-2, 3\times6\equiv1, 3\times7\equiv4, 3\times8\equiv7$

$n=3, \Rightarrow \left(\frac{3}{17}\right)=(-1)^3=-1$

$\left(\frac{3}{17}\right)=\left(\frac{17}{3}\right)$

$17\equiv2 \bmod 3$: $\left(\frac{2}{3}\right)=-1$

Proof of Gauss' Lemma

$a\cdot2a\cdot\cdots\frac{p-1}{2}a=a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!$

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

need to prove, $a^{\frac{p-1}{2}}\equiv(-1)^n$

Claim: if $1\leq s<t\leq\frac{p-1}{2}$, $sa\not\equiv ta \bmod p$, $sa\not\equiv -ta \bmod p$

If $sa\equiv ta \bmod p$, $p\mid(ta-sa)$, $ta-sa=(t-s)a$

$\Rightarrow$ impossible, since $0<t-s\leq\frac{p-1}{2}$,

let $r_s\equiv sa \bmod p$, $-\frac{p-1}{2}\leq r_s\leq\frac{p-1}{2}$,

then $r_s\not\equiv r_t \bmod p$, $r_s\not\equiv -r_t \bmod p$

also $r_s\not\equiv 0 \bmod p$

so, $|r_1|, |r_2|, \cdots, |r_{\frac{p-1}{2}}|$ are all distinct and permutation of $(1,2,\cdots,\frac{p-1}{2})$

$r_1 r_2 \cdots r_{\frac{p-1}{2}} \equiv (-1)^n \cdot 1\cdot 2 \cdots \frac{p-1}{2} \mod p = a^{\frac{p-1}{2}}\, 1\cdot 2\cdots \frac{p-1}{2}$.

Hence, $a^{\frac{p-1}{2}} \equiv (-1)^n \mod p$

Lemma: p odd prime, a odd, $p \nmid a$.
then $\left(\frac{a}{p}\right) = (-1)^t$, $t = \left[\frac{a}{p}\right] + \left[\frac{2a}{p}\right] + \cdots + \left[\frac{\frac{p-1}{2}\cdot a}{p}\right]$

where $[x]$ is the greatest integer $\leq x$, e.g. $[1.3]=1$

e.g. $a=3, p=17, \frac{17-1}{2}=8, t=\left[\frac{3}{17}\right]+\left[\frac{6}{17}\right]+\cdots+\left[\frac{24}{17}\right]=\left[\frac{18}{17}\right]+\left[\frac{21}{17}\right]+\left[\frac{24}{17}\right]=3$

$\Rightarrow (-1)^n = (-1)^t$, t & n have the same parity

$t \equiv n \mod 2$

Proof: reduce ta mod p, $t=1,2,\cdots,\frac{p-1}{2}$.
So that they are all between $-\frac{p-1}{2}$ & $\frac{p-1}{2}$.
Let $r_1,\cdots,r_n$ be negative ints in the list
$s_1,\cdots,s_m$ ... positive
i.e. $m+n=\frac{p-1}{2}$ and $\left(\frac{a}{p}\right)=(-1)^n=(-1)^t$

Claim: $t \equiv n \mod 2$

Euclid Algorith: $a=bq+r$, $0\leq r\leq b$, $q=\left[\frac{a}{b}\right]$

If $ka \equiv s_k \mod p$, $ta \equiv p\left[\frac{ka}{p}\right]+s_k$

If $ka \equiv r_k \mod p$, $ta \equiv p\left[\frac{ka}{p}\right]+p+r_k$ because $r_t<0$.

$5\times 3 = 15 = 17\left[\frac{15}{17}\right]+(17-2)$, $r_t=-2$.

Add together; $a+2a+\cdots+\frac{p-1}{2}a = \sum_{k=1}^{\frac{p-1}{2}} p\left[\frac{ka}{p}\right] + \sum_{i=1}^{n}(p+r_i) + \sum_{j=1}^{m} s_j$

$1+2+\cdots+\frac{p-1}{2} = \sum_{i=1}^{n}(-r_i) + \sum_{j=1}^{m} s_j$

subtract: $(a-1)\left[1+2+\cdots+\frac{p-1}{2}\right] = p\cdot t + \sum_{k=1}^{m}(p+2r_k) = p(t+n) + 2\sum_{k=1}^{n} r_k$

$p(t+n)$ is even, so $t+n$ is even $\Rightarrow t, n$ have the same parity $t \equiv n \mod 2$