Lecture 27
March 16th, 2015

Review

From A4. $\sigma(mn)=\sigma(m)\sigma(n)$ if $\gcd(m,n)=1$

$\sigma(n)=\sum_{i=1}^{r} d_i$, $d_1,\cdots,d_r$ divisors of m

$\sigma(m)=\cdots$ $e_1,\cdots,e_s$ divisors of n

Claim: d_ie_j : $i=1,\cdots,r$, $j=1,\cdots,s$ are divisors of mn

$$\sigma(mn)=\sum_{i=1}^{r}\sum_{j=1}^{s} d_ie_j=\left(\sum_{i=1}^{r} d_i\right)\left(\sum_{j=1}^{s} e_j\right)=\sigma(m)\sigma(n)$$

$d_ie_j \mid mn$

Suppose $d \mid mn$, let $d_i=\gcd(d,m)$, $d_i \mid d$

$e_j=\gcd(d,n)$, $e_j \mid d$

so $d_ie_j \mid d$, then we need $d \mid d_ie_j$ (by Euclid Algorithm)

Then $d=d_ie_j$

A5 #5

$\left(\frac{5}{p}\right)=-1$ if $p\equiv 2 \mod 5$

By QRL $\Rightarrow \left(\frac{p}{5}\right)=\left(\frac{2}{5}\right)=-1$

by QRL (part II)

Without QRL: do $1,2,\cdots,\frac{p-1}{2}$

times 5 $\quad 5,10,15,\cdots,\frac{5(p-1)}{2}$

reduce them between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$

then count the number of negatives (which should be odd)

then $\left(\frac{5}{p}\right)=-1^{\#\text{ of negatives}}$.

$p=5k+2$, p odd $\Rightarrow k$ odd, $k=2l+1$

$\frac{p-1}{2}=5l+3$ $\quad$ so between $-(5l+3), 5l+3$

$5\frac{p-1}{2}=5(5l+3)$

$5,10,\cdots,5l$

$5(l+1), 5(l+2),\cdots,5(2l+1)$ subtract $p=10l+7\cdots\cdots -5l-2\rightarrow -2\cdots l$ numbers

$5(2l+2)\cdots \quad ,5(3l+2)$ subtract p, $3\longrightarrow 5l+3$ .. positive number not our concerns

$5(3l+3)\cdots \quad ,5(4l+2)$ subtract $-2p\cdots -5l+1\longrightarrow -4\cdots\cdots l$ numbers

$5(4l+3)\cdots \quad ,5(5l+3)=5\frac{p-1}{2}$

subtract $-2p\cdots 1\longrightarrow 5l+1\cdots$ positive not concerns

So by Euler's Criterion: $\left(\frac{5}{p}\right)\equiv 5^{\frac{p-1}{2}}\equiv(-1)^{2l+1}=-1$

A5 #6.

Show there are inf. many primes $\equiv 1 \bmod 3$

Suppose $p_1, \cdots, p_r$ distinct primes $\equiv 1 \bmod 3$

Consider $A = (2p_1 \cdots p_r)^2 + 3$

$= q_1 \cdots q_s$

Since A is odd, q_j odd prime.

Claim: (1) $q_i \neq p_j$ for each i, j

(2) $q_i \equiv 1 \bmod 3$

(1) is clear b/c q_i's $\mid A$ but $p_j \nmid A$

(2) $A \equiv 0 \bmod q_i$

It means $x^2 \equiv -3 \bmod q_i$

$x^2 + 3 \equiv 0 \bmod q_i$ has a solution

So $\left(\frac{-3}{q_i}\right) = 1$

$$\left(\frac{-1}{q_i}\right)\left(\frac{3}{q_i}\right) = \cancel{(-1)^{\frac{q_i-1}{2}}} \left(\frac{q_i}{3}\right) \cancel{(-1)^{\frac{q_i-1}{2}}}$$

So $\left(\frac{q_i}{3}\right) = 1 \Rightarrow q_i \equiv 1 \bmod 3$