Feb 4th

Lemma: If $\gcd(m,n)=1$
$\varphi(nm)=\varphi(n)\varphi(m)$

compute $\varphi(nm)$

$\gcd(k,nm)=1$
$\Rightarrow \gcd(k,n)=1$
$\gcd(k,m)=1$

$\gcd(qm+r,m)$
$=\gcd(r,m)$

$\{1,2,3,\dots,m$
$m+1, m+2, m+3 \cdots 2m$
$\vdots$
$(n-1)m+1 \cdots \quad nm\}$

$\varphi(m) \to$ "columns"

$\varphi(nm)=\varphi(n)\varphi(m)$

The r'th column contains as many solu $(k,n)=1$ as $\{0,1,2,\cdots,n-1\}$

For Q4.

Q: Compute $\varphi(p^2)$
$\gcd(k,p^2)=1, p, \cancel{p^2}$

$\varphi(p^2)=\#\{k: \gcd(k,p^2)=1 \quad k=1,2,3,\cdots,2p,\cdots,3p,\cdots,\cancel{p^2}\}=p^2-\#\{k:\gcd(k,p^2)=p\}$
$=p^2-p$

$\gcd(k,p^2)=p \Rightarrow p|k$
and $p|k$ and $k\le p^2 \Rightarrow \gcd(k,p^2)=p$

Euclidean Algorithm

given m and n compute $\gcd(m,n)$

$n=k_0m+r_0$, $r_0<m$
$m=k_1r_0+r_1$, $r_1<r_0$
$r_0=kr_1+r_2$, $r_2<r_1$
$\cdots$

$\gcd(qm+r,m)=\gcd(r,m)$

$\gcd(m,n)=\gcd(\underbrace{[m] \bmod n}_{m'},n)=\gcd(m',n)=\gcd(\underbrace{[n] \bmod m'}_{n'},m')=\gcd(n',m')$

$\gcd(13,8)=\gcd(1\times 8+5,8)$
$=\gcd(5,8)$
$=\gcd(5,3)$
$=\gcd(3,2)$
$=\gcd(2,1)$
$=1$

Eduard Lamé (1887?)

If a,b are the least a,b s.t computing $\gcd(a,b)$ takes N steps to compute $\sim \log_2 \min\{a,b\}$

Bezout's Identity (?)

For any x and y there exist a and b s.t. $ax+by=\gcd(x,y)$

find a and b s.t. $a8+b13=1$

$13=1\times 8+5$
$8=1\times 5+3$
$5=1\times 3+2$
$3=1\times 2+1$
$2=1\times 1+1$

$1=3-2$
$=(8-5)-(5-3)$
$=(8-(13-8))-((13-8)-(8-(13-8)))$
$=8-13+8-13+8+8-13+8$
$=8\times 5-13\times 3$

Thm (Chinese Remainder Theorem)

If $\gcd(m,n)=1$ then there is an $x \equiv a \bmod m$
$\equiv b \bmod n$ for any a and b

Bezout $\Rightarrow$ There are α, β s.t.
$\alpha m + \beta n = 1$
$\Rightarrow \alpha n \equiv 1 \bmod n$
$\Rightarrow \beta n \equiv 1 \bmod n$

Take $x = a\alpha m + b\beta n$
$\equiv a\alpha m \bmod n \equiv b \bmod n$
$\equiv a \cdot 1 \bmod n$
$\equiv a$

Find x st $x \equiv 1 \bmod 13$
$\equiv 2 \bmod 7$

$2\times 7 - 13\times 1 \equiv 1$

...

Q: Claim: If p is an odd prime

$a^{2p-1} \equiv a \bmod 2p$ for all a

If $\gcd(a,b)=1$
$a|n, b|n \Rightarrow ab|n$

Want $a^{2p-1}-a$ is divisible by $2p$
Check: $2 | a^{2p-1}-a$
Check: $p | a^{2p-1}-a$

$a^{2p-1}-a = a(a^{2p-2}-1)$
$= a((a^{p-1})^2-1)$
If $\gcd(a,p)=1$ then by Fermat
$a^{p-1} \equiv 1 \bmod p$
If $\gcd(a,p)=p$ then $a \equiv 0 \bmod p$.

For HW2:
For any m and n there is $r<m$ $r \equiv n \bmod n$
For $n=0$ we have $r=0$, $r \equiv n \bmod m$
Sps have $n \equiv r \bmod m$
$\Rightarrow \boxed{n+1} \equiv r+1 \bmod m$
Let $r' = r+1$ then $n+1 = n'$

Case $r+1 < m$
Let $r' = r+1$
then $n+1 \equiv r' \bmod m$
Case $r+1 = m$
let $r'=0$ and then
$n+1 \equiv 0 \bmod m$
$\Rightarrow n+1 = r' \bmod m$

n	$n \bmod 3$
0	0
1	1
2	2
3	~~3~~ 0
4	1
5	2
6	0
7	