CIS 3362 10/19/22

last time → Fermat's Thm

1) Euler Phi Function $\phi(n)$

2) Euler's Thm (generalization of Fermat's)

$\phi(n)$ = the # of values in the set $\{1, 2, 3, \ldots n-1\}$ that are relatively prime with n.

$\phi(6) = 2$ $\quad gcd(1,6) = gcd(5,6) = 1$, but $gcd(2,6) \neq 1$
$gcd(3,6) \neq 1$
$gcd(4,6) \neq 1$

$\phi(7) = 6$

$\phi(p) = p-1$, $p \in$ Prime

Goal can we derive a formula for $\phi(n)$ given n's prime factorization?

What about $\phi(p^k)$ where $p \in$ Prime $k \in \mathbb{Z}^+$

$\boxed{1, 2, 3, \ldots \cancel{p}} \boxed{\ldots \cancel{2p}} \boxed{\ldots \cancel{3p}} \ldots \boxed{, p^2-1, \cancel{p^2}}$

p^2 total values − p values share common factor w/p

$\phi(p^2) = p^2 - p$, Out of p^k values p^{k-1} are divisible by p

thus $\phi(p^k) = p^k - p^{k-1}$

Prove a critical fact:

if $gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

This means phi is a multiplicative function.

→ all we have to do is multiply each term of form $\phi(p^k)$ to get ϕ(any int)

Let's prove if $\gcd(m,n)=1$, $\phi(mn)=\phi(m)\phi(n)$

1. Cross off values that share common factor w/ n.

1	$\cancel{2}$	3	$\cancel{4}$	$\dots$	$\times$	$\cancel{n}$
$n+1$	$\cancel{n+2}$	$n+3$	$\cancel{n+4}$	$\dots$		$\cancel{2n}$
$2n+1$	$\cancel{2n+2}$	$\dots$	$\times$			$\cancel{3n}$
$\vdots$			$\times$			$\times$
	$\times$		$\times$			
$(m-1)n+1$	$\cancel{(m-1)n+2}$	$\dots$	$\times$			$\cancel{mn}$

Nature of GCD is if $\gcd(i,n)>1$ then
$\gcd(i+n,n)>1$ and
$\gcd(i+nj,n)>1$, $1\le i\le n-1$, ~~$j\in\mathbb{Z}$~~ $0\le j\le m-1$

$\boxed{\text{By definition } \phi(n) \text{ columns survive!}}$

Next goal: Prove that in each column, exactly $\phi(m)$ values "survive", they are relatively prime with m.

Column i has the m values described in this set

$$U=\{i+nj \mid j\in\mathbb{Z} \wedge 0\le j\le m-1\}$$

Prove that each item in U is distinct mod m.

We use proof by contradiction to prove this
assume to the contrary that $\exists\, j_1, j_2 \in \mathbb{Z} \wedge$
$j_1 \neq j_2 \wedge 0 \leq j_1, j_2 \leq m-1$

Such that

$$i + nj_1 \equiv i + nj_2 \pmod{m}$$
$$nj_1 \equiv nj_2 \pmod{m}$$
$$nj_1 - nj_2 \equiv 0 \pmod{m}$$
$$n(j_1 - j_2) \equiv 0 \pmod{m}$$
$$\Longrightarrow m \mid (n * (j_1 - j_2))$$

$\boxed{\text{Rule if } \gcd(a,b)=1 \text{ and } a \mid bc\text{, then } a \mid c.}$

Since $\gcd(m,n)=1$, it follow that $m \mid (j_1 - j_2)$
$1 \leq |j_1 - j_2| \leq m-1$ so the divisibility assertion is contradicted by our known info about the difference btw j_1 and j_2.

$\Longrightarrow$ each column has exactly $\phi(m)$ values relatively prime with m.

Total # of surviving values $= \underbrace{\phi(n)}_{\#\text{ columns}} \times \underbrace{\phi(m)}_{\text{values in each col}}$

$m = 7, n = 6$

0	1	~~2~~	~~3~~	~~4~~	5	~~6~~
6	~~7~~	~~8~~	~~9~~	~~10~~	11	~~12~~
12	13	~~14~~	~~15~~	~~16~~	17	~~18~~
18	19	~~20~~	~~21~~	~~22~~	23	~~24~~
24	25	~~26~~	~~27~~	~~28~~	29	~~30~~
30	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~
36	37	~~38~~	~~39~~	~~40~~	41	~~42~~

1. Cross off all share common factor w/6

2. In each column cross off values that share common factor w/7

$\phi(7) = 6$
so 6 elements

$\phi(6) = 2$ column