CIS 3362 - 10/13/23

established Euler's Thm $\gcd(a,n)=1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$

Goal: Determine Formula for $\phi(n)$.

$\phi(p) = p-1$ for prime number p.

$\phi(3^3)$?

1 2 ~~3~~
4 5 ~~6~~
7 8 ~~9~~
. . . . X
25 26 ~~27~~

equiv question: how many int 1 to 27 are not divisible by 3?

$3^3 - 3^2$

$\phi(p^k)$

1 .. 2 ~~p~~
$p+1$ $p+2$ .. ~~2p~~
X
X
~~p^k~~
$p^k - p+1$

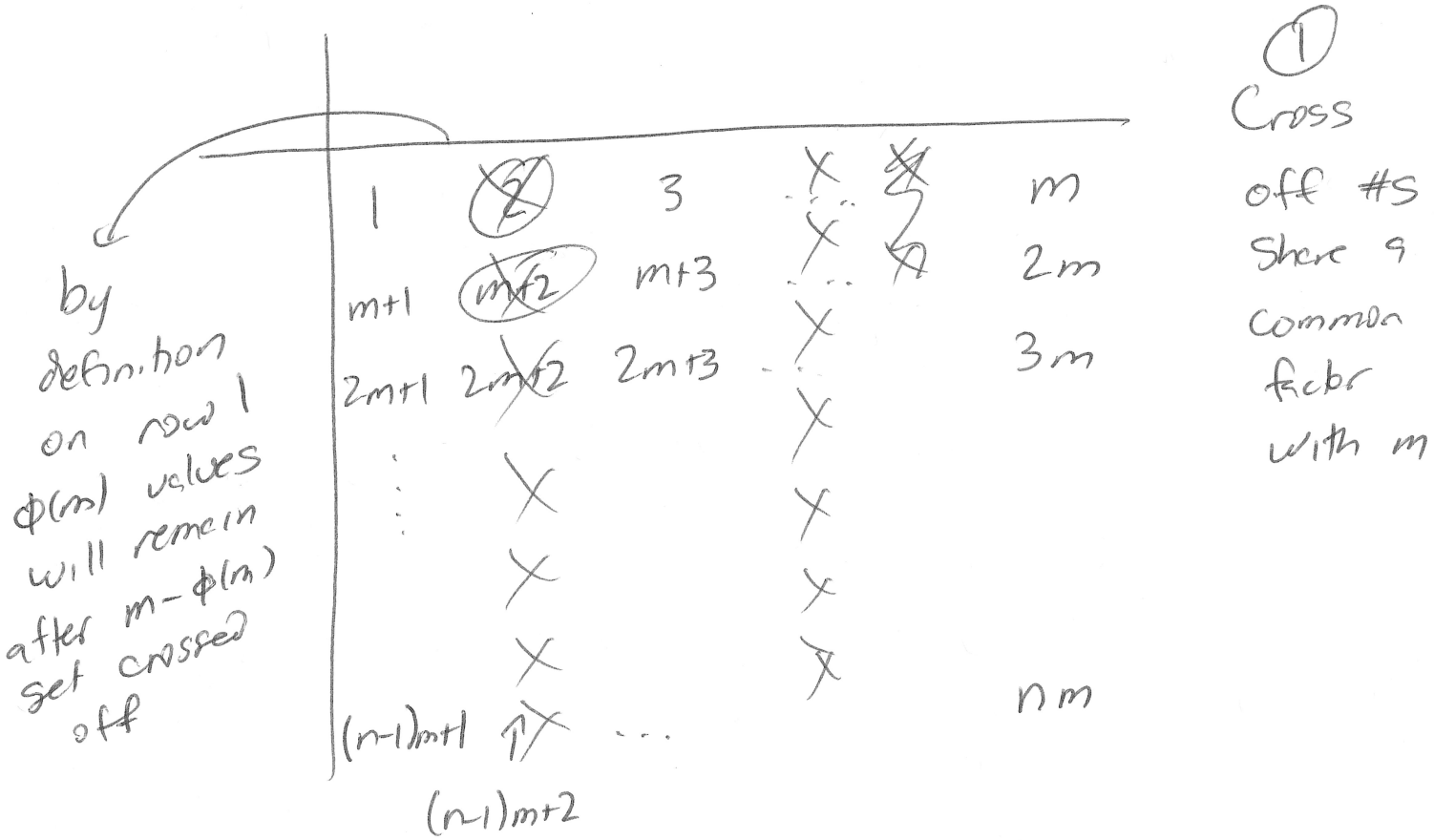
$p^k - p^{k-1}$

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

$\phi(n)$ turns out to be a multiplicative function

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

Use grid technique to calculate $\phi(mn)$



if $\gcd(a,m) > 1$, then $\gcd(a+mk, m) > 1$

Imagine running $\gcd(mk+a, m)$

$mk+a = \underline{m}(k) + \underline{a}$

$\gcd(mk+a, m) = \gcd(m, a)$

by 1st step gcd alg.

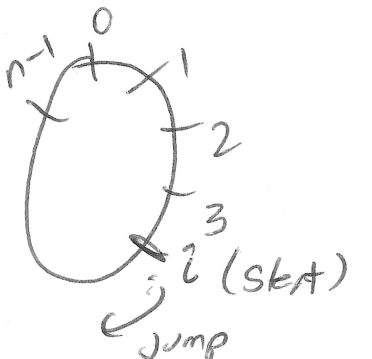
After step one we have $\phi(m)$ rows remaining each with n values. A single row looks like:

$$i,\ m+i,\ 2m+i,\ \ldots\ (n-1)m+i$$

$\gcd(i,m)=1$

Now let's cross off every item that shares a common factor with n!

→ Argue that these n values are ALL distinct mod n.



Proof by contradiction. Assume the opposite that 2 different values on the list are equivalent mod n.

$$xm+i \equiv ym+i \pmod n \qquad \boxed{0 \le y < x \le n-1}$$

$$xm-ym \equiv 0 \pmod n$$

$$m(x-y) \equiv 0 \pmod n$$

if $\gcd(m,n)=1$ and $n \mid mC$, then $n \mid C$.

$$n \mid m(x-y) \text{ but } \gcd(n,m)=1.$$

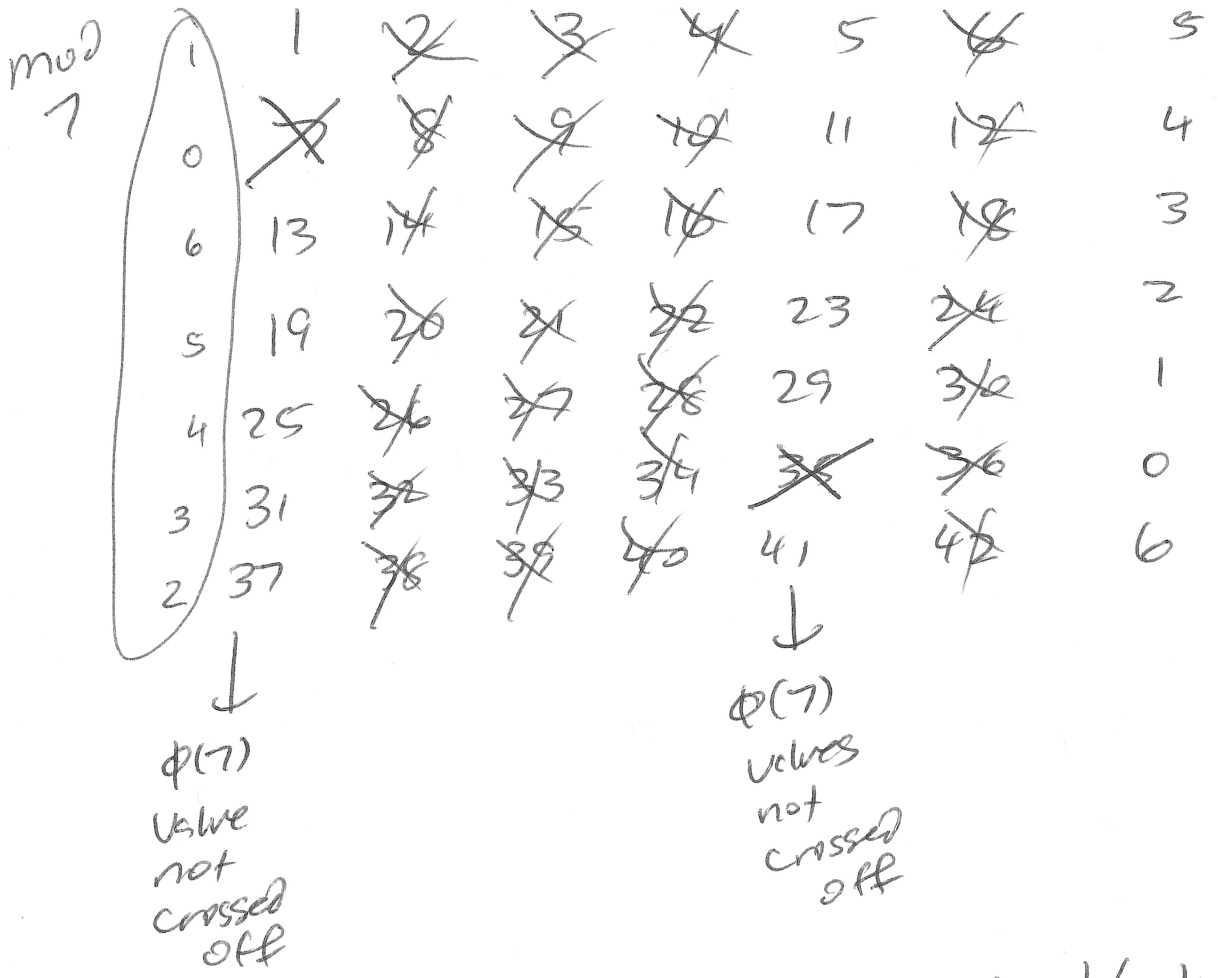
$$\Longrightarrow n \mid (x-y) \qquad \boxed{0 < x-y < n}$$

Contradiction! $\Longrightarrow$ all values on the list are unique mod n

List of #s $\equiv 0, 1, 2, \ldots n-1 \pmod{n}$

If we cross off all values that share a common factor with n, we'll be left with $\phi(n)$ values on <u>each</u> of $\phi(m)$ rows for a total of $\phi(m) \times \phi(n)$.

$m = 6, \quad n = 7$ $\qquad \phi(6 \times 7) = \phi(6) \times$



If $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m) \times \phi(n)$

$$n = p_1^{q_1} p_2^{q_2} p_3^{q_3} \cdots \qquad n = \prod p_i^{q_i}$$

$$\phi(n) = \phi(p_1^{q_1})\,\phi(p_2^{q_2} p_3^{q_3} \cdots)$$

$$= p_1^{q_1}\left(1 - \frac{1}{p_1}\right)\phi(p_2^{q_2})\,\phi(p_3^{q_3} p_4^{q_4} \cdots)$$

$$= p_1^{q_1}\left(1 - \frac{1}{p_1}\right) p_2^{q_2}\left(1 - \frac{1}{p_2}\right) p_3^{q_3}\left(1 - \frac{1}{p_3}\right) \cdots$$

$$\phi(n) = \prod_{p_i \in \text{Prime over primes in the factorization}} p_i^{q_i}\left(1 - \frac{1}{p_i}\right) = n \prod_{p_i \in \text{Prime in the factorization of } n} \left(1 - \frac{1}{p_i}\right)$$

$$\phi(60) = 60 \times \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

$$= \cancel{60}^{\,4} \times \frac{1}{\cancel{2}} \times \frac{\cancel{2}}{\cancel{3}} \times \frac{4}{\cancel{5}}$$

$$= \boxed{16}$$

$$n \times \frac{(p-1)}{p} \qquad \underbrace{n/p}_{\text{int}} * (p-1)$$