Euler ϕ function

$\phi(n)$ = # integers from 1 to n relatively prime with n.

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

$\phi(p^k) = p^k - p^{k-1}$, $p \in$ Prime

$= p^{k-1}(p-1)$

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

What about $\phi(mn)$, where $\gcd(m,n)=1$?

$\phi(5*7)$?

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

mn = total

$-m$ = mults of n.

$-n$ = mults of m

$+1$ = 1 mult n,m.

for $m=5$, $n=7$, $\phi(mn) = mn - m - n + 1$

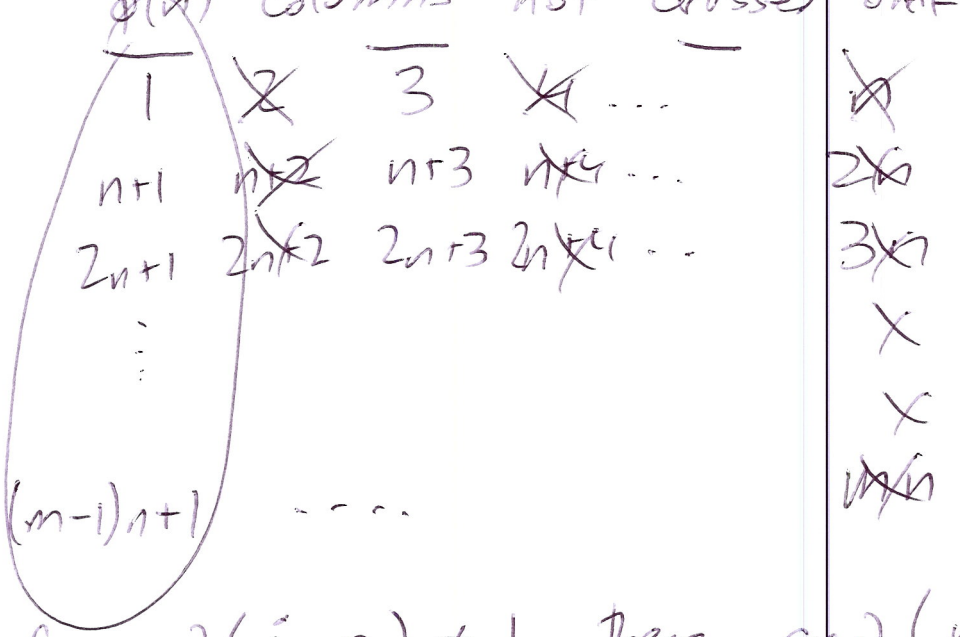
$= (m-1)(n-1)$

In this example $\phi(mn) = \phi(m) * \phi(n)$.

Will this be true in general?

Try this exercise again but for arbitrary m, n w/ $\gcd(m,n) = 1$.

$\phi(n)$ columns not crossed off



if $\gcd(i,n) \neq 1$, then $\gcd(n+i, n) \neq 1$.

$\gcd(jn+i, n) \neq 1$

~~Count cross offs~~

Count remaining values not crossed off!

$\phi(n)$ columns, each column has m items

$\phi(n) \times m$ items NOT crossed off

Consider an arbitrary column i. It has value $i, n+i, 2n+i, \ldots (m-1)n+i$. [$\gcd(n,i) = 1$]. The only way we'll cross something off is if it shares a common factor with n.

Claim: All m values in the column are inequivalent mod m.

Goal: Prove from the list
$\{i, n+i, 2n+i, \ldots, (m-1)n+i\}$ each value is a ~~2~~ different mod value mod m.

Pf by contradiction - Assume 2 different #s in the set are ~~equal~~ equivalent mod m =

$$xn + i \equiv yn + i \pmod m, \quad x \neq y, \quad 0 \leq x, y \leq m-1$$

$$xn \equiv yn \pmod m$$
$$xn - yn \equiv 0 \pmod m$$
$$n(x-y) \equiv 0 \pmod m$$
$$\Rightarrow m \mid n(x-y).$$

Thm if $\gcd(a,b)=1$ and $a \mid bc$, then $a \mid c$.

Since $\gcd(m,n)=1$, $m \mid (x-y)$ but the contradicts the fact that $1 \leq |x-y| \leq m-1$.
But no values in range $\{1, m-1\}$ are divisible by m.
Our assumption was wrong. All values are inequivalent mod m.

Since these are all possible values mod m, exactly $\phi(m)$ of them do NOT share a common factor with m.
So, from then $\phi(n)$ columns we'll still have exactly $\phi(m)$ values each.
Total # of uncrossed values = $\phi(n)\phi(m)$

Formula $\phi(n)$

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

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

$$= (p_1^{q_1} - p_1^{q_1-1})(p_2^{q_2} - p_2^{q_2-1}) \dots$$

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

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_{nc}}\right)$$

for each prime that divides evenly into n.

$$\phi(120) = 120 \cdot \frac{1}{2} \times \cancel{\frac{2}{3}} \times \frac{4}{5} = 8 \times 4 = 32$$

$\Downarrow$

$2, 3, 5$

$120 = 2^3 \times 3 \times 5$

$$= (2^3 - 2^2)(3-1)(5-1)$$

$$= 4 \times 2 \times 4 = 32$$

Euler's Thm

fermat's: if ~~gcd~~ $\gcd(a,p)=1$, $a^{p-1} \equiv 1 \pmod{p}$

euler asks: what is p isn't prime

If $\gcd(a,n)=1$, what can we say about $a^k \bmod n$? Can we get a formula for some k s.t. $a^k \equiv 1 \bmod n$ (cycle len)

if $\gcd(a,n)=1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$

Define a reduced residue set mod n to be any $\phi(n)$ values s.t. each value is inequivalent mod n and none of the values share a common factor with n.

RRS mod 15 $= \{1,2,4,7,8,11,13,14\}$

another RRS mod 15 $= \{61,2,19,37,38,-4,43,59\}$

Start with the set of remainders mod n $\quad n=15$
relatively prime with n, call this set S

$S = \{1,2,4,7,8,11,13,14\}$

Create set T by multiplying each item by a $\quad a=4$

$T = \{4,8,16,28,32,44,52,56\}$

T is also a RRS mod n.

① no values are equiv mod n
② no values share common factor n

(2) If I start with values that don't share a common factor w/ n and multiply it by something (a) that doesn't share a common factor w/ n, the product won't either. ✓

$$S = a_1, a_2, a_3 \ldots a_{\phi(n)}$$

$$T = aa_1, aa_2, aa_3 \ldots aa_{\phi(n)}$$

Assume the opposite, that 2 value in T are equiv mod n

$$aa_i \equiv aa_j \pmod n \quad i \neq j$$

$$aa_i - aa_j \equiv 0 \pmod n$$

$$a(a_i - a_j) \equiv 0 \pmod n$$

$$\Rightarrow n \mid a(a_i - a_j), \text{ since } \gcd(a,n) = 1 \Rightarrow n \mid (a_i - a_j)$$

↪ Contradicts the fact that $a_i \not\equiv a_j \pmod n$.

This proves no 2 values in T are equivalent mod $n \Rightarrow$ T is a RRS mod n.

Euler says okay multiply all elements in S and T look mod n

$$\prod_{i=1}^{\phi(n)} a \cdot a_i \equiv \prod_{i=1}^{\phi(n)} a_i \pmod n$$

$\prod$ over T $\quad$ $\prod$ over S

$$\prod_{i=1}^{\phi(n)} a \cdot q_i - \prod_{i=1}^{\phi(n)} q_i \equiv 0 \pmod{n}$$

$$a^{\phi(n)} \left(\prod_{i=1}^{\phi(n)} q_i \right) - \prod_{i=1}^{\phi(n)} q_i \equiv 0 \pmod{n}$$

$$\left(\prod_{i=1}^{\phi(n)} q_i \right) \left(a^{\phi(n)} - 1 \right) \equiv 0 \pmod{n}$$

$$\Rightarrow n \mid \left(\prod_{i=1}^{\phi(n)} q_i \right) \left(a^{\phi(n)} - 1 \right)$$

Since $\gcd\left(n, \prod_{i=1}^{\phi(n)} q_i\right) = 1 \Rightarrow n \mid \left(a^{\phi(n)} - 1 \right)$

$$a^{\phi(n)} - 1 \equiv 0 \pmod{n}$$

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$$