

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	3
$p+1$	$p+2$	...	$2p$
...	...	...	X
...	...	...	X
$p^k - p + 1$	...	...	p^k

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

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

$\phi(n)$ 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 $\phi(mn)$

by definition on row 1 $\phi(m)$ values will remain after $m - \phi(m)$ set crossed off

1	2	3	X	X	m
m+1	m+2	m+3	X	X	2m
2m+1	2m+2	2m+3	X		3m
...	X		X		
	X		X		
	X		X		
(n-1)m+1	(n-1)m+2	...	X		nm
(n-1)m+2					

① Cross off #s share a common factor with m

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.

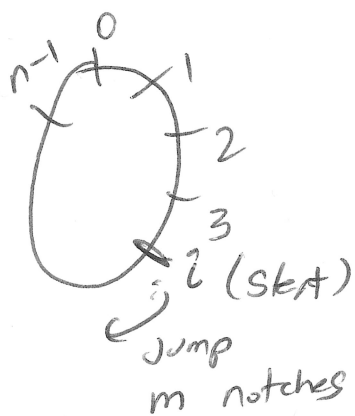
After step one we have $\phi(m)$ rows remaining each with n values. A single row looks like:

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

$$\gcd(i, m) = 1$$

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 .

$$xm+i \equiv ym+i \pmod{n}$$

$$xm - ym \equiv 0 \pmod{n} \quad \boxed{0 \leq y < x \leq n-1}$$

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

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

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

$$\Rightarrow n \mid (x-y)$$

$$\boxed{0 < x-y < n}$$

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

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

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

$$m=6, n=7$$

$$\phi(6 \times 7) = \phi(6) \times$$

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

$\downarrow$
 $\phi(7)$
 Value not crossed off

$\downarrow$
 $\phi(7)$
 values not crossed off

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

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

$$n = \prod p_i^{q_i}$$

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

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

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

$$\phi(n) = \prod (p_i^{q_i} (1 - \frac{1}{p_i})) = n \prod (1 - \frac{1}{p_i})$$

$p_i \in \text{Prime}$
over primes
in the
factorization

$p_i \in \text{Prime}$ in the
factorization of n

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

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

$$= \boxed{16}$$

$$n \times \frac{(p-1)}{p}$$

$$\lfloor \frac{n}{p} \rfloor * (p-1)$$

int