CIS 3362 10/10/25

If $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$

p=Prime Fermet's Thm

$67^{100} \equiv 1 \pmod{101}$, 101 is prime

mod 17

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
1	2	4	8	16	15	13	9	1

Fermet's guarantees $2^{16} \equiv 1 \pmod{17}$ but maybe cycle size is smaller (2's cycle size mod 17 is 8) Nob: All cycle sizes mod p are divisors of p-1

But what about modular expo mod a composite?

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

Define $\phi(n)$.

is the number of integers in the set $\{1, 2, 3, 4, \ldots n-1, n\}$ that are relatively prime to n.

1 2 ~~3~~ 4 ~~5~~ ~~6~~ 7 8 ~~9~~ ~~10~~ 11 ~~12~~ 13 14 ~~15~~

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

$\phi(15) = 8$

for an affine ~~Eqn~~ cipher alpha size n,

valid keys $= n\,\phi(n)$

ϕ function

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

$\phi(7) = 6$ 1, 2, 3, 4, 5, 6

$\phi(17) = 16$ 1, 2, ... 16

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

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

3^3

1 2 ~~3~~

4 5 ~~6~~

⋮ ~~X~~

~~X~~

25 26 ~~27~~

$\phi(3^3) = 3^3 - 3^2$

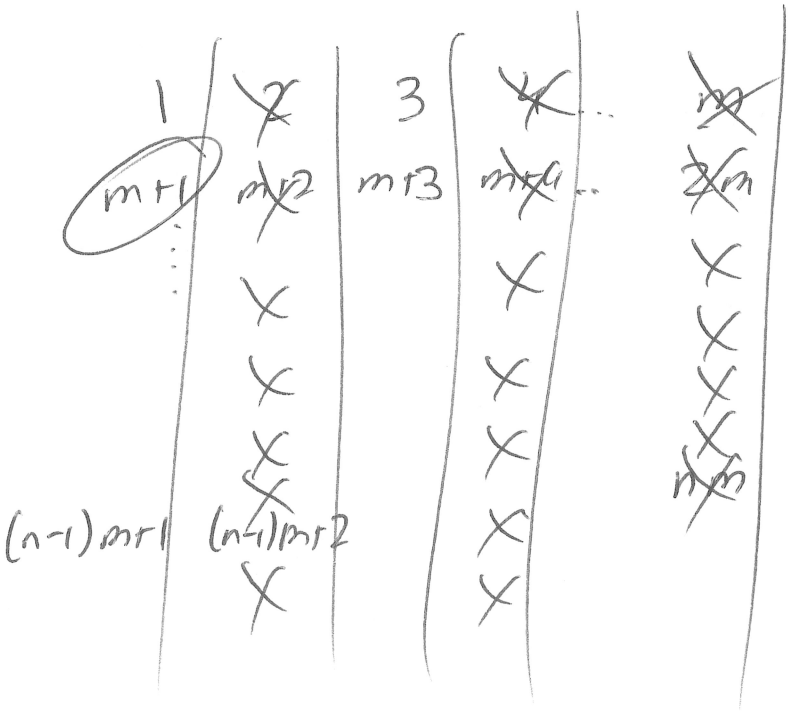
$= 3^2(3-1)$

Multicative Function

if $\gcd(m,n) = 1$

then $\phi(mn) = \phi(m) \times \phi(n)$

$\phi(p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}) = \phi(p_1^{a_1}) \phi(p_2^{a_2}) \phi(p_3^{a_3}) \phi(p_4^{a_4}) \cdots \phi(p_k^{a_k})$



1) Cross off all # Share common factor m

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

remaining columns is $\phi(m)$ by def.

left = $n\,\phi(m)$

Each column has the structure

$a\Phi, m+a, 2m+a, 3m+a, \ldots (n-1)m+a$] n values

$1 \le a \le m$.

Prove that each value is distinct mod n.

Prove via contradiction. Assume the opposite that some pair of distinct values on the list are equivalent mod n

$$\cancel{a + im \equiv a + jm \pmod{n}}, \quad i \neq j, \quad 0 \le i, j \le n-1$$

$$im - jm \equiv 0 \pmod{n} \qquad 1 \le |i-j| \le n-1$$

$$m(i-j) \equiv 0 \pmod{n}$$

$n \mid m(i-j)$, Rule if $\gcd(a,b)=1$ and $a \mid bc$, then $a \mid c$.

Since $\gcd(n,m)=1$, it follows that

$n \mid (i-j)$ Contradicts fact $0 < |i-j| < n$

Thus our initial assumption was wrong!

It follows that all n values on the list are unique mod n.

In every column after cancellation exactly $\phi(n)$ values will remain!

$n = 6 \quad m = 7 \qquad \phi(42)$

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~~	~~36~~
37	~~38~~	~~39~~	~~40~~	41	~~42~~

left w/ $\phi(6)$ cols.

d

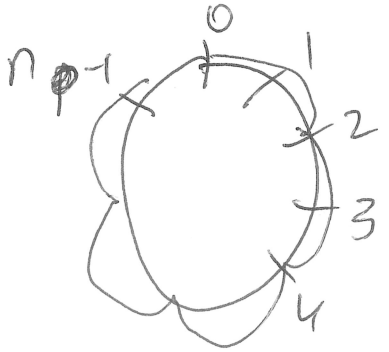
in both columns $\phi(7)$ values remain because all #s are distinct mod 7, but cross offs are in different places

1, 7, 13, 19, 25, 31, 37

1 0 6 5 4 3 2

5 11 17 23 29 35 41

5 4 3 2 1 0 6



n notches wheel
jump by m
gcd (n, m) = 1

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

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

$$\prod_{p_i \in Prime} \left(p_i^{q_i} - p_i^{q_i-1}\right)$$

$$= \left(\prod_{p \in Prime} p_i^{q_i}\right) \prod_{p_i \in Prime} \left(1 - \frac{1}{p_i}\right)$$

$$= n \prod_{p_i \in Prime} \left(1 - \frac{1}{p_i}\right)$$

$$\left(\frac{p_i - 1}{p_i}\right)$$

phi is/it dependent on exponents & primes, just each unique prime in the prime factorization

$$\phi(2^2 \times 3 \times 5^2) = \phi(300)$$

n	ϕ
300	300
~~75~~	$\frac{300 \times 1}{2} = 150$
~~25~~	$\frac{150 \times 2}{3} = 100$
1	$\frac{100 \times 4}{5} = 80$

Euler said define a reduced residue system mod n as any set of $\phi(n)$ integers each inequivalent mod n to each other

$n=15$ $\quad a=4$ $\quad a,\ \gcd(a,n)=1$

$S=\{1,2,4,7,8,11,13,14\}$ $\quad S=\{a_1\ a_2 \cdots a_{\phi(n)}\}$

$T=\{4,8,16,28,32,44,52,56\}$ $\quad T=\{aa_1, aa_2, \ldots aa_{\phi(n)}\}$

$4\ \ 8\ \ 1\ \ 13\ \ 2\ \ 14\ \ 7\ \ 11$

T and S are same mod n

Prove via contradiction that all values in T are distinct mod n

Assume

$$aa_i \equiv aa_j \pmod n \qquad a_i \not\equiv a_j \pmod n$$

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

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

$$\rightarrow n \mid (a(a_i - a_j))$$

Since $\gcd(n,a)=1$, $n \mid (a_i - a_j)$ but contradicts given info $a_i \not\equiv a_j \pmod n$

$$\prod_{a_i \in S} a a_i \equiv \prod_{a_i \in S} a_i \pmod{n}$$

$$\prod_{a_i \in S} a a_i - \prod_{a_i \in S} a_i \equiv 0 \pmod{n}$$

$$a^{\phi(n)} \prod_{a_i \in S} a_i - \prod_{a_i \in S} a_i \equiv 0 \pmod{n}$$

$$\left(\prod_{a_i \in S} a_i\right)\left(a^{\phi(n)} - 1\right) \equiv 0 \pmod{n}$$

$n \mid \left(\prod_{a_i \in S} a_i\right)\left(a^{\phi(n)} - 1\right)$, but

$\gcd\left(n, \prod_{a_i \in S} a_i\right) = 1$, it follows that

$n \mid \left(a^{\phi(n)} - 1\right)$

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

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

$\gcd(a, n) = 1$

EULER'S THM