CIS 3362 10/16/24

(1) Don't come to class on 10/18/24
- I've recorded the video + put notes up.
  Miller-Rabin + Fast Modular Exponentiation
  Format for the program for HS.

Today: Euler's Theorem + Euler Phi Function

if p is prime and $\gcd(a,p)=1$, then $a^{p-1} \equiv 1 \pmod p$
Fermat

What about composite n where $\gcd(a,n)=1$?
Is there a different # s.t. $a^? \equiv 1 \pmod n$?

$n=15$, $a=2$ ⇓

exp	0	1	2	3	4	5	6		
$2^{exp} \bmod n$	1	2	4	8	1	1	2	4	8
$a=4$	1	4	1	4	1 ...				
$a=7$	1	7	4	13	1 ...				
$a=8$	1	8	4	2	1				
$a=11$	1	11	1	11	1 ...				
$a=13$	1	13	4	7	1				
1, 14									

If you're going cycle through values, you can't hit any more value than the ones that are possible. If $\gcd(a,n)=1$, then $\gcd(a^i,n)=1$.
Cycle length $\leq$ # of values of a s.t. $\gcd(a,n)=1$.

For how many values, a, in the set $\{1,2,3,\ldots n\}$ does $\gcd(a,n)=1$? → we define this answer as $\phi(n)$, the Euler Phi Function

If n is prime, answer is $\underline{\underline{n-1}}$

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

$n = 3\times 5 = 15$

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

$\phi(15) = 8$

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

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

1 2 3 .. ~~p~~

p+1 p+2 p+3 ..

2p+1 ...

~~2p~~

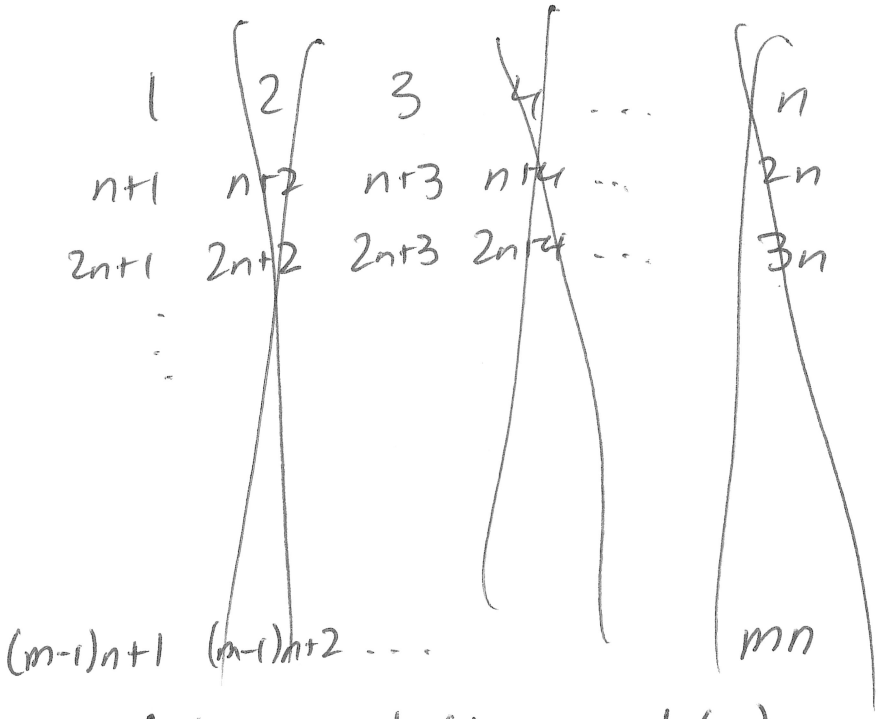
~~3p~~

~~p²~~

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

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

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



Cross off all # that share a common factor with n.

If $\gcd(a,n)\neq 1$, then $\gcd(n+a,n)\neq 1$

$\gcd(ni+a,n)\neq 1$.

Columns left $=\phi(n)$

Values left $=m\,\phi(n)$, each column has m values.

We must cross off each value that shares a common factor with m.

An arbitrary column has form

$i, (n+i), (2n+i), (3n+i), \ldots ((m-1)n+i)$

where $\gcd(i,n)=1$.

Q: How many values on this list are relatively prime to m?

→ All of these values are unique mod m.

Assume the opposite that 2 values in a column are equivalent mod m:

$$nx + i \equiv ny + i \pmod m$$

$$0 \le y < x \le m-1$$

$$nx - ny \equiv 0 \pmod m$$

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

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

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

Since $\gcd(m,n)=1$, it follows that $m \mid (x-y)$.

$$0 < x-y \le m-1$$

} Contradiction m doesn't divide evenly into any integer in between 1 and $m-1$, inclusive!

The # values in all columns are equivalent to $0, 1, 2, \ldots, m-1 \pmod m$. Exactly $\phi(m)$ these do NOT share a common factor with m. It follows that the # of integers from 1 to nm that are relatively prime with nm is $\phi(n) \times \phi(m)$

if $\gcd(m,n)=1$, $\phi(nm) = \phi(n) \cdot \phi(m)$

$$\phi(p^k q^m r^n s^x) = \phi(p^k) \times \phi(q^m) \times \phi(r^n) \times \phi(s^x)$$

$$= (p^k - p^{k-1})(q^m - q^{m-1})(r^n - r^{n-1})(s^x - s^{x-1})$$

if $p, q, r, s \in$ Primes

What is $\phi(175) = \phi(5^2 \times 7) = \phi(5^2) \times \phi(7)$

$= (5^2 - 5) \times (7-1)$

$= 20 \times 6$

$= 120$

$= p^k q^m r^n s^x \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\left(1 - \frac{1}{s}\right)$

$= N \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\left(1 - \frac{1}{s}\right)$

$\phi(5)$ $\quad n = 40 = 8 \times 5, \quad \gcd(8,5) = 1$

1	2	3	4	5	6	7	8	$\phi(8) = 4$ columns
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	

$1, 9, 17, 25, 33 \Rightarrow 1, 4, 2, 0, 3 \pmod 5$

$3, 11, 19, 27, 35 \Rightarrow 3, 1, 4, 2, 0$

$5, 13, 21, 29, 37 \Rightarrow 0, 3, 1, 4, 2$

$7, 15, 23, 31, 39 \Rightarrow 2, 0, 3, 1, 4$

$\phi(40) = \phi(2^3)\phi(5)$

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

$= 4 \times 4$

$= 16$

Let $S = \{a_1, a_2, a_3, \ldots a_{\phi(n)}\}$ where each a_i is unique mod n and $\gcd(a_i, n) = 1$.
Reduced Residue System mod n.

~~Create~~ Let $\gcd(a, n) = 1$, create a new set T

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

All elements in T are equivalent to elements in S mod n. The sets are equal sets under mod n.

$\gcd(aa_i, n) = 1$ because $\gcd(a, n) = 1$ and $\gcd(a_i, n) = 1$

Prove that all values in T are unique mod n

Assume the opposite that $aa_i \equiv aa_j \pmod n$
$\gcd(a, n) = 1$, $\gcd(a_i, n) = 1$, $\gcd(a_j, n) = 1$ and $a_i \not\equiv a_j \pmod n$

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

Since $\gcd(a, n) = 1$, thus $n \mid (a_i - a_j)$

$\Longrightarrow a_i \equiv a_j \pmod n$

Contradicts our given info that $a_i \not\equiv a_j \pmod n$.

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

$a = 4$ $\quad T = \{4, 8, 16, 28, 32, 44, 52, 56\} \pmod{15}$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

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

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

Product of everything in T $\qquad$ Product of everything in S

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

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

Since $\gcd\left(n, \prod_{i=1}^{\phi(n)} a_i\right) = 1$

$$\rightarrow n \mid \left(\prod_{i=1}^{\phi(n)} a_i\right)\left(a^{\phi(n)} - 1\right),$$

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

as a mod eqn: $a^{\phi(n)} - 1 \equiv 0 \pmod{n}$

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