CIS 3362 10/21/26

(0) Handed Back Exam (42% grade computed)
A ~ 85%, B ~ 65%, C ~ 45%

(1) Continue w/ Num Theory
- complete $\phi(n)$ computation
- Euler's Thm
- Miller-Rabin Primality Test
- Discrete Log Problem

$\phi(n)$ = # ints in set $\{1, 2, 3, \ldots n\}$ relatively prime to n.

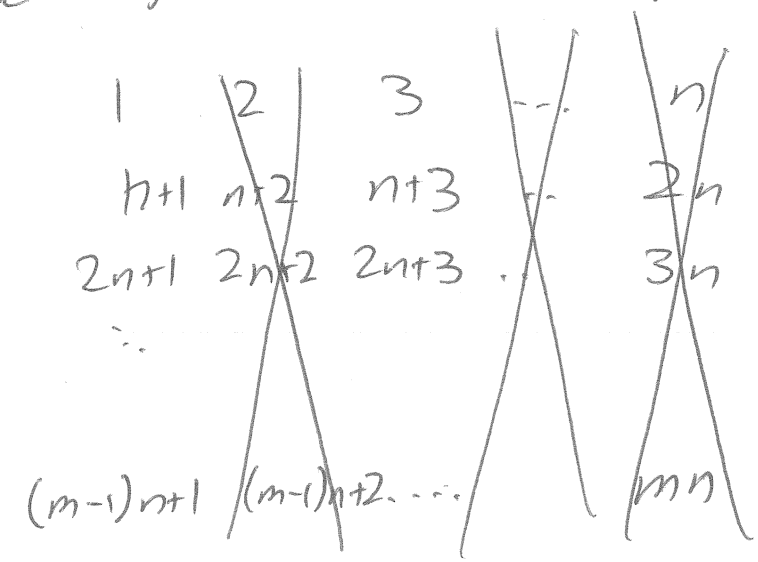
$\phi(p) = p-1$, $p \in$ Prime

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

Goal: if $\gcd(m,n)=1$, then $\phi(mn) = \phi(m)\cdot\phi(n)$.

If true $\phi(p_1^{q_1} p_2^{q_2} p_3^{q_3} \cdots p_k^{q_k}) = \phi(p_1^{q_1})\phi(p_2^{q_2})\phi(p_3^{q_3})\cdots\phi(p_k^{q_k})$

Goal: $\gcd(m,n)=1$. Compute $\phi(mn)$



if $\gcd(a,n)=1$ then $\gcd(a+in,n)=1$

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

Left w/ $\phi(n)$ columns of form

$a, n+a, 2n+a, \ldots (m-1)a$, $\gcd(a,n)=1$.

↳ How MANY OF THESE are also relatively prime to m?

* Note exactly m values → we'll prove they all all unique mod m.

Prove that all values list above are unique mod m.

Assume the opposite that

$$ni+a \equiv nj+a \pmod m, \quad \exists\, i>j\geq 0 \qquad (i,j \leq m-1)$$

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

$m \mid n(i-j)$

$\gcd(m,n)=1 \longrightarrow m \mid (i-j)$

$i-j>0$, $i-j\leq m-1$ CONTRADICTION

Lemma: if $n \mid ab$ & $\gcd(n,a)=1$, then $n \mid b$.

It follows that each item on our list is unique mod $n \Rightarrow \phi(n)$ values on the list are relatively prime to n.

$$\phi(n) * \phi(m) = \phi(nm)$$

columns item/column

$$\phi(2^5 3^2 5^4) = \phi(2^5)\phi(3^2)\phi(5^4)$$

$$= (2^5 - 2^4)(3^2 - 3)(5^4 - 5^3) \qquad 3000$$

$$= 16 \times 6 \times 500$$

$$= 48000$$

express ans in prime factorized form

$$= \underline{2^4 \times 2} \times 3 \times 5 \times \underline{2^2} \times 5^2$$

let $n = 2^5 \cdot 3^2 \cdot 5^4$ $\quad = 2^7 \times 3 \times 5^3$

$$\phi(2^5)\phi(3^2)\phi(5^4) = \underline{2^5}\left(1 - \tfrac{1}{2}\right)\underline{3^2}\left(1 - \tfrac{1}{3}\right)\underline{5^4}\left(1 - \tfrac{1}{5}\right)$$

$$= n \times \underbrace{\tfrac{1}{2} \times \tfrac{2}{3} \times \tfrac{4}{5}}$$

$$\phi(n) = n \cdot \prod_{p_i \in \text{Primefact}(n)} \frac{p_i - 1}{p_i}$$

Euler's Theorem

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

Generalization of Fermat's Thm.

Let $S = \{q_i \mid \gcd(q_i,n)=1 \text{ and } q_i \not\equiv q_j \pmod{n}\}$

$|S| = \phi(n)$

Reduced Residue System mod n

$n=15$, $S = \{1,2,4,7,8,11,13,14\}$

$S' = \{31, \cancel{\#}17, 4, 7, -7, 11, 13, 14\}$

} both are reduced residue systems mod n

Start w/S a reduced residue system mod n

$S = \{q_1, q_2, q_3 \cdots, q_{\phi n}\}$

Let $\gcd(a,n)=1$, consider set T elements are of the form $a \cdot q_i$

$T = \{aq_1, aq_2, aq_3, \ldots a \cdot q_{\phi(n)}\}$

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

$a=7$ $T = \{7, 14, 28, 49, 56, 77, 91, 98\}$

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

Prove T is ALSO a reduced residue system mod n

Prove: (1) all vals in T unique mod n
(2) all vals in T are relatively prime n.

↳ $\gcd(a, n) = 1 \quad \gcd(a_i, n) = 1$

$\Rightarrow \gcd(aa_i, n) = 1.$

$a_i \not\equiv a_j \pmod n$

Proof by contradiction. Assume to the contrary, that $a \cdot a_i \equiv a \cdot a_j \pmod n$

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

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

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

it follows that $n \mid (a_i - a_j)$ but this means $a_i - a_j \equiv 0 \mod n$

$$a_i \equiv a_j \mod n$$

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

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

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

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

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

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

$$n \mid \left[\left(\prod_{i=1}^{\phi(n)} q_i\right)\left(a^{\phi(n)} - 1\right)\right] \quad \text{and}$$

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

(since $\gcd(n, q_i) = 1$ for all q_i) $\quad n \mid \left(a^{\phi(n)} - 1\right)$

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

$$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$$ Euler's thm!

$n = 15$ $\quad 3 \times 5$ $\quad$ what is $11^{97} \equiv x \bmod 15$

$\phi(15) = (3-1)(5-1) = 2 \times 4 = 8$ $\quad \gcd(11, 15) = 1$ $\quad (11^8)^{12} \equiv 1^{12} \bmod 15$

$11^{96} \equiv 1 \bmod 15$

$$11^{97} \equiv 11 \times 11^{96}$$
$$\equiv 11 \times (11^8)^{12}$$
$$\equiv 11 \times 1 \pmod{15}$$
$$\boxed{\equiv 11 \pmod{15}}$$

~~Discrete Log Problem~~ Miller-Rabin Alg.

Old test for primality takes $O(\sqrt{n})$ time but this is prohibitive if $n \sim 10^{300}$...

Property of all primes if $\gcd(a,p)=1$

$$a^{p-1} \equiv 1 \pmod{p}$$

Thus given n, if I find an a s.t. $\gcd(a,n)=1 \wedge a^{n-1} \not\equiv 1 \pmod{n}$, then I have proof n IS composite!

Carmichael Numbers s.t. these are composite but for all a $\gcd(a,n)=1$, $a^{n-1} \equiv 1 \bmod n$.

Miller-Rabin Realized the following to catch Carmichael #s as fake primes:

Pick random a. Verify $\gcd(a,n)=1$.

Take $n-1 = 2^k \cdot m$, $m \in \text{Odd}$, $k \in \mathbb{Z}^+$.

Compute $a^m, a^{2m}, a^{4m}, \ldots a^{2^k m}$ a^{n-1}

(last 1 from $a^{2^k m}$)

if $a^m \equiv 1 \bmod n$, "IS PROBABLE PRIME"

else

one of $a^m, a^{2m}, a^{4m}, \ldots$ MUST EQUAL $-1 \bmod n$, an if not, it's definitively composite.

Returns either 100% composite

or "IS PROBABLE PRIME"

↳ it's correct at least 75% of the time!

each a is independent

If we test 100 a's and all pass probability number is composite

$$< \left(\frac{1}{4}\right)^{100}.$$