CIS 3362 10/21/22

$\phi(n)$ = # values $\{1, 2, 3, \ldots n\}$ relatively prime with n.

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

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

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

$$\underbrace{n = \prod_{p_i \in \text{Prime}} p_i^{a_i}}_{\text{Prime factorized}}, \quad \phi(n) = \prod_{p_i \in \text{Prime}} (p_i^{a_i} - p_i^{a_i - 1})$$

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

$$= \boxed{\prod_{p_i \in \text{Prime}} p_i^{a_i}} \prod_{p_i \in \text{Prime}} \frac{p_i - 1}{p_i}$$

$$= n \prod_{p_i \in \text{Prime}} \frac{p_i - 1}{p_i}$$

only over unique primes in factorization of n.

$n = 96$

primes $= 2, 3$

$96 \times \frac{1}{2} \times \frac{2}{3} = \boxed{32}$

keys affine cipher w/ alphabet size of n

$= n\,\phi(n)$

choices for b

choices for a

Today

1) Euler's Theorem
2) ~~Mat~~ Miller-Rabin Primality Test

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

Start w/a set $S = \{a_1, a_2, \dots a_{\phi(n)}\}$
$a_i \in \{1,2,3,\dots n\} \wedge \gcd(a_i, n)=1$ a_i's unique.

Reduced Residue System mod n

if $n=6$ $\quad S=\{1,5\}$
if $n=15$ $\quad S=\{1,2,4,7,8,11,13,14\}$

Pick any value a, $\gcd(a,n)=1$ and create a set $T = \{aa_1, aa_2, aa_3, \dots, aa_{\phi(n)}$

if $a=\cancel{3}\ 5, n=6$ $\quad T=\{\cancel{3}\ 5, \cancel{15}\ 25\}$
if $a=4, n=15$ $\quad T=\{4, 8, 16, 28, 32, 44, 52, 56\}$
$\qquad\qquad 8, 1, 13, 2, 14, 7, 11$

Prove all elements in T mod n are equivalent to elements in S.

$\Longrightarrow$ 1) All values in T are unique mod n
2) All values in T are relatively prime to n.

Proof of #2: $\gcd(a,n)=1$, $\gcd(a_i,n)=1$
$\Longrightarrow \gcd(aa_i, n)=1.$

Proof by contradiction for #1

assume $\exists\, a_i, a_j \in S \mid a_i \neq a_j$ but

$$aa_i \equiv aa_j \pmod{n}$$

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

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

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

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

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

Contradiction $1 \leq a_j, a_i \leq n-1 \wedge a_i \neq a_j$

so $1 \leq |a_i - a_j| \leq n-2$

Product of items in S

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

Product items in T

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

Let $Z = \prod_{i=1}^{\phi(n)} a_i$

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

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

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

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

Because $\gcd(n, Z) = 1$, it follows that $n \mid (a^{\phi(n)} - 1)$

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

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

Euler's Theorem

What is the remainder when 67^{201} is divided by 15

$$67^{201} \equiv 7^{201} \pmod{15}$$

$\gcd(7, 15) = 1$, so by Euler's Theorem

$$7^{\phi(15)} \equiv 7^{8} \equiv 1 \pmod{15}$$

$$7^{201} = 7^{200+1} \equiv 7^{8 \times 25} \times 7^{1}$$

$$\equiv (7^8)^{25} \times 7 \pmod{15}$$

$$\equiv 1^{25} \times 7$$

$$\equiv \boxed{7 \pmod{15}}$$

Primality Testing

Probabilistic Algorithm!

- if ~~Ma~~ Miller-Rabin says "no", the number is definitely composite.
- if the alg. says "yes" it really means "is probably prime"

$$\gcd(a,p)=1 \qquad a^{p-1} \equiv 1 \pmod p$$] True for all primes!

Is this true for composites?
Or how often is it true for composites

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

if n is composite, $\phi(n) < n-1$

$$\begin{aligned} a^{n-1} &\equiv a^{\phi(n)} \times a^{n-\phi(n)-1} \\ &\equiv 1 \times a^{n-\phi(n)-1} \\ &\equiv \underbrace{a^{n-\phi(n)-1}}_{\text{Could be 1, we don't know}} \pmod n \end{aligned}$$

Turns out it's rarely equal to 1 for composites.

FOR a random composite n, random int a ($\gcd(a,n)=1$), probability this is 1 is $< \frac{1}{2}$.

Orginal Idea

might fail upto 50% of the time

```
isPrime(int n) {
    a = randint(1, n-1)
    ~~exp~~
    if (gcd(a,n) ≠ 1)
        return false
    ans = pow(a, n-1) % n
    return ans == 1;
}
```

Fix #1

Probability a composite makes it through this is $(50\%)^{rep}$

if rep=100

$\frac{1}{2^{100}}$

crazy small

```
isPrime(int n, int rep) {
    for(i=0; i<rep; i++) {
        a = randint(1, n-1)
        if (gcd(a,n) != 1)
            return false;
        ans = pow(a, n-1) % n;
        if (ans != 1) return false;
    }
    return true; // Is Probably Prime
}
```

Probability correct $\sim 1-\left(\frac{1}{2}\right)^{rep}$

* This isn't Miller-Rabin...
We'll get there on Monday.