CIS 3362 10/15/21

(1) Prime Numbers
(2) Prime Factorization
(3) & Slow Prime Test
(4) Fermat's Little Thm

] last time

Today
(1) Primality Testing (Miller-Rabin)
(2) Euler ϕ Function

All primes, p, satisfy if $\gcd(a,p)=1$, then $a^{p-1} \equiv 1 \pmod{p}$.

IDEA: Pick random $a<p$, if $\gcd(a,p) \neq 1$, return comp.
Calculate $a^{p-1} \not\equiv 1 \pmod{p} \Rightarrow$ composite
else "is probably prime"

PROBLEM: Some composite #s pass this test.

IMPROVEMENT: Try 50 or 100 random a's
if any of them give $a^{p-1} \not\equiv 1 \pmod{p}$ say composite, else say "is probably prime".

In most circumstances, given a composite number n, and a with $\gcd(a,n)=1$, probability $a^{n-1} \equiv 1 \pmod{n}$ is $< \frac{1}{2}$.

probability passing 50 times in a row $< \left(\frac{1}{2}\right)^{50}$

EXCEPTION: Carmichael #s. 341 or (561 is 1st one)
560 times

Miller-Rabin

```
isPrime (int n) {

Recurk  n-1 = 2^k · n',  n' ∈ Odd

Pick random a.
if X = a^n' ≡ 1 (mod n)
    return isProbablyPrime
for (i = 0; i<k; i++) {
    if X ≡ (n-1) mod n
        return isProbablyPrime
    X = (X*X) mod n
}
return Composite;
}
```

MILLER-RABIN

Account for Carmichael #s!

$n = 121$

Pick $a = 2$

$n - 1 = 120 = 2^3 \times 15$

Step 1: rewrite $n - 1 = n' \cdot 2^k$ where $n' = \text{odd}$.

If the Fermat test, we would do 2^{120}.

Miller Rabin, we do 2^{15}

if $2^{15} \equiv 1 \pmod{121} \Rightarrow$ return "isProbPrime"

else {

Calculate 2^{15}, 2^{30}, 2^{60} } if one of these is -1, return isProbPrime"

~~if any of these is~~

if none are -1, then return composite.

~~Miller~~ $2^{15} \equiv 65536 \pmod{121}$

$\equiv 75 \pmod{121}$ NOT 1

$2^{30} \equiv 75 * 75 = 5625 \equiv 59$

$2^{60} \equiv 59 * 59 = 3481 \equiv 93$

$2^{120} \equiv 93 * 93 = 8649 \equiv 58$ (STOP!)

NOT PRIME

Euler ϕ Function

$\phi(n)$ = # of values in the set $\{1, 2, 3, \ldots n\}$ relatively prime with n. (all ints $n \geq 2$)

$\phi(6) = 2$ $\quad \{1, 5\}$

Primes p, $\phi(p) = p - 1$. $\phi(7) = 6$, $\phi(101) = 100$.

From Affine cipher, # of valid a's was just $\phi(\text{alphabetsize})$, so $\phi(26) = 12$.

What about $\phi(p^n)$ where p is prime?

$\phi(7^3) = ?$

1, 2, 3, 4, 5, 6, (7) ... (14) ... 21, ... (343)

7^3 numbers lists

7^2 # on list share a common factor with 7^3.

$\phi(7^3) = 7^3 - 7^2 \Rightarrow \phi(p^n) = p^n - p^{n-1}$

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

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

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