CIS 3362 10/8/25

Next Section: Public key Cryptography (allows us to exchange message w/o ever exchanging a secret key w/ someone else)

→ BASED ON LOTS OF NUMBER THEORY

Sec4 (for Quiz4) – Number Theory Background for Public key Crypto.

Prime Number: Integer greater than 1 whose only positive divisors are 1 and itself.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ... INFS...

Prime Testing if $n = a * b$ then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

trial division upto $\sqrt{n}$

```
for (int i = 2; i*i <= n; i++)
    if (n%i == 0)
        return false;
return true;
```

function Sketch

$O(\sqrt{n})$

→ ok $n \approx 10^{12}$

Prime Sieve → not used for crypto.

Prime Factorization of an integer

→ keep on looking for divisors, divide them out until you get to sqrt

```
list of pairs;
i=2
while (i*i <= n) {

    int exp=0;
    while (n%i ==0) {
        exp++;
        n /= i
    }
    if (exp >0) {
        list.add([i, exp]);
    }
    i++;
}
if (n >1)
    list.add([n, 1]);
```

$O(\sqrt{n})$

a | b - "b is divisible by a" means there exists an integer c such that b = ac.

Fermat

Famous for Last Theorem: No pos int sol $a^n + b^n = c^n$ for $n > 2$.

1994-5 Andrew Wiles finally proved it

Simon Singh Fermat's Enigma

$S = \{1, 2, 3, \ldots, p-1\}$ $T = \{a, 2a, 3a, 4a, \ldots (p-1)a\}$

all non-zero remainders mod p

if we reduce elements in T mod p we'll get a permutation of the elements in S

let $\gcd(a,p) = 1$.

$p = 7$ $a = 4$

1	2	3	4	5	6
4	8	12	16	20	24
↓	↓	↓	↓	↓	↓
1	5	2	6	3	

all remainders of T in btw 0 and $p-1$, but 0 isn't possible since all terms in T equal ai, $1 \le i \le p-1$, but $p \nmid a$ and $p \nmid i$. In between 1 and $p-1$.

Prove no repeats in T

Assume the opposite that 2 distinct values in T are equivalent mod p

$j \quad i$

$a_i \equiv a_j \pmod{p} \quad 1 \leq j < i \leq p-1$

$a_i - a_j \equiv 0 \pmod{p}$

$a(i-j) \equiv 0 \pmod{p}$

$\Rightarrow p \mid (a(i-j))$

$\Rightarrow p \mid a \vee p \mid (i-j)$

$\times$ false $\gcd(a,p) = 1$

$\downarrow$ $i - j > 0 \wedge i - j < p-1$

$\times$

Contradiction!

If p is prime and $p \mid (ab)$ then $p \mid a \vee p \mid b$.

It follows that all items in T are distinct and a permutation of items in S.

$S = \{1, 2, 3, \ldots p-1\}$ $T = \{a, 2a, 3a, 4a, \ldots (p-1)a\}$

$$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} (ai) \pmod{p}$$

prod of # in S

prod of in T

$$\prod_{i=1}^{p-1} i \equiv a^{p-1} \prod_{i=1}^{p-1} i \pmod{p}$$

$$a^{p-1}(p-1)! - (p-1)! \equiv 0 \pmod{p}$$

$$(p-1)!\left(a^{p-1} - 1\right) \equiv 0 \pmod{p}$$

$$\rightarrow p \mid (p-1)! \quad \vee \quad p \mid (a^{p-1} - 1)$$

not possible

$$\Rightarrow a^{p-1} - 1 \equiv 0 \pmod{p}$$

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

For all pos ints a, primes p, if $\gcd(a,p)=1$

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