CIS 3362 10/~~20~~/26

Finished Private/Symmetric Key Cryptography Section!

Moving onto Public/Asymmetric Key Cryptography ...

NUMBER THEORY!

Prime Number - positive integer 2 or greater whose only divisors are 1 and itself.

1st few - 2, 3, 5, 7, 11, 13, ...

1 Important Skill - Primality Testing

Easy way: trial division

If n is compositive (not prime >1)

$\exists\, a, b \in \mathbb{Z}^+ \quad n = ab, \quad a > 1 \wedge b > 1$

Either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Assume opposite that $a > \sqrt{n} \wedge b > \sqrt{n}$

$$n = a \cdot b$$
$$> \sqrt{n} \cdot \sqrt{n}$$
$$= n \quad \text{Contradiction} \quad n > n.$$

Assumption was incorrect thus $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Basic Primality Test

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

Single Ops $O(\sqrt{n})$

Modular Exponentiation

Common Computation we'll need is $a^x \bmod n$

Standard Way

```
int modexp(int a, int x, int n) {
    int ans=1;
    for (int i=0; i<x; i++)
        ans = (ans*a)%n;
    return ans;
}
```

Runtime $O(x)$

$a^{16} \bmod n$ $\quad a^{16} = a^8 \times a^8 \bmod n$

let $x = a^8 \bmod n$, then I just need $x*x \bmod n$

Idea for speed up

a^x → if x is even do $Y = a^{x/2} \bmod n$ then return $(Y * Y) \bmod n$

→ if x is odd do $Y = a^{x-1} \bmod n$ return $(Y * a) \bmod n$

→ if $x = 0$ or 1 return ans

Never do 2 slow steps in a row

Max # fast steps, k is such that

$$\frac{X}{2^k} = 1 \qquad X = 2^k \rightarrow k = \log_2 X$$

```
int fastModExp(int a, int x, int n) {
    if (x == 0) return 1;
    if (x % 2 == 0) {
        int temp = fastModExp(a, x/2, n);
        return (temp*temp) % n;
    }
    return (a * fastModExp(a, x-1, n)) % n;
}
```

$O(\log x)$

if $x = 10^{100}$ very big

$\log_2 10^{100} = 100 \log_2 10 \sim 332$

Fermat (mathematician whose Last Theorem went unproved for 350+ years!)

Consider a prime number p and the set $S = \{1, 2, 3, \ldots, p-1\}$

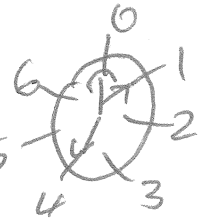
$\gcd(i, p) = 1$ for $1 \leq i \leq p-1$.

$p = 7$ $S = \{1,2,3,4,5,6\}$ $T = \{4, 8, 12, 16, 20, 24\}$

4 1 5 2 6 3

$a = 4$, create set T so that each element in $T = ai$, $1 \leq i \leq p-1$. (take each element of S and multiply it by a.)

Now reduce T mod p.



Prove: sets S and T are identical under mod p. Let a be chosen $\gcd(a,p) = 1$.

#1: All item in T are unique mod n

#2: No item in $T \equiv 0 \pmod p$.

Assume to the contrary that 2 items in T are equivalent mod p.

$ai \equiv aj \pmod p$ $\quad 1 \leq j < i \leq p-1$

↳ $ai - aj \equiv 0 \pmod p$ If $p \in$ Prime $\wedge$ $p \mid ab$,

$a(i-j) \equiv 0 \pmod p$ $a, b \in \mathbb{Z}$, then $p \mid a \vee p \mid b$.

$\Longrightarrow p \mid a(i-j) \longrightarrow p \mid a \vee p \mid (i-j)$ FALSE

FALSE $\gcd(a,p) = 1$ $\quad 1 \leq i-j \leq p-2$

THIS IS A CONTRADICTION. IT FOLLOWS THAT ALL ITEMS IN T ARE UNIQUE mod p.

To prove that no item $\equiv 0 \pmod p$ note that $p \mid a_i$ where $1 \le i \le p-1$ can't be true because $p \nmid a$ & $p \nmid 1$ & $p \nmid 2$, ... $p \nmid (p-1)$.

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

$4 \times 8 \times 12 \times \ldots 24$

$\prod$ means multiply!

Product of items in T is same as product of items in S under mod p.

$a \cdot 1 \cdot a \cdot 2 \cdot a \cdot 3 \ldots a \cdot (p-1)$

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

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

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

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

$$p \mid (p-1)! \quad \vee \quad p \mid \left[a^{p-1} - 1\right]$$

$p \mid (p-1)!$ is false because

$\gcd(p, i) = 1$ for $1 \leq i \leq p-1$.

Thus it must be the case that

$$p \mid (a^{p-1} - 1)$$

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

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

If $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$

$p \in$ Primes, Fermat's Theorem!

Euler was curious, is there a similar fact true for ALL integers? (Fermat's Thm only applies to primes.)

$\phi(n)$ - "Euler phi function"

= # of integers in the set $\{1, 2, 3, \ldots n\}$ such that $\gcd(i, n) = 1$.

$\phi(6) = 2$, $\gcd(1,6) = \gcd(5,6) = 1$

2, 3, 4, 6 share common factors w/ 6.

# of valid Affine keys = $n\,\phi(n)$, where n = alphabet size.

$\phi(p) = p - 1$ 1, 2, ... $p-1$ all work

$\phi(p^n) = p^n - p^{n-1}$ ✓

$= p^{n-1}(p-1)$ ✓

$= p^n\left(1 - \frac{1}{p}\right)$ ✓

5^3

p cols

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

p^{n-1} rows

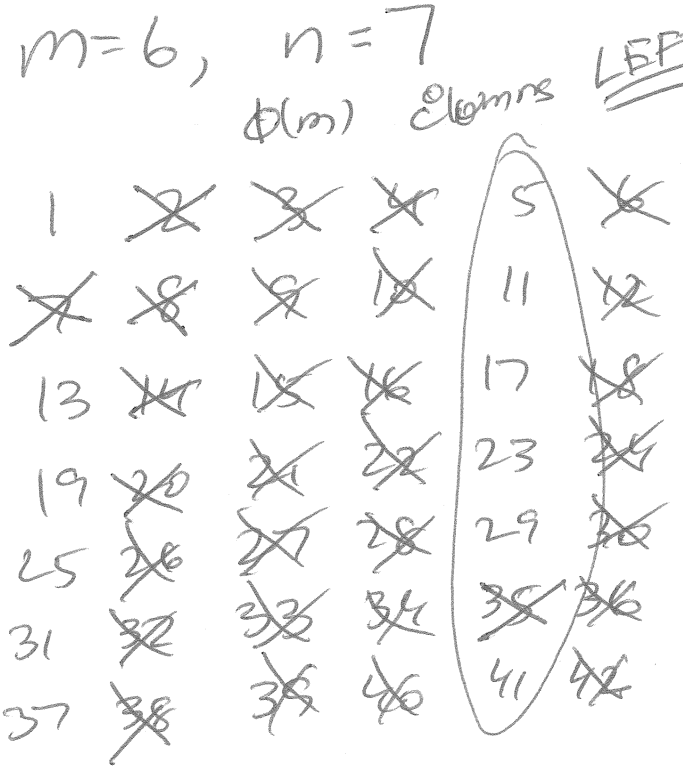
$p^{n-1}(p-1)$

total = p^n, crossoffs = p^{n-1}

$\phi(n)$ is a multiplicative function:

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

$m=6$, $n=7$



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

STAGE 1 cross offs left w $n\cdot\phi(m)$ values not crossed off

Column of form: $\gcd(a,m)=1$

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

How many of these n values share a common ~~fact~~ factor with n?

→ Prove that these n values ARE ALL UNIQUE mod n!

$$\phi(42)=\phi(2)\,\phi(3)\,\phi(7)$$
$$=1\times 2\times 6=12$$

Must prove all n values are unique mod n. Pf by contradiction. Assume the opposite that 2 values in a column are equivalent mod n:

$$a + mi \equiv a + mj \pmod{n}$$

$$0 \le j < i \le n-1$$

$$mi - mj \equiv 0 \pmod{n}$$

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

$$n \mid (m \cdot (i-j))$$

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

Since $\gcd(n,m) = 1$, it follows that

$n \mid (i-j)$, but $0 < i-j \le n-1$

THIS IS IMPOSSIBLE!

It follows that in each column exactly $\phi(n)$ value "survive"

each column is the set $\{0, 1, 2, \ldots n-1\}$ mod n

So each column is a permutation of mod n