CIS 3362 10/18/23

Number Theory

prime numbers ⇒ Fermat's Thm → Euler's Thm → Miller Rabin Primality Test
mod, mod inverse (already seen)

→ RSA requires the use of 2 large primes + reason it works is based on Euler's Thm.

* Discrete Log Problem (El Gamal Public Key System)

What's a regular log? $\log_2 64 = 6$
because $2^6 = 64$

log is inverse of the exponent problem.

Input (Given): Ans, Base
Output : Exponent

New Problem

Input: Ans, Base, Mod
Output: exponent

What's smallest positive int x that makes this true?

$$5^x \equiv 6 \pmod{11}$$

Exp	0	1	2	3	4	5
Ans	1	5	3	4	9	1

OOPS no ans!

$25 \equiv 3$ $\quad 15 \equiv 4$ $\quad 20 \equiv 9$

$$3^x \equiv 6 \pmod{11}$$

Exp	0	1	2	3	4	5
Ans	1	3	9	5	4	1

$$2^x \equiv 6 \pmod{11}$$

$x=9$ answer

Exp	0	1	2	3	4	5	6	7	8	9	10
Ans	~~8~~ 1	2	4	8	5	10	9	7	3	6	1

This is the discrete log problem

for prime numbers, p, we can calculate the cycle length for each possible base in modular exponentiation. We previously proved that the cycle length, c, for and base divides evenly into p-1.

$p=11$, $p-1=10$, all cycle length are either 1, 2, 5 or 10

Did program for $p=11$

---

* cycle len $=10$	$2,6,7,8$	$\phi(10)=4$
cycle len $=5$	$3,4,5,9$	$\phi(5)=4$
cycle len $=2$	10	$\phi(2)=1$
cycle len $=1$	1	$\phi(1)=1$

→ these values have property that they produce each possible non-zero mod value in a reasonably unpredictable order.

→ primitive roots OR generators

Once we know a primitive roots exists, then we can prove there are exactly $\phi(p-1)$ of them.

$$2^{10} \equiv 1 \mod 11$$

and $$2^2 \equiv 4 \mod 11$$

$$4^5 \equiv (2^2)^5 \equiv 2^{10} \equiv 1 \mod 11$$

The Discrete Log Problem will be use with mod = prime, base = primitive root
$\Rightarrow$ each possible ans exists.

Easiest/Slowest alg to solve

b, a, p mod

```
res=1
for (int i=0; i<p; i++) {
    if (res == a) return i;
    res = (res * b) % p;
}
```

Run time $O(p * oper)$

An alg that is a little bit faster

let $n = \lceil \sqrt{p} \rceil$ ceiling (least int $\geq \sqrt{p}$)

goal: find integers c and d such that

$$a^{nc-d} \equiv b \pmod{p}$$

Imagine $p=97$ $n=10$

loop through
c 1 to 10
d 0 to 10

if $c=1$, set $d = 0, 1, 2, 3, \ldots 10$

$a^{10-0}, a^{10-1}, a^{10-2}, \ldots a^{10-10}$

$c=2$ $a^{20-0}, a^{20-1}, \ldots a^{20-10}$

(1) Calculate a^{nc} for $c = 0, 1, 2, \ldots n$

store answers in a chart

(2) Calculate a^{d} for $d = 0, 1, 2, \ldots n$

$$a^d \left(a^{nc-d}\right) \equiv (b) a^d \mod p$$

$$\Rightarrow \quad a^{nc} \equiv b \cdot a^d \mod p$$

TABLE

$a^{nc} \to c$

for each d mult $b \times a^d$ and see if a^{nc} is in the lookup chart

Step 1 takes $O(\sqrt{p})$ time

Step 2 takes + $O(\sqrt{p})$ time

$$\boxed{O(\sqrt{p})}$$