CIS 3362 10/17/25

Discrete Log -

$y = b^x \bmod p$

Given b, y and p find x.

table seq $b^1, b^2, b^3 \ldots b^{p-1}$, $b^{p-1} \equiv 1 \bmod p$ and after that it repeats, so all rows have a cycle length that is either $p-1$, or divides evenly into $p-1$.

Special bases are ones where the row has each value from 1 to $p-1$ exactly once (cycle len = $p-1$.)

primitive roots of generators mod p (prime)

2 is a generator mod 29

$2^1, 2^2, 2^3 \ldots 2^{28} \bmod 29$ is a seemingly random permutation of 1 to 28.

* Why this will be useful
* Patterns in chart
* Algorithm to solve Disc Log a little bit faster.

for encryption we like processes that are "easy" calculate forwards, hard to "invert" or undo.

~~Distro~~ Discrete Log is exactly this!

ONE-WAY FUNCTION!

If a generator, g, exists for a prime p, we can prove that there are exactly $\phi(p-1)$ generators.

Given: $g^1, g^2, g^3, \ldots g^{p-1}$ are all unique mod p

exactly $\phi(p-1)$ integers in the range 1 to $p-1$ do NOT share a common factor with $p-1$.

Let a be an arbitrary int $1 \leq a \leq p-1$ s.t $\gcd(a, p-1) = 1$.

Prove g^a is also a generator.

$$g^a, g^{2a}, g^{3a}, g^{4a} \ldots g^{(p-1)a}$$

We know that $g^x \equiv g^{x \bmod (p-1)} \bmod p$

$p = 7 \quad g^{20} \equiv g^2 \bmod 7$

because $20 \equiv 2 \pmod 6$

$$g^{20} = (g^6)^3 g^2 \equiv 1^3 \cdot g^2 \equiv g^2 \bmod p$$

What is $24^{20} \bmod 7$, since $24 \equiv 3 \bmod 7$

$\equiv 3^{20} \bmod 7$, since $20 \equiv 2 \bmod 6$ ($\phi(a \cdot p)$)

$\equiv 3^2 \bmod 7$

Need to Prove exponents: $a, 2a, 3a, \ldots (p-1)a$ are all distinct mod $p-1$.

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

Assume the contrary,

$$ai \equiv aj \pmod{p-1}, \quad i \neq j, \quad 1 \leq i, j \leq p-1$$

$$ai - aj \equiv 0 \pmod{p-1}$$

$$a(i-j) \equiv 0 \pmod{p-1}$$

$\longrightarrow (p-1) \mid a(i-j)$, but since $\gcd(a, p-1) = 1$

$\longrightarrow (p-1) \mid (i-j)$, contradicts fact that $1 \leq |i-j| \leq p-2$

CONCLUSION is # generators has to be equal to $\phi(p-1)$. (last part if $\gcd(a, p-1) > 1$, then g^a isn't generator.)

$p = 29 \quad p-1 = 28 \qquad \phi(28) = (2^2 - 2^1)(7-1)$

$= 2 \times 6 = 12$ generators

how many bases have cycle length 14 $\longrightarrow \phi(14) = (2-1)(7-1) = 6$

$$\sum_{d \mid (p-1)} \phi(d) = p-1$$

$d \mid (p-1)$

$d \in$ Prime

$\phi(4) = (2^2 - 2) = 2$

$\phi(7) = (7-1) = 6$

$\phi(2) = (2-1) = 1$

$\phi(1) = 1$

Discrete Log in $\sqrt{p}$ time

Req DiscLog

```
                    base  ans  mod
int  discLog(int b, int y, int p)  {
     int ans=1;
     for (int i=0; i<p; i++) {
          if (ans == y) return i;
          ans = (ans*b) %p;
     }
```

O(p)

---

p=29

base $\sqrt{p}$ ish

$g^a = g^{6x+y}$ ← $6x+y$

$0 \le x < 5$

$0 \le y \le 5$

$= g^{6x-y}$ } can do + or − smaller term!

Calculate $g^6, g^{12}, g^{18}, g^{24}, g^{30}$] run time is $O(\sqrt{p})$

Store answers in a table

$g^6 \to 6$

$g^{12} \to 7$

$g^{18} \to 13$

$g^{24} \to 20$

$g^{30} \to 4$

$2^{16} \equiv 25 \mod 29$

$2^{6x} \cdot 2^{y} \equiv 25 \mod 29$

~~$25^{-1}\ 2^{6x} \cdot 2^{y} \equiv 1 \mod 29$~~

$$2^{6x} \cdot 2^{y} \equiv 25 \mod 29$$

$$2^{-y} \times 2^{6x} \times 2^{y} \equiv 25 \times 2^{-y} \mod 29$$

$$2^{6x} \equiv 25 \times 2^{-y} \mod 29$$

MAP

6 → 6
7 → 12
13 → 18
20 → 24
4 → 30

COM

$2^{y} \cdot 2^{6x} \cdot 2^{-y} \equiv 2^{y} 25 \mod 29$

$2^{6x} \equiv 2^{y} \cdot 25 \mod 29$

$y=0 \rightarrow 25$

$y=1 \rightarrow 50 \equiv 21 \mod 29$

$y=2 \rightarrow 42 \equiv 13$

$2^{18} \equiv 2^{2} \times 2^{5} \mod 29$

$18-2=16$