CIS 3362 10/24/22

Discrete Log Problem
Typed Notes Added!

reg log

$2^5 = 32 \longleftrightarrow \log_2 32 = 5$

exp func inv exp

What power do I raise 2 to, to obtain 32?

$2^x = 32$ What is x?

Assuming $b > 1$, if $x < y$, then $\log_b x < \log_b y$.

Goal: Calc $\log_2 128$, and I find out that $\log_2 32 = 5$, then I know my ans > 5.

* We can solve for a regular log quickly!

Discrete Log Problem

$2^x \equiv 3 \pmod{11}$ What is x?

ans = 8

exp	0	1	2	3	4	5	6	7	8	9	10
$2^{exp} \bmod 11$	1	2	4	8	5	10	9	7	3	6	1

(almost a permutation random of 1 to 10.)

NO SIMPLE PATTERN!

$10^{exp} \bmod 11$	1	10	1	10	1	10	...

$$10^x \equiv 3 \pmod{11} \ ?$$

No answer!

Not a good base because many "answers" aren't possible.

For each possible base $(1, 2, 3, \ldots p-1)$ we know by Fermat's $b^{p-1} \equiv 1 \pmod p$
But for some bases $\exists x \mid x < p-1, x > 0$ and $b^x \equiv 1 \pmod p$.

Define term: primitive root / generator is a value b such that the ~~min~~ minimum positive integer x such that $b^x \equiv 1 \pmod p$ for a prime p is $x = p - 1$.

(1) Generate Program to list each base to each power for a prime
→ look table pick out primitive roots

(2) Assuming 1 primitive root exists, we'll count the # of primitive roots

(3) Write program to generate all the primitive roots (OR test if a value is a primitive)

ord(b) mod p is min value of x s.t. $b^x \equiv 1 \pmod{p}$.

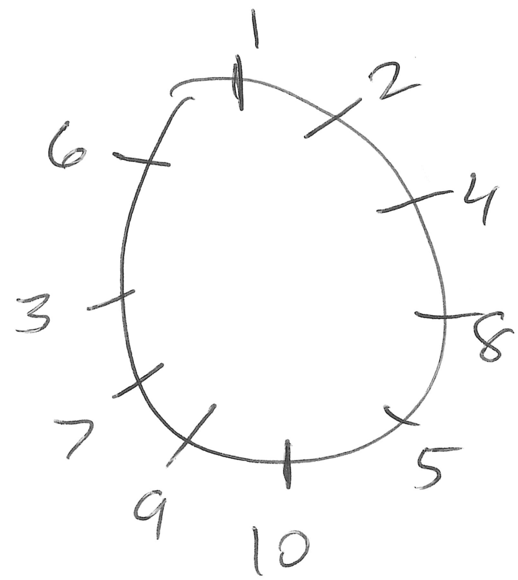
if ord(b) = p−1, it's a primitive root

$$4^3 = (2^2)^3 = 2^6$$

so row for 4 is skipping every other item on the row for 2.

$2^3 = 8$, so 8^k will be skipping 2 items.

So modular exponentiation is like running around a track 2^x



every running around goes k notches each second $1 \leq k \leq 10$. If $\gcd(k, 10) \neq 1$, then we'll never visit all notches.

\# of primitive roots = # ints 1 to p−1 that are relatively prime to p−1. = $\phi(p-1)$.

~~write~~

How to test for a primitive root

$p = 17$

$p-1 = 16$

$= 2^4$

✓ $b^{\frac{16}{2}} \not\equiv 1 \bmod p$

$p = 37$

$p-1 = 36 = 2^2 \cdot 3^2$

$b^{\frac{36}{2}} \not\equiv 1 \bmod p$ and

$b^{\frac{36}{3}} \not\equiv 1 \bmod p$

find each unique prime divisor of $p-1$

$q_1, q_2, \ldots q_k$

if $b^{\frac{p-1}{q_i}} \not\equiv 1 \bmod p$ for each $1 \le i \le k$, then b is a primitive root.