CIS 3362
~~COT 3100~~ 10/21/24

Discrete Log Problem

- $a^b = x$, given a and x find b
  - $2^b = 64$ what is b?
    - $b = 6$
  - $b = \log_a x$, by definition

$$a^b \equiv x \pmod n$$

- Given a, x and n, what is b?
  - Discrete Log Problem

Regular log function if $\log_a x < \log_a y$ then $x < y$. Similarly if $x < y$, then $\log_a x < \log_a y$, assuming $a > 1$.

Let's look at exponents under mod
$n = 11$ $a = 3$

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

If you do this with many examples the answer (bottom row) seem to defy any pattern at least in their order.

If n is prime, $a^{n-1} \equiv 1 \pmod{n}$ if $\gcd(a,n)=1$.

Given any prime p, and any base a, $1 \le a \le p-1$ the cycle size of a^x as $x = 0, 1, 2, \ldots$ must divide evenly into $p-1$.

exp	0	1	2	3	4	5	6	7	8	9	10
2^x	1	2	4	8	5	10	9	7	3	6	1

every int from 1 to $p-1$ appears once in a random permutation here, then it'll repeat.

$3^x \equiv 2 \pmod{11}$ → NO ANS

$2^x \equiv 6 \pmod{11}$ → min + ans = 9

↳ for all ints 1 to $p-1$ we could put here, there's an answer!

For a prime p, and an int a, $1 < a < p-1$ such that the smallest positive integer k for which $a^k \equiv 1 \bmod p$ is $k = p-1$, we will call a either a generator mod p or a primitive root mod p.

All odd primes p have at least 1 generator/primitive root a, $1 \leq a \leq p-1$.

Given the result above, prove that a prime p has exactly $\phi(p-1)$ primitive roots.

Other problem hmk asks you to investigate the lengths of all the cycles for each base mod a prime.

Given a primitive root a of a prime p and a value x, it's difficult to determine the int b, $0 \leq b \leq p-1$ such that $a^b \equiv x \pmod{p}$.

Multiple Public Key Cryptosystems security is based on the fact that the Discrete Log Problem is Intractable. (not solvable in a reasonble amt of time) depends on size of prime...

Speeding Up Brute Force (a little bit) to Solve Discrete Log upto 10^{12} pretty quickly

$$base^{exp} \equiv ans \mod p$$

let m be an integer a bit bigger than $\sqrt{p}$

$p = 10007$

$m = 101$

$$base^{101x+y} \equiv ans \mod p$$

$$\frac{base^{101x}}{base^{y}} \equiv ans \mod p$$

$base^{101\times 55} \equiv base \times ans$

$base^{101\times 55 - 1} \equiv ans$

mod inv

$$base^{101x} \equiv base^{y} \times ans \mod p$$

exist x, y with $x \le 101$, $y \le 100$ to solve this

table

$y = 0$ $base^{y} \times ans = 6782$

$y = 1$ $base^{y} \times ans = 7133$

891

$\vdots$

$y = 100$

$m - 1$

Run time ~ 100 steps

$O(m)$ steps

MAP

$6782 \to 0$

$7133 \to 1$

$891 \to 2$

$\vdots$

$x = 55$

$\downarrow$

7133

$O(m)$

successively plug in $x = 0, 1, 2, \ldots$

$base^{101\cdot 0}$

$base^{101}$

$base^{100\cdot 1}$

each look up in the map if that ans exist

Total Run Time $O(m) + O(m) = O(m)$

$m \sim \sqrt{p}$. $O(\sqrt{p})$ is faster than brute force $O(p)$...

Solve by hand $27^x \equiv 19 \pmod{29}$

Note: $27 \equiv -2 \pmod{29}$

$$27^{6a+b} \equiv 19 \pmod{29}$$

$$27^{6a} \equiv 27^b \times 19 \pmod{29}$$

$(-2)^{6a}$

64^a

6^a

$a = 0 \rightarrow 1$

$a = 1 \rightarrow 6$

$a = 2 \rightarrow 36 \rightarrow 7$

$a = 3 \rightarrow 7 \times 6 \rightarrow 42 \rightarrow 13$

$a = 4 \rightarrow 6 \times 13 \rightarrow 78 \rightarrow 20$

b	$27^b \times 19$
0	19
1	$(-2) \times 19 = -38 = 20$
2	$4 \times 19 = 18$
3	$-8 \times 19 = -8 \times (-10) = 80 = 22$
4	$16 \times 19 = 16 \times (-10) = -160 = 14$
5	$-32 \times 19 = (-3) \times 19 = -57 = 1$

58
76
-58

$19 \rightarrow 0$

$20 \rightarrow 1$

$18 \rightarrow 2$

$22 \rightarrow 3$

$14 \rightarrow 4$

$5 \rightarrow 1$

$27^{24} \equiv 27^1 \times 19 \bmod 29$

$27^{23} \equiv 19 \bmod 29$