CIS 3362 10/26/26

1) Miller-Rabin Code Up
2) Discrete Log Problem
3) Generators

Miller-Rabin

test n see if it's prime

Compute $a^{n-1} \bmod n$

Pick a randomly

Pick a randomly $1 < a < n$

if $\gcd(a,n) \neq 1$, then ~~not prime~~ composite

if $a^{n-1} \not\equiv 1 \bmod n \rightarrow n$ is composite!

Carmichael Numbers pass this test so we need to do something different to mark these as composite

$$n-1 = 2^m x, \quad x \in \text{Odd}$$

Compute $y = a^x \bmod n$

if this equals $1 \rightarrow$ "is prob prime"

Otherwise compute $y, y^2, y^4, y^8, \ldots y^{n-1}$

$$\underbrace{a^x, a^{2x}, a^{4x}, \ldots a^{2^m x}}_{m+1 \text{ terms}}$$

if $a^x \not\equiv 1 \bmod n$, then if n is prime -1 must appear in the sequence

$$x^2 \equiv 1 \mod p$$

$$(x^2-1) \equiv 0 \mod p$$

$$(x-1)(x+1) \equiv 0 \mod p$$

$p \mid (x-1)$ or $p \mid (x+1)$

only if $x = 1$

$x+1 \equiv 0 \mod p$

$x \equiv -1 \mod p$

Discrete Log Problem

Regular log $\log_2 64 = ?$

Solve for x in the equation $2^x = 64$.

Inverse function of the exponential function $f(2,6) = 64$ $f^{-1}(2,64) = 6$.

$2^x \equiv 3 \mod 101$ → only look @ PRIMES

What is x?

Let's make a table but for smaller values $p = 29$

$3^x \equiv 7 \mod 17$ What is x?

Since the minimum positive value of x for which $3^x \equiv 1 \bmod 17$ is $x = 16$, x is a generator / primitive root mod 17.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3^x \bmod 17$	1	3	9	10	13	5	15	~~6~~ 11	16	14	8	7	4	12	2	~~6~~ 6	1

$3^6 \equiv 15 \bmod 17$

$3^7 \equiv 15 \times 3 \equiv (-2) \times 3 \equiv -6 \equiv 11 \bmod 17$

$3^8 = 11 \times 3 \equiv 33 \equiv 16 \bmod 17$

FOR all generators $g \bmod p$,

$$g^{\frac{p-1}{2}} \equiv -1 \bmod p$$

a generator mod p shuffles the values from 1 to $p-1$ in the list

$g^0, g^1, g^2, g^3, \ldots g^{p-2}$ in a random order

ONE-WAY FUNCTION - EASY COMPUTE FORWARDS, HARD TO UNDO!

Brute Force algorithm to compute discrete log runs in $O(p)$ time p is prime.

Improve to run in $O(\sqrt{p})$ time using $O(\sqrt{p})$ memory.

$$2^x \equiv 53 \pmod{101}$$

$\sqrt{101} \sim 10.\overline{2} \rightarrow 11$

(a) Compute $\lceil$sqrt of $p\rceil$ $x = \lceil\sqrt{p}\rceil$.

(b) Table of the list

$2^x, 2^{2x}, 2^{3x}, \ldots 2^{x^2} \pmod{p}$

2^{11}

2^{22}

$2^{33} \equiv 35 \pmod{101}$

2^{99}

2^{110}

y	2^y
0	1
1	2
2	4
3	8
⋮	
6	64
7	27

$2^{-y} \cdot 2^{33} \equiv 2^{y} \cdot 53 \equiv 53 \pmod{101}$

$2^{-y} \times 35 \equiv 53 \pmod{101}$

$2^{y} \cdot 2^{-y} \times 35 \equiv 2^{y} \cdot 53 \pmod{101}$ → Create lookup chart $y = 0, 1, 2, \ldots 10$

$35 \equiv 2^{y} \times 53 \pmod{101}$

$(53^{-1} \bmod 101) \times 35 \equiv 2^{y} \times 53 \times (53^{-1} \bmod 101)$ → $b^{-1} \bmod p$

$2^{y} \equiv 35 \times (53^{-1} \bmod 101)$ → $2^x \bmod p$

y chart

$1 \to 0$
$2 \to 1$
$4 \to 2$
$8 \to 3$
$16 \to 4$
$32 \to 5$
$64 \to 6$
$27 \to 7$
⋮

$1^x \equiv 3 \mod 101$

DUH NO SOLS

Order of $a \mod p$ is minimum value of x such that $x > 0$ and $a^x \equiv 1 \mod p$

↳ all orders are divisors of $p-1$

* Exercise: figure out HOW MANY values of a have each different ORDER.