CIS 3362 10/15/25

Fermat Test for Primality

based on Fermat's Thm

if $\gcd(a,p) = 1$, $a^{p-1} \equiv 1 \bmod p$

$p \in$ Prime.

Idea: if n isn't prime, usually $a^{n-1} \not\equiv 1 \bmod n$

pick random a, calculate $a^{n-1} \bmod n$

if ans $\neq 1$, retrn composite

else retrn is probably prime.

TO IMPROVE - REPEAT k times (50-100)

ISSUE is Carmichael #s (composites, n, such that if $\gcd(a,n)=1$, then $a^{n-1} \equiv 1 \bmod n$.

Miller-Rabin

Noticed for primes if you take any base and do repeated exponentiation, specifically squaring: $a^{p-1}, a^{\frac{p-1}{2}}, a^{\frac{p-1}{4}}, a^{\frac{p-1}{8}}, \ldots a^{\left(\frac{p-1}{2^k}\right)}$

mult exp by 2

$a = 2$

$p = 97$

$a^{96} = \left(a^{48}\right)^2$

a^3 a^6 a^{12} a^{24} a^{48} a^{96}

8 64 22 -1 1 1 mod 97

96

$97 - 1 = 96 = 2^5 \cdot 3$

$a^{48} \equiv 1 \bmod 97$

$a^{48} - 1 \equiv 0 \bmod 97$

$(a^{24}-1)(a^{24}+1) \equiv 0 \bmod 97$

$\rightarrow 97 \mid (a^{24}-1)$ or $97 \mid (a^{24}+1)$

because 97 ∉ prime

$a^{24} \equiv 1 \bmod 97$ or $a^{24} \equiv -1 \bmod 97$

NOT TYPICALLY TRUE OF CARMICHAEL #S

Basic MillerRabin (BigInteger n)

1. Pick random a, $1 < a < n-1$

k=0
while e%2==0:
k++;
e=e/2

2. $n-1 = 2^k \cdot m$, $m \in$ odd

3. Calculate $a^m \bmod n$
if ans = 1, return "is prob prime"

4. Let CUR = $a^m \bmod n$
for (i = 0; i < k; i++)
CUR = (CUR * CUR) % n] squaring
if CUR == -1 (n-1)
return is Probably Prime

5. If we get here it's COMPOSITE

If we run once will be correct at least 75% of the time.

Repeat 50-100 times with different choices of a

Prob failure $1-\left(\frac{1}{4}\right)^r$, r = # repeat test

Discrete Log Problem

Modular Expo

$a^1, a^2, a^3, a^4 \ldots$ Creating this list

Input: a, base
e exp
p prime

Calculate $Y = a^e \bmod p$

Inverse Problem: Given Y ans pepix
Given a base
Given p mod

What is the value of e such that

$$a^e \equiv Y \bmod p ?$$

THIS IS the discrete log problem.

In reals log is inverse of exp

$exp(2,6) = 64$

$\hookrightarrow \log_2 64 = 6$

$exp(3,4) = 81, \hookrightarrow \log_3 81 = 4$

→ NO ONE KNOWS A FAST WAY TO DO THIS!

Example tried $p = 29$

Printed $a^0, a^1, a^2, \ldots a^{27}$ for all a

$a \in \{2, 3, 4, \ldots 27\}$

Noticed: Some row are a permutation of

$1, 2, 3, \ldots, 28$

Other rows repeat a cycle of 14 or 7 or 4 numbers.

$a^{28} \equiv 1 \mod 29$

Freranet

So all cycle sizes MUST divide evenly into $p-1 = 28$.

The values for a which produce a row that is a permutation of 1 to $p-1$ are called primitive roots, they are also called generators.

By inspection 27 is a generator mod 29

Min of $m > 0$ for which $27^m \equiv 1 \mod 29$ is $m = 28$.

$(27^4)^7 \equiv 27^{28} \equiv 1 \mod 29$ so

27^4 is NOT a generator

27^b will not be a generator if $\gcd(b, 28) \neq 1$.

$(27^{(6)14}) \equiv (27^{28})^3 \equiv 1 \mod 29$

Thus, given that 27 is a generator mod 29 we can get all other generators by calculating

27^b where $\gcd(b, 28) = 1$.

The number of generators mod p is $\phi(p-1)$, which is the # of integers in $\{1, 2, \ldots p-1\}$ that are relatively prime to $p-1$.

$$\phi(28) = \phi(2^2)\phi(7) = (2^2 - 2)(7-1)$$
$$= 2 \times 6$$
$$= 12$$

$27^{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27}$