CIS 3362 - 10/16/23

Primality Testing : Miller-Rabin Primality Test

Orig alg - trial division $O(\sqrt{n})$, but if $n \sim 10^{200}$, this isn't viable!!!

Properties of prime #s.

Fermat's Thm if p prime $\gcd(a,p)=1$, then $a^{p-1} \equiv 1 \pmod{p}$

If n is composite a^{n-1} frequently $\not\equiv 1 \pmod{n}$

BASIC IDEA

1. pick random a
2. calc $a^{n-1} \bmod n$
3. if ans $\neq 1 \Rightarrow$ COMPOSITE
   else $\Rightarrow$ "PROBABLY PRIME"

HOW TO IMPROVE

If prob given a comp int that $a^{n-1} \equiv 1 \pmod{n}$ $\leq 50\%$

why not test a bunch of different values of a?

IMPROVED IDEA

Repeat 100 times:

pick random a $(2 \le a \le n-2)$ → if $\gcd(a,n) \ne 1$ return COMPOSITE

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

if ans $\ne 1$

return COMPOSITE

return "PROBABLY PRIME"

pretty close to the MILLER-RABIN PRIMALITY TEST

Special #s called Carmichael #s.

(1) Composite

(2) if $\gcd(a,n)=1$ $a^{n-1} \equiv 1 \pmod n$

Carmichael # would almost always "appear prime" to our primality test.

If n is actually prime, we know that $a^{n-1} \equiv 1 \bmod n$ and that the cycle size for exponentiating a divides evenly into $n-1$.

$1^2 = 1$, but also $(-1)^2 = 1$

Imagine calculating $a^{n-1}, a^{\frac{n-1}{2}}, a^{\frac{n-1}{4}}, a^{\frac{n-1}{8}}, \ldots$ (if n is prime there's a good chance we'll see a -1 in this chain

$\boxed{1} \quad \boxed{1} \quad \boxed{1} \quad \boxed{-1}$

Miller Rabin says:

when testing n for primality

first rewrite $n-1 = 2^k m$, $m \in$ Odd

Repeat 100 times:

Choose random a $2 \le a \le n-2$

Compute $b = a^m \bmod n$

if $b == 1$ continue → comp = true

for ($i = 0$; $i < k$; i++)

if $b == -1$ ($n-1 \bmod n$)

break; → comp = false

else

$b = (b * b) \bmod n$ // squares b

this never happens most of the time for the carmichael #s

* ~~Re~~ if comp return COMPOSITE

---

return PROBABLY PRIME

Run Miller Rabin for

$n = 561$

$n-1 = 560 = 8 \times 70 = 16 \times 35 = 2^4 \times 35$

$k=4, \, m=35$

pick $a = 7$

Calculate

$k = 0$ to 4

$7^{35} \bmod 561 \rightarrow 241$

$7^{70} \equiv 241^2 \bmod 561 \rightarrow 298$

$7^{140} \equiv 298^2 \bmod 561 \rightarrow 166$

$7^{280} \equiv 166^2 \bmod 561 \rightarrow 67$

$7^{560} \equiv 67^2 \bmod 561 \rightarrow 1$

$n = 37$

$n-1 = 36 = 2^2 \times 9$

$a = 5$

1. $5^9 \bmod 37 = 6$ ✓
2. $5^{18} = 6^2 \bmod 37 = 36 \equiv -1 \bmod 37$

   passes
3. $5^{36} = (-1)^2 \bmod 37 = 1$

Prob Success $\geq 1 - \left(\frac{1}{2}\right)^{100}$

quite good!