AMRITA VISHWA VIDYAPEETHAM

RABIN-MILLER THEOREM

FROM TEAM

Introduction:

This algorithm determines whether a given integer has a high probability of being prime. Here, we use a randomised approach. Specifically, the Miller-Rabin Test, which successfully identifies primes from composites with a high amount of accuracy. It can be included into a variety of RSA encryption-based software programmes.

This algorithm shows us the actual test on all inputs except a small set of bad composite numbers, namely, Carmichael Numbers. On all other inputs, it replicates the performance of the actual Miller–Rabin Test.

Theorem:

The MILLER-RABIN ALGORITHM for **Composites** is a yes-biased Monte Carlo algorithm.

PROOF We will prove this by assuming that Algorithm 6.7 answers "n is composite" for some prime integer n, and obtain a contradiction. Since the algorithm answers "n is composite," it must be the case that $a^m \not\equiv 1 \pmod{n}$. Now consider the sequence of values b tested in the algorithm. Since b is squared in each iteration of the **for** loop, we are testing the values $a^m, a^{2m}, \ldots, a^{2^{k-1}m}$. Since the algorithm answers "n is composite," we conclude that

$$a^{2^i m} \not\equiv -1 \pmod{n}$$

for $0 \leq i \leq k-1$.

Now, using the assumption that n is prime, Fermat's theorem (Corollary 6.6) tells us that

$$a^{2^k m} \equiv 1 \pmod{n}$$

since $n-1 = 2^k m$. Then $a^{2^{k-1}m}$ is a square root of 1 modulo n. Because n is prime, there are only two square roots of 1 modulo n, namely, $\pm 1 \bmod n$. We have that

$$a^{2^{k-1}m} \not\equiv -1 \pmod{n},$$

so it follows that

$$a^{2^{k-1}m} \equiv 1 \pmod{n}.$$

Then $a^{2^{k-2}m}$ must be a square root of 1. By the same argument,

$$a^{2^{k-2}m} \equiv 1 \pmod{n}.$$

Repeating this argument, we eventually obtain

$$a^{m} \equiv 1 \pmod{n},$$

Algorithm:

write $n-1=2^k m,$ where m is odd
choose a random integer $a, 1 \le a \le n-1$
$b \leftarrow a^m \bmod n$
if $b \equiv 1 \pmod{n}$
  then return ("n is prime")
for $i \leftarrow 0$ **to** $k-1$

$$\textbf{do}\ \begin{cases} \textbf{if}\ b \equiv -1 \pmod{n} \\ \quad \textbf{then return}\ (\text{“}n \text{ is prime”}) \\ \quad \textbf{else}\ b \leftarrow b^2 \bmod n \end{cases}$$

return ("n is composite")

EXAMPLE 1:

n = 29

n-1 = 28

$\Rightarrow \left(\frac{28}{2^1}\right) = 14$

$\Rightarrow \left(\frac{28}{2^2}\right) = 7$

$\Rightarrow \left(\frac{28}{2^3}\right) = 3.5$ (not a whole number)

$\Rightarrow 28 = (2^2)\,(7)$

m=7 (ODD), k=2

1 =< a =< n- 1

Consider **a = 5**

$$\boldsymbol{b \cong a^m (mod\, n)}$$

$$b \cong 5^7\ (mod\ 29)$$

$$\cong 5(25)^3\ (mod\ 22)$$

$$\cong 5(-4)^3$$

$$\cong -20(16)\ (mod\ 29)$$

$$\cong 28\ mod(\ 29)$$

$$\cong -1\ mod(29)$$

Therefore, b ≅ -1

So, the number is Prime

EXAMPLE 2:

n=71

n-1 = 70

$\Rightarrow \left(\frac{70}{2^1}\right) = 13$

$\Rightarrow \left(\frac{70}{2^2}\right) = 17.5$ (not a whole number)

$\Rightarrow 70 = (2)^1\,(35)$

k=1, m=35

1 =< a =< n- 1

⇒ 1 =< a =< 70

Consider **a=5**

$\boldsymbol{b \cong a^m (mod\ n)}$

$b \cong (5^{125})\ (mod\ 71)$

$\cong (25)(54)^{11}\ (mod\ 71)$

$\cong (25)(54)(-17)^{10}\ (mod\ 71)$

$\cong (25)(54)(289)^5\ (mod\ 71)$

$\cong (125)(54)(25)^2\ (mod\ 71)$

$\cong (125)(54)(289)^5\ (mod\ 71)$

$\cong (25)(54)(25)^2\ (mod\ 71)$

$\cong (54)(54)(25)^2\ (mod\ 71)$

$\cong (289)(25)^2\ (mod\ 71)$

$\cong (5)(25)^2\ (mod\ 71)$

$\cong (5)(625)\ (mod\ 71)$

$\cong (5)(57)\ (mod\ 71)$

$\cong 285\ (mod\ 71)$

$\cong 1\ (mod\ 71)$

Therefore, b=1

So, the number is Prime.

EXAMPLE 3:

n=27

n-1 = 26

$\Rightarrow \left(\frac{26}{2^1}\right) = 18$

$\Rightarrow \left(\frac{26}{2^2}\right) = 7.5$ (not a whole number)

$\Rightarrow$ 26 = (2)(13)

k=1, m=13

1 =< a =< n- 1

$\Rightarrow$ 1 =< a =< 26

Consider **a = 12**

$\boldsymbol{b \cong a^m (mod\ n)}$

$b \cong (12)(144)^6\ (mod\ 27)$

$\cong (12)(9)^6\ (mod\ 27)$

$\cong (12)(81)^3\ (mod\ 27)$

$\cong (12)(0)\ (mod\ 27)$

$\cong 0\ (mod\ 27)$

So, the number is Composite

Verification:

27 = 3 x 3 x 3 x 1 = 27 x 1

This has more than "2" factors

So, the number is a composite number.

EXAMPLE 4:

n = 561

n-1 = 560

$$\Rightarrow \left(\frac{560}{21^1}\right) = 280$$

$$\Rightarrow \left(\frac{560}{2^2}\right) = 140$$

$$\Rightarrow \left(\frac{560}{2^3}\right) = 70$$

$$\Rightarrow \left(\frac{560}{2^4}\right) = 35$$

$$\Rightarrow \left(\frac{560}{2^5}\right) = 17.5 \text{ (not a whole number)}$$

$$\Rightarrow 560 = (2^4)(35)$$

k=4, m=35(odd)

1 <= a <= n-1

Consider **a=5**

$$\boldsymbol{b = a^m (mod\ n)}$$

$$\cong (5)^{35}\ (mod\ 561)$$

$$\cong (5)^3 (5^4)^8\ (mod\ 561)$$

$$\cong (5)^3 (625)^8\ (mod\ 561)$$

$$\cong (125)(64)^8\ (mod\ 561)$$

$$\cong (125)(169)^4\ (mod\ 561)$$

$$\cong (125)(511)^2\ (mod\ 561)$$

$$\cong (125)(256)\ (mod\ 561)$$

$$\cong 23\ (mod\ 561)$$

CONTINUED…

Since, b is not congruent to 1 (mod 561)

We go into the loop

$$\Rightarrow \mathrm{b1} \cong (23)^2 \ (mod\ 561)$$

$$\cong (-32)(mod\ 561)$$

$$\Rightarrow b2 \cong (-32)^2 \ (mod\ 561)$$

$$\cong (-98)(mod\ 561)$$

$$\Rightarrow b3 \cong (-98)^2 \ (mod\ 561)$$

$$\cong (67)\ (mod\ 561)$$

$$\Rightarrow b4 \ \cong (67)^2 \ (mod\ 561)$$

$$\cong 1\ (mod\ 561)$$

According to algorithm the loops are over and the answer (b4) says it is a composite number.

On Fernet's Theorem $a^{p-1} \cong 1 \ (mod \ p)$; p = prime

1 <= a <= n-1

a = 5

$$5^{560} \cong 1 \, mod(561)$$

From this we can say that 561 is prime but we know that 561 is composite. So, this is a contradiction.

THANK YOU!!