SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

AN AUTONOMOUS INSTITUTION

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

UNIT 3

Prime numbers have fascinated mathematicians and more generally curious minds for thousands of years. What is a prime number? Well, 2, 3, 5, 7, 11, 13, . . . , 9973 are prime numbers. The defining property of a prime number p is that it is a positive integer $p \geq 2$ that is only divisible by 1 and p. Equivalently, p is prime if and only if p is a positive integer $p \geq 2$ that is not divisible by any integer m such that $2 \leq m < p$. A positive integer $n \geq 2$ which is not prime is called composite. Observe that the number 1 is considered neither a prime nor a composite. For example, $6 = 2 \cdot 3$ is composite. Is 3 215 031 751 composite? Yes, because 3 215 031 751 = 151 · 751 · 28351.

FERMAT TESTING

Some of the **proofs of Fermat's little theorem** given below depend on two simplifications.

The first is that we may assume that *a* is in the range $0 \leq a \leq p - 1$. This is a simple consequence of the laws of modular arithmetic; we are simply saying that we may first reduce *a* modulo *p*. This is consistent with reducing modulo *p*, as one can check.

Secondly, it suffices to prove that

for *a* in the range $1 \leq a \leq p - 1$. Indeed, if the previous assertion holds for such *a*, multiplying both sides by *a* yields the original form of the theorem,

On the other hand, if $a = 0$ or $a = 1$, the theorem holds trivially.

Fermat's Little Theorem:

If n is a prime number, then for every a, 1 < a < n-1,

$\mathbf{a^{n-1 \equiv 1\ (mod\ n)}}$

OR

$\mathbf{a^{n-1}} \% n = 1$

Example: Since 5 is prime, $2^4 \equiv 1 \pmod 5$ [or $2^4 \% 5 = 1$],
$3^4 \equiv 1 \pmod 5$ and $4^4 \equiv 1 \pmod 5$

Since 7 is prime, $2^6 \equiv 1 \pmod 7$,
$3^6 \equiv 1 \pmod 7$, $4^6 \equiv 1 \pmod 7$
$5^6 \equiv 1 \pmod 7$ and $6^6 \equiv 1 \pmod 7$

If a given number is prime, then this method always returns true. If the given number is composite (or non-prime), then it may return true or false, but the probability of producing incorrect results for composite is low and can be reduced by doing more iterations.

Below is algorithm:

```
// Higher value of k indicates probability of correct
// results for composite inputs become higher. For prime
// inputs, result is always correct
1)  Repeat following k times:
      a) Pick a randomly in the range [2, n - 2]
      b) If gcd(a, n) ≠ 1, then return false
      c) If $a^{n-1}$ &nequiv; 1 (mod n), then return false
2) Return true [probably prime].
```

Miller Rabin Algorithm:

Miller Rabin is a fast approach to test primality of the large numbers. This algorithm is called a Rabin-miller primality test and this algorithm decides whether number is prime which is same to other tests including Fermat primality Test and Solovay- Strassen primality test.

This test is based on equality or group of equalities that hold the true for prime values, thus checks whether they hold for the number, that it is required to test for primality.

This algorithm is most useful known primality testing algorithm and can be used in different software libraries that based on RSA encryption and best instance is OpenSSL.

Miller Rabin validate that the number is composite. So this is called compositeness test rather than primality test. The miller Rabin test identify all composites. For each composite number n, there can be at least 3/4 (Miller Rabin) of numbers a are witnesses of compositeness of n.

Miller Rabin is associatively simple extension of Fermats little Theorem that enable us to test for primality with a much larger probability than Fermats little theorem.

Algorithm : Pseudocode for Miller-Rabin test −

```
Miller-Rabin-Test (n, a) // n is the number; a is the base{
  Find m and k such that $n − 1 = m x 2^k$
  T ← $a^m$ mod n
  If (T = ±1)return "a prime"
  for (i ← 1 to k − 1) // k – 1 is the maximum number of steps{
    T ← $T^2$ mod n
    if (T = ±1) return "a composite"
    if (T = −1) return "a prime"
  }
  return "a composite"
}
```

There ex$_i$sts a proof that each time a number passes a Miller-Rabin test, the probability that it is not a prime is ¼. If the number passes m tests (with m different passes), the probability that is not a prime is $(1/4)^m$.

Example: Apply Miller-Rabin Algorithm using base 2 to test whether the number 341 is composite or not.

Solution: Using Miller-Rabin Algorithm, we can test the number 341 as follows −

Step1: $341 - 1 = 2^2 \times 85$. Thus $p = 341$, $k = 2$ and $q = 85$

Step2: $x = 2$ (given)

Step3: $S = x^q \bmod p$

$= 2^{85} \bmod 341 = (2^{10}) \times 2^5 \bmod 341$ 8

$= 2^{10} \bmod 341 \times 2^{13} \bmod 341$

$= 1 \times 8192 \bmod 341 = 8192 \bmod 341$

$= 8$

Step4: As $8 \neq 1$, we move to the next step.

Step5: For $j = 1$, $S = x^{2q} \bmod p$

$= 2^{170} \bmod 341 = (2^{20})^8 \times 2^{10} \bmod 341$

$= 2^{20} \bmod 341 \times 2^8 \bmod 341 \times 2^{10} \bmod 341$

$= 1 \times 256 \times 1 = 256$

Now, $= 256 \neq 1$

and result is inconclusive

So, 341 is not a composite number.

Advantages

- This Algorithm can be used to test high numbers for primality.
- Because of its advantage in speed when compared to other primality tests, Miller Rabin test will be the test of choice for several cryptographic applications.
- When compared to Euler and Solovay-Strassen tests, Miller Rabin is more dynamic and essential aspect is that the probability of failure is decreased.
- According to the fermat test there are too many liars for all Carmichael numbers n, the error probability is near to 1, this disadvantage is prevented in Miller Rabin.