# Implementation of Miller Rabin Primality Test

R Siva Girish
*Computer Science*
*PES University*
PES1201700159
sivagirish81@gmail.com

***Abstract***

Miller-Rabin primality test is a probabilistic test statistic for determining whether a number is prime or not. Miller Rabin Test will always conclude accurately that a number is composite but does end up giving a few false positives in very rare situations.Especially in cases where the algorithm is run for very few iterations.

***Keywords***

*Miller-Rabin; Prime; Composite; modulus; Power; Iterations; Strong Liars;*

## I. Problem Statement

The Problem at hand is to develop the Miller-Rabin Primality test and measure its accuracy.

## II. Implementation

To implement Miller Rabin we take the input number and fix the number of iterations we intend to use in order to check for primality.

- ISPrime(n,k) : We run miller test on n, k number of times to check for primality.In the process we calculate the values of d and r as well.If the number n is even then directly return composite provided the number is not equal to 2.

  $$n - 1 = 2^r * d$$

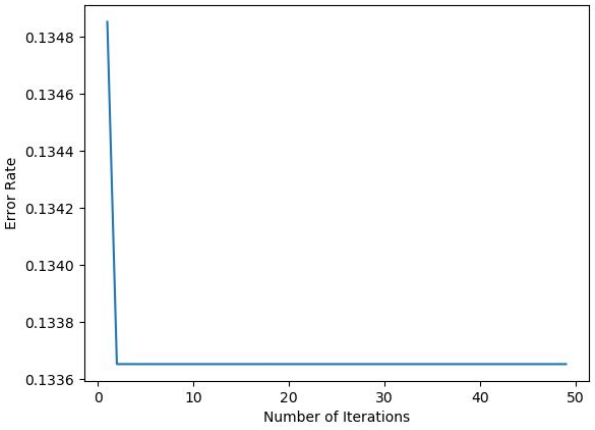
- Miller(d,n,r) : Generate a random number within the range 2 to n-2.Find the value of x such that x :

  $$x = (a^d \% n)$$

  If x is either 1 or n -1 then the number could be prime else return composite.Run the loop r - 1 times and keep squaring x in the process and modding it with n.

- Plot graphs for the results obtained from Miller Rabin test.We take a dataset consisting of all the prime numbers within the range(0, 5000).Run Miller Rabin on first 5000 numbers and plot the error percentage for varied number of iterations.

## III. Analysis




From the above plot it can be inferred that whenever the number of iterations is low the error rate is high and the error rate is almost negligible as the number of iterations is more than around 4.Four iterations would be a good heuristic to set as the number of iterations for determining whether a number is prime or not.

This particular trend can be explained on the basis that whenever the number of iterations is less there is a high chance that the random number generated can be a strong liar for the chosen number and hence it is incorrectly flagged as a prime.Hence the need for multiple iterations in Miller Rabin test for primality.

## IV. Conclusion

Hence we can conclude that the accuracy of rabin miller test for primality is heavily dependent on the number of iterations used . It is a very rare case when the random number generator generates all strong liars for a particular number therefore for higher number of iterations the error rate will be minimal and hence the number can be considered as prime if predicted so by Rabin Miller test.