Miller-Rabin Primality Test

Hitesh Kumar
PES1201701511
PES University
Bangalore , India
hiteshkumarhk.info@gmail.com

***Abstract*—A primality test is a test to determine whether or not a given number is prime, as opposed to actually decomposing the number into its constituent prime factors. The major application of prime numbers are that they are used in cryptography. One of the standard cryptosystem - RSA algorithm uses a prime number as key which is usually over 1024 bits to ensure greater security.**

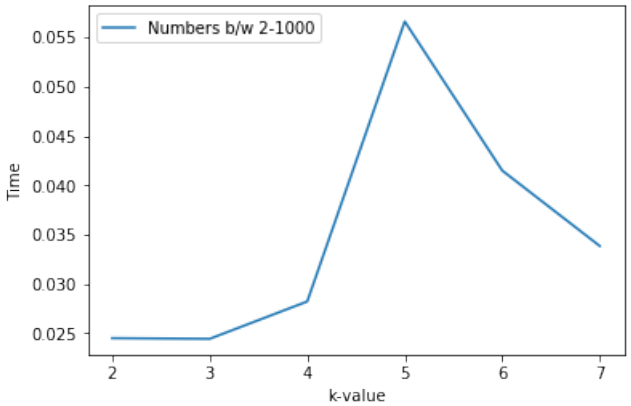
I. Introduction

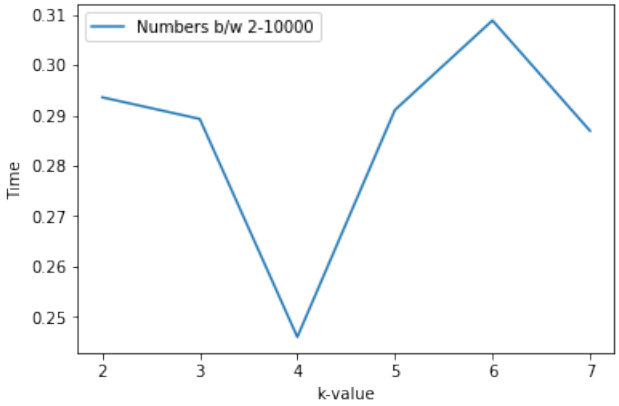
Miller-Rabin primality test was named,when Michael Rabin discovered a randomized polynomial-time algorithm in 1980 to test whether a number is prime, which was closely related to a deterministic algorithm studied by Gary Miller in 1976. Miller Rabin is relatively simple extension of Fermats little Theorem that allows us to test for primality with a much higher probability than Fermats little theorem.Miller-Rabin primality test could only determine if a number is a probable prime.

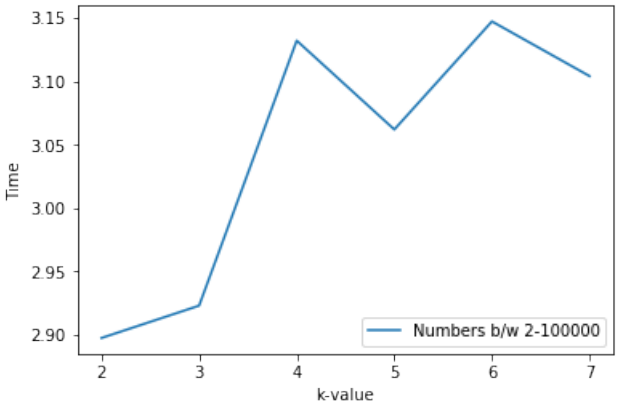
II. Implementation

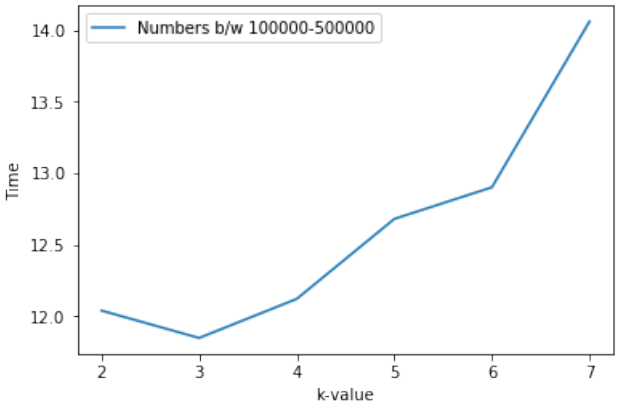
Miller-Rabin primality test is based on a basic principle where if $X^2 = Y^2$ modN , but X! = +-YmodN , then N is composite. By varying the values of k from 2 to 7 prime numbers have been found . For k in this range prime numbers between 2 to 1000 , 2 to 10000 , 2 to 100000 and 100000 to 500000 has been found a long with the time complexities . Similarly prime numbers between any range can be found .

A. Visualization









B. Reference

https://en.wikipedia.org/wiki/Millerhttps://www.geeksforgeeks.org/primality-test-set-3-miller-rabin/ https://rosettacode.org/wiki/Miller