ADS ASSIGNMENT

PRIMALITY TEST

-Ateefa Ateeque

FERMAT TEST

- It states that for every prime and its coprime it holds that:

  a^p-1 = 1(mod p)

- If the equality does not hold, then we can be sure that the number is not a prime. If it does hold, the number might be a prime.

- The main flaw of the Fermat's primality test is existence of *Carmichael numbers*. The Carmichael numbers are absolute Fermat's pseudoprimes, which means that they will always pass this test as primes

  #https://www.programming-algorithms.net/article/48367/Fermat's-test

MILLER-RABIN

- It is based on a basic principle where if X^2 = Y^2 (mod n),but X != ± Y ,then n is composite.

- /t generally preferred over Fermat's method.

#https://www.hackerearth.com/practice/math/number-theory/primality-tests/tutorial/

SOLOVAY-STRASSEN

- The Solovay–Strassen primality test is a probabilistic test to determine if a number is composite or probably prime.

- This method uses two mathematics symbols

  Legendre Symbol

  Jacobian Symbol

- If the input n is composite then it is possible for the output to be incorrectly probably prime. The number n is then called a Euler-Jacobi pseudoprime

https://www.geeksforgeeks.org/primality-test-set-4-solovay-strassen/