Primality tests

Testing primes of extremely large digits can not be precise and is instead based on probability.

Fermat primality:

This is gotten from Fermat's little theorem which states that if *n* is prime and *a* is not divisible by *n*, then

$a^{n-1} \equiv 1 \bmod n$

if one wants to test whether *n* is prime, then we can nick random integers *a* not divisible by *n* and see whether the congruence holds. If it does not hold for a value of *a*, then *n* is composite. But if it does hold for one or more values of *a*, then we say that *n* is probably prime.

Example:

Lets say n =5

1 < a < 4

a = 2

2^4 =16

16= 1 mod 5

And the algorithm, takes in an input n and k

Where k is the number of times we nick a random a and test to see if $a^{n-1} \equiv 1 \bmod n$ holds

The run time for this is $\tilde{O}(k \log^2 n)$

FLAW

Fermat's primality test has a notable flaw: **i**t is not always reliable due to the existence of "Fermat liars" and "Carmichael numbers." These are numbers which pass the primality test as a prime but are composite.

the Carmichael numbers are numbers for which Fermat pseudoprimes to all bases exist

Therefore improvements have been made to the fermat primality test. Such as miller-rabin, baillie-PSW and Solovay-Strassen

Miller-Rabin:

For an odd integer n,

n = $2^s d$ where,

s is a positive integer and d is an odd positive integer

lets an integer *a* and call it a base.

a is coprime to n.

*coprimes are numbers which are both primes and only share 1 as a common factor

Then n is said to be a strong probable prime to base *a* if one of these congruence relations hold:

$a^d \equiv 1 \bmod n$ or

$a^{(2\text{^}r)d} \equiv -1 \bmod n$ for 0 <= r < s

so first checking $a^d \equiv 1 \bmod n$ then checking $a^{(2\text{^}r)d} \equiv -1 \bmod n$ for successive values of r.

but if n is not a strong probable prime to base a. a is called a witness for the compositeness of n

No composite number is a strong pseudoprime to all bases at the same time (unlike fermats test which has Carmichael numbers).

Selecting *a* without selecting a witness is quite difficult. The miller test is used to find witnesses more efficiently.

The run time for this algorithm is also Õ ($k \log^2 n$)

The average accuracy of this is 4^{-k} and it improves for larger numbers

REFERENCES:

- Wikipedia Contributors (2019). *Fermat primality test*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Fermat_primality_test.
- Wikipedia Contributors (2019). *Miller*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Miller