Outline

primality testing

- Fermat little's test
- Miller-Rabin test

} probabistic

There is a polynomial deterministic algorithm for primality test.

Large prime (prime number with 1024 bits)

How do we find prime number?

How do we test if a number n is prime?

Brute-Force : Try all number less than n and check if it divides n.

Recap on Fermat's little theorem:

If p is prime, for all $a = 1, 2, \ldots, p-1$

$$a^{p-1} \equiv 1 \mod p$$

Fermat's litte test

Given a number n, check if n is prime.

Take an element a in $[2, 3, \ldots, n-2]$

Check if $a^{n-1} \equiv 1 \mod n$

If $a^{n-1} \not\equiv 1 \mod n$, then n can not be prime.

If $a^{n-1} \equiv 1 \mod n$, then can we conclude that n is a prime? NO. Try different value of a.

Do there exist an integer n which is not prime but for all a in [1, ..., n-1]

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

Yes. There exists such an integer. carmichael integer

The smallest such integer is 561.

It is rare but there are infinite of them.

Hence, Fermat little test is not sufficient to tell carmichael integer is not a prime

---

Remark.

For Fermat little test, we skip $a = 1$ and $a = -1$.

Because when $a = 1$ and $a = -1$,

$a^{n-1} \equiv 1 \mod n$ for all odd n integer (not just prime)

> $1^x \equiv 1 \mod n$ for any integer n
>
> $(-1)^{n-1} \equiv 1 \mod n$ when n is odd integer n

Theorem

If p is an odd prime, then for all $a \in [1, \ldots, p-1]$

(1) $a^{p-1} \equiv 1 \mod p$ (Fermat's little)

(2) the only square root of 1 is 1 and -1.

---

proof (2)

Suppose $x \in \mathbb{Z}_p^*$ such that

$$x^2 = 1 \mod p$$

Then $x^2 - 1 = 0 \mod p$

$$(x-1)(x+1) = 0 \mod p$$

p is prime. So, $p \mid x-1$ or $p \mid x+1$

This implies $x = 1$ or $x = p-1 \equiv -1 \mod p$

Theorem

If p is an odd prime, write $p-1 = 2^e q$, where q is odd, then for $a \in [1, \dots p-1]$

Then one of the following two condition is true.

(a) $a^q \equiv 1 \mod p$

(b) $a^{2^i q} \equiv -1 \mod p$ for at least one i

$0 \leq i < e$