Primality Testing

1. Deterministic Algo.: Always gives a correct answer.
2. Probabilistic Algo.: Gives a correct answer most of the time.

Primality Testing Algo.

① Divisibility Algo:

* Most elementary test for primality.
* n is a given no., then n is a composite no. if n is divisible by any +ve integer less than or equals to $\sqrt{n}$.
  Otherwise n is a prime number.

```
Prime_divi_test(n)
   r = 2
   while (r < [√n])
      if r|n
      return ("n is a composite no.")
      r = r+1;
   end
return ("n is a prime no.")
end
```

* If we assume that each arithmatic operation uses only one bit operation, then the bit operation complexity of this algo.

$$f(n_b) = \sqrt{2^{n_b}} \quad \text{where } n_b = \text{No. of bits in } n.$$
$$= 2^{n_b/2}$$

$$O(2^{n_b})$$

$\Rightarrow$ The bit operation complexity of the divisibility test alg. is exponential.

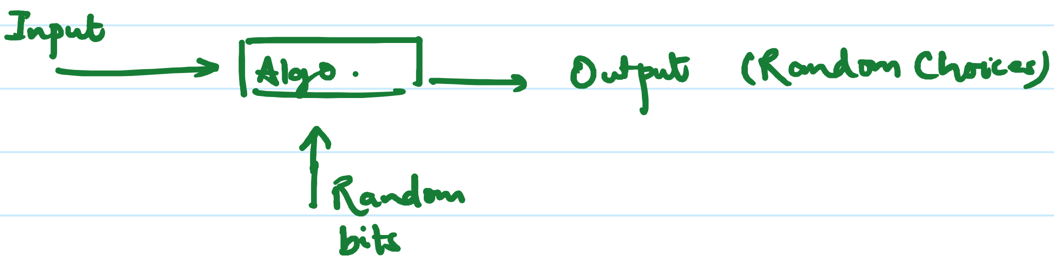
AKS Algorithm: Given by Agrawal, Kayal & Saxena in 2002.

* Complexity is $O((\log_2 n_b)^{12})$

* For very large n it takes too much time.

Probabilistic Algorithms (Randomized Algo.)

It receives, in addition to the input, a stream of random bits that it can use for the purpose of making random choices.



* For a fixed input different runs of a randomized algo. may gives different results

There are two types of prob. algo.

1. Monte Carlo Algo.
2. Las Vegas Algo.

An Introduction to randomized Algorithms
by Richard M. Karp
Discrete Applied Mathematics.

Fermat Test: It is based on the Fermat's little theorem.

If n is prime and if $n \nmid a$ then $a^{n-1} \equiv 1 \bmod n$

$\Rightarrow$ If n is prime and $n \nmid a$, then $a^{n-1} \equiv 1 \bmod n$.

This doesn't imply that if $a^{n-1} \equiv 1 \bmod n$ then n is a prime no. & $n \nmid a$.

* To test the primality of a given number n, we pick and random integer a s.t. $n \nmid a$ and if $a^{n-1} \equiv 1 \bmod n$ doesn't hold then n is a composite number.

* This congruence ($a^{n-1} \equiv 1 \bmod n$) is unlikely to hold for a random a if p is composite.

Now, if $a = 1$ then $a^{n-1} = 1 \bmod n$

and if $a \equiv -1 \bmod n$ & n is odd
$\equiv n-1$

$$\begin{aligned}
a^{n-1} &\equiv (-1)^{n-1} \bmod n \\
&\equiv (-1)^{n} (-1)^{-1} \bmod n \\
&\equiv (-1)(-1) \bmod n \\
&\equiv \underline{1 \bmod n}
\end{aligned}$$

Therefore, we choose a number a in the interval $1 < a < n-1$.

Miller - Rabin Test:

* Any +ve odd integer $n \geq 3$ can be written as
$$n-1 = 2^k \cdot \underline{q} \quad \text{with } k > 0, \ q \text{ odd}.$$

* If p is prime and a is a +ve integer less than p then $a^2 \bmod p = 1$ if and only if either $a \bmod p = 1$ or $a \bmod p = -1 = \underline{p-1}$

Proof: If $a^2 \bmod p = (a \bmod p)(a \bmod p)$

if $a \bmod p = 1$ or $a \bmod p = -1$ then

$a^2 \bmod p = 1 \bmod p$

* If p is a prime number greater than 2 then

$p-1 = 2^k \cdot q$, $k>0$, q odd

Let a be any integer s.t. $1<a<p-1$

Then one of the following conditions is true.

(1) $a^q \equiv 1 \bmod p$.

(2) One of the numbers a^q, a^{2q}, $a^{4q}, \dots, a^{2^{k-1}q}$ is congruent to $-1 \bmod p$.

Proof: By Fermat's theorem, for $1<a<p-1$

$a^{p-1} \equiv 1 \bmod p$, if p is prime.

Now, we have, $p-1 = 2^k \cdot q$

$$\Rightarrow \quad a^{p-1} \bmod p = a^{2^k \cdot q} \bmod p$$

$$1 = a^{2^k \cdot q} \bmod p$$

$$\Rightarrow \quad a^{2^k \cdot q} \equiv 1 \bmod p \quad \text{———} \quad (1)$$

Now, consider the following list

$a^q \bmod p$, $a^{2q} \bmod p$, $a^{4q} \bmod p, \dots, a^{2^{k-1} \cdot q} \bmod p$, $a^{2^k \cdot q} \bmod p$

Now, $a^{2^k \cdot q} \equiv 1 \bmod p$

$\therefore \left(a^{2^{k-1} \cdot q}\right)^2 \bmod p = 1$

$\Rightarrow a^{2^{k-1} \cdot q} \bmod p = 1$ or -1

$\Rightarrow$ Either $a^{2^{k-1}\cdot q} \bmod p = -1 = p-1$

or $a^{2^{k-1}\cdot q} \bmod p = 1$

if $a^{2^{k-1}\cdot q} \bmod p = 1$

$\left(a^{2^{k-2}\cdot q}\right)^2 \bmod p = 1$

$\Rightarrow a^{2^{k-2}\cdot q} \bmod p = -1$ or 1

$\Rightarrow$ Either $a^{2^{k-2}\cdot q} \bmod p = p-1$ or

$a^{2^{k-2}\cdot q} \bmod p = 1.$

$\vdots$

$(a^q)^2 \bmod p = 1$

$\Rightarrow a^q \bmod p = 1$ or -1

Therefore, either $a^q \bmod p = 1$ and hence all subsequent no. in the list are equal to $1 \bmod p$.

or some numbers in the list doesn't equal 1 but its square mod p equal 1.

i.e. one of the no. $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}\cdot q}$ is congruent to -1. i.e. $p-1$.

Miller-Rabin Test:

If n is prime, the either $a^q \bmod n = 1$ (and hence $a^{2q}, a^{4q}, \ldots a^{2^{k-1}\cdot q} \bmod n = 1$)

or some elements in the list $\{a^q, a^{2q}, \ldots, a^{2^{k-1}\cdot q}\}$ equals -1.

Otherwise n is composite.

Note: If the condition met for a no. n then this does not imply that n is prime.

Ex: $n = 2047 = \underline{23 \times 89}$

$n-1 = 2046 = 2 \times \underline{1023}$ $(2^k \cdot q,\ k=1,\ q=1023)$

$2^{1023} \bmod 2047 = 1$

$\Rightarrow$ 2047 meets the condition but n is not prime.

Algorithm

Test(n)

(i) Find k & q $(k>0,\ q \text{ odd})$ so that
$$n-1 = 2^k \cdot q$$

(ii) Select a random integer a, $1 < a < n-1$.

(iii) If $a^q \bmod n = 1$ then return("Inconclusive")

(iv) For $j = 0$. to $k-1$
if $a^{2^j \cdot q} \bmod n = n-1$ then
return ("Inconclusive")

(v) Return ("n is composite")

Ex: $n = 29$ $\quad j = \underline{0, 1}$

$n-1 = 28 = 2^2 \cdot 7$ $(k=2,\ q=7)$ $\quad a^{2^j \cdot 7}$

Now, we choose a $(1 < a < 28)$

Let $a = 10$

then $10^7 \bmod 29$. which is neither 1 nor $n-1$.

test cont.

$(10^7)^2 \bmod 29 = 28 = n-1 \Rightarrow$ Test is inconclusive (29 may be a prime)

Let $a = 2$

then $2^7 \bmod 29 = 12$

$(2^7)^2$ " " $= \underline{28} = n-1$

Again test is inconclusive.

for all $1 < a < 28$ we get the return inconclusive (i.e. 29 may be a prime)

Now, for $\underline{n} = \underline{221} = 13 \times 17$

$(n-1) = 220 = 2^2 \times 55$ ($\Rightarrow$ $k=2$, $q=55$)

Let $\underline{a = 5}$ then $\underline{a^q, a^{2q}}$

$$\left.\begin{array}{l} \underline{5}^{55} \bmod 221 = \underline{112} \\ \underline{(5^{55})}^2 \bmod 221 = \underline{168} \end{array}\right\} \neq 1 \text{ or } -1$$

$\Rightarrow$ 221 is definitely a composite number.