Primality testing Problem

Given a input n as an integer check weather it is prime or not.

`Input:` n

`Output`: 1 if n is prime and 0 otherwise

Miller-Rabin

Given input a integer p

1. if p is even, accept if p = 2(return that number is prime); otherwise , reject.
2. Select any k random positive integers say $a_1, a_2 \cdots, a_k$
3. For each i from 1 to k:
   1. Compute $a_i^{p-1} \mod p$ and reject if different from 1.
   2. Let p-1 = st where s is odd and t is a power of 2 ($t = 2^h$)
   3. Compute the sequence $a_i^{s.2^0}, a_i^{s.2^1}, a_i^{s.2^2}, \cdots, a_i^{s.2^h}$ modulo p.
   4. If some element of this sequence is not 1, find the last element that is not 1 and reject if that element is not = -1
4. All steps have passed at this point so accept.

Probabilistic Correctness of Algorithm

1. It will accept all prime with probability 1
2. It will accept odd composite with probability< $1/2^k$

Proof from daily diary

Proof for statement 1

If the prime number is 2 then we already accept it at first step itself with probability 1.

For the remaining odd prime no.'s

They will definitely not get rejected at step 3-1 due to Fermat's little theorem which states that if p is prime then $a^{p-1} \equiv 1 \mod p$.

Now to prove that it doesn't get rejected at step 3-4 , we need to prove that the first number from right to left which is not 1 is equal to -1 for a given odd prime number.

Proof

We notice that while computing the sequence $a_i^{s.2^0}, a_i^{s.2^1}, a_i^{s.2^2}, \cdots, a_i^{s.2^h}$ modulo p, we are just computing repeated squares of the term $a_i^{s.2^0}$. Hence any element in this sequence is just a square of the previous term.

Assuming the first term that is not equal to 1 is b. So $b \neq 1 \mod p$ trivally.

Now from the above statement we can say that the term next term in the sequence is = b^2. And since b was the first term(form right to left) that is not equal to 1, the term next to it will be 1. Hence $b^2 = 1 \mod p \implies b^2 - 1 = 0 \mod p$.

We can factorize $b^2 - 1$ as

$$b^2 - 1 = (b-1)(b+1) = 0 \mod p$$

Since p is a odd prime number and $(b-1)(b+1) = 0 \mod p$ implies that at least one of the two factor should be divisible by p.

Now since $b \neq 1$ the only possible case is when $(b+1) = 0 \mod p$. Hence $b = -1 \mod p$.

Hence prooved

Proof for statement 2

Let;

a_i is a witness = composite number is rejected by a_i .

a_i is non-witness = composite number is accepted by a_i

To prove this statement true we have to show that if p is an odd composite number and a is any randomly selected positive integer then;

$$P(\text{a is witness}) \geq \frac{1}{2}$$

To do this we will try to demonstrate that there are at least as many witnesses as non-witnesses by finding unique witness for each non-witness.

We try to prove this by giving a one-one function from set of non-witnesses to set of witnesses. As this directly implies $P(\text{a is witness}) \geq \frac{1}{2}$.

Notice that for every non-witness, the sequence computed in step 3-3 will be either all 1s or -1 at some position, followed by 1s.

Assuming **h** to be the non-witness(of kind -1 at some position, followed by 1s.) for which -1 appears in the largest position and let that position be **j** in the sequence, where the sequence positions are numbered starting at 0. Hence trivially $h^{s.2^j} \equiv -1 \pmod p$

Note:-

- $h^{s.2^i} \equiv 1$ (mod p)for every $i > j$
- For every other non-witness a the value $a^{s.2^j}$ can be equal to either 1 or -1 since j is the maximum of right most positions from each non-witness.

Since p is a composite number, so there are 2 possible cases

1. p is the power of prime
2. p is the product of 2 numbers q and r

For Case 2

Applying the Chinese remainder theorem on second case implies that some positive integer t whereby

$$t \equiv h(\text{mod q}) \text{ and } t \equiv 1(\text{mod r})$$

Therefore

$$t^{s.2^j} \equiv -1 \pmod{\text{q}}$$

$$t^{s.2^j} \equiv 1 \pmod{\text{r}}$$

From this we have $t^{s.2^j} = c_0(q-1) = c_1(r+1) \neq \pm 1$ (mod p) and $t^{s.2^{j+1}} \equiv 1$ (mod p) this implies that t is witness. -------- Statement(1)

Now We simply have to show that $dt \mod p$ is a unique witness for each non-witness d by making two observations.

Recall from the note above , $d^{s.2^j} \equiv \pm 1 \text{ (mod p)}$ implies $d^{s.2^{j+1}} \equiv 1 \text{ (mod p)}$.--------statement(2)

From the statement (1) and statement(2) we can say $(dt)^{s.2^j} \not\equiv \pm 1 \text{ (mod p)}$ and $(dt)^{s.2^{j+1}} \equiv 1 \text{ (mod p)}$. Hence $dt \mod p$ is a witness.

If d_1 and d_2 are distinct non-witness then $d_1 t \mod p \neq d_1 t \mod p$.

Proof by Contradiction

Given $d_1 \neq d_2$

$t^{s.2^{j+1}} \mod p = 1 \implies t.\, t^{s.2^{j+1}-1} \mod p = 1.$

If we assume $d_1 t \mod p = d_1 t \mod p$, then

$$d_1 = t.\, t^{s.2^{j+1}-1} d_1 \mod p = t.\, t^{s.2^{j+1}-1} d_2 \mod p = d_2$$

which contradicts with initial statement $d_1 \neq d_2$. Hence proved that $d_1 t \mod p \neq d_1 t \mod p$

Since we got one-one function implies witness > no. of non-witness

For Case 1

Assuming $t = (1 + q^{e-1})$. Expanding t^p using binomial theorem

$$t^p = 1 + p.\, q^{e-1} + \text{multiples of higher power of} q^{e-1}$$

Now this t is witness for step 3-1 as if $t^{p-1} \equiv 1$ (mod p), then $t^p \equiv t \neq 1$ (mod p)

Now we can do same thing as in the last case and try to generate wtiness using this t. If d is non-witness , we have $d^{p-1} \equiv 1$ (mod p) but then dt is witness and with same proof as in previous case If d_1 and d_2 are distinct non-witness then $d_1 t \mod p \neq d_1 t \mod p$.

Hence the no. of witnesses must be larger then no. of non- witnesses.

Time Complexity

- Calculating $a^{s.2^i}$ using the repeated squaring method will take Order of (logn)^2
- Multiplying and taking maodulo will take order of logn times
- This whole test is done k times so

FInal time complexity = O(klog^3n).