Miller Rabin Algorithm

MRA is an extension of Fermat's little theorm. And it has got a higher probability than FLT

check if 7 is prime.

Ex: $n = 7$

Should represent as: $n-1 = 2^s \times d$ → odd no.

$s, d \in$ N +ve Z

$7-1 = 2^1 \times 3$

$6 = 2^1 \times 3$ here $s = 1$, $d = 3$

Next, we have to compute x,

$x \equiv a^d \pmod n$, $2 \leq a \leq n-2$

here. $2 \leq a \leq 2$ assume $a = 3$ here.

$x = 3^3 \bmod 7$

$27 \bmod 7$

$x \Rightarrow 6$

---

check if $x \equiv \pm 1 \bmod n$ or not.

ie, $6 \equiv +1 \bmod 7$

also written as. $\Rightarrow$ $6 \bmod 7 = \pm 1 \bmod 7$

$6 \neq 1 \bmod 7$

is $6 = -1 \bmod 7$?

$\Rightarrow 7-(1 \bmod 7)$

$\Rightarrow 7-(1) = 6$

$\therefore 6 = 6$

so $6 \equiv -1 \bmod 7$

$x \equiv -1 \bmod n$

$\therefore$ n is probably prime!

$\therefore$ Stop algorithm.

$n = 41$

$n-1 = 2^s \times d \rightarrow$ odd no.

$40 = 2^3 \times 5$

$d = 5$

$s = 3$

$2 \leq a \leq n-2$

$2 \leq a \leq 39$

let $a = 3$.

$x = a^d \bmod n$.

$= 3^5 \bmod 41$

$= 243 \bmod 41 = 38$

$x = 38$ check $x \equiv \pm 1 \bmod n$.

(*).

$38 \bmod 41 = 1 \bmod 41$

$38 \neq 1$

$3^3 \bmod 41 = -1 \bmod 41$

$= 41 - (1) = 40$

$3^3 \neq \pm 1$

$\therefore x \neq \pm 1 \bmod n$

Is $s = 1$, nope $n = 2$.

so take $r = 1$,

$q = 3, \quad d = 5, \quad s = 3$.

for $(r = 1, \quad r \leq s-1 \quad , \quad r = r+1)$

$3-1$

2.

$a^{2^r \times d} \bmod n \equiv 1 \bmod n \rightarrow$ Not prime.

else.

$a^{2^r \times d} \bmod n \equiv -1 \bmod n \rightarrow$ prime.

$3^{2^1 \times 5} \bmod 41 = 1 \bmod 41$

$3^{10} \bmod 41 \equiv 1 \bmod 41$

$9 \not\equiv 1$

Not congr

$3^{10} \bmod 41 \equiv -1 \bmod 41$

$9 \not\equiv 40$.

not congr.

now $r = 2$,

$3^{2^2 \times 5} \bmod 41 = 1 \bmod 41$.

$3^{20} \bmod 41 = 1 \bmod 41$

$40 \neq 1$

$= -1 \bmod 41$

$41 - (1) = 1$

$40 = 41 - 1$ ✓

$a^{2^r \times d} \bmod n \equiv -1 \bmod n \Rightarrow$ probably prime.