Probabilistic Primality test

GOPI
Page No.:
Date: / /

Miller-Rabin Test (Primality test)

↓

Any test that is used to find out a given no is prime or not.

① Perform $n-1$ such that $n-1 = m \times 2^k$

② If $k \leq 1$, calculate T s.t $T = a^m \bmod n$

If $(T = \pm 1)$, no is prime, else composite.

If $k > 1$, calculate T s.t $T = T^2 \pmod n$

If $(T = 1)$, no is composite.

If $(T = -1)$, no is prime,

Else, no. is composite.

eg:- $n = 27$, $a = 2$.

Find if $n = 27$ is prime or not.

Sol:- $n-1$ s.t $(n-1) = m \times 2^k$

$26 = 13 * 2^1$, $m = 13$ & $k = 1$

$T = a^m \pmod n$

$= 2^{13} \pmod{27}$

$= 2^5 * 2^5 * 2^3 \pmod{27}$ $\quad \frac{25}{200}\ \frac{8}{4}$

$= 5 * 5 * 8 \pmod{27}$

$= 200 \pmod{27} = 11$. Here $T = 11 \neq \pm 1$

$\Rightarrow n = 27$ is composite.

Page No.
Date: / /

Q Is 53 prime?

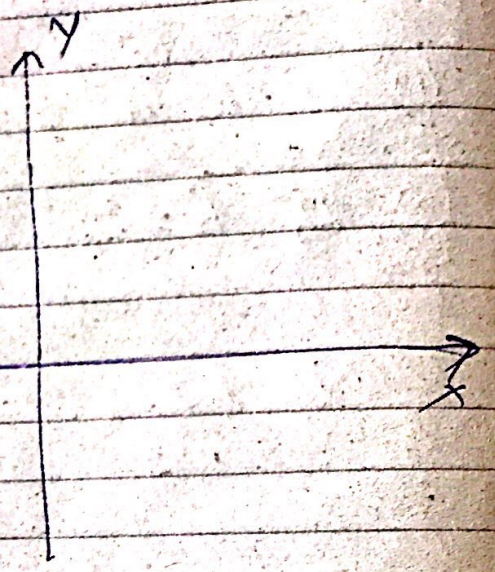
Elliptic Curve Cryptography.

$y^2 = x^3 + ax + b$.

$y = \sqrt{x^3 + ax + b}$

$E_{11}(1,6)$ (mod 11)

$a=1,\ b=6$.



eg:- $y^2 = x^3 + ax + b \pmod{11}$

($a \to 1$, $b \to 6$)

$y^2 = x^3 + x + 6 \pmod{11}$ (Find the pts on this elliptic curve)

$0, 0 \cdots, 10 \left[(p-1)\right]$

Since $p = 11$.

B.H.S.

x	$x^3 + x + 6 \pmod{11}$	y	$y^2 \pmod{11}$
0	6	0	0
1	8	1	1
2	5	2	4
3	3	3	9
4	8	4	5
5	4	5	3
6	8	6	3
7	4	7	5
8	9	8	9
9	7	9	4
10	4	10	1

$36 \pmod{11} = 3$.

(2, 4) is a pt on the curve

(2, 7)

(3, 5), (3, 6), (5, 2), (5, 9), (7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9)