TEST (n) is:

1. Find biggest k, $k > 0$, so that $(n-1)=2^k q$
2. Select a random integer a, $1<a<n-1$
3. **if** $a^q \bmod n = 1$ **then** return ("maybe prime");
4. **for** $j = 0$ **to** $k - 1$ **do**
    5. **if** $(a^{2^j q} \bmod n = n-1)$
       then return(" maybe prime ")
6. return ("composite")

$a^q \bmod n = 1$ ×

$a^q \bmod n = n-1$ ×

$a^{2q} \bmod n = n-1$ ×

$a^{4q} \bmod n = n-1$

$a^{8q} \bmod n = n-1$

$a^{16q} \bmod n = n-1$

$a^{2^5 q} \bmod n = n-1$

Q: check 1729 is prime using Miller-Rabin test?

Sol:

$1729-1 = 1728 = 2^6 \times 27$

$k = 6, \; q = 27$

$j = 0, 1, 2, 3, 4, 5$

$a = 671$

$a^q \bmod n = 671^{27} \bmod 1729 = 1084$

$a^{2q} \bmod n = (1084)^2 \bmod 1729 = 1065$

$a^{4q} \bmod n = (1065)^2 \bmod 1729 = 1$

Composite.

Q: $n = 104513$, $a = 3$ } What is Miller-Rabin Test decision ?

$n-1 = 104512 = 2^6 \times 1633$, $j = 0,1,2,3,4,5$

$a^q = 3^{1633} \pmod{n} = 88958 \neq 1$
$\neq n-1$

$a^{2q} = (88958)^2 \pmod{n} = 10430 \neq n-1$

$a^{2^2 q} = (10430)^2 \bmod n = 91380 \neq n-1$

$a^{2^3 q} = (91380)^2 \bmod n = 29239 \neq n-1$

$a^{2^4 q} = (29239)^2 \bmod n = 2781 \neq n-1$

$a^{2^5} = (2781)^2 \bmod n = 104512 = n-1$ ✓

returns (may be prime).

Q: $n = 280001$, $a = 105532$

check the decision of Miller-Rabin Test?

Sol:

$$n-1 = 280000 = 2^6 \times 4375$$

$$a^q = (105532)^{4375} \bmod n = 236926 \neq 1, \neq n-1$$

$$a^{2q} = (236926)^2 \bmod n = 168999 \neq n-1$$

$$a^{2^2 q} = (168999)^2 \bmod n = 280000 = n-1$$

Conclusion: may be prime.