Miller Rabin Algo

① $n = 29$ Find k and q

$n-1 = 2^k q$ $\quad k > 0$

$28 = 2^2 \times 7$ $\quad k = 2 \quad q = 7$

② Select a $\quad a > 1$

$a = 10$ $\quad a < n-1$

③ $a^q \bmod n = 10^7 \bmod 29 = 17$

Stop 1 or $n-1$

④ Loop $j = 0$

$a^{2^j q} \bmod n \Rightarrow a^q \bmod n$

$j = 1$

$a^{2 \times 7} \bmod n = 10^{14} \bmod 29 = 28$

May be Prime

Try again $a = 2$

③ $a^q \bmod n = 2^7 \bmod 29 = 12$

Stop 1 or $n-1$

④ $j = 0 \quad a^q \bmod n = 12$

$j = 1 \quad a^{2q} \bmod n$

$= 2^{2 \times 7} \bmod 29 = 28$

Go through 1 to 28 and get same Result-

means n being Prime