Miller Rabin test

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

(2) If $k \leq 1$, calculate 'T' such that $T = a^m \bmod n$

If $(T = \pm 1)$, no. is Prime else Composite

If $k > 1$,

calculate 'T' such that $T = T^2 \bmod n$

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

If $(T = -1)$, no. is Prime

else no. is Composite

e.g 1 $n = 27$, $a = 2$, find $n = 27$ is Prime or not

Sol^n $(n-1) = m \times 2^k$

$26 = 13 \times 2^1$, here $m = 13$

$k = 1$, here $k = 1$

Calculate 'T' such that

$T = a^m \bmod n$

$= 2^{13} \bmod 27$

$= 11 \Rightarrow T \neq \pm 1 \Rightarrow n$ is Composite

$\Rightarrow$

e.g 2 $n = 61$, $a = 2$

$\Rightarrow (n-1) = m \times 2^k$

$= 30 \times 2^1$

$= 15 \times 2^2$ ✓

$m = 15$

$k = 2$

$\Rightarrow T = a^m \bmod n$

$= 2^{15} \bmod 61$

$\Rightarrow \boxed{T = 11}$

$\Rightarrow T = T^2 \bmod n$

$\Rightarrow T = (11)^2 \bmod 61$

$\Rightarrow T = 60$

$\Rightarrow T \approx -1 \Rightarrow n = 61$ is Prime.