1°. Test if 2879 is prime:

1) we find k and m in $n-1 = 2^k \cdot m$, such that m is odd

$2879 - 1 = 2^k \cdot m$

$2878 = 2^k \cdot m$

2878	2
1439	1439
1	

$\Rightarrow k = 1$; $m = 1439$

2) we pick a random base a, s.t $1 < a < 2879$

let $a = 2$

3) we start computing the sequence $a^m, a^{2m} \dots a^{2^k m}$

$s_0 = a^m \bmod n$

$s_0 = 2^{1439} \bmod 2879$

we compute this by using the repeated squaring method.

write 1439 in binary (powers of 2)

$1439 = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^7 + 2^8 + 2^{10}$

$2^{(2^0)} = 2 \bmod 2879 = 2$

$2^{(2^1)} = 2^{(2^0)} \cdot 2^{(2^0)} = 4 \bmod 2879 = 4$

$2^{(2^2)} = 2^{(2^1)} \cdot 2^{(2^1)} = 16 \bmod 2879 = 16$

$2^{(2^3)} = 2^{(2^2)} \cdot 2^{(2^2)} = (16 \cdot 16) \bmod 2879 = 256$

$2^{(2^4)} = 2^{(2^3)} \cdot 2^{(2^3)} = 65536 \bmod 2879 = 2198$

$2^{(2^5)} = 2^{(2^4)} \cdot 2^{(2^4)} = (2198 \cdot 2198) \bmod 2879 = 242$

$2^{(2^6)} = 2^{(2^5)} \cdot 2^{(2^5)} = (242 \cdot 242) \bmod 2879 = 984$

$2^{(2^7)} = 2^{(2^6)} \cdot 2^{(2^6)} = (984 \cdot 984) \bmod 2879 = 912$

$2^{(2^8)} = 2^{(2^7)} \cdot 2^{(2^7)} = (912 \cdot 912) \bmod 2879 = 2592$

$2^{(2^9)} = 2^{(2^8)} \cdot 2^{(2^8)} = (2592 \cdot 2592) \bmod 2879 = 1757$

$2^{(2^{10})} = 2^{(2^9)} \cdot 2^{(2^9)} = (1757 \cdot 1757) \bmod 2879 = 761$

$2^{1439} \bmod 2879 = (\underbrace{2 \cdot 4 \cdot 16 \cdot 256 \cdot 2128}_{\bmod 2879} \cdot 912 \cdot 2592 \cdot 761) \bmod 2879$

$= (121 \cdot 912 \cdot 2592 \cdot 761) \bmod 2879 = 1$ //

Since the sequence starts with 1, we can conclude that the number 2879 is probably prime.

Test if 259 prime:.

1) we find k and m in $n-1 = 2^k \cdot m$, s.t. m is odd

$259-1 = 2^k \cdot m$

$258 = 2 \cdot 129$

258	2
129	129
1	

2) we pick a random base a s.t. $1 < a < 259$

let $a = 3$

3) we start computing the sequence a^m, a^{2m}, ... $a^{2^k m}$

$s_0 = a^m \bmod n$

$s_0 = 3^{129} \bmod 259$

compute with repeated squaring

write 129 in binary

$129 = 2^0 + 2^7$

$3^{(2^0)} = 3 \bmod 259 = \boxed{3}$

$3^{(2^1)} = 3^{(2^0)} \cdot 3^{(2^0)} = 9 \bmod 259 = 9$

$3^{(2^2)} = 3^{(2^1)} \cdot 3^{(2^1)} = 81 \bmod 259 = 81$

$3^{(2^3)} = 3^{(2^2)} \cdot 3^{(2^2)} = (81 \cdot 81) \bmod 259 = 86$

$3^{(2^4)} = 3^{(2^3)} \cdot 3^{(2^3)} = (86 \cdot 86) \bmod 259 = 144$

$3^{(2^5)} = 3^{(2^4)} \cdot 3^{(2^4)} = (144 \cdot 144) \bmod 259 = 16$

$3^{(2^6)} = 3^{(2^5)} \cdot 3^{(2^5)} = (16 \cdot 16) \bmod 259 = 256$

$3^{(2^7)} = 3^{(2^6)} \cdot 3^{(2^6)} = (256 \cdot 256) \bmod 259 = \boxed{9}$

$3^{129} \bmod 259 = (3 \cdot 9) \bmod 259 = 27$

The algorithm ends since $k = 1$

since the sequence didn't start with 1 or contained ...1,1...

$\Rightarrow$ the number 259 is composite.

We try with another base:

let $a = 2$

we again compute $s_0 = a^m \bmod n$

$= 2^{129} \bmod 259$ with repeated squaring

129 in binary is $10000001 \Rightarrow 129 = 2^7 + 2^0$

$2^{(2^0)} = 2 \bmod 259 = 2$

$2^{(2^1)} = 2^{(2^0)} \cdot 2^{(2^0)} = 4 \bmod 259 = 4$

$2^{(2^2)} = 2^{(2^1)} \cdot 2^{(2^1)} = 16 \bmod 259 = 16$

$2^{(2^3)} = 2^{(2^2)} \cdot 2^{(2^2)} = 256 \bmod 259 = 256$

$2^{(2^4)} = 2^{(2^3)} \cdot 2^{(2^3)} = (256 \cdot 256) \bmod 259 = 9$

$2^{(2^5)} = 2^{(2^4)} \cdot 2^{(2^4)} = 81 \bmod 259 = 81$

$2^{(2^6)} = 2^{(2^5)} \cdot 2^{(2^5)} = (81 \cdot 81) \bmod 259 = 86$

$2^{(2^7)} = 2^{(2^6)} \cdot 2^{(2^6)} = (86 \cdot 86) \bmod 259 = 144$

$2^{129} \bmod 259 = 2 \cdot 144 \bmod 259 = 29$

again the algorithm ends and the sequence is [29] $\Rightarrow$

259 is composite

We try with another base:

let $a = 5$

we again compute $s_0 = a^m \bmod n$

$= 5^{129} \bmod 259$ with repeated squaring

129 in binary is $10000001 \Rightarrow 129 = 2^7 + 2^0$

$5^{(2^0)} = 5 \bmod 259 = 5$

$5^{(2^1)} = 25 \bmod 259 = 25$

$5^{(2^2)} = (25 \cdot 25) \bmod 259 = 625 \bmod 259 = 107$

$5^{(2^3)} = (107 \cdot 107) \bmod 259 = 53$

$5^{(2^4)} = (53 \cdot 53) \bmod 259 = 219$

$5^{(2^5)} = (219 \cdot 219) \bmod 259 = 46$

$5^{(2^6)} = (46 \cdot 46) \bmod 259 = 41$

$5^{(2^7)} = (41 \cdot 41) \bmod 259 = 123$

$5^{129} \bmod 259 = (5 \cdot 123) \bmod 259 = 97$

Again the algorithm ends and the sequence is $[97]$ which means 259 is composite

After trying with the bases $a \in [2, 3, 5]$, we can safely conclude that 259 is composite, so in any way not prime.