

```
In[189]:=
      n = 1256634425088001
```

```
Out[189]= 1256634425088001
```

```
In[191]:=
      b = Random[Integer, {1, n}]
```

```
Out[191]= 234255535767447
```

```
In[192]:=
      PowerMod[b, n - 1, n]
```

```
Out[192]= 1
```

So n does NOT fail FLT for this choice of b. I.e. n is a pseudoprime for this b.

```
In[193]:=
      PowerMod[b, (n - 1) / 2, n]
```

```
Out[193]= 1
```

```
In[194]:=
      JacobiSymbol[b, n]
```

```
Out[194]= 1
```

The $(n - 1) / 2$ power agrees with the Jacobi symbol. So n does not fail Euler ' s Criterion for this choice of b, i.e. n is an Euler pseudoprime for this b. Since we don ' t yet know if n is prime or composite. We can continue with the above choice of b by using Rabin - Miller.

Recall we need to determine the largest power of 2 dividing n - 1. We do this with the IntegerExponent command.

```
In[195]:=
      IntegerExponent[n - 1, 2]
```

```
Out[195]= 11
```

We now compute $(n - 1) / 2^i$ powers of b to try to find a non - trivial square root of 1.

```
In[196]:=
      PowerMod[b, (n - 1) / 2^2, n]
```

```
Out[196]= 1
```

```
In[197]:=
      PowerMod[b, (n - 1) / 2^3, n]
```

```
Out[197]= 1
```

```
In[198]:= PowerMod[b, (n - 1) / 2^4, n]
```

```
Out[198]= 1
```

```
In[199]:= PowerMod[b, (n - 1) / 2^5, n]
```

```
Out[199]= 1
```

```
In[200]:= PowerMod[b, (n - 1) / 2^6, n]
```

```
Out[200]= 1
```

```
In[201]:= PowerMod[b, (n - 1) / 2^7, n]
```

```
Out[201]= 1
```

```
In[202]:= PowerMod[b, (n - 1) / 2^8, n]
```

```
Out[202]= 87727638212709
```

Note this integer is NOT $n - 1$

```
In[205]:= n - 1
```

```
Out[205]= 1256634425088000
```

So it must be a non - trivial square root of one. We check this.

```
In[203]:= PowerMod[87727638212709, 2, n]
```

```
Out[203]= 1
```

Hence the Rabin - Miller test for this value of b shows n is composite.