

Let ' s use the Rabin - Miller test to determine whether or not some numbers are composite .

```
In[354]:=
      n = 172081
```

```
Out[354]= 172081
```

Let ' s see if $2^{(n-1)}$ is congruent to 1 (mod n) .

```
In[355]:=
      PowerMod[2, n - 1, n]
```

```
Out[355]= 1
```

$n - 1$ is divisible by 2. We can find what power of 2 divides $n - 1$ by using the IntegerExponent command

```
In[356]:=
      IntegerExponent[n - 1, 2]
```

```
Out[356]= 4
```

This tells us 2^4 divides $n - 1$.

```
In[357]:=
      (n - 1) / 2^4
```

```
Out[357]= 10755
```

So $(n - 1) = 2^4 * q$ with $q = 10755$

Now compute powers of 2 with decreasing powers of 2.

```
In[358]:=
      PowerMod[2, (n - 1) / 2, n]
```

```
Out[358]= 1
```

```
In[359]:=
      PowerMod[2, (n - 1) / 2^2, n]
```

```
Out[359]= 1
```

```
In[360]:=
      PowerMod[2, (n - 1) / 2^3, n]
```

```
Out[360]= 128465
```

This is not 1 or - 1 (mod n) so is a non - trivial square root of 1 (mod n) .

```
In[361]:= PowerMod[128465, 2, n]
```

```
Out[361]= 1
```

**If we load the Prime Q package we will see that
Mathematica used the same test we did to show n is composite.**

```
In[362]:= PrimeQ[n]
```

```
Out[362]= False
```

We load the PrimeQ package.

```
In[363]:= << "NumberTheory`PrimeQ`"
```

```
In[364]:= PrimeQCertificate[n]
```

```
Out[364]= {128465, 2, 172081}
```

**Mathematica says the number isn't prime since
(128465)^2 is congruent to 1 (mod n). I.e. Mathematica determined
it wasn't prime using the Rabin - Miller Test which we did above.**

Let's see if n = 172081 is a Carmichael number.

```
FactorInteger[n]
```

```
{{7, 1}, {13, 1}, {31, 1}, {61, 1}}
```

```
(n - 1) / 6
```

```
28680
```

```
(n - 1) / 12
```

```
14340
```

```
(n - 1) / 30
```

```
5736
```

$(n - 1) / 60$

2868

Since n is the product of distinct odd primes, and $(p - 1)$ divides $(n - 1)$ for all p dividing n , we see that n is a Carmichael number.

We try a larger integer to try :

In[368]:=

n = 1373653

Out[368]= 1373653

In[369]:=

PowerMod[2, n - 1, n]

Out[369]= 1

In[370]:=

IntegerExponent[n - 1, 2]

Out[370]= 2

In[371]:=

PowerMod[2, (n - 1) / 2, n]

Out[371]= 1373652

This is $(-1) \pmod{n}$. So we have to choose a different a . Let 's try $a = 3$.

In[372]:=

PowerMod[3, n - 1, n]

Out[372]= 1

In[373]:=

PowerMod[3, (n - 1) / 2, n]

Out[373]= 1

In[374]:=

PowerMod[3, (n - 1) / 2^2, n]

Out[374]= 1

We can ' t continue further since 2^2 is the highest power that divides $n - 1$. We try $n = 5$.

```
In[375]:= PowerMod[5, n - 1, n]
```

```
Out[375]= 1370338
```

So we see that this n is composite because it fails FLT with a = 5.

Rather than proceeding with a = 2, 3, 5, 6, etc. we could also just choose a random a, $1 < a < n$ and do the Rabin - Miller test with that value of a.

```
In[344]:= Random[Integer, {1, n}]
```

```
Out[344]= 253966964
```

```
In[376]:= a = 253966964
```

```
Out[376]= 253966964
```

```
In[377]:= PowerMod[a, n - 1, n]
```

```
Out[377]= 1
```

```
In[378]:= PowerMod[a, (n - 1) / 2, n]
```

```
Out[378]= 1370338
```

Since this is not $-1 \pmod n$ we have a non - trivial square root of 1 $\pmod n$ and n is composite.

```
In[379]:= PowerMod[1370338, 2, n]
```

```
Out[379]= 1
```