

In[1]:= $1 + 1$

Out[1]= 2

In[2]:= $n = 285\,707\,540\,662\,569\,884\,530\,199\,015\,485\,750\,433\,489$

Out[2]= 285 707 540 662 569 884 530 199 015 485 750 433 489

In[3]:= $\text{PowerMod}[2, n - 1, n]$

Out[3]= 161 591 896 740 488 434 629 592 418 561 956 941 261

Since $2^{(n-1)}$ is not congruent to 1 (mod n) we immediately have that n is COMPOSITE

Let ' s try another value of n .

In[4]:= $n = 285\,707\,540\,662\,569\,884\,530\,199\,015\,485\,751\,094\,149$

Out[4]= 285 707 540 662 569 884 530 199 015 485 751 094 149

In[5]:= $\text{PowerMod}[2, n - 1, n]$

Out[5]= 1

In[6]:= $\text{PowerMod}[3, n - 1, n]$

Out[6]= 1

In[7]:= $\text{PowerMod}[5, n - 1, n]$

Out[7]= 1

In[8]:= $\text{PowerMod}[7, n - 1, n]$

Out[8]= 1

**n is starting to look like a prime,
but recall that we cannot show n is prime no matter how many $a^{(n-1)} = 1 \pmod{n}$ since n could be a Carmichael number
(that is composite, but still satisfies $a^{(n-1)} = 1 \pmod{n}$ for all a with $(a, n) = 1$).**

So we can instead try to show n is composite. We do this by first factoring $n - 1$. Note : We have said factoring is hard in general, but note $n - 1$ is EVEN, so it will be easier to factor than a large odd number.

In[9]:=

FactorInteger[n - 1]

Out[9]= {{2, 2}, {1 476 241 557 300 827, 1}, {48 384 280 209 696 856 047 731, 1}}

Here $n - 1$ is the product of three primes, 2, $p_1 = 1\,476\,241\,557\,300\,827$, and $p_2 = 48\,384\,280\,209\,696\,856\,047\,731$. We apply Luca's Theorem to see if we can find a number $a \pmod{n}$ with order $n - 1$, i.e. a primitive root.

In[10]:=

p1 = 1 476 241 557 300 827

Out[10]= 1 476 241 557 300 827

In[11]:=

p2 = 48 384 280 209 696 856 047 731

Out[11]= 48 384 280 209 696 856 047 731

We start by trying $a = 2$.

In[12]:=

a = 2

Out[12]= 2

In[13]:=

PowerMod[a, n - 1, n]

Out[13]= 1

In[14]:=

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

Out[14]= 285 707 540 662 569 884 530 199 015 485 751 094 148

In[15]:=

PowerMod[a, (n - 1) / p1, n]

Out[15]= 85 123 374 597 353 559 026 878 384 594 727 525 044

In[16]:=

PowerMod[a, (n - 1) / p2, n]

Out[16]= 212 515 114 150 837 464 246 496 688 100 132 326 772

**We luck out on our first try!
 $a = 2$ is a primitive root for our n by Luca's Theorem, So n is prime.**

NOTE : 2 will NOT always be a primitive root for prime p . In fact it is unknown whether or not 2 will be an primitive root for infinitely many p . Since no choice of a number a is more likely to be a primitive root than any other number one could also try to find a primitive root by picking a random number a .

In[17]:=

```
a = Random[Integer, {2, n - 1}]
```

Out[17]= 211 234 412 019 328 624 870 031 838 401 793 240 663

We first test to see if the $(n - 1)$ st power of a is one. (If it is not then n is composite since it fails FLT for x).

In[18]:=

```
PowerMod[a, (n - 1), n]
```

Out[18]= 1

We get one, so we now run the tests to see whether or not a is a primitive root (mod n).

In[19]:=

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

Out[19]= 1

In[20]:=

```
PowerMod[a, (n - 1) / p1, n]
```

Out[20]= 49 997 390 898 395 840 136 049 600 219 109 965 841

In[21]:=

```
PowerMod[a, (n - 1) / p2, n]
```

Out[21]= 106 761 124 733 486 022 593 356 494 948 463 636 110

If all of the above numbers are NOT equal to one. Then a is a primitive root and n is prime. If a single one of the above numbers IS equal to 1, then a is not a primitive root so we cannot conclude n is prime or composite. We must choose another a at random and compute the above numbers again.

We note than if n is prime the probability that a randomly chosen value of x will be a primitive root is $(\text{EulerPhi}[n - 1]) / (n - 1)$. We will compute this for our example (to get a decimal value put N[]).

In[22]:=

```
N[EulerPhi[n - 1] / (n - 1)]
```

Out[22]= 0.5

So our chances of picking a primitive root seem to be 50 % !! This is pretty good. Is it really 50 % ? We ask Mathematica to be more accurate.

In[23]:=

```
N[EulerPhi[n - 1] / (n - 1), 10]
```

Out[23]= 0.5000000000

Still looks like 50 %. We can ask for even more accurate.

```
In[24]:= N[EulerPhi[n - 1] / (n - 1), 20]
```

```
Out[24]= 0.499999999999999966130
```

So we see that our chances weren't exactly 50% but pretty close. The fewer prime factors $n - 1$ has the better your chances of finding a primitive root. However with fewer prime factors of $n - 1$ it is more difficult to factor !