\[ \text{In}[1] := 1 + 1 \]
\[ \text{Out}[1] = 2 \]

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

\[ \text{In}[3] := \text{PowerMod}[2, n-1, n] \]
\[ \text{Out}[3] = 161\,591\,896\,740\,488\,434\,629\,592\,418\,561\,956\,941\,261 \]

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.

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

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

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

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

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

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 (mod n) since n could be a Carmichael number (that is composite, but still satisfies \(a^{n-1}\) = 1 (mod 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.
Here $n - 1$ is the product of three primes, 2, $p_1 = 1476241557300827$, and $p_2 = 48384280209696856047731$. We apply Luca’s Theorem to see if we can find a number $a \mod n$ with order $n - 1$, i.e. a primitive root.

We start by trying $a = 2$.

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]= 211234412019328624870031838401793240663

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 \((\text{mod } n)\).

In[19]:=
    PowerMod[a, (n - 1)/2, n]
Out[19]= 1

In[20]:=
    PowerMod[a, (n - 1)/p1, n]
Out[20]= 49997390898395840136049600219109965841

In[21]:=
    PowerMod[a, (n - 1)/p2, n]
Out[21]= 106761124733486022593356494948463636110

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 that 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]= 0.500000000

Still looks like 50%. We can ask for even more accurate.
In[24]:=
   N[EulerPhi[n - 1] / (n - 1), 20]

Out[24]= 0.4999999999999996130

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!