

1 + 1
2

Here is a large odd number.

m = 1 195 068 768 795 265 792 518 361 315 725 116 351 898 245 581
1 195 068 768 795 265 792 518 361 315 725 116 351 898 245 581

We will ask Mathematica whether this number is prime or not.

PrimeQ[m]
False

We can ask Mathematica HOW it knows the above number is not a prime.

To do this we must first load the PrimalityProving package. NOTE
that it is necessary to put the ` (left quote) mark at the end !!

<< PrimalityProving`

Now we can ask Mathematica to tell us why it knows this integer is NOT prime.

PrimeQCertificate[m]
{1 195 068 768 795 265 792 518 263 537 659 322 626 328 455 738,
2, 1 195 068 768 795 265 792 518 361 315 725 116 351 898 245 581}

When it returns an answer of {s, 2, m} with s not equal
to 1 or m - 1 that means that s^2 is congruent to 1 (mod m),
i.e. it has found a non-trivial square root of one. Lets label the solution Mathematica gave us as s.

s = 1 195 068 768 795 265 792 518 263 537 659 322 626 328 455 738
1 195 068 768 795 265 792 518 263 537 659 322 626 328 455 738

We will now show how we can find the non-trivial solutions of $x^2 = 1$ (mod m) from the prime factorization of m.

This integer is not too large for Mathematica to factor, so we do so :

NOTE : Of course you KNOW the prime factors of your own m !

FactorInteger[m]
{{24 444 516 448 431 392 447 461, 1}, {48 889 032 896 862 784 894 921, 1}}

We note that it took longer for Mathematica to factor this integer than it did to tell us that it was composite. However now that we know it has two prime factors we know there are two non-trivial solutions to x^2 congruent to 1 (mod m).

Let ' s find BOTH of them using
Mathematica. (One of them should be the one Mathematica gave us above) .

p = 24 444 516 448 431 392 447 461

24 444 516 448 431 392 447 461

q = 48 889 032 896 862 784 894 921

48 889 032 896 862 784 894 921

Mathematica has a built - in Chinese Remainder Command ! We use it to solve $x = 1 \pmod{p}$ and $x = -1 \pmod{q}$.

ChineseRemainder[{1, -1}, {p, q}]

1 195 068 768 795 265 792 518 263 537 659 322 626 328 455 738

Let ' s label this s1

s1 = 1 195 068 768 795 265 792 518 263 537 659 322 626 328 455 738

1 195 068 768 795 265 792 518 263 537 659 322 626 328 455 738

Is this the one Mathematica gave us ? Let ' s see

s1 - s

0

IT IS!

Let ' s find the other one, which is given by a solution to $x = -1 \pmod{p}$ and $x = 1 \pmod{q}$.

ChineseRemainder[{-1, 1}, {p, q}]

97 778 065 793 725 569 789 843

Let ' s label this s2

s2 = 97 778 065 793 725 569 789 843

97 778 065 793 725 569 789 843

We can check that $s1^2$ and $s2^2$ are both congruent to 1 (mod m) :

Mod[s1^2, m]

1

```
Mod[s2^2, m]
```

```
1
```

NOTE : The command `Mod[a, m]` computes $a \pmod{m}$. However to compute large powers such as $a^n \pmod{m}$ where n is large one needs to use `PowerMod[a, n, m]`. Since in the above $n = 2$ is small the regular `Mod` command works fine.

We have found our two non - trivial square roots of 1 !!