

You and I are going to flip coins electronically using my value of $m = 32353319$, which is the product of two primes p and q . You will win if you can factor my m by playing the following game and I will win if you can't.

$m = 32353319$

32353319

You choose a value of a , $1 < a < m$, such that $a^2 > m$. Let's suppose you choose a randomly

```
In[40]:= a = Random[Integer, {2, m - 1}]
```

```
Out[40]= 29814599
```

```
In[41]:= a^2 - m
```

```
Out[41]= 888910281177482
```

$a^2 > m$ so it is OK.

You calculate $a^2 \pmod{m}$. Let's call this sqm (for square (mod m))

```
In[43]:= sqm = Mod[a^2, m]
```

```
Out[43]= 26913729
```

You send me the number sqm .

It will be a square (mod m) if and only if it is a square (mod p) and a square (mod q). I can check this by using the `JacobiSymbol` command. I enter my p and q (which only I know).

NOTE: It is NOT enough just to check `JacobiSymbol[sqm, m]` since this is equal to `JacobiSymbol[sqm, p] * JacobiSymbol[sqm, q]` and if they are both (-1) the value will be 1 even though sqm is NOT a square (mod m).

$p = 5683$

5683

$q = 5693$

5693

```
In[44]:=
      JacobiSymbol[sqm, p]
```

```
Out[44]= 1
```

```
In[45]:=
      JacobiSymbol[sqm, q]
```

```
Out[45]= 1
```

I ' m going to calculate a solution to $x^2 =$
 $sqm \pmod{m}$. I do this by calculating a solution to $x^2 = sqm \pmod{p}$ and a solution to $x^2 =$
 $sqm \pmod{q}$ and then using CRT to get a solution \pmod{m} .

First reduce $sqm \pmod{p}$. We ' ll call the result $sqmp$.

```
In[46]:=
      sqmp = Mod[sqm, p]
```

```
Out[46]= 4724
```

(If get a warning message telling me $sqmp$ is close in spelling to sqm
but I ignore it since I want to use $sqmp$) Let ' s check Mathematica knows $sqmp$

```
In[47]:=
      sqmp
```

```
Out[47]= 4724
```

I want to solve
 $x^2 \pmod{p}$. Since $p =$
 $3 \pmod{4}$ I can do this by calculating the $(p + 1) / 4$ - th power as noted in
Exercise 25.6 of our book. We ' ll call the answer $solp$ (for solution \pmod{p}) .

```
In[48]:=
      solp = PowerMod[sqmp, (p + 1) / 4, p]
```

```
Out[48]= 4102
```

Let ' s check this is a solution

```
In[49]:=
      Mod[solp^2, p]
```

```
Out[49]= 4724
```

We now reduce $sqm \pmod{q}$ and call the result $sqmq$.

```
In[51]:=
      sqmq = Mod[sqm, q]
```

```
Out[51]= 2918
```

I want to solve $x^2 = sqmq \pmod{q}$. Since $q = 5693$ is not congruent to 3 (mod 4), but it is congruent to 5 (mod 8) so I know by Exercise 25.7 that one of the formulas given there will give me a solution. Furthermore I know by the exercise (and by what we showed in class) that the first formula will work if $sqmq^{((q-1)/4)} \equiv 1 \pmod{q}$ and the second one will work if $sqmq^{((q-1)/4)} \equiv -1 \pmod{q}$.

```
In[52]:=
      PowerMod[sqmq, (q - 1) / 4, q]
```

```
Out[52]= 5692
```

Based on this answer I compute 1) OR 2) below.

1) If we get + 1 we the following formula gives the answer, which we will call solq

```
solq = PowerMod[sqmq, ((q + 3) / 8), q]
```

2) If we get - 1 we use the other formula. The other possible solution to $x^2 = sqmq \pmod{q}$ is :

```
In[53]:=
      solq = Mod[(2 * sqmq) * PowerMod[(4 * sqmq), ((q - 5) / 8), q], q]
```

```
Out[53]= 358
```

Let ' s see if our answer is a solution.

```
In[55]:=
      sqmq
```

```
Out[55]= 2918
```

```
In[54]:= Mod[solq^2, q]
```

```
Out[54]= 2918
```

So we have solutions $x = +$ or $-$ $\text{solp} \pmod{p}$ and $x = +$ or $-$ $\text{solq} \pmod{q}$

I choose one solution (i.e. $+$ or $-$) to each at random. Suppose I choose $+$ $\text{solp} \pmod{p}$ and $-$ $\text{solq} \pmod{q}$.

I now want to find the solution \pmod{m} that corresponds to these two solutions using the Chinese Remainder Theorem.

Let 's choose a possibility randomly. I 'll use 1) for ++, 2) for +-, 3) for -+ and 4) for --.

```
In[56]:= Random[Integer, {1, 4}]
```

```
Out[56]= 4
```

If we load a Number Theory package into Mathematica there is a Chinese Remainder command that will combine these congruences for us.

```
<< NumberTheory`NumberTheoryFunctions`
```

Let 's call the solution c .

```
In[57]:= c = ChineseRemainder[{- solp, -solq}, {p, q}]
```

```
Out[57]= 23750838
```

Let 's check that this is indeed a solution to $x^2 = b \pmod{m}$

```
In[58]:= sqm
```

```
Out[58]= 26913729
```

```
In[59]:= PowerMod[c, 2, m]
```

```
Out[59]= 26913729
```

It is.

For the purposes of this demo let 's see if it is equal to your original value a , which is also a solution. Note that I wouldn ' t know your choice of a however,

```
In[60]:= a
```

```
Out[60]= 29814599
```

I email you my solution solm, which is c. One possibility is that my solution c is your original a, but this occurs only with probability 1 / 4. It could also be - a , but the probability it is + a or - a is exactly 1 / 2.

Now you try to factor my m using this number. You do so by computing gcd of a + c and m.

```
In[61]:= GCD[a + c, m]
```

```
Out[61]= 5693
```

If the GCD is NOT 1 or m, the result is one of my prime factors (i.e. either p or q) and YOU WIN. If you get 1 or m. I WIN.

You WON this flip!.