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.

\[ m = 32353319 \]

You choose a value of \( a \), \( 1 < a < m \), such that \( a^2 > m \). Let’s suppose you choose a randomly

\[ a = \text{Random}[\text{Integer}, \{2, m-1\}] \]

\[ a = 29814599 \]

\[ a^2 - m \]

\[ a^2 > m \text{ so it is OK.} \]

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

\[ \text{sqm} = \text{Mod}[a^2, m] \]

\[ \text{sqm} = 26913729 \]

You send me the number \( \text{sqm} \).

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 \text{JacobiSymbol} command. I enter my \( p \) and \( q \) (which only I know).

\[ p = 5683 \]

\[ 5683 \]

\[ q = 5693 \]

\[ 5693 \]
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 \( sqmq \).
I want to solve $x^2 = sqm\mod q$. 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 $sqm^{(q-1)/4} = 1 \mod q$ and the second one will work if $sqm^{(q-1)/4} = -1 \mod q$.

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[sqm, (q + 3)/8, q]

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

Let’s see if our answer is a solution.


\[ \text{In[54]} := \quad \text{Mod[solq}^2, q] \]

\[ \text{Out[54]} = 2918 \]

So we have solutions \( x = + \text{ or } - \text{ solp (mod p)} \) and \( x = + \text{ or } - \text{ solq (mod q)} \)

I choose one solution (i.e. + or -) to each at random. Suppose I choose + solp (mod p) and - solq (mod q). I now want to find the solution (mod 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 --.

\[ \text{In[56]} := \quad \text{Random[Integer, \{1, 4\}] } \]

\[ \text{Out[56]} = 4 \]

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

\[ << \text{NumberTheory`NumberTheoryFunctions} \]

Let’s call the solution c.

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

\[ \text{Out[57]} = 23750838 \]

Let’s check that this is indeed a solution to \( x^2 \equiv b \pmod{m} \)

\[ \text{In[58]} := \quad \text{sqm} \]

\[ \text{Out[58]} = 26913729 \]
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!