Modular Arithmetic Equations and the Euclidean Algorithm
Berkeley Math Circle, April 8, 2014 Ayelet Lindenstrauss

In previous weeks you learned how to add, subtract, and multiply in modular arithmetic. Now we want to solve simple equations:

1. Can you find an integer x so that $4x \equiv 2 \pmod 5$?
   Can you find another solution?
   How about $x = -22$? Does it work?
   Show that if x is a solution, so are $x + 5$ and $x - 5$.
   Explain why if x and y are both solutions, then $x - y$ is divisible by 5.

2. Can you find an integer x so that $4x \equiv 2 \pmod 6$?
   Can you find another solution?
   Is it true that if x is a solution, so are $x + 6$ and $x - 6$?
   Is it true that if x and y are both solutions, then $x - y$ is divisible by 6?

3. Can you solve $4x \equiv 1 \pmod 6$?
   How about $4x \equiv 3 \pmod 6$? $4x \equiv 4 \pmod 6$? $4x \equiv 5 \pmod 6$? $4x \equiv 0 \pmod 6$?
   Can you solve $3x \equiv 5 \pmod 6$?

Explanation:

For any integers a, x and k, if you look at $ax + 6k$ it will always be divisible by $\gcd(a, 6)$. If we would like it to equal some number b which is **not** divisible by $\gcd(a, 6)$, this isn't going to work.

Question:

But what if that isn't an issue? Will we then have a solution?
When the numbers grow, it becomes harder to guess.

4. Can you solve $17x \equiv 4 \pmod{37}$? (Here $\gcd(17, 37) = 1$, so that does not stop us.)
   A magician drops you a note that says:

   HINT: $17 \cdot (-13) + 37 \cdot 6 = 1$

   Does that help you solve $17x \equiv 1 \pmod{37}$?
   Does that help you solve $17x \equiv 4 \pmod{37}$?

But how did the magician come up with that good hint?

The answer involves the Euclidean Algorithm, but before we learn it, we can start with a story. Two merchants are riding their horses to the big market. Each of them has three sacks on his horse: one big sack with things he wants to sell, and two smaller sacks of coins, to be able to give change when people buy things. But to simplify carrying the coins, they have only two kinds: one bag of 10 cent coins and one bag of 25 cent coins.

As they ride, they tell each other of all the things they are selling, and they begin to want to buy each other's merchandise. So they want to sell things to each other along the way. Merchant A wants to buy a pen that Merchant B is selling for 50 cents, so he gives him two 25 cent coins. But then, he decides he also wants a pencil that Merchant B is selling for 40 cents. Can they handle it?

What if Merchant A wants a comb that Merchant B is selling for 35 cents?

What if Merchant A wants a brush that Merchant B is selling for 45 cents?

What if Merchant A wants a piece of gum that Merchant B is selling for 5 cents?

Can they buy or sell anything with a price that is a multiple of 5 cents, without I.O.U.'s?

What if Merchant A wants a piece of candy that Merchant B is selling for 7 cents?

In a foreign country with another currency, we have another pair of merchants in the same situation, except that there, each merchant has one bag of 3 pennypod coins and one bag of 7 pennypod coins. Can the foreign Merchant A sell the foreign Merchant B a piece of candy that costs 1 pennypod? Can he sell him anything that costs a whole number of pennypods?

What we're doing: We're taking two integers x and y ($x = 10$ and $y = 25$ in the first example, or $x = 3$ and $y = 7$ in the second). In our examples, they are both positive. We're trying to find all the numbers that can be written as $ax + by$, with a and b integers. (The numbers a and b are allowed to be negative because each merchant has his own sacks of coins, so they can also give change.)

Clearly, if $\gcd(x, y) = z$ then z will also divide $ax + by$ for any integers a and b. If we could manage to write $z = ax + by$ for suitable integers a and b, we could also do it for any multiples of z, and then we would know we had come up with the maximal list of numbers that could be written that way.

Thie is where the **Euclidean Algorithm** comes in. It allows you to find greatest common divisors and write them as a combination of your original numbers: Take your x and y. For our purposes, you might as well assume they are non-negative. Let $\mathbf{x_1}$ be the bigger of the two, and $\mathbf{x_2}$ the smaller.

Example: Say $x = 72$ and $y = 233$. So $\mathbf{x_1} = \mathbf{233}$ and $\mathbf{x_2} = \mathbf{72}$.

Now divide $\mathbf{x_1}$ by $\mathbf{x_2}$ with remainder, and call that remainder $\mathbf{x_3}$. Note that $\mathbf{x_3} < \mathbf{x_2}$.

In Our Example: $\mathbf{233} = 3 \cdot \mathbf{72} + \mathbf{17}$, so we let $\mathbf{x_3} = \mathbf{17}$.

Now divide $\mathbf{x_2}$ by $\mathbf{x_3}$ with remainder, and call that remainder $\mathbf{x_4}$. Note that $\mathbf{x_4} < \mathbf{x_3}$.

In Our Example: $\mathbf{72} = 4 \cdot \mathbf{17} + \mathbf{4}$, so we let $\mathbf{x_4} = \mathbf{4}$.

Keep going. This cannot go on forever (why?) so at some point you will, for the first time, have $\mathbf{x_n} = 0$. Then you will have $\mathbf{x_{n-1}} = \gcd(\mathbf{x_1}, \mathbf{x_2})$. And why is that? Because if an integer k divides both $\mathbf{x_1}$ and $\mathbf{x_2}$, it would have to also divide $\mathbf{x_3}$, but then dividing $\mathbf{x_2}$ and $\mathbf{x_3}$, it would also have to divide $\mathbf{x_4}$, and so on, up to $\mathbf{x_{n-1}}$. But on the other hand, if k divides $\mathbf{x_{n-1}}$, it would also divide $\mathbf{x_{n-2}}$, and dividing both $\mathbf{x_{n-1}}$ and $\mathbf{x_{n-2}}$, it would have to divide $\mathbf{x_{n-3}}$, and so on, up to $\mathbf{x_2}$ and $\mathbf{x_1}$.

In Our Example: $\mathbf{17} = 4 \cdot \mathbf{4} + \mathbf{1}$, so we let $\mathbf{x_5} = \mathbf{1}$. Then $\mathbf{4} = 4 \cdot \mathbf{1} + \mathbf{0}$, so we finish when $n = 6$ and have $\mathbf{1} = \mathbf{x_5} = \gcd(\mathbf{233}, \mathbf{72})$.

And Now Work Backwards to Recover the Coefficients:

$$\begin{aligned}\mathbf{1} &= \mathbf{17} - 4 \cdot \mathbf{4} = \mathbf{17} - 4 \cdot (\mathbf{72} - 4 \cdot \mathbf{17}) \\ &= (-4) \cdot \mathbf{72} + 17 \cdot \mathbf{17} = (-4) \cdot \mathbf{72} + 17(\mathbf{233} - 3 \cdot \mathbf{72}) = 17 \cdot \mathbf{233} - 55 \cdot \mathbf{72},\end{aligned}$$

and we are done!