Math Circles - Lesson 1
Introduction to Linear Diophantine Equations

Zack Cramer - zcramer@uwaterloo.ca

February 28, 2018

(I) Mario has forgotten how to run, and instead can only jump forward or backward. He can make long jumps 8 metres in length, or short jumps 3 metres in length. A goomba (who has also forgotten how to run) stands 10 metres away.

Is there a sequence of jumps that will allow Mario to land on the goomba?

(II) Squidward operates a shoe store in Bikini Bottom. He can buy shoes from his supplier in bundles of 14 or 35, and can sell them in the same quantities.

Is there a way to buy and sell bundles so that exactly 4 shoes remain at the end of the day?

(III) Becky needs $2.15 to buy an extra large coffee. She only has quarters and dimes, and the cashier insists that she pay with exact change.

Is there a combination of quarters and dimes that will total $2.15?

1 Diophantine Equations

A **Diophantine equation**, named after Diophantus of Alexandria (right), is a polynomial equation with integer coefficients that is intended to be solved with integer solutions. You may have never heard of Diophantine equations, but I bet you've seen some examples.

Diophantus of Alexandria
3rd Centrury A.D.

The equation

$$x^2 + y^2 = z^2$$

reminds us of the ____________________ ______________. Positive integer solutions to this equation (e.g. $x = 3$, $y = 4$, $z = 5$) correspond to right triangles with integer side lengths. These solutions are called *Pythagorean triples.* Can you think of any more?

The equations

$$x^n + y^n = z^n \qquad (n \geq 3)$$

are famous as well. In 1994, Andrew Wiles showed that these equations have no non-trivial integer solutions! This provided an answer to a question dating back to 1637, which we know today as ____.

2 Linear Diophantine Equations

As you can see, Diophantine equations can be pretty complicated! The equations we'll be studying are much simpler. A (two-variable) **linear Diophantine equation** (**LDE**) has the form

$$ax + by = c$$

for some integers a, b, and c.

The three word problems we started with can be expressed as LDEs:

(I) Let x be the number of long jumps Mario makes.

Let y be the number of short jumps Mario makes.

We are looking for a solution to the LDE $8x + 3y = 10$.

(II) Let x be the number of 14-shoe bundles exchanged.

Let y be the number of 35-shoe bundles exhanged.

We are looking for a solution to the LDE ______________________________.

(III) Let x be ____.

Let y be ____.

We are looking for a solution the LDE ______________________________.

As we saw above, some LDEs have solutions, and others do not. For example, can we tell if the equation

$$3x + 6y = 2$$

has a solution? Notice that the numbers on the left side are divisible by 3. If we divide both sides by 3, the equation becomes

$$x + 2y = \frac{2}{3}.$$

Uh oh... do you see a problem?

This LDE does not have a solution because

What went wrong here? The problem is that there's an integer (in this case 3) that divides both coefficients in our LDE, but does not divide the number of the right-hand side. In general, we have the following result:

Proposition (Necessary Condition for Solutions)**.** If d is a number that divides both a and b, but d does not divide c, then the LDE

$$ax + by = c$$

has no solutions.

Example. Let's go back to problem (II). Does the LDE

$$14x + 35y = 4$$

have a solution? No: _____ divides 14 and 35, but does not divide 4. Sorry Squidward!

If we're going to discuss whether or not we can solve LDEs, it looks like we'll need to talk about *common divisors*.

3 GCDs and the Euclidean Algorithm

Definition. Suppose that a and b are integers.

(i) If c is an integer that divides both a and b, we call c a **common divisor** of a and b.

(ii) The biggest integer dividing both a and b is called the **greatest common divisor** of a and b, denoted $\gcd(a, b)$.

Example. What is $\gcd(48, 32)$? Let's list the divisors:

Divisors of 48: ____

Divisors of 32: ____

The biggest one they have in common is _____, so $\gcd(48, 32) =$_____.

Writing out all the divisors wasn't *too* bad in this example, but what if I asked you to calculate $\gcd(1\,053, 993)$? What about $\gcd(7\,404, 7\,032)$? Our goal for this section is to find a better way to calculate $\gcd(a, b)$. The first step is the **division algorithm**.

The Division Algorithm. Let a and b be integers with $b > 0$. There are unique integers q (the *quotient*) and r (the *remainder*) such that

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < b.$$

Furthermore, $\gcd(a, b) = \gcd(b, r)$.

Example. Let's try a few examples using the division algorithm.

(i) If $a = 8$ and $b = 3$, then $8 = 3(\underline{\ \ 2\ \ }) + \underline{\ \ 2\ \ }$.

(ii) If $a = 46$ and $b = 10$, then $46 = 10(\underline{\hspace{1.5cm}}) + \underline{\hspace{1.5cm}}$.

(iii) If $a = 384$ and $b = 171$, then $384 = 171(\underline{\hspace{1.5cm}}) + \underline{\hspace{1.5cm}}$.

The last line in the statement of the division algorithm says that $\gcd(a, b) = \gcd(b, r)$. How can this help us calculate $\gcd(a, b)$?

Effectively, this allows us to replace a with r, and calculate $\gcd(b, r)$ instead. This is easier to compute because the numbers are smaller.

Example. From previous question, we see that

(i) $\gcd(8, 3) = \gcd(\underline{\ \ 3\ \ }, \underline{\ \ 2\ \ })$.

(ii) $\gcd(46, 10) = \gcd(\underline{\hspace{1.5cm}}, \underline{\hspace{1.5cm}})$.

(iii) $\gcd(384, 171) = \gcd(\underline{\hspace{1.5cm}}, \underline{\hspace{1.5cm}})$.

But why stop here? We can repeat the division algorithm on the pair (b, r) and get an *even easier* gcd to calculate. This process is known as the **Euclidean algorithm**.

The Euclidean Algorithm.

Step 1: Arrange a and b so that $a \geq b$.

Step 2: Write $a = bq + r$ where $0 \leq r < b$.

Step 3: If $r = 0$, then stop! We get $\gcd(a, b) = \gcd(b, 0) = b$.

Step 4: Replace (a, b) with (b, r) and return to Step 1.

Example. Let's use the Euclidean algorithm to find the following GCDs.

(i) $\gcd(8, 3)$

$$8 = 3(2) + 2 \quad \Rightarrow \quad \gcd(8, 3) = \gcd(3, 2) \tag{1}$$

$$3 = 2(1) + 1 \quad \Rightarrow \quad \gcd(3, 2) = \gcd(2, 1) \tag{2}$$

$$2 = 1(2) + 0 \quad \Rightarrow \quad \gcd(2, 1) = \gcd(1, 0) \tag{3}$$

Here we can stop. Since the remainder in line (3) is 0, the Euclidean algorithm tells us that $\gcd(8, 3) = \gcd(1, 0) = 1$.

(ii) $\gcd(46, 10)$

$$46 = 10(4) + 6 \quad \Rightarrow \quad \gcd(46, 10) = \gcd(10, 6) \tag{1}$$

$$\Rightarrow \tag{2}$$

$$\Rightarrow \tag{3}$$

$$\Rightarrow \tag{4}$$

Here we can stop. Since the remainder in line (4) is 0, the Euclidean algorithm tells us that $\gcd(46, 10) =$ ____________________.

(iii) $\gcd(384, 171)$

One thing you may have noticed is that the GCD is the **last non-zero remainder** seen in the Euclidean algorithm.

4 Solving LDEs with the Euclidean Algorithm

Notice that we didn't have to keep track of our steps in the above examples, though it turns out that this careful bookkeeping is a good idea.

Why? It's because the Euclidean algorithm not only finds $\gcd(a, b)$, but by working backwards we can actually use it to solve LDEs!

Example. Find a solution for each of the following LDEs:

(i) $8x + 3y = 10$

Solution. Recall the following steps from the Euclidean algorithm in the last example:

$$\begin{aligned} 8 &= 3(2) + 2 \qquad (1) \\ 3 &= 2(1) + 1. \qquad (2) \end{aligned}$$

We found that $\gcd(8, 3) = 1$. From (2), we get

$$1 = 3 - \underline{\ 2\ }(1)$$

Using (1), we can replace the underlined number with $8 - 3(2)$:

$$\begin{aligned} 1 &= 3 - [8 - 3(2)](1) \\ &= 3 - [8 - 3(2)] \\ &= 8(-1) + 3(3). \end{aligned}$$

Neat! The Euclidean algorithm gave us the equation

$$8(-1) + 3(3) = 1.$$

Now how can we get a solution to our LDE? Multiply by 10! A solution is

$$\underline{8(-10) + 3(30) = 10}.$$

(ii) $46x + 10y = 2$

Solution. Recall the following steps from the Euclidean algorithm in the last example:

$$\begin{aligned} 46 &= \underline{\hspace{12em}} \qquad (1) \\ \underline{\hspace{2.5em}} &= \underline{\hspace{12em}} \qquad (2) \\ \underline{\hspace{2.5em}} &= \underline{\hspace{12em}}. \qquad (3) \end{aligned}$$

We found that $\gcd(46, 10) = \underline{\hspace{2.5em}}$. From (3), we get

$$\underline{\hspace{2.5em}} = \underline{\hspace{12em}}.$$

Using (2), we can replace the underlined number with $\underline{\hspace{7em}}$:

Using (1), we can replace the underlined number with $\underline{\hspace{7em}}$:

We arrive at the solution $\underline{46(\hspace{2em}) + 10(\hspace{2em}) = 2}$.

(iii) $384x + 171y = 24$

Solution.

The following theorem summarizes what we have observed on solutions to LDEs:

Theorem. The LDE

$$ax + by = c$$

has a solution if and only if $\gcd(a, b)$ divides c.

Using the Euclidean algorithm and working backwards, we get an equation of the form

$$ax_0 + by_0 = \gcd(a, b).$$

The solution to the LDE can then be obtained by multiplying both sides of this equation by $\frac{c}{\gcd(a,b)}$. So we have $ax + by = c$ where

$$x = x_0 \cdot \frac{c}{\gcd(a,b)} \quad \text{and} \quad y = y_0 \cdot \frac{c}{\gcd(a,b)}.$$