# Grade 9/10 Math Circles

## February 9, 2022

## Linear Diophantine Equations Part 1

## Introduction

In this lesson (and the next), we will explore *linear Diophantine equations*. For this lesson, we will focus on what these equations are, when a solution exists, and how to find a solution when one exists. In the lesson two weeks from now, we will explore how to find all solutions to linear Diophantine equations, and also look at finding solutions under various constraints.

## Diophantine Equations

A **Diophantine equation**, named after Diophantus of Alexandria, is a polynomial equation with integer coefficients that is intended to be solved with integer solutions.

One Diophantine equation you've likely seen is

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

Positive integer solutions to this Diophantine equation (for example, $x = 3$, $y = 4$, $z = 5$) correspond to right-angled triangles with integer side lengths.

Another famous Diophantine equation is

$$x^n + y^n = z^n$$

where $n$ is an integer $\geq 3$. It has been shown that this Diophantine equation has no solution where $x$, $y$, and $z$ are positive integers. This was first stated by the mathematician Fermat in the 1600s, but was not proven until 1994 by the mathematician Andrew Wiles.

## Linear Diophantine Equations

In this lesson, we're going to focus on *linear* Diophantine equations. A (two-variable) **linear Diophantine equation** is an equation of the form

$$ax + by = c$$

where $a$, $b$, and $c$ are given integers and we are interested in solving for *integers* $x$ and $y$.

**Example 1**

Sara needs \$2.15 to buy a 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?

*Solution:*

We need to solve the equation $25x + 10y = 215$, where $x$ and $y$ are integers. Since $x$ and $y$ represent the number of quarters and dimes, respectively, that Sara uses, notice that it makes sense that we are only interested in integer solutions to this equation. Further, we should also ensure that $x$ and $y$ are not negative.

By using systematic guess and check, we can come up with the following possible solutions:

$$x = 1 \text{ and } y = 19, \text{ or } x = 3 \text{ and } y = 14, \text{ or } x = 5 \text{ and } y = 9, \text{ or } x = 7 \text{ and } y = 4$$

There are no other solutions. Can you see why?

**Example 2**

A robot can move backwards or forwards with big steps (130 cm) or small steps (50 cm). Is there a series of moves that the robot can make to end up 10 cm ahead of where it started?

*Solution:*

We need to solve the equation $130x + 50y = 10$, where $x$ and $y$ are integers.

Using guess and check, we find one (of many) solutions to be $x = 2$ and $y = -5$. That is, if the robot takes 2 big steps forward and 5 small steps backward, it will end up 10 cm ahead of where it started.

There are many other solutions. Can you find another solution?

It is not always easy to find a solution to a linear Diophantine equation by trial-and-error.

For example, trial-and-error could be time consuming if we used that technique to find integers $x$ and $y$ that satisfy the linear Diophantine equation

$$1053x + 481y = 13$$

**Main Question for this Lesson**

Given three integers $a$, $b$, and $c$, how can we find a solution to $ax + by = c$, where $x$ and $y$ are integers?

Be careful! There may not be an integer solution! In this lesson, we will determine conditions on $a$, $b$, and $c$ that guarantee an integer solution to the equation $ax + by = c$, and learn a method for finding such a solution, in the case where one exists.

### When does a solution exist?

Consider the linear Diophantine equation

$$3x + 6y = 5$$

If we divide both sides by 3, the equation becomes

$$x + 2y = \frac{5}{3}$$

**Stop and Think**

Before reading further, can you see a problem with it being true that $x + 2y = \frac{5}{3}$?

Since we are told $3x + 6y = 5$ is a linear Diophantine equation, a solution must have both $x$ and $y$ being integers. If $x$ and $y$ are both integers, $x + 2y$ must also be an integer, but $\frac{5}{3}$ is not an integer! Therefore, the equation $3x + 6y = 5$ cannot have any integer solutions.

In general, we have the following result:

**Necessary Condition for Solutions**

If $d$ is an integer that divides both $a$ and $b$, but $d$ does not divide $c$, then the linear Diophantine equation

$$ax + by = c$$

has no solutions.

**Exercise 1**

Does the linear Diophantine equation $14x + 35y = 4$ have a solution?

If we're going to discuss whether or not we can solve the linear Diophantine equation $ax + by = c$ for integers $x$ and $y$, it appears as though we'll need to investigate *common divisors* of $a$ and $b$.

## GCDs and the Euclidean Algorithm

Suppose $a$ and $b$ are integers. If $d$ is an integer that divides both $a$ and $b$, we call $d$ a **common divisor** of $a$ and $b$. The largest integer that divides both $a$ and $b$ is called the **greatest common divisor** of $a$ and $b$, denoted $\gcd(a, b)$.

**Example 3**

What is $\gcd(48, 32)$?

*Solution:*

Let's list the positive divisors of each.

Positive divisors of 48: 1, 2, 3, 4, 6, 8, 12, 16, 24, 48

Positive divisors of 32: 1, 2, 4, 8, 16, 32

Since the largest divisor that they have in common is 16, $\gcd(48, 32) = 16$.

Finding $\gcd(a, b)$ by factoring $a$ and $b$ may be very time consuming if $a$ and $b$ are large.

For example, try to calculate $\gcd(3551, 4399)$ or $\gcd(104\,723, 103\,093)$ by factoring.

Instead, we will use a method that does not require us to find a single divisor of $a$ or $b$. 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

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

For example, suppose $a = 15$ and $b = 6$. We can write $15 = 6 \cdot 2 + 3$, so $q = 2$ and $r = 3$. Notice that it is also true that $15 = 6 \cdot 1 + 9$ and $15 = 6 \cdot 3 + (-3)$; however, neither 9 nor $-3$ satisfy the requirement that they are $\geq 0$ and also $< b$. So, it turns out that $q = 2$ and $r = 3$ are the unique $q$ and $r$ satisfying the division algorithm when $a = 15$ and $b = 6$.

**Example 4**

For $a$ and $b$, calculate $q$ and $r$ from the division algorithm.

(a) $a = 30$, $b = 6$

(b) $a = 9$, $b = 6$

(c) $a = -2$, $b = 6$

*Solution:*

(a) $30 = 6 \cdot 5 + 0$, so $q = 5$, $r = 0$.

(b) $9 = 6 \cdot 1 + 3$, so $q = 1$, $r = 3$.

(c) $-2 = 6 \cdot (-1) + 4$, so $q = -1$, $r = 4$.

Now that we know how to find $q$ and $r$ in the division algorithm, we are ready to learn an important fact that will help us calculate greatest common divisors more efficiently.

**Important Fact**

If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

As we saw above, when $a = 15$ and $b = 6$, we have $q = 2$ and $r = 3$. Notice that $\gcd(15, 6) = 3$ and $\gcd(6, 3) = 3$. So the important fact holds, since $\gcd(15, 6) = \gcd(6, 3)$.

Similarly, in Example 4, we saw that when $a = 30$ and $b = 6$, we have $q = 5$ and $r = 0$. Notice that $\gcd(30, 6) = 6$ and $\gcd(6, 0) = 6$. So the important fact holds, since $\gcd(30, 6) = \gcd(6, 0)$. Note that $\gcd(a, 0) = a$ for any positive integer $a$, since 0 is divisible by every positive integer.

**Exercise 2**

For $a$ and $b$, verify that the important fact holds.

(a) $a = 9$, $b = 6$

(b) $a = -2$, $b = 6$

How can we use the important fact to calculate greatest common divisors more efficiently? We will iterate the division algorithm and apply the important fact each time.

**Example 5**

Calculate $\gcd(117, 55)$.

*Solution:*

Since $117 = 55 \cdot 2 + 7$, we have $q = 2$ and $r = 7$ from the division algorithm. Thus, by the important fact, we know $\gcd(117, 55) = \gcd(55, 7)$.

Now, let's repeat this process on 55 and 7.

Since, $55 = 7 \cdot 7 + 6$, we have $q = 7$ and $r = 6$ from the division algorithm. Thus, by the important fact, we know $\gcd(55, 7) = \gcd(7, 6)$.

Now, let's repeat this process on 7 and 6.

Since, $7 = 6 \cdot 1 + 1$, we have $q = 1$ and $r = 1$ from the division algorithm. Thus, by the important fact, we know $\gcd(7, 6) = \gcd(6, 1)$.

Thus, we can conclude that $\gcd(117, 55) = \gcd(55, 7) = \gcd(7, 6) = \gcd(6, 1) = 1$.

This method of repeatedly using the division algorithm along with the important fact to find the greatest common divisor of two integers is called **the Euclidean algorithm**.

**The Euclidean Algorithm**

*Input:* Positive integers $a$ and $b$.

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

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

Step 3: If $r = 0$, then stop! If $r > 0$, then go back to Step 1, this time with the pair $(b, r)$.

*Output:* The last non-zero remainder $r$ if such an $r$ exists, or else output $b$.

The greatest common divisor of the two integers will be equal to the last non-zero remainder that is seen in the Euclidean algorithm. When working through this algorithm, we will use the fact that $\gcd(a, 0) = a$, for any positive integer $a$.

Let's work through another example to convince ourselves that this algorithm will always output $\gcd(a, b)$.

**Example 6**

Calculate $\gcd(481, 1053)$ using the Euclidean algorithm.

*Solution:*

Here we will apply the Euclidean algorithm to the pair $(481, 1053)$. We will keep track of what is happening with the gcd on the right-hand side.

| | |
|---|---|
| As $481 < 1053$, set $a = 1053$ and $b = 481$ | $\gcd(481, 1053) = \gcd(1053, 481)$ |
| Write $1053 = 481 \cdot 2 + 91 \quad (r = 91)$ | $\gcd(1053, 481) = \gcd(481, 91)$ |
| Write $481 = 91 \cdot 5 + 26 \quad (r = 26)$ | $\gcd(481, 91) = \gcd(91, 26)$ |
| Write $91 = 26 \cdot 3 + 13 \quad (r = 13)$ | $\gcd(91, 26) = \gcd(26, 13)$ |
| Write $26 = 13 \cdot 2 + 0 \quad (r = 0)$ | $\gcd(26, 13) = \gcd(13, 0) = 13$ |

From the gcd equalities on the right hand side, we see that $\gcd(481, 1053) = \gcd(13, 0) = 13$.

**Stop and Think**

Since $r < b$, the integers get smaller after each iteration of the division algorithm, and so this procedure must eventually stop. Can you convince yourself that you will always reach a remainder of zero, and that the output will always be $\gcd(a, b)$?

**Exercise 3**

Calculate $\gcd(427, 616)$ using the Euclidean algorithm.

## Using the Euclidean algorithm to solve linear Diophantine equations

As we'll see in our next example, the Euclidean algorithm not only finds $\gcd(a, b)$, but by working backwards, we can actually use it to solve linear Diophantine equations!

**Example 7**

Find integers $x$ and $y$ such that $1053x + 481y = 13$.

*Solution:*

As we saw in Example 6, the Euclidean algorithm gives

$$1053 = 481 \cdot 2 + 91 \tag{1}$$
$$481 = 91 \cdot 5 + 26 \tag{2}$$
$$91 = 26 \cdot 3 + 13 \tag{3}$$
$$26 = 13 \cdot 2 + 0 \tag{4}$$

And so $\gcd(1053, 481) = 13$. Notice that this is the value of $c$ in the equation. We can exploit this fact by tracing our steps in the Euclidean algorithm and working backwards as follows:
From (3):

$$13 = \underline{91} - 3 \cdot \underline{26}$$

Substituting for 26 using (2):

$$13 = \underline{91} - 3(\underline{481} - 5 \cdot \underline{91})$$

Simplifying:

$$13 = 16 \cdot \underline{91} - 3 \cdot \underline{481}$$

Substituting for 91 using (1):

$$13 = 16(\underline{1053} - 2(\underline{481})) - 3 \cdot \underline{481}$$

Simplifying:

$$13 = 16(\underline{1053}) - 35(\underline{481})$$

That is, $1053(16) + 481(-35) = 13$. Therefore, one solution is $x = 16$, $y = -35$. Check!

**Exercise 4**

Find integers $x$ and $y$ such that $427x + 616y = 7$.

We now have a strategy to find integers $x$ and $y$ such that $ax + by = c$ when $c = \gcd(a, b)$: We can work backwards through our steps in the Euclidean algorithm, starting with the line where

$r = \gcd(a, b)$, as we saw in Example 7. But what if we need to solve $ax + by = c$, where $c$ is not equal to $\gcd(a, b)$?

**Example 8**

Find integers $x$ and $y$ such that $1053x + 481y = 39$.

*Solution:*

Notice that $39 = 3 \times 13$. From the Example 7, we know that $1053(16) + 481(-35) = 13$. Multiplying the entire equation by 3 gives

$$\begin{aligned} 3\,(1053(16) + 481(-35)) &= 3(13) \\ 3\,(1053(16)) + 3\,(481(-35)) &= 3(13) \\ 1053(3 \cdot 16) + 481(3 \cdot (-35)) &= 39 \\ 1053(48) + 481(-105) &= 39 \end{aligned}$$

Thus, there is a solution, namely $x = 48$, $y = -105$. Check!

From Example 8, we can see that if $\gcd(a, b)$ divides $c$, then we can use a solution to $ax+by = \gcd(a, b)$ to find a solution to the equation $ax + by = c$. What if $\gcd(a, b)$ does not divide $c$?

**Example 9**

Find integers $x$ and $y$ such that $1053x + 481y = 50$.

*Solution:*

Suppose that integers $x$ and $y$ that satisfy the above equation. Since $13 = \gcd(1053, 481)$, we can factor 13 out of the left hand side of the equation:

$$\begin{aligned} 1053x + 481y &= 50 \\ (13 \cdot 81)x + (13 \cdot 37)y &= 50 \\ 13\,(81x + 37y) &= 50 \\ 81x + 37y &= \frac{50}{13} \end{aligned}$$

But since $x$ and $y$ are integers, this last equality is impossible!

Therefore, there is no solution to the linear Diophantine equation $1053x + 481y = 50$.

From Example 9, we can see that if $\gcd(a, b)$ does not divide $c$, then the equation $ax + by = c$ does not have a solution where $x$ and $y$ are integers.

The following theorem summarizes what we have observed about solutions to linear Diophantine equations.

**Theorem**

The linear Diophantine equation

$$ax + by = c$$

has a solution if and only if $\gcd(a, b)$ divides $c$.
Using the Euclidean algorithm and working backwards, we can find integers $x$ and $y$ such that

$$ax + by = \gcd(a, b)$$

Once we have found $x$ and $y$ such that $ax + by = \gcd(a, b)$, we can multiply this solution by $\dfrac{c}{\gcd(a, b)}$ to get a solution to $ax + by = c$.

**Exercise 5**

Find integers $x$ and $y$ such that $427x + 616y = 91$.

**Exercise 6**

Find integers $x$ and $y$ such that $427x + 616y = 101$.