Linear Diophantine Equations

Ryan C. Daileda

Trinity University

Number Theory

Introduction

A *Diophantine equation* is any equation (usually polynomial) in one or more variables that is to be solved in $\mathbb{Z}$.

For example, a *pythagorean triple* is a solution to the Diophantine equation

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

such as $(3, 4, 5)$ or $(5, 12, 13)$.

Solving Diophantine equations is substantially more difficult than solving equations over $\mathbb{R}$, say, since $\mathbb{Z}$ is discrete while $\mathbb{R}$ is continuous and we can appeal to the tools of analysis.

Today we will consider the simplest of all Diophatine equations: linear Diophantine equations in two variables.

Motivating Examples

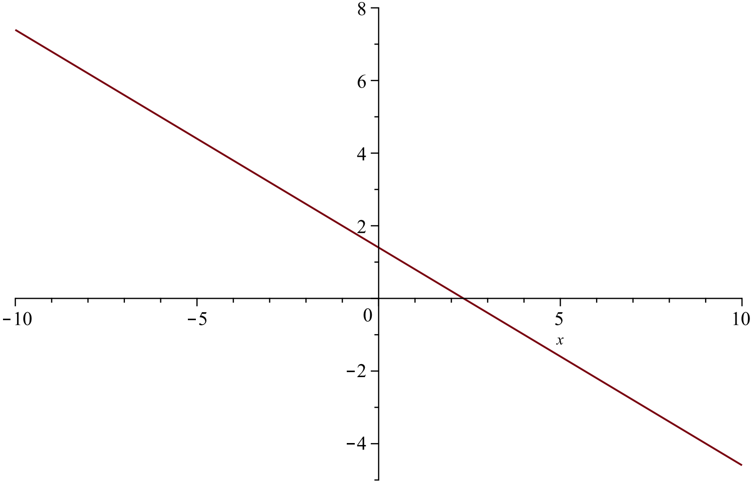
Consider the equation

$$3x + 5y = 7. \tag{1}$$

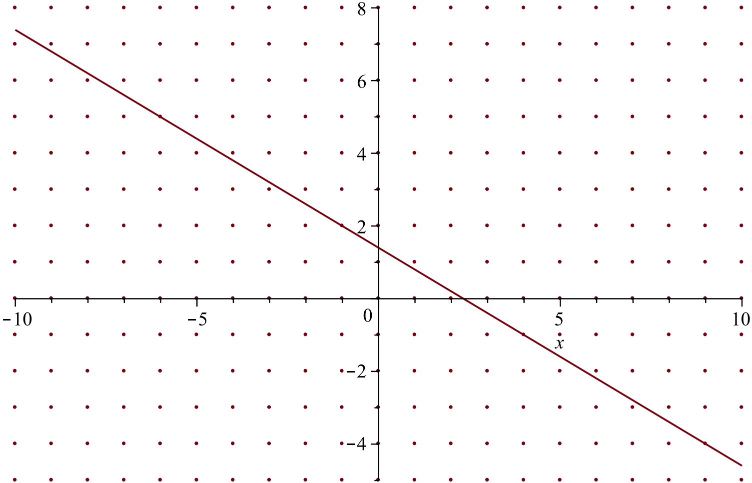
If we work in $\mathbb{R}$, for any x we can solve for y so that (1) holds.

If we plot the points that solve (1) in $\mathbb{R}^2$, we get a line.

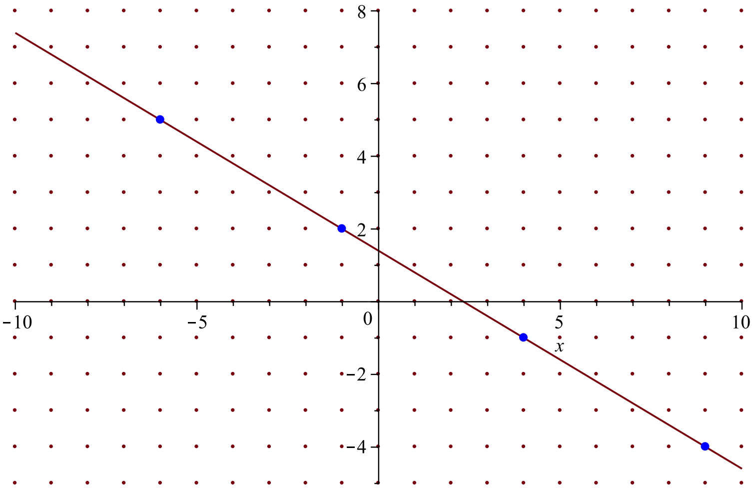
The *integral* solutions to (1) are where this line intersects the *lattice* $\mathbb{Z}^2$ of points with integral coordinates.



The line $3x + 5y = 7$ in $\mathbb{R}^2$.



The lattice $\mathbb{Z}^2$.



The integral solutions to $3x + 5y = 7$.

We immediately observe (and can easily verify) the solutions:

$$x = -6 \text{ and } y = 5; \;\; x = -1 \text{ and } y = 2;$$
$$x = 4 \text{ and } y = -1; \;\; x = 9 \text{ and } y = -4;$$

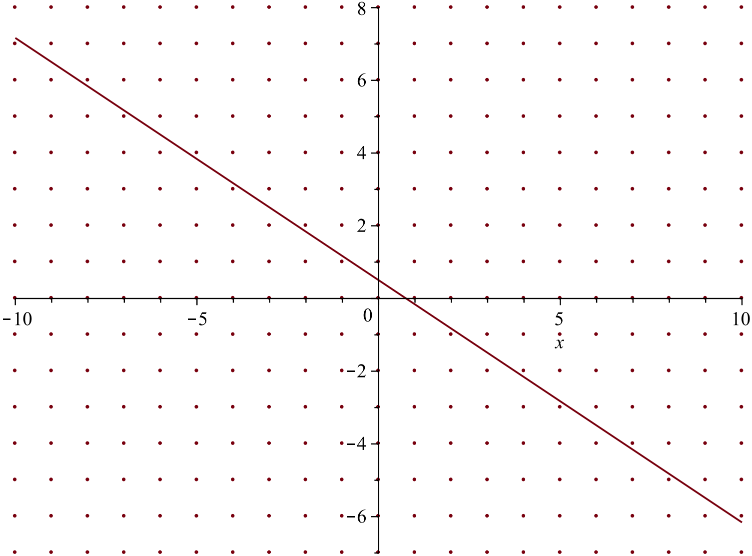
which are regularly spaced on the line.

On the other hand, the equation

$$4x + 6y = 3$$

has *no* integral solutions (why not?).

That is, the line with equation $4x + 6y = 3$ completely avoids the lattice $\mathbb{Z}^2$.



The line $4x + 6y = 3$.

Linear Diophantine Equations

As we will see, these are the only two possible situations.

Fix $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$, and consider the *linear Diophantine equation*

$$ax + by = c. \tag{2}$$

Goal: Describe all solutions to (2) in $\mathbb{Z}$.

Notice that if $(x, y) \in \mathbb{Z}^2$ solves (2), then

$$c \in a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}.$$

So a necessary condition for the existence of solutions to (2) is

$$(a, b)|c.$$

This condition is also sufficient. To see this, suppose $(a, b) | c$.

Write $c = (a, b)d$ with $d \in \mathbb{Z}$.

By Bézout's lemma, we can find $r, s \in \mathbb{Z}$ so that

$$ar + bs = (a, b).$$

If we multiply both sides by d we obtain

$$a(rd) + b(sd) = (a, b)d = c.$$

Thus $x = rd$, $y = sd$ is a solution to $ax + by = c$.

Summary

Theorem 1

Let $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$. The Diophantine equation

$$ax + by = c$$

has a solution if and only if $(a, b)|c$. In this case, one solution is given by

$$x_0 = r\frac{c}{(a, b)}, \quad y_0 = s\frac{c}{(a, b)},$$

where $r, s \in \mathbb{Z}$ satisfy $ar + bs = (a, b)$.

Because we can use the Euclidean algorithm to effectively compute (a, b), r and s, we can always produce at least one solution to $ax + by = c$ (when it exists).

Examples

Example 1

Solve the Diophantine equation $3x + 6y = 7$.

Solution. Since $(3,6) = 3$, and $3 \nmid 7$, this equation has *no solutions in* $\mathbb{Z}$. $\square$

Example 2

Solve the Diophantine equation $3x + 5y = 7$.

Solution. Since $(3,5) = 1$ the equation

$$3x + 5y = 7$$

must have integral solutions: $x = -1, y = 2$ and $x = 4, y = -1$ work, for instance. Can we find them all?

Solving $ax + by = c$

We begin by assuming $(a, b) = 1$.

Since $1|c$ for all $c \in \mathbb{Z}$, we are guaranteed the existence of *at least one* (integral) solution $x = x_0, y = y_0$.

Suppose $x = x_1, y = y_1$ is another solution. We then have

$$\begin{aligned} ax_0 + by_0 &= c, \\ ax_1 + by_1 &= c. \end{aligned}$$

Subtraction yields

$$\begin{aligned} a(x_0 - x_1) + b(y_0 - y_1) = 0 \;\Rightarrow\; & a(x_0 - x_1) = -b(y_0 - y_1) \\ \Rightarrow\; & a|b(y_0 - y_1). \end{aligned}$$

Since $(a, b) = 1$, Euclid's lemma implies that $a \big| (y_0 - y_1)$. Write

$$y_0 - y_1 = ak.$$

Then $y_1 = y_0 - ak$ and back substitution yields

$$a(x_0 - x_1) = -abk \;\Rightarrow\; x_0 - x_1 = -bk \;\Rightarrow\; x_1 = x_0 + bk.$$

Thus, every solution to $ax + by = c$ has the form

$$\begin{aligned} x &= x_0 + bk, \\ y &= y_0 - ak, \end{aligned}$$

for *some* $k \in \mathbb{Z}$.

At the same time, for *any* $k \in \mathbb{Z}$ we have

$$a(x_0 + bk) + b(y_0 - ak) = ax_0 + by_0 + abk - abk = c + 0 = c.$$

Combining this with our earlier work, we have proven:

Theorem 2

Let $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$. If $(a, b) = 1$, then the set of solutions to the Diophantine equation $ax + by = c$ is given by

$$x = rc + bk,$$
$$y = sc - ak,$$

where $k \in \mathbb{Z}$ is arbitrary and r, s satisfy $ar + bs = 1$.

Example 2 (Continued)

Finish solving $3x + 5y = 7$.

Solution. It's easy to note that $2 \cdot 3 + (-1)5 = 1$.

So we may take $r = 2$ and $s = -1$.

Thus the general solution is given by

$$\begin{aligned} x &= 14 + 5k, \\ y &= -7 - 3k, \end{aligned}$$

with $k \in \mathbb{Z}$.

Example 3

Describe the set of solutions to the Diophantine equation $313x + 510y = 2$.

Solution. If we apply the Euclidean algorithm, it takes 8 divisions to determine that $(313, 510) = 1$.

The first 7 quotients are $q = 1, 1, 1, 1, 2, 3, 5,$ and multiplication of the associated matrices $\left(\begin{smallmatrix} 0 & 1 \\ 1 & -q \end{smallmatrix}\right)$ (in the opposite order) yields the matrix

$$\begin{pmatrix} * & * \\ 143 & -233 \end{pmatrix}.$$

Thus

$$-233 \cdot 313 + 143 \cdot 510 = 1.$$

So we may take $r = -233$ and $s = 143$.

Therefore the general solution to $313x + 510y = 2$ is given by

$$\begin{aligned} x &= 2 \cdot (-233) + 510k = -466 + 510k, \\ y &= 2 \cdot 143 - 313k = 286 - 313k, \end{aligned}$$

where $k \in \mathbb{Z}$ is arbitrary. $\square$

Solving $ax + by = c$ in General

Now let $a, b, c \in \mathbb{Z}$ (with $a, b \neq 0$) be arbitrary integers satisfying $(a, b)|c$. The Diophantine equation

$$ax + by = c$$

is then equivalent to the equation

$$\frac{a}{(a, b)}x + \frac{b}{(a, b)}y = \frac{c}{(a, b)}.$$

Since

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1,$$

the latter equation can be solved using our previous result.

We write

$$\frac{a}{(a,b)}r + \frac{b}{(a,b)}s = 1 \quad \text{or} \quad ar + bs = (a,b)$$

and set

$$\begin{aligned} x &= r\frac{c}{(a,b)} + \frac{b}{(a,b)}k, \\ y &= s\frac{c}{(a,b)} - \frac{a}{(a,b)}k, \end{aligned}$$

with $k \in \mathbb{Z}$.

We've now completely solved the Diophantine $ax + by = c$.

Summary

Theorem 3

Let $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$. The Diophantine equation

$$ax + by = c$$

can be solved if and only if $(a,b)|c$. In this case, the set of solutions is given by

$$x = r\frac{c}{(a,b)} + \frac{b}{(a,b)}k,$$
$$y = s\frac{c}{(a,b)} - \frac{a}{(a,b)}k,$$

where $k \in \mathbb{Z}$ is arbitrary and $r, s \in \mathbb{Z}$ satisfy $ra + sb = (a,b)$.

Because we can compute r and s from the EA, we can completely describe the solutions to any given linear Diophantine equation.

Example 4

The neighborhood theater charges \$1.80 for adult admissions and \$.75 for children. On a particular evening the total receipts were \$90. Assuming that more adults than children were present, how many people attended?

Solution. Let x be the number of adults who attended and y be the number of children.

We need to solve the Diophantine equation

$$180x + 75y = 9000$$

in *nonnegative* integers $x > y$.

The EA gives $(75, 180) = 15$ in three steps, and we find that

$$5 \cdot 75 + (-2)180 = 15.$$

So the general solution is given by

$$\begin{aligned} x &= -2 \cdot \frac{9000}{15} + \frac{75}{15}k = -1200 + 5k \geq 0, \\ y &= 5 \cdot \frac{9000}{15} - \frac{180}{15}k = 3000 - 12k \geq 0. \end{aligned}$$

Putting the two inequalities together yields

$$240 \leq k \leq 250.$$

But we also require that $x > y$:

$$-1200+5k > 3000-12k \;\Leftrightarrow\; 17k > 4200 \;\Leftrightarrow\; k > \frac{4200}{17} > 247.05.$$

Together with our earlier inequalities we obtain

$$248 \leq k \leq 250.$$

This means $k = 248, 249$ or 250. Thus the possible solutions are

$$\boxed{\begin{array}{l} x = 40, \quad y = 24, \\ x = 45, \quad y = 12, \\ x = 50, \quad y = 0. \end{array}}$$

$\square$