2-4-2019

Linear Diophantine Equations

A **Diophantine problem** is one in which the solutions are required to be integers. Abusing terminology, I'll refer to **Diophantine equations**, meaning equations which are to be solved over the integers.

For example, the equation $x^3 + y^3 = z^3$ has many solutions over the reals. Here's a solution:

$$x = 1, \quad , y = 1, \quad z = \sqrt[3]{2}.$$

However, this equation has no nonzero integer solutions. This is a special case of **Fermat's Last Theorem**.

On the other hand, the following equation has infinitely many integer solutions:

$$9x + 100y = 1.$$

$(-11, 1)$ and $(89, -8)$ are examples of solutions.

In this section, I'll look at equations like the last one. They're called **linear Diophantine equations**.

Theorem. Let $a, b, c \in \mathbb{Z}$. Consider the Diophantine equation

$$ax + by = c.$$

(a) If $(a, b) \nmid c$, there are no solutions.

(b) If $(a, b) = d \mid c$, there are infinitely many solutions of the form

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t.$$

Here (x_0, y_0) is a particular solution, and $t \in \mathbb{Z}$.

If you've had a course in differential equations, you may have seen something like this. $x = \frac{b}{d}t$ and $y = -\frac{a}{d}t$ give a general solution to the homogeneous equation

$$ax + by = 0.$$

(x_0, y_0) is a particular solution to $ax + by = c$. Their sum gives a general solution to the given (nonhomogeneous) equation.

Before I give the proof, I'll give some examples, and also discuss the three variable equation $ax+by+cz = d$.

Example. Solve $6x + 9y = 21$.

Since $(6, 9) = 3 \mid 21$, there are infinitely many solutions. Divide the equation by 3 to get

$$2x + 3y = 7.$$

By inspection, $x = 2$ and $y = 1$ is a particular solution. Hence, the general solution is

$$x = 2 + 3t, \quad y = 1 - 2t.$$

For example, setting $t = 5$ produces the solution $x = 17$, $y = -9$. □

In general, you may not be able to see a particular solution by inspection. In that case, you can use the Extended Euclidean algorithm to generate one. We'll see how to do this in examples that follow.

Example. Solve $6x + 9y = 5$.

Since $(6, 9) = 3 \not| 5$, the equation has no solutions. □

Example. Find all the solutions (x, y) to the following Diophantine equation for which x and y are both positive.

$$11x + 13y = 369.$$

$(11, 13) = 1 \mid 369$, so there are solutions.

It is too hard to guess a particular solution, so I'll use the Extended Euclidean algorithm:

13	-	6
11	1	5
2	5	1
1	2	0

$$11 \cdot 6 + 13 \cdot (-5) = 1$$
$$11 \cdot 2214 + 13 \cdot (-1845) = 369$$

Matching this with the given equation $11x + 13y = 369$, I see that $(x, y) = (2214, -1845)$ is a particular solution. The general solution is

$$x = 2214 + 13t, \quad y = -1845 - 11t.$$

I want solutions for which x and y are both positive. So

$$2214 + 13t > 0, \quad \text{so} \quad t > -\frac{2214}{13} = -170.30769\ldots.$$

$$-1845 - 11t > 0, \quad \text{so} \quad t < -\frac{1845}{11} = -167.72727\ldots.$$

The integers which satisfy both of these inequalities are $t = -170, -169, -168$. Here are the values of x and y:

t	x	y
-171	-9	36
-170	4	25
-169	17	14
-168	20	3
-167	43	-8

The solutions are $(x, y) = (4, 25)$, $(17, 14)$, and $(20, 3)$. □

The requirement that the solutions be positive can come up in real-world problems.

Example. Phoebe buys large shirts for \$18 each and small shirts for \$11 each. The shirts cost a total of \$1188. What is the smallest total number of shirts she could have bought?

Let x be the number of large shirts and let y be the number of small shirts. Then

$$18x + 11y = 1188.$$

Since $(18, 11) = 1 \mid 1188$, there are solutions.
I'll use the Extended Euclidean algorithm to get a particular solution:

18	-	5
11	1	3
7	1	2
4	1	1
3	1	1
1	3	0

$$18 \cdot (-3) + 11 \cdot 5 = 1$$
$$18 \cdot (-3564) + 11 \cdot 5940 = 1188$$

$x = -3564$ and $y = 5940$ is a particular solution. The general solution is

$$x = -3564 + 11t, \quad y = 5940 - 18t.$$

Since the number of shirts can't be negative, I have $x \geq 0$ and $y \geq 0$.

$$x \geq 0 \quad \text{gives} \quad -3564 + 11t \geq 0 \quad \text{so} \quad t \geq \frac{3564}{11} = 324.$$

$$y \geq 0 \quad \text{gives} \quad 5940 - 18t \geq 0 \quad \text{so} \quad t \leq \frac{5940}{18} = 330.$$

Thus, $324 \leq t \leq 330$.
The total number of shirts is

$$x + y = (-3564 + 11t) + (5940 - 18t) = 2376 - 7t.$$

For $324 \leq t \leq 330$, this is smallest for $t = 330$, which gives

$$x = 66, \quad y = 0, \quad x + y = 66.$$

She bought 66 large shirts, no small shirts, and a total of 66 shirts. □

Consider a 3-variable equation

$$ax + by + cz = d.$$

The equation has solutions if and only if $(a, b, c) \mid d$. If it has solutions, there will be infinitely many, determined by two integer parameters.

You can solve a 3-variable equation by reducing it to a 2-variable equation. Group the first two terms and factor out the greatest common divisor of their coefficients. Introduce a new variable, defining it to be what is left after the greatest common divisor is factored out. The new equation is a 2-variable Diophantine equation, which you can solve using the method described earlier.

Example. Find the general solution to the following Diophantine equation.

$$8x + 14y + 5z = 11.$$

$$2(4x + 7y) + 5z = 11.$$

Let $w = 4x + 7y$.

$$2w + 5z = 11.$$

$w = -22$ and $z = 11$ is a particular solution. So

$$w = -22 + 5s \quad \text{and} \quad z = 11 - 2s.$$

Then

$$4x + 7y = w = -22 + 5s.$$

$x = -44 + 10s$ and $y = 22 - 5s$ is a particular solution. The general solution is

$$\begin{aligned} x &= -44 + 10s + 7t \\ y &= 22 - 5s - 4t \\ z &= 11 - 2s \quad \square \end{aligned}$$

A general linear Diophantine equation has the form

$$a_1x_1 + \cdots a_nx_n = c.$$

There are solutions if $(a_1, \ldots a_n) \mid c$. If there is a solution, it will in general have $n - 1$ parameters — exactly as you'd expect from linear algebra.

Here's the proof of the theorem for the two-variable case.

Proof. (two variable case) Consider the linear Diophantine equation

$$ax + by = c.$$

Case 1. Suppose $(a, b) \not| c$. If x and y are solutions to the equation, then

$$(a, b) \mid ax + by = c.$$

This contradiction shows that there cannot be a solution.

Case 2. Suppose $(a, b) \mid c$. Write $c = k(a, b)$ for $k \in \mathbb{Z}$. There are integers m and n such that

$$am + bn = (a, b).$$

Then

$$amk + bnk = (a, b)k = c.$$

Hence, $x = km$, $y = kn$, is a solution.
Suppose $x = x_0$, $y = y_0$, is a particular solution. Then

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = \frac{ab}{d}t - \frac{ab}{d}t + (ax_0 + by_0) = 0 + c = c.$$

This proves that $x = x_0 + \dfrac{b}{d}t$, $y = y_0 - \dfrac{a}{d}t$ is a solution for every $t \in \mathbb{Z}$.
Finally, I want to show that every solution has this form. Suppose then that (x, y) is a solution. Then $ax + by = c$ and $ax_0 + by_0 = c$ imply

$$a(x - x_0) + b(y - y_0) = c - c = 0.$$

Therefore,

$$\frac{a}{(a,b)}(x-x_0)+\frac{b}{(a,b)}(y-y_0)=0,$$

$$\frac{b}{(a,b)}(y-y_0)=-\frac{a}{(a,b)}(x-x_0).$$

Now $\dfrac{b}{(a,b)}$ divides the left side, so it divides the right side. However, $\left(\dfrac{a}{(a,b)},\dfrac{b}{(a,b)}\right)=1$. Therefore,

$$\frac{b}{(a,b)}\ \Big|\ x-x_0, \quad \text{or} \quad x-x_0=t\cdot\frac{b}{(a,b)} \quad \text{for some} \quad t\in\mathbb{Z}.$$

Thus,

$$x=x_0+t\cdot\frac{b}{(a,b)}.$$

Substitute $x-x_0=t\cdot\dfrac{b}{(a,b)}$ back into the last x-y equation above:

$$\begin{aligned}
\frac{b}{(a,b)}(y-y_0)&=-\frac{a}{(a,b)}(x-x_0)\\
\frac{b}{(a,b)}(y-y_0)&=-\frac{a}{(a,b)}t\cdot\frac{b}{(a,b)}\\
y-y_0&=t\cdot\frac{a}{(a,b)}\\
y&=y_0-t\cdot\frac{a}{(a,b)}
\end{aligned}$$

Thus,

$$x=x_0+t\cdot\frac{b}{(a,b)} \quad \text{and} \quad y=y_0-t\cdot\frac{a}{(a,b)}. \quad \square$$