6. Linear Diophantine equations

We consider the problem of trying to find integral solutions to linear equations with integer coefficients. The general problem of finding integral solutions to polynomial equations with integer coefficients is called a Diophantine problem, so we are looking at linear Diophantine equations.

The general linear Diophantine equation in two variables has the form

$$ax + by = c,$$

where a, b and $c \in \mathbb{Z}$. Our goal is to describe all solutions (x, y) with integer coordinates, $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$.

Geometrically the equation $ax + by = c$ describes a line in the plane $\mathbb{R}^2$. It is possible that this line misses the integral points $\mathbb{Z}^2$. However if there is one integral point on the line then there are infinitely many.

We first start by solving a special case, when $c = 0$ and $(a, b) = 1$. When $c = 0$ one solution is clear $x = y = 0$, the origin $(0, 0)$ is a point of the line

$$ax + by = 0.$$

On the hand we could increase x by b and decrease y by a, to get another point $(b, -a)$ of the line. More generally if $k \in \mathbb{Z}$ is an integer then could we could increase x by kb and decrease y by ka, to get another point $(kb, -ak)$ of the line.

On the other hand, if you consider the equation

$$ax = -by,$$

it is clear that every point of the line has the form $(bt, -at)$, for some real number t. For this to be an integer point, $t = k/l$ has to be rational, where k and $l > 0$ are coprime integers and we must have $bk/l \in \mathbb{Z}$ and $ak/l \in \mathbb{Z}$. Suppose that $l \neq 1$. Then some prime p divides l. p does not divide k, as $(k, l) = 1$ and p does not divide both a and b, as $(a, b) = 1$, a contradiction. Thus $t = k$ and the general solution to the equation

$$ax + by = 0$$

is $(kb, -ka)$, where $k \in \mathbb{Z}$ is an integer.

Now we turn to the case when $(a, b) = 1$ but c is arbitrary. In this case we may find (λ, μ) such that $\lambda a + \mu b = 1$. If we multiply this equation by c then we get

$$a(c\lambda) + b(c\mu) = c.$$

Hence, if we put

$$x_0 = c\lambda \qquad \text{and} \qquad y_0 = c\mu$$

then (x_0, y_0) is a solution of the equation $ax + by = c$. Suppose that (x, y) is another solution, so that

$$\begin{aligned} ax_0 + by_0 &= c \\ ax + by &= c. \end{aligned}$$

If we subtract the first equation from the second equation we get

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

We have already seen that the general solution of this equation is

$$(x - x_0, y - y_0) = (bk, -ak),$$

so that the general solution of the equation $ax + by = c$ is

$$x = x_0 + bk \qquad \text{and} \qquad y = y_0 - ak,$$

where k is an integer.

Finally suppose that $(a, b) = d$. If we can solve $ax + by = c$ then c must be a multiple of d. In this case consider the equation

$$(a/d)x + (b/d) = c/d.$$

As $d|a$, $d|b$ and $d|c$ this is a linear Diophantine equation. $(a/d, b/d) = 1$ and so the general solution to this equation is

$$x = x_0 + \frac{kb}{d} \qquad \text{and} \qquad y = y_0 - \frac{ka}{d},$$

where (x_0, y_0) is one solution and k is an integer.

Question 6.1. *Find all solutions of the linear Diophantine equation*

$$258x + 147y = 369.$$

We first find the greatest common divisor of 258 and 147. Note that both 258 and 147 are divisible by 3, $258 = 3 \cdot 86$ and $147 = 3 \cdot 49$. As $49 = 7^2$ is coprime to $66 = 6 \cdot 11$, the greatest common divisor of 258 and 147 is 3. As 369 is a multiple of 3 it follows that the linear Diophantine equation

$$258x + 147y = 369$$

has a solution.

Since we want to solve a linear Diophantine equation we still have to run Euclid's algorithm.

$$\begin{aligned} 258 &= 1 \cdot 147 + 111 \\ 147 &= 1 \cdot 111 + 36 \\ 111 &= 3 \cdot 36 + 3 \\ 36 &= 12 \cdot 3 + 0. \end{aligned}$$

Thus the greatest common divisor is 3, as we already knew. Going backwards, from

$$111 = 3 \cdot 36 + 3 \qquad \text{we get} \qquad 3 = 111 - 3 \cdot 36.$$

From

$$147 = 1 \cdot 111 + 36 \qquad \text{we get} \qquad 36 = 147 - 1 \cdot 111,$$

so that

$$\begin{aligned} 3 &= 111 - 3 \cdot 36 \\ &= 111 - 3 \cdot (147 - 1 \cdot 111) \\ &= 4 \cdot 111 - 3 \cdot 147. \end{aligned}$$

Finally, from

$$258 = 1 \cdot 147 + 111 \qquad \text{we get} \qquad 111 = 258 - 1 \cdot 147$$

so that

$$\begin{aligned} 3 &= 4 \cdot 111 - 3 \cdot 147 \\ &= 4 \cdot (258 - 1 \cdot 147) - 3 \cdot 147 \\ &= 4 \cdot 258 - 7 \cdot 147. \end{aligned}$$

Thus $(4, -7)$ is a solution of the equation

$$258x + 147y = 3.$$

Multiplying through by 123 gives the solution $(492, -861)$ to the equation

$$258x + 147y = 369$$

The general solution to this equation is then

$$x = 492 + 49k \qquad \text{and} \qquad y = -861 - 86k.$$

Note that to get from one solution to the next we go across b/d units and we go down a/d units. Thus the distance between two successive solutions is

$$\frac{1}{d}\sqrt{a^2 + b^2}.$$

Suppose that a, b and $c > 0$. Then the line $ax + by = c$ intersects the first quadrant. The intercepts are at $(c/a, 0)$ and $(0, c/b)$. The distance between these two points is

$$\sqrt{\left(\frac{c}{a}\right)^2 + \left(\frac{c}{b}\right)^2} = \frac{c}{ab}\sqrt{a^2 + b^2}.$$

It is therefore guaranteed that there is a integral solution in the first quadrant if

$$\frac{c}{ab} > \frac{1}{d},$$

and $d|c$.