Solution set (general case)

Solution set (general case)

Now, we back to the general case:

$$a \cdot x + b \cdot y = c.$$

Lemma 1.4.1.

Suppose (x_1, y_1) *is a solution of above Diophantine equation. Then the solution set* $\left\{(x, y) \in \mathbb{Z}^2 \,\middle|\, a \cdot x + b \cdot y = c\right\}$ *can be expressed as*

$$(x_1, y_1) + \left\{(x, y) \in \mathbb{Z}^2 \,\middle|\, a \cdot x + b \cdot y = 0\right\}.$$

Solution set (general case)

Before we move to the proof, let's consider the corresponding proposition in geometry:

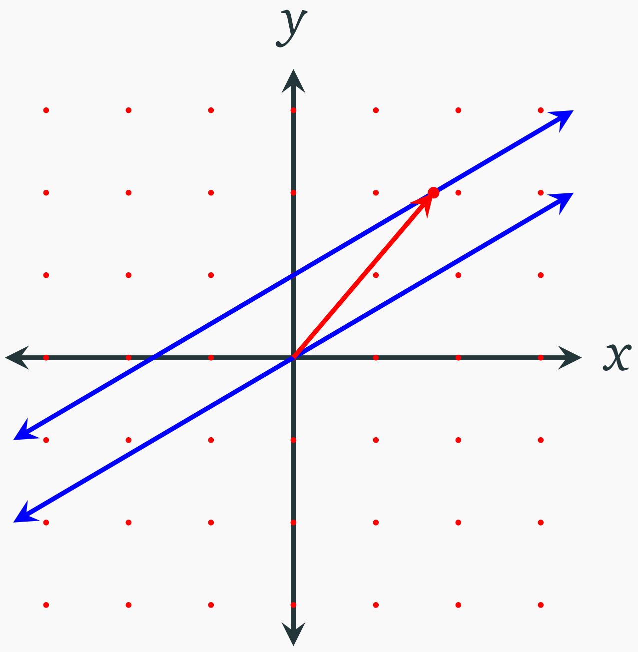
The line defined by the equation

$$a \cdot x + b \cdot y = c$$

can be obtained from the line

$$a \cdot x + b \cdot y = 0$$

by adding a vector $\langle x_1, y_1 \rangle$ from the origin to a point (x_1, y_1) on the first line.



Proof. Suppose (x_2, y_2) is a solution of our Diophantine equation $a \cdot x + b \cdot y = c$, then we have:

$$a \cdot (x_1 - x_2) + b \cdot (y_1 - y_2) = 0.$$

Namely, $(x_1 - x_2, y_1 - y_2)$ is a solution of the corresponding homogeneous Diophantine equation $a \cdot x + b \cdot y = 0$.

$$a x_1 + b y_1 = c$$
$$a x_2 + b y_2 = c$$

Proof. Suppose (x_2, y_2) is a solution of our Diophantine equation $a \cdot x + b \cdot y = c$, then we have:

$$a \cdot (x_1 - x_2) + b \cdot (y_1 - y_2) = 0.$$

Namely, $(x_1 - x_2, y_1 - y_2)$ is a solution of the corresponding homogeneous Diophantine equation $a \cdot x + b \cdot y = 0$.

Conversely, if (x_2, y_2) is a solution of the corresponding homogeneous Diophantine equation $a \cdot x + b \cdot y = 0$, then we have

$$a \cdot (x_1 + x_2) + b \cdot (y_1 + y_2) = c.$$

Namely, $(x_1 + x_2, y_1 + y_2)$ is a solution of our Diophantine equation $a \cdot x + b \cdot y = c$. $\square$

$$a x_1 + b y_1 = c$$
$$a x_2 + b y_2 = 0$$

Solution set (general case)

Theorem 1.4.2.

Given integers a, b, c, the solutions of the Diophantine equation

$$a \cdot x + b \cdot y = c$$

can be obtained through the following steps:

1. *Using division algorithm to find $\gcd(a, b)$ and then determine whether the Diophantine equation has an integer solution by whether c is a multiple of $\gcd(a, b)$.*
2. *If this is the case, the Bézout's identity gives a pair of integers (x_0, y_0) such that $ax_0 + by_0 = \gcd(a, b)$. Suppose $c = m\gcd(a, b)$. Then (mx_0, my_0) is a solution of our Diophantine equation.*

Theorem 1.4.2.

3. *Once we have a solution* (x_1, y_1) *of our Diophantine equation, the solution set can be expressed as*[1]

$$(x_1, y_1) + \mathbb{Z}\left(\frac{\operatorname{lcm}(a,b)}{a}, -\frac{\operatorname{lcm}(a,b)}{b}\right).$$

Namely, the general solution is

$$\begin{cases} x = x_1 + \frac{\operatorname{lcm}(a,b)}{a} t \\ y = y_1 - \frac{\operatorname{lcm}(a,b)}{b} t \end{cases} \qquad (t \in \mathbb{Z}).$$

Proof. The first two are proved in previous lecture, the third is the combination of theorem 1.3.3 and lemma 1.4.1. □

[1] Recall the conventions on set notations

An example

Let's continue the example

$$133x + 85y = 1.$$

We have seen that $\gcd(133, 85) = 1$ and that

$$133 \cdot (-23) + 85 \cdot (36) = 1.$$

Since $\gcd(133, 85) = 1$, we have $\operatorname{lcm}(133, 85) = 133 \cdot 85$. Therefore, the general solution is

$$\begin{cases} x = -23 + 85t \\ y = 36 - 133t \end{cases} \qquad (t \in \mathbb{Z}).$$