THE LINEAR DIOPHANTINE EQUATION $ax + by = c$

A **Diophantine equation** is a polynomial equation that allows two or more variables to take integer values only.

The most famous Diophantine equations are the **Pythagorean equations** whose integer solutions are the Pythagorean triples, and its generalisation to higher dimensions as in **Fermat's last theorem**, $a^n + b^n = c^n$.

In this section we apply the Euclidean Algorithm to the simplest of all Diophantine equations, the linear Diophantine equation $ax + by = c$ where $a, b, c \in \mathbb{Z}$ are constants, and $x, y \in \mathbb{Z}$ are the variables.

Linear Diophantine equations are always to be solved (or proved insolvable) in the integers or sometimes in just the positive integers. There are two variables (x and y) in the equation, and there are either an infinite number of solutions in $\mathbb{Z}$, or none.

For example:

- $3x + 6y = 18$ has an infinite number of solutions in the integers
- $2x + 10y = 17$ has none at all, since $2x + 10y$ is even for all $x, y \in \mathbb{Z}$, whereas 17 is odd.

Theorem:

Suppose $a, b, c \in \mathbb{Z}$, and let $d = \gcd(a, b)$.

(1) $ax + by = c$ has solutions $\Leftrightarrow$ $d \mid c$.

(2) If x_0, y_0 is any particular solution, all solutions are of the form

$$x = x_0 + \left(\frac{b}{d}\right)t, \quad y = y_0 - \left(\frac{a}{d}\right)t \quad \text{where } t \in \mathbb{Z}.$$

Proof:

(1) $(\Rightarrow)$ $d = \gcd(a, b) \Rightarrow d \mid a$ and $d \mid b$

$\Rightarrow a = dr$ and $b = ds$ for some integers r and s

Now if $x = x_0$ and $y = y_0$ is a solution of $ax + by = c$ then $ax_0 + by_0 = c$

$\Rightarrow c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0)$

$\Rightarrow d \mid c$

$(\Leftarrow)$ If $d \mid c$ then $c = dt$ for some integer t .... (1)

Now since $d = \gcd(a, b)$, there exist $x_0, y_0 \in \mathbb{Z}$ such that $d = ax_0 + by_0$.

Multiplying by t gives $dt = (ax_0 + by_0)t$

$\therefore\ c = a(x_0t) + b(y_0t)$ {using (1)}

Hence $ax + by = c$ has a particular solution $x = tx_0$, $y = ty_0$.

(2) x_0, y_0 is a known solution of $ax + by = c$, so $ax_0 + by_0 = c$.

If x', y' is another solution then $ax_0 + by_0 = c = ax' + by'$

$\Rightarrow a(x_0 - x') = b(y' - y_0)$ .... (1)

Since $d = \gcd(a, b)$, there exist integers r and s which are relatively prime with $a = dr$ and $b = ds$.

$\Rightarrow\ dr(x_0 - x') = ds(y' - y_0)$

$\Rightarrow\ r(x_0 - x') = s(y' - y_0)$

$\Rightarrow\ r \mid s(y' - y_0)$ with $\gcd(r, s) = 1$ .... (2)

Now **Euclid's Lemma** states that if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

$\therefore$ from (2), $r \mid (y_0 - y')$

$$\therefore\ y_0 - y' = rt \quad \text{for some } t \in \mathbb{Z}$$
$$\therefore\ y' = y_0 - rt$$

Substituting into (1), $a(x_0 - x') = b(-rt)$

$$\therefore\ dr(x_0 - x') = ds(-rt)$$
$$\therefore\ x_0 - x' = -st$$
$$\therefore\ x' = x_0 + st$$

So, $x' = x_0 + st$ and $y' = y_0 - rt$

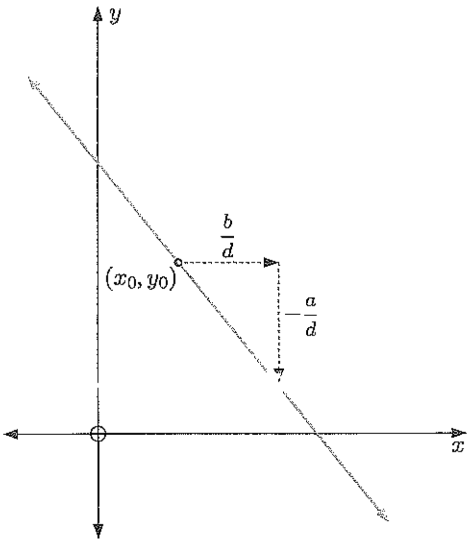
$$\therefore\ x' = x_0 + \left(\frac{b}{d}\right)t \quad \text{and} \quad y' = y_0 - \left(\frac{a}{d}\right)t, \quad t \in \mathbb{Z}$$

Checking the solution for any $t \in \mathbb{Z}$:

$$ax + by = a\left(x_0 + \left(\frac{b}{d}\right)t\right) + b\left(y_0 - \left(\frac{a}{d}\right)t\right) = ax_0 + \frac{abt}{d} + by_0 - \frac{abt}{d} = ax_0 + by_0 = c \quad \checkmark$$

$\therefore$ the given solutions constitute all, infinitely many, solutions.

Graphically, the theorem takes this form:



The equation $ax + by = c$ is that of a straight line with gradient $-\frac{a}{b}$.

Since $\gcd(a, b) \mid c$, c is a multiple of $d = \gcd(a, b)$.

$\therefore$ there exists an integer pair solution (x_0, y_0) on this line.

The general solution is obtained by moving the horizontal distance $\frac{b}{d}$ (an integer) to the right, then moving downwards the vertical distance $-\frac{a}{d}$ (also an integer) back to the line.

Thus all of solutions are integer pairs (x, y).

Example 25

Solve $172x + 20y = 1000$ for x, y in: **a** $\mathbb{Z}$ **b** $\mathbb{Z}^+$.

a We first find $\gcd(172, 20)$ using the Euclidean Algorithm.

$$172 = 20(8) + 12$$
$$20 = 12(1) + 8$$
$$12 = 8(1) + 4$$
$$8 = 4(2) \qquad \therefore\ \gcd(172, 20) = 4$$

Now $4 \mid 1000$, so integer solutions exist.

We now need to write 4 as a linear combination of 172 and 20.

Working backwards: $4 = 12 - 8$

$= 12 - (20 - 12)$

$= 2 \times 12 - 20$

$= 2(172 - 20(8)) - 20$

$= 2 \times 172 - 17 \times 20$

Multiplying by 250 gives $1000 = 500 \times 172 - 4250 \times 20$

$\therefore$ $x_0 = 500$, $y_0 = -4250$ is one solution pair.

All other solutions have the form $x = 500 + \left(\frac{20}{4}\right)t$, $y = -4250 - \left(\frac{172}{4}\right)t$,

which is, $x = 500 + 5t$, $y = -4250 - 43t$, $t \in \mathbb{Z}$.

b If x and y are in $\mathbb{Z}^+$ we need to solve for $t \in \mathbb{Z}$ such that:

$500 + 5t > 0$ *and* $-4250 - 43t > 0$

$\therefore$ $5t > -500$ *and* $43t < -4250$

$\therefore$ $t > -100$ *and* $t < -98.33....$

$\therefore$ $t = -99$

$\therefore$ $x = 500 + 5(-99)$ and $y = -4250 - 43(-99)$

$\therefore$ $x = 5$ and $y = 7$ is the unique solution for which $x, y \in \mathbb{Z}^+$.

Corollary:

If $\gcd(a, b) = 1$ and if x_0, y_0 is a particular solution of $ax + by = c$, then all solutions are given by $x = x_0 + bt$, $y = y_0 - at$, $t \in \mathbb{Z}$.

Linear Diophantine equations often are observed in word puzzles, as in the following example.

Example 26

A cow is worth 10 pieces of gold, a pig is worth 5 pieces of gold, and a hen is worth 1 piece of gold. 220 gold pieces are used to buy a total of 100 cows, pigs, and hens.

How many of each animal is bought?

Let the number of cows be c, the number of pigs be p, and the number of hens be h.

$\therefore$ $c + p + h = 100$ {the total number of animals}

and $10c + 5p + h = 220$ {the total number of gold pieces}

Subtracting these equations gives $9c + 4p = 120$ where $\gcd(9, 4) = 1$.

By observation, $c_0 = 0$ and $p_0 = 30$ is one solution pair.

$\therefore$ $c = 0 + 4t$ and $p = 30 - 9t$, $t \in \mathbb{Z}$ is the general solution,

which is, $c = 4t$, $p = 30 - 9t$, $h = 100 - p - c = 70 + 5t$.

But c, p, and h are all positive

$$\therefore\ 4t > 0 \quad and \quad 30 - 9t > 0 \quad and \quad 70 + 5t > 0$$

$$\therefore\ t > 0 \quad and \quad t < \tfrac{30}{9} \quad and \quad t > -\tfrac{70}{5}$$

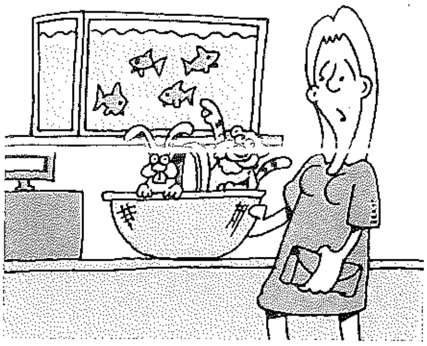
$\therefore\ 0 < t < 3.33$ where $t \in \mathbb{Z}$.

So, there are three possible solutions, corresponding to $t = 1$, 2, or 3. These are:

$\{c = 4,\ p = 21,\ h = 75\}$ or $\{c = 8,\ p = 12,\ h = 80\}$ or $\{c = 12,\ p = 3,\ h = 85\}$

EXERCISE 1D.3

1. Find, where possible, all $x, y \in \mathbb{Z}$ such that:
   - a $6x + 51y = 22$
   - b $33x + 14y = 115$
   - c $14x + 35y = 93$
   - d $72x + 56y = 40$
   - e $138x + 24y = 18$
   - f $221x + 35y = 11$
2. Find all positive integer solutions of:
   - a $18x + 5y = 48$
   - b $54x + 21y = 906$
   - c $123x + 360y = 99$
   - d $158x - 57y = 11$
3. Two positive numbers add up to 100. One number is divisible by 7, and the other is divisible by 11. Find the numbers.
4. There are a total of 20 men, women, and children at a party.
   Each man has 5 drinks, each woman has 4 drinks, and each child has 2 drinks. They have 62 drinks in total. How many men, women, and children are at the party?
5. I wish to buy 100 animals. Cats cost me €50 each, rabbits cost €10 each, and fish cost 50 cents each. I have €1000 to spend, and buy at least one of each animal.
   If I spend all of my money on the purchase of these animals, how many of each kind of animal do I buy?



6. The cities A and M are 450 km apart. Smith travels from A to M at a constant speed of 55 km h^{-1}, and his friend Jones travels from M to A at a constant speed of 60 km h^{-1}. When they meet, they both look at their watches and exclaim: "It is exactly half past the hour, and I started at half past!". Where do they meet?
7. A person buys a total of 100 blocks of chocolate. The blocks are available in three sizes, which cost \$3.50 each, \$4 for three, and 50 cents each respectively. If the total cost is \$100, how many blocks of each size does the person buy?