# Diophantine Equations

Equations where we look for solutions in a restricted class of numbers are called Diophantine equations.

$$x^2 + y^2 = z^2, \qquad x^4 + y^4 = z^4$$

These equations have infinitely many solutions in the reals, but the second equation has no nontrivial integer solutions.

We will consider the linear Diophantine equation,

$$ax + by = c, \quad a, b, c \in \mathbb{Z}$$

We want solutions where $x, y \in \mathbb{Z}$.

**Example**

Are there any solutions in the integers to the equation:

$$7x + 21y = 6$$

---

Suppose that there is a solution. Since $7 \mid 7x$ and $7 \mid 21y$, if there is a solution, $7 \mid 6$. This is a contradiction since $7 \nmid 6$. Therefore, this has no solutions in $\mathbb{Z}$.

**Lemma : (3.1)**

If $x_0, y_0$ is a solution of $ax + by = c$, then for any integer $t$,

$$x = x_0 + bt$$
$$y = y_0 - at$$

is also a solution.

*Proof.* Supposing that $ax_0 + by_0 = c$,

$$\begin{aligned} ax + by &= a(x_0 + bt) + b(y_0 - at) \\ &= ax_0 + abt + by_0 - abt \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

Therefore, $x = x_0 + bt$ and $y = y_0 - at$ satisfy the equation. □

**Example**

Find the integer solutions of the equation:

$$5x + 6y = 17$$

---

By inspection, we see that one solution is $x = 1$, $y = 2$. From Lemma 3.1, it follows that $x = 1 + 6t$ and $y = 2 - 5t$ are also solutions, where $t \in \mathbb{Z}$.

**Lemma : (3.2)**

Consider the equation $ax + by = c$. If $(a, b) \mid c$, then $ax + by = c$ has a solution. If $(a, b) \nmid c$, then $ax + by = c$ has no solutions.

*Proof.* Suppose that there are integers $x_0$ and $y_0$ such that $ax_0 + by_0 = c$. Consider $(a, b) = d$, $d \mid a$ and $d \mid b$. Then, $d \mid (ax_0)$ and $d \mid (by_0)$ so $d \mid c$. Therefore, $(a, b) \mid c$ as wanted.

Conversely, suppose that $(a, b) \mid c$. Then, $c = m\,(a, b)$ for some $m$. From Theorem 1.4, we know that there are integers $r$ and $s$ such that:

$$\begin{aligned} ar + bs &= (a, b) \\ a\,(rm) + b\,(sm) &= m\,(a, b) \\ a\,(rm) + b\,(sm) &= c \end{aligned}$$

Therefore, $x = rm$ and $y = sm$ is a solution. □

**Example**

Which of the following Linear Diophantine equations has no solutions?

$$14x + 34y = 90$$

$$14x + 36y = 93$$

---

1. $14x + 34y = 90$

   $$(14, 34) = 2$$

   $$2 \mid 90$$

   By Lemma 3.2, this has solutions.

2. $14x + 36y = 93$

   $$(14, 36) = 2$$

   $$2 \nmid 93$$

   By Lemma 3.2, this has no solutions.

**Lemma : (3.3)**

Consider the equation:

$$ax + by = c$$

Suppose that $(a, b) = 1$ and $(x_0, y_0)$ is a solution, then:

$$x = x_0 + bt, \quad y = y_0 - at$$

provides all of the solutions.

*Proof.* Consider $ax + by = c$. Suppose $(a, b) = 1$, we have $1 \mid c$, therefore, there exists a

solution $(x_0, y_0)$.

Suppose that $(r, s)$ is a solution, then show

$$r = x_0 + bt, \quad s = y_0 - at$$

Consider the equations:

$$\begin{aligned} ax_0 + by_0 &= c \\ ar + bs &= c \end{aligned}$$

Then,

$$\begin{aligned} ax_0 + by_0 - (ar + bs) &= c - c \\ a(x_0 - r) + b(y_0 - s) &= 0 \end{aligned}$$

$a \mid a(x_0 - r)$ and $a \mid 0$, so $a \mid b(y_0 - s)$. Since $(a, b) = 1$, Corollary 1.1 tells us $a \mid (y_0 - s)$.

$$\begin{aligned} y_0 - s &= at \\ s &= y_0 - at \end{aligned}$$

Now, substitute this back into the equation above.

$$\begin{aligned} a(x_0 - r) + b(y_0 - s) &= 0 \\ a(x_0 - r) + b(y_0 - (y_0 - at)) &= 0 \\ a(x_0 - r) + b(at) &= 0 \\ (x_0 - r) + bt &= 0 \\ x_0 + bt &= r \end{aligned}$$

So we have that:

$$s = y_0 - at, \quad r = x_0 + bt$$

□

**Theorem : (3.1)**

Consider $ax + by = c$, if $(a, b) \mid c$, then there are infinitely many solutions of the form

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

Where $x_0, y_0$ is any solution, and $t \in \mathbb{Z}$.

**Example**

Find all integer solutions of $2x + 6y = 20$.

---

Notice that $x = 1$ and $y = 3$ is a particular solution. The greatest common divisor is $(2, 6) = 2$. By Theorem 3.1, the general solution is given by:

$$x = 1 + \frac{6}{2}t = 1 + 3t, \quad y = 3 - \frac{2}{2}t = 3 - t$$

**Example**

Find all integer solutions of $14x + 21y = 196$.

---

Notice that $x = 14$ and $y = 0$ is a particular solution. The greatest common divisor is $(14, 21) = 7$. By Theorem 3.1, the general solution is given by:

$$x = 14 + \frac{21}{7}t = 14 + 3t, \quad y = 0 - \frac{14}{7}t = -2t$$