

6. Linear Diophantine Equations.

Definition

A *diophantine equation* is one which is polynomial in its variables. It is *linear* if each term contains *at most* one variable.

One variable : equations of the form $ax = b$, $a \neq 0$.

We have

- a solution if and only if $a \mid b$
- If $a \mid b$, then $b = au$, and the only solution is $a = u$.

The theory of equations with *at least two* variables can be deduced from the theory for *exactly two* variables.

In the introduction, we saw that the study of such equations can have quite different outcomes.

For example, $6x+8y = 20$ has a solution $x = 2$, $y = 1$, and many others.

On the other hand $6x+9y = 20$ has *no* solutions in integers. To see this, observe that the right side can be written as $3(2x+3y)$. If x, y are integers, so is $2x+3y$. Thus, 3 divides the right side. As 3 does not divide 20, there are *no* solutions.

Theorem 1 - The Existence Theorem

Let $a, b, c \in \mathbf{Z}$, with $a, b \neq 0$, and put $d = \gcd(a,b)$.

The equation $ax+by = c$ has an integer solution if and only if $d \mid c$.

Proof

As $d = \gcd(a,b)$, $d \mid a$, $d \mid b$ and we have integers with $d = au+bv$.

First, suppose that we have a solution x,y . As d divides a, b it divides any combination of a, b . In particular, $d \mid ax+by$, i.e. $d \mid c$.

Now suppose that $d \mid c$. Then $c = dk$, with $k \in \mathbf{Z}$. As noted above, we have integers u, v with $d = au+bv$. Then

$$c = dk = (au+bv).k = a.(uk) + b.(vk)$$

Thus we have a solution $x = uk$, $y = vk$, each of which is an integer as $u, v, k \in \mathbf{Z}$.

Notice that the proof not only demonstrates the truth of the result, it also shows a useful method of *finding* a solution when one exists. It depends on finding integers u, v with $d = au+bv$. We know that such integers can be found *quickly* using the Euclidean Algorithm.

Example

Determine which of the following equations have integer solutions.

1. $2765x + 4655y = 50$,

2. $84x + 154y = 42$.

Find a solution when one exists.

Solution

1. From an earlier example, we know that $\gcd(2765, 4655) = 35$.
Now $35 \nmid 50$, so the Theorem states that *no* integer solutions exist.

2. We begin by finding $\gcd(84, 154)$.

$$154 = 1 \cdot 84 + 70$$

$$84 = 1 \cdot 70 + 14$$

$$70 = 5 \cdot 14 + 0$$

Now $14 \mid 42$, so the Theorem shows that integer solutions *exist*.

We now backtrack to express 14 as a combination of the coefficients 84 and 154.

$$\begin{aligned} 14 &= 84 - 70 \\ &= 84 - (154 - 84) \\ &= 2 \cdot 84 - 154 \end{aligned}$$

Thus, $14 = 2 \cdot 84 - 154$.

Also, $42 = 3 \cdot 14$, so that

$$\begin{aligned} \frac{42}{2} &= 3(2 \cdot 84 - 154) \\ &= 6 \cdot 84 - 3 \cdot 154 \\ &= 6 \cdot 84 + (-3) \cdot 154. \end{aligned}$$

Hence, we have a solution $x = 6$, $y = -3$.

The above Example shows how to find an *integral* solution of a diophantine equation when such solutions are known to exist. We now look at the problem of finding all *integral* solutions.

Our first result depends on the observation that, if u, v, x, y are integers such that $ux+vy = 1$, then $\gcd(u,v) = 1$. This is so since we know that $\gcd(u,v)$ must divide any combination of u, v . Thus the gcd *divides* 1, so must *be* 1.

Lemma If a, b, d are integers with $d = \gcd(a,b)$, then

1. a/d and b/d are integers, and
2. $\gcd(a/d,b/d) = 1$.

Proof

From the Corollary to the Euclidean Algorithm, $d = ax+by$ for some *integers* x,y .

As $d = \gcd(a,b)$, $d \mid a$ and $d \mid b$. Then $a = du, b = dv$, for some *integers* u, v .

In other words, $u = a/d$, and $v = b/d$ are integers, as required.

As $d = ax+by$, we can divide through by d to get

$$\begin{aligned} 1 = d/d &= (ax+by)/d \\ &= (a/d)x + (b/d)y \\ &= ux+vy. \qquad \text{as } u = a/d, \text{ and } v = b/d \end{aligned}$$

From our earlier remark, we have $\gcd(u,v) = 1$, i.e. $\gcd(a/d,b/d) = 1$.

For example, earlier, we found that $\gcd(2765,4655) = 35$.

With a calculator, it is easy to *verify* that $2765/35 = 79$, and $4655/35 = 133$.

The Lemma guarantees that $\gcd(79,133) = 1$.

Exercise Use the Euclidean Algorithm to show that $\gcd(79,133) = 1$.

Theorem 2 – The General Solution

Let a, b, c be integers such that $d = \gcd(a, b)$ divides c .

Let X, Y be an integer solution of the equation $ax+by = c$ (see Theorem 1).

Then any integer solution of the equation has the form

$$x = X + (b/d)t, \quad y = Y - (a/d)t, \quad t \in \mathbf{Z}.$$

Note that a/d and b/d are integers as $d \mid a$ and $d \mid b$.

Proof

As $d \mid c$, Theorem 1 guarantees the existence of integers X, Y with $aX+bY = c$.

Now suppose that x, y is another integral solution, so that $ax+by = c$.

As each equals c

$$aX+bY = ax+by \quad (1)$$

Rearranging

$$b(Y-y) = a(x-X) \quad (2)$$

As in the Lemma, as $\gcd(a, b) = d$, $u = a/d$, $v = b/d$ are integers with $\gcd(u, v) = 1$.

Then, canceling d from each side of equation (2), we have

$$v(Y-y) = u(x-X). \quad (3)$$

Now, u divides the right side, so it also divides the left side, i.e. $u \mid v(Y-y)$.

As $\gcd(u, v) = 1$, Euclid's Lemma shows that $u \mid (Y-y)$, so $Y-y = ut$, with $t \in \mathbf{Z}$.

Thus, $y = Y-ut$.

We then put ut for $Y-y$ in equation (3) to get

$$vut = u(x-X) \quad (4)$$

Cancelling u from each side of equation (4), we get $vt = x-X$, so $x = X+vt$.

Thus, $x = X+vt$, $y = Y-ut$, $t \in \mathbf{Z}$. As $u = a/d$, $v = b/d$, we have the result.

We say that $\{ x = X+(b/d)t, y = Y-(a/d)t : t \in \mathbf{Z} \}$ is the *general solution of the equation* $ax+by = c$.

Notes

- the expression for x involves b , the coefficient of y in the equation,
- the expression for y involves a , the coefficient of x in the equation,
- the terms involving t have *opposite* sign.

Example

I bought some second class stamps at 20p each, and some first class stamps at 26p each. The total cost was £2.64. How many stamps of each kind did I buy?

Solution

Let x be the number of second class stamps, and y the number of first class.

Then $x, y \in \mathbf{Z}$, with $20x+26y = 264$, and $x, y \geq 0$.

We now find an integer solution of the equation (using the Euclidean Algorithm).

$$26 = 1 \cdot 20 + 6$$

$$20 = 3 \cdot 6 + 2$$

$$6 = 3 \cdot 2 + 0$$

Backtracking :

$$2 = 20 - 3 \cdot 6$$

$$= 20 - 3 \cdot (26 - 20)$$

$$= 4 \cdot 20 - 3 \cdot 26$$

Thus, $2 = 4 \cdot 20 - 3 \cdot 26$. Now $264 = 132 \cdot 2$, so we multiply through by 132 to get

$$264 = 132 \cdot (4 \cdot 20 - 3 \cdot 26) = 528 \cdot 20 - 396 \cdot 26$$

From this, the general solution is $x = 528 + (26/2)t$, $y = -396 - (20/2)t$, $t \in \mathbf{Z}$. In other words,

$$x = 528 + 13t, \quad y = -396 - 10t, \quad t \in \mathbf{Z}.$$

We also require that x and y are non-negative.

$x \geq 0$ is equivalent to $528 + 13t \geq 0$, i.e. $t \geq -528/13 = -(40+8/13)$.

As $t \in \mathbf{Z}$, we must have $t \geq -40$.

$y \geq 0$ is equivalent to $-396 - 10t \geq 0$, i.e. $t \leq -396/10 = -(39+6/10)$.

As $t \in \mathbf{Z}$, we must have $t \leq -40$.

The only common solution has $t = -40$.

This gives $x = 528 + (-40) \cdot 13 = 8$, and $y = -396 - (-40) \cdot 10 = 4$.

In other words, I bought 8 second class, and 4 first class stamps.

Example

Show that the diophantine equation $206x+446y = 40$ has integer solutions.
Find the solution (x,y) for which $x+y$ takes its *smallest positive* value.

Solution

$$\begin{aligned} 446 &= 2 \cdot 206 + 34 \\ 206 &= 6 \cdot 34 + 2 \\ 34 &= 2 \cdot 17 \end{aligned}$$

Thus $\gcd(206,446) = 2$.

As $2 \mid 40$, there are integer solutions (Theorem 1)

Backtracking

$$\begin{aligned} 2 &= 206 - 6 \cdot 34 \\ &= 206 - 6 \cdot (446 - 2 \cdot 206) \quad \text{as } 34 = 406 - 2 \cdot 206 \\ &= 13 \cdot 206 - 6 \cdot 446 \end{aligned}$$

Now, $40 = 20 \cdot 2$, so, multiplying through by 20, we get

$$\begin{aligned} 40 &= 20 \cdot (13 \cdot 206 - 6 \cdot 446) \\ &= 260 \cdot 206 - 120 \cdot 446 \end{aligned}$$

Thus a solution is $x = 260, y = -120$.

Then the *general solution* is

$$\begin{aligned} x &= 260 - (446/2)t = 260 - 223t \\ y &= -120 + (206/2)t = -120 + 103t \end{aligned} \quad \left. \vphantom{\begin{aligned} x \\ y \end{aligned}} \right\} \text{ with } t \in \mathbf{Z}$$

For this, $x+y = 140 - 120t$, and t is an *integer*, so

$x+y$ takes its least positive value for $t = 1$ for $t \geq 2$, $x+y$ is *negative*,
for $t \leq 0$, $x+y > 140$

Thus, the required solution is $x = 37, y = -17$.