Section 4

Linear Diophantine Equations

A *Diophantine equation* is an equation involving a number of variables all of whose coefficients are integers and to which we seek solutions which are integers.

Diophantine Equations with One Variable: These are essentially uninteresting: one simply attempts to solve them as ordinary equations by any method possible and then examines whether the solutions obtained are integers or not.

The behaviour becomes much more interesting if we consider an equation involving two variables.

Example 4.1 Consider

$$x + y = 1.$$

For every choice of x there is a unique solution for y, namely $y = 1 - x$. Thus the equation has infinitely many solutions, all of the form $(x, 1 - x)$ for $x \in \mathbb{Z}$.

Example 4.2 Consider the equation

$$x + 2y = 1.$$

This time we see that a solution for x cannot be arbitrary: it must also be an odd number. On the other hand, given any y there is always a solution for x, namely $x = 1 - 2y$. Thus this equation also has infinitely many solutions, all of the form $(1 - 2y, y)$ for $y \in \mathbb{Z}$.

Example 4.3 Consider the equation

$$3x + 6y = 1.$$

This equation has no solutions: the left-hand side is always a multiple of 3 no matter what choice is made for x and y, while the right-hand side is not a multiple of 3.

Let us now move on to consider the general situation. We start by defining the object of concern.

Definition 4.4 A *linear Diophantine equation* (in two variables) is an equation of the form

$$ax + by = c$$

where a, b and c are integers.

In view of our previous discussion, we have the following natural questions to consider:

- Under what conditions does the above equation have integer solutions?
- If the equation does have solutions, how many solutions does it have?
- How can we find all the solutions?

In view of the last example, it should be unsurprising that the common divisors of a and b are of relevance. We shall address each of these questions in turn.

Existence of Solutions

Consider the general linear Diophantine equation

$$ax + by = c \tag{4.1}$$

where a, b and c are integers. Assume that a and b are both non-zero (so the equation genuinely involves two variables). Let

$$d = \gcd(a, b).$$

Then d divides both a and b so we may write

$$a = da_1 \qquad \text{and} \qquad b = db_1$$

for some integers a_1 and b_1.

Suppose that we do have a solution (x_0, y_0) to the equation. This means $ax_0 + by_0 = c$. Now since d divides a and b, we deduce $d \mid (ax_0 + by_0)$; that is, $d \mid c$.

Conversely suppose $d \mid c$. Write $c = dc_1$. We make use of part (ii) of Theorem 2.6. It tells us that there exist integers u and v such that

$$d = ua + vb.$$

Hence upon multiplying c_1 we obtain

$$uac_1 + vbc_1 = dc_1;$$

that is,

$$a(uc_1) + b(vc_1) = c.$$

Therefore (uc_1, vc_1) is a solution of the equation.

Conclusion: The equation has a solution if and only if $d \mid c$.

Number of Solutions

Suppose that we do have a solution (x_0, y_0) to Equation (4.1). We can find other solutions by taking

$$x = x_0 + b_1 t, \qquad y = y_0 - a_1 t$$

for any integer t. Indeed

$$\begin{aligned} ax + by &= ax_0 + ab_1 t + by_0 - ba_1 t \\ &= (ax_0 + by_0) + (da_1 b_1 t - db_1 a_1 t) \\ &= c + 0 = c. \end{aligned}$$

Since t can be any integer we deduce that our equation has infinitely many solutions.

Finding all Solutions

We have (under the condition $d \mid c$) infinitely many solutions to our linear Diophantine equation. But could there be others about which we are currently unaware?

We shall need the following result in the course of our discussion.

Lemma 4.5 *Let r, s and t be integers and assume that r and s are coprime. If $r \mid st$, then $r \mid t$.*

Recall that to say r and s are coprime is to say that their greatest common divisor is 1.

PROOF: $\gcd(r, s) = 1$, so by part (ii) of Theorem 2.6, there exist integers u and v such that

$$ur + vs = 1.$$

Therefore

$$t = t(ur + vs) = utr + vst.$$

Now $r \mid st$ by assumption, while clearly r divides utr. Hence $r \mid (utr + vst)$, so $r \mid t$, as claimed. □

Now let us return to our linear Diophantine equation (4.1). Suppose we have fixed one solution (x_0, y_0) to (4.1). Let (x, y) be any other solution. So we have

$$ax + by = c = ax_0 + by_0.$$

Hence

$$a_1 d(x - x_0) = b_1 d(y - y_0).$$

Dividing by d gives

$$a_1(x - x_0) = b_1(y - y_0).$$

Now $a_1 = a/d$ and $b_1 = b/d$, so we have $\gcd(a_1, b_1) = 1$ (see Question 3 on Tutorial Sheet II). Hence a_1 and b_1 are coprime, while the above equation tells us

$$a_1 \mid b_1(y - y_0).$$

Hence Lemma 4.5 tells us that

$$a_1 \mid (y_0 - y).$$

This means that $y_0 - y = a_1 t$ for some $t \in \mathbb{Z}$. Substituting into the above equation gives

$$a_1(x - x_0) = b_1 a_1 t.$$

Therefore

$$x - x_0 = b_1 t.$$

Hence $x = x_0 + b_1 t$ and $y = y_0 - a_1 t$.

So we have shown that all solutions to (4.1) arise in the form we previously presented.

We summarise our finding as follows:

Theorem 4.6 *Let a, b and c be integers with a and b not both zero.*

(i) *The linear Diophantine equation*

$$ax + by = c$$

has a solution if and only if $d = \gcd(a, b)$ divides c.

(ii) *If $d \mid c$, then one solution may be found by determining u and v such that $d = ua + vb$ and then setting*

$$x_0 = uc/d \qquad \text{and} \qquad y_0 = vc/d.$$

All other solutions are given by

$$x = x_0 + (b/d)t, \qquad y = y_0 - (a/d)t$$

for $t \in \mathbb{Z}$.

Example 4.7 We shall find all solutions of

$$77x + 42y = 35.$$

First we calculate $\gcd(77, 42)$ using the Euclidean Algorithm:

$$\begin{aligned}
77 &= 42 \cdot 1 + 35\\
42 &= 35 \cdot 1 + 7\\
35 &= 7 \cdot 5 + 0
\end{aligned}$$

So

$$\gcd(77, 42) = 7.$$

Since 7 does divide 35, this means that the linear Diophantine equation does have integer solutions. To actually find the solutions we first reverse the steps in the Euclidean Algorithm:

$$\begin{aligned}
7 &= 42 - 35\\
&= 42 - (77 - 42)\\
&= (-1) \cdot 77 + 2 \cdot 42.
\end{aligned}$$

So we take $u = -1$ and $v = 2$. One solution is then

$$x_0 = (-1) \cdot 35/7 = -5, \qquad y_0 = 2 \cdot 35/7 = 10.$$

All the solutions are given by

$$\begin{aligned}
x &= x_0 + (42/7)t = -5 + 6t\\
y &= y_0 - (77/7)t = 10 - 11t
\end{aligned}$$

where $t \in \mathbb{Z}$.

We can also apply these techniques to other types of problem, for example:

Example 4.8 *A customer bought some apples and some oranges, 12 pieces of fruit in total, and they cost him £1.32. If an apple costs 3p more than an orange, and if more apples than oranges were purchased, how many pieces of each fruit were bought?*

Solution: Let x be the number of apples bought. Then $12 - x$ is the number of oranges bought. Let y be the cost of an apple. Then $y - 3$ is the cost of an orange. We obtain the following equation

$$xy + (12 - x)(y - 3) = 132.$$

Therefore

$$xy + 12y - 36 - xy + 3x = 132$$
$$3x + 12y = 168$$
$$x + 4y = 56$$

We can solve this equation by inspection:

$$x = 56 - 4t, \quad y = t \qquad (\text{for } t \in \mathbb{Z}).$$

But we have further requirements: $6 < x < 12$, so

$$6 < 56 - 4t < 12.$$

Therefore

$$44 < 4t < 50$$
$$11 < t < 12\tfrac{1}{2}.$$

Hence $t = 12$. We deduce that

$$x = 8, \qquad y = 12.$$

So the customer bought 8 apples at 12p each and 4 oranges at 9p each.

(Finally check our working: $8 \cdot 12 + 4 \cdot 9 = 132$.)

Example 4.9 *Suppose that we have available postage stamps in two denominations: 5p and 7p. What values can one make using combinations of stamps?*

(E.g., $10 = 5 + 5$, $12 = 5 + 7$, etc.)

Solution: We are asking for what values of c does

$$5x + 7y = c$$

have (non-negative) solutions? Now $\gcd(5,7) = 1$, so our theory tells us that the equation does always have solutions (but possibly they are negative and one cannot put a negative number of stamps on a parcel!)

Let us instead follow the standard method and adjust at the appropriate point to ensure we are getting non-negative solutions. First apply the Euclidean Algorithm:

$$7 = 5 \cdot 1 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 1 \cdot 2 + 0.$$

(So the greatest common divisor is indeed 1.) Reversing these steps:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(7-5) \\ &= 3 \cdot 5 + (-2) \cdot 7. \end{aligned}$$

So take $u = 3,\ v = -2$. One solution to the linear Diophantine equation is then:

$$x_0 = 3c, \qquad y_0 = -2c.$$

The general solution to the problem is then

$$x = 3c - 7t, \qquad y = -2c + 5t.$$

To achieve non-negative solutions we require

$$3c - 7t \geqslant 0, \qquad\qquad \text{i.e., } t \leqslant 3c/7$$

and

$$-2c + 5t \geqslant 0, \qquad\qquad \text{i.e., } t \geqslant 2c/5.$$

Hence we require that the integer t lie between $2c/5$ and $3c/7$; that is, that there is at least one integer between these numbers. How far apart are they?

$$3c/7 - 2c/5 = (15c - 14c)/35 = c/35.$$

Hence if $c \geqslant 35$, this gap is $\geqslant 1$ and there definitely will be an integer in the region we want. Thus for $c \geqslant 35$, non-negative solutions exist.

Conclusion: Any value of 35p or greater can be achieved using 5p and 7p stamps.

(Values smaller than 35p will have to be checked by hand.)

In fact, it turns out that the crucial point here is that the a and b we are considering here (5 and 7) are coprime. Provided we know this there will always be some point beyond which all integers can be achieved using a combination of multiples of a and b.

Theorem 4.10 *Let a and b be coprime positive integers. Then every number $c \geqslant ab$ can be expressed as $\lambda a + \mu b$ with λ and μ non-negative integers.*

The proof is omitted, but essentially it is the same argument as supplied to solve the above problem.