2.5 LINEAR DIOPHANTINE EQUATIONS

Trina wants to order a new line of clothing for the store. She wants to order shirts and sweaters costing \$20 for each shirt and \$23 for each sweater. She has a total of \$745 to invest. Trina is interested in knowing how many ways the order can be placed. Suppose that Trina orders x number of shirts and y number of sweaters. Then the problem can be stated as: Find all positive integers x and y such that

$$20x + 23y = 745.$$

We discussed a similar problem, in Section 2.3 (Mathematical Induction), which was stated as follows: A local post office temporarily ran out of stamps except for 3- and 5-cent stamps. Using the second principle of mathematical induction, we showed that, to mail letters, any postage charges greater than or equal to 8 cents can be made by using 3- and 5-cent stamps.

Suppose Ron wants to use 80-cent stamps. How many ways can Ron do this? This problem (see Worked-Out Exercise 5, at the end of this section) can be stated as follows: Find all positive integers x and y such that

$$3x + 5y = 80,$$

where x is the number of 3-cent stamps and y is the number of 5-cent stamps.

The mathematician Diophantus of Alexandria initiated the study of such equations in addition to carrying out extensive studies of problems relating to indeterminate equations. It is customary to apply the term Diophantine to any equation with integer coefficients that is to be solved in integers.

A **Diophantine equation** is an algebraic equation in one or more unknowns with integer coefficients, for which integer solutions are sought. Such an equation may have no solution, a finite number of solutions, or an infinite number of solutions. The famous equation

$$x^n + y^n = z^n$$

of Fermat's Last Theorem is also a Diophantine equation.

In this section, we consider linear Diophantine equations only and discuss the necessary and sufficient condition for such an equation to admit integral solutions. We will then apply the results obtained to problems such as the one stated above.

DEFINITION 2.5.1 ▶ A linear equation of the form $ax + by = c$, where a, b, c are integers and x, y are variables such that the solutions are restricted to integers, is called a **linear Diophantine equation in two variables**.

Historical Notes

Diophantus
(ca. 200–284 A.D.)
Much of what is known about Diophantus' life is taken from a cryptic riddle called The Greek Anthology. It implies that Diophantus married at 26 years of age and had a son who died four years before his own death at 84, though there is speculation that the puzzle is completely fictitious. What is somewhat more certain is that he was a Hellenized Babylonian living in Alexandria during the Silver Age.

Diophantus is best known for his collection of writings called *Arithmetica*, of which 6 of the 13 original volumes still exist today. The book considers 130 mathematical problems and their solutions—specifically, positive rational solutions. Today, Diophantine equations only allow for linear solutions.

Let

$$ax + by = c$$

be a linear Diophantine equation. If (x_0, y_0) is a pair of integers such that $ax_0 + by_0 = c$, then (x_0, y_0) is said to be an *integral solution* of this equation.

Consider the Diophantine equation

$$14x + 12y = 33.$$

Suppose this equation has an integral solution (x_0, y_0). Then

$$14x_0 + 12y_0 = 33.$$

Now 2 divides $14x_0 + 12y_0$. Hence 2 divides 33, which is not true. So we find that a Diophantine equation may not automatically have an integral solution. The next theorem tells us when a Diophantine equation has an integral solution.

Theorem 2.5.2: The linear Diophantine equation

$$ax + by = c \tag{2.20}$$

with $a \neq 0, b \neq 0$ has a solution if and only if d divides c, where $d = \gcd(a, b)$. Moreover, if $x = x_0, y = y_0$ is a particular solution of this equation, then all solutions of this equation are given by

$$x = x_0 + \frac{b}{d}n, \qquad y = y_0 - \frac{a}{d}n,$$

where n is any integer.

Proof: Let $d = \gcd(a, b)$.

Suppose (x_0, y_0) is a solution of $ax + by = c$. Then

$$ax_0 + by_0 = c.$$

Because $d = \gcd(a, b)$, we have d divides a and b, and so by Theorem 2.1.14(iii), d divides $ax_0 + by_0$. This in turn implies that d divides c.

Conversely, suppose d divides c. Then $c = dk$ for some integer k. Because $d = \gcd(a, b)$, by Theorem 2.1.19, there exist integers r and t such that $ar + bt = d$. Now

$$\begin{aligned} & ar + bt = d \\ \Rightarrow\ & ark + btk = dk \\ \Rightarrow\ & ark + btk = c && \text{because } c = dk \\ \Rightarrow\ & a(rk) + b(tk) = c \end{aligned}$$

Now rk and tk are integers. Therefore, $x = rk$ and $y = tk$ is a solution of the Diophantine equation $ax + by = c$.

Suppose now that (x_0, y_0) is a particular solution of $ax + by = c$ and (x', y') is another solution of $ax + by = c$. Then

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

Dividing both sides by d, we get

$$\frac{a}{d}x' + \frac{b}{d}y' = \frac{a}{d}x_0 + \frac{b}{d}y_0,$$

which is equivalent to

$$\frac{a}{d}(x' - x_0) = \frac{b}{d}(y_0 - y'). \tag{2.21}$$

Now $d = \gcd(a, b)$, so we have

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

From (2.21), we have $\frac{a}{d}$ divides $\frac{b}{d}(y_0 - y')$. Because $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, we must have $\frac{a}{d}$ divides $y_0 - y'$. Therefore, there exists an integer k such that

$$y_0 - y' = \frac{a}{d}k.$$

This implies that

$$y' = y_0 - \frac{a}{d}k.$$

Substitute $y_0 - y' = \frac{a}{d}k$ in (2.21) to get

$$\frac{a}{d}(x' - x_0) = \frac{b}{d} \cdot \frac{a}{d}k.$$

Because $\frac{a}{d} \neq 0$, canceling $\frac{a}{d}$ from both sides we get

$$x' - x_0 = \frac{b}{d}k,$$

or

$$x' = x_0 + \frac{b}{d}k.$$

Therefore, for the solution (x', y') of the Diophantine equation $ax + by = c$, there exists an integer k such that

$$x' = x_0 + \frac{b}{d}k \quad \text{and} \quad y' = y_0 - \frac{a}{d}k.$$

In fact, for any integer n,

$$\left(x_0 + \frac{b}{d}n, \quad y_0 - \frac{a}{d}n\right)$$

is a solution of $ax + by = c$ because

$$\begin{aligned} a\left(x_0 + \frac{b}{d}n\right) + b\left(y_0 - \frac{a}{d}n\right) &= (ax_0 + by_0) + \frac{ab}{d}n - \frac{ab}{d}n \\ &= ax_0 + by_0 = c. \end{aligned}$$

Consequently, if (x_0, y_0) is a solution of (2.20), then all solutions are given by

$$x = x_0 + \frac{b}{d}n, \qquad y = y_0 - \frac{a}{d}n,$$

where $n \in \mathbb{Z}$. ∎

EXAMPLE 2.5.3 In this example, we solve the problem posed at the beginning of this section. That is, find the integral solution of the following linear Diophantine equation.

$$20x + 23y = 745. \tag{2.22}$$

Now $\gcd(20, 23) = 1$ and by using the division algorithm, we have

$$\begin{aligned}23 &= 1 \cdot 20 + 3,\\ 20 &= 6 \cdot 3 + 2,\\ 3 &= 1 \cdot 2 + 1,\\ 2 &= 2 \cdot 1 + 0.\end{aligned}$$

Hence,

$$\begin{aligned}1 &= 3 - 1 \cdot 2\\ &= 3 - 1(20 - 6 \cdot 3)\\ &= 3 - 1 \cdot 20 + 6 \cdot 3\\ &= 7 \cdot 3 - 1 \cdot 20\\ &= 7 \cdot (23 - 1 \cdot 20) - 1 \cdot 20\\ &= 7 \cdot 23 - 8 \cdot 20.\end{aligned}$$

Thus, $1 = 7 \cdot 23 - 8 \cdot 20$. Multiply both sides of this equation by 745 to get

$$745 = 20(-5960) + 23(5215).$$

This implies that $x = -5960$ and $y = 5215$ is an integral solution of (2.22). Hence, all integral solutions of (2.22) are

$$x = -5960 + 23n, \qquad y = 5215 - 20n \quad \text{for any integer } n.$$

Because we must have $x > 0, y > 0$, we find that

$$-5960 + 23n > 0 \quad \text{and} \quad 5215 - 20n > 0.$$

Therefore,

$$\frac{5960}{23} < n < \frac{5215}{20},$$

i.e.,

$$259\frac{3}{23} < n < 260\frac{15}{20}.$$

Thus, $n = 260$. Because there is only one choice for n, it follows that there is only one way the order can be placed. Moreover, for $n = 260$,

$$x = -5960 + 23 \cdot 260 = 20 \quad \text{and} \quad y = 5215 - 20 \cdot 260 = 15.$$

Hence, the number of shirts is 20 and the number of sweaters is 15.

EXAMPLE 2.5.4 In this example, we determine all solutions of the equation

$$8x + 14y = 58. \tag{2.23}$$

Here $a = 8$, $b = 14$, and $c = 58$. Now $\gcd(a, b) = \gcd(8, 14) = 2$ and $2 \mid 58$. Hence, by Theorem 2.5.2, (2.23) has a solution. Now

$$2 = 2 \cdot 8 + (-1) \cdot 14.$$

Multiply both sides with 29 to get

$$58 = 8 \cdot 58 + 14 \cdot (-29).$$

This implies that $x_0 = 58$ and $y_0 = -29$ is a solution of (2.23).

Again by Theorem 2.5.2, all integral solutions are given by

$$x = 58 + \frac{14}{2}n \quad \text{and} \quad y = -29 - \frac{8}{2}n \quad \text{for all integers } n,$$

i.e.,

$$x = 58 + 7n \quad \text{and} \quad y = -29 - 4n \quad \text{for all integers } n.$$

The following algorithm determines the integral solutions, if any, of a linear Diophantine equation.

ALGORITHM 2.11: Determine the integral solutions of a linear Diophantine equation.

Input: Integers a, b, and c

Output: (x, y), specifying integral solutions of the linear Diophantine equation $ax + by = c$

```
1.  procedure integralSolutions(a,b,c)
2.  begin
3.    d := gcd(a,b);
4.    if c mod d = 0 then   //d divides c
5.    begin
6.      determine integers s and t such that d = sa + tb
7.      k := c div d;
8.      x0 := s * k;
9.      y0 := t * k;
10.     print (x0 + (b/d)n, y0 - (a/d)n)
11.   end
12.   else
13.     print "The equation has no integral solutions."
14. end
```

Suppose x_0, y_0, a, b, and $d = \gcd(a, b)$ are as in Example 2.5.4. Then the print statement in Line 10 outputs $(58 + 7n, -29 - 4n)$.

WORKED-OUT EXERCISES

Exercise 1: Find all the integral solutions of the equation $15x + 14y = 7$.

Solution: Now $\gcd(15, 14) = 1$ and 1 divides 7. Therefore, $15x + 14y = 7$ has an integral solution. Now

$$1 = 15 \cdot 1 + 14(-1).$$

We multiply this equality by 7 to get

$$15 \cdot 7 + 14(-7) = 7.$$

This implies that $x = 7$ and $y = -7$ is an integral solution of the given equation. All integral solutions of the given equations are given by

$$x = 7 + \frac{14}{1}n \quad \text{and} \quad y = -7 - \frac{15}{1}n \quad \text{for any integer } n,$$

i.e.,

$$x = 7 + 14n, \qquad y = -7 - 15n$$

for any integer n.

Exercise 2: Which of the following linear equations cannot be solved in integers?

(a) $28x + 16y = 6$ (b) $51x + 18y = 12$
(c) $21x + 35y = 45$

Solution:

(a) $\gcd(28, 16) = 4$ and 4 does not divide 6. Hence, this equation has no integral solution.
(b) $\gcd(51, 18) = 3$ and 3 divides 12. This implies that the given equation has solutions in integers.
(c) $\gcd(21, 35) = 7$ and 7 does not divide 45. Hence, the given equation has no integral solution.

Exercise 3: Find all positive integral solutions of $19x + 37y = 500$.

Solution: The $\gcd(19, 37) = 1$ and 1 divides 500. Hence, $19x + 37y = 500$ has integral solutions.

By the division algorithm,

$$37 = 19 \cdot 1 + 18$$
$$19 = 1 \cdot 18 + 1.$$

Thus,

$$18 = 37 - 19.$$
$$1 = 19 - 18 = 19 - (37 - 19) = 19 \cdot 2 + 37 \cdot (-1).$$

This implies that

$$500 = 19 \cdot (1000) + 37 \cdot (-500).$$

Thus, an integral solution of the given equation is $x = 1000, y = -500$. All integral solutions of the given equation are given by

$$x = 1000 + 37n, \qquad y = -500 - 19n,$$

for all integers n.

When the solutions are positive, then

$$1000 + 37n > 0 \quad \text{and} \quad -500 - 19n > 0.$$

The integer n must satisfy

$$-\frac{1000}{37} < n < -\frac{500}{19}$$
$$-27.027 < n < -26.31.$$

Therefore, $n = -27$. The equation $19x + 37y = 500$ has exactly one positive integral solution and this is

$$x = 1000 + 37 \cdot (-27) = 1,$$
$$y = -500 - 19 \cdot (-27) = 13,$$

That is, the positive solution of the given Diophantine equation is $(1, 13)$.

Exercise 4: Steve has \$1000 to buy certain bags and boxes filled with surprise gifts. If each bag costs \$25 and each box costs \$35, how many ways can the items be bought? Also, for each choice, determine the number of each item bought.

Solution: Suppose Steve bought x bags and y boxes. Then

$$25x + 35y = 1000. \tag{2.24}$$

Now $\gcd(25, 35) = 5$. Because $5 \mid 25$ and $5 \mid 35$, the preceding equation has a solution.

By using the division algorithm, we have

$$35 = 1 \cdot 25 + 10,$$
$$25 = 2 \cdot 10 + 5,$$
$$10 = 2 \cdot 5 + 0.$$

Hence,

$$\begin{aligned} 5 &= 25 - 2 \cdot 10 \\ &= 25 - 2(35 - 1 \cdot 25) \\ &= 25 - 2 \cdot 35 + 2 \cdot 25 \\ &= 3 \cdot 25 - 2 \cdot 35. \end{aligned}$$

Multiplying both sides by 200, we get

$$1000 = 600 \cdot 25 - 400 \cdot 35.$$

This implies that $x_0 = 600$ and $y_0 = -400$ is an integral solution of (2.24). Hence, all integral solutions of (2.24) are

$$\begin{aligned} x &= 600 + \frac{35}{5}n = 600 + 7n, \\ y &= -400 - \frac{25}{5}n = -400 - 5n, \end{aligned} \tag{2.25}$$

for any integer n.

Because we must have $x > 0, y > 0$, we find that

$$600 + 7n > 0 \quad \text{and} \quad -400 - 5n > 0.$$

This implies that

$$600 > -7n \quad \text{and} \quad -5n > 400$$

or

$$\frac{600}{7} > -n \quad \text{and} \quad -n > 80.$$

Let us write $m = -n$. Then

$$\frac{600}{7} > m \quad \text{and} \quad m > 80.$$

Therefore,

$$80 < m < \frac{600}{7}.$$

The integers greater than 80 and less than $85\frac{5}{7}$ are 81, 82, 83, 84, and 85. Thus, there are five ways Steve can buy the items.

Substitute $n = -m$ in (2.25) to get

$$x = 600 - 7m, \qquad y = -400 + 5m,$$

where $m = 81, 82, 83, 84$, or 85. For each choice of m, the item can be bought as follows.

m	81	82	83	84	85
Number of bags: x	33	26	19	12	5
Number of boxes: y	5	10	15	20	25

Exercise 5: A local post office temporarily ran out of stamps except for 3- and 5-cent stamps. Ron wants to mail a letter that needs 80 cents' worth of stamps. How many ways can Ron use 3- and 5-cent stamps to pay the 80-cents postage charge?

Solution: This problem is equivalent to finding all the positive integral solutions of $3x + 5y = 80$.

The $\gcd(3, 5) = 1$ and 1 divides 80. Therefore, $3x + 5y = 80$ has an integral solution.

Now,

$$1 = 3 \cdot 2 + 5(-1).$$

This implies that

$$80 = 3(160) + 5 \cdot (-80).$$

Thus, an integral solution of the given equation is $x = 160, y = -80$. All integral solutions of the given equation are given by

$$x = 160 + 5n, \qquad y = -80 - 3n,$$

for all integers n.

When the solutions are positive, then

$$160 + 5n > 0 \quad \text{and} \quad -80 - 3n > 0.$$

This implies n must satisfy

$$-\frac{160}{5} < n < -\frac{80}{3}$$

or

$$-32 < n < -26.66.$$

Because n is an integer, we must have $n = -31, -30, -29, -28$, and -27. Therefore, the equation $3x + 5y = 80$ has exactly five positive integral solutions and these are

$$x = 160 + 5 \cdot (-31) = 5, \qquad y = -80 - 3 \cdot (-31) = 13,$$
$$x = 160 + 5 \cdot (-30) = 10, \qquad y = -80 - 3 \cdot (-30) = 10,$$
$$x = 160 + 5 \cdot (-29) = 15, \qquad y = -80 - 3 \cdot (-29) = 7,$$
$$x = 160 + 5 \cdot (-28) = 20, \qquad y = -80 - 3 \cdot (-28) = 4,$$
$$x = 160 + 5 \cdot (-27) = 25, \qquad y = -80 - 3 \cdot (-27) = 1.$$

That is, the positive integral solutions are $(5, 13)$, $(10, 10)$, $(15, 7)$, $(20, 4)$, and $(25, 1)$. To pay for the 80-cents postage charges, Ron can use the available stamps as follows

Number of 3-cent stamps	Number of 5-cent stamps
5	13
10	10
15	7
20	4
25	1.

Section Review

Key Term

Diophantine equation

Key Definition

1. A linear equation of the form $ax + by = c$, where a, b, c are integers and x, y are variables such that the solutions are restricted to integers, is called a linear Diophantine equation in two variables.

Key Result

1. The linear Diophantine equation

$$ax + by = c$$