

A Diophantine equation is any equation for which you are interested only in the integer solutions to the equation.

Thus a ***linear Diophantine equation*** is a linear equation  $ax + by = c$  with integer coefficients for which you are interested only in finding integer solutions.

In the last lesson you saw how to use a TI-83/84 to solve the linear Diophantine equation  $x + 4y = 44$  subject to the constraint  $6 < x < 12$ .

Had this equation not been subject to a constraint on  $x$ , there would have been an infinite number of solutions  $x_0, y_0$ . Using a TI-83/84 to find them would be an impossible task unless you are quite adept at recognizing obscure patterns.

In this lesson you will see how to solve linear Diophantine equations using nothing more than pencil and paper.

This will require you to recall a theorem from the previous lesson titled:

Books VII – IX of the *Elements*,  
Part 1: Divisibility.

## Theorem D1

**For any nonzero integers  $a$  and  $b$ , there exist integers  $x^*$  and  $y^*$  such that**

$$\mathbf{gcd(a,b) = ax^* + by^* .}$$

In that previous lesson you also saw in detail how to use the Euclidean Algorithm to find the values of  $gcd(a,b)$ ,  $x^*$ , and  $y^*$ .

Later in this lesson I will review, without explanation, how this is done.

When you have a linear Diophantine equation to solve, the first question you should ask about that Diophantine equation is whether or not the equation admits solutions in integers.

The following theorems tell you how to find the answer to these question.

## Theorem D2

If  $\gcd(a,b) \nmid c$ , then the linear Diophantine equation  $ax + by = c$  has no solution.

**Proof:** Let  $d = \gcd(a,b)$ . Then there are integers  $r$  and  $s$  such that  $dr = a$  and  $ds = b$ .

By way of contradiction, assume that  $ax + by = c$  does have a solution  $x_0, y_0$ .

Then  $c = ax_0 + by_0 = drx_0 + dsy_0$ .

But this says that  $d \mid c$  since  $c = d(rx_0 + sy_0)$ .

Since this is a contradiction, the Diophantine equation has no solution.

### Theorem D3

If  $\gcd(a,b) \mid c$ , then the linear Diophantine equation  $ax + by = c$  has a solution.

**Proof:** Let  $d = \gcd(a,b)$ . Since  $d \mid c$ ,  $dp = c$  for some integer  $p$ .

By theorem D1, there are integers  $x^*$  and  $y^*$  such that  $d = ax^* + by^*$ .

So  $c = dp = a(x^*p) + b(y^*p)$ .

Hence  $ax + by = c$  has a solution, namely  $x_0 = x^*p$  and  $y_0 = y^*p$ .

# Examples

- By Theorem D2, the Diophantine equation  $2x + 10y = 17$  has no solution (in integers) since  $\gcd(2, 10) = 2 \nmid 17$ .
- By Theorem D3, the Diophantine equation  $3x + 6y = 18$  does have solutions (in integers) since  $\gcd(3, 6) = 3 \mid 18$ .

If a linear Diophantine equation  $ax + by = c$  does have a solution (that is if  $\gcd(a,b) \mid c$ ), how do you solve it?

## Theorem D4

If the linear Diophantine equation  $ax + by = c$  does have a solution, then all such solutions are given by

$$x = x_0 + (b/d)t \text{ and } y = y_0 - (a/d)t$$

where  $d = \gcd(a, b)$ ,  $x_0, y_0$  is a particular solution to the equation and  $t$  ranges over the integers.

If  $d = \gcd(a, b) \mid c$ , then the solutions to  $ax + by = c$  are  $x = x_0 + (b/d)t$  and  $y = y_0 - (a/d)t$  where  $x_0, y_0$  is a particular solution and  $t$  ranges over the integers.

To solve  $ax + by = c$ :

- Use the Euclidean Algorithm to find  $\gcd(a, b)$ .
- Use the Euclidean Algorithm to find  $x^*$  and  $y^*$  such that  $d = ax^* + by^*$ .
- Find  $p$  such that  $c = dp$ . ( $p$  exists since  $d \mid c$ .)
- Then  $x_0 = x^*p$  and  $y_0 = y^*p$  are particular solutions since  $c = dp = a(x^*p) + b(y^*p)$ .
- Then all solutions are  $x = x_0 + (b/d)t$  and  $y = y_0 - (a/d)t$  where  $t$  is an integer.

Find all solutions to the Diophantine equation  
 $172x + 20y = 1000$ .

- Use the Euclidean Algorithm to find  $d = \gcd(172, 20)$ .

$20 \overline{)172} \quad 8 \text{ R. } 12$      $12 \overline{)20} \quad 1 \text{ R. } 8$      $8 \overline{)12} \quad 1 \text{ R. } 4$      $4 \overline{)8} \quad 2 \text{ R. } 0$

**gcd = last nonzero remainder**

- Use the Euclidean Algorithm to find  $x^*$  and  $y^*$  such that  $d = ax^* + by^*$ .

Solve for the remainder.

$$20 \overline{)172} \begin{array}{l} 8 \\ \hline \end{array} \text{ R. 12} \quad \Rightarrow \quad 12 = 172 - 1 \cdot 20 \quad \text{Eq.1}$$

$$12 \overline{)20} \begin{array}{l} 1 \\ \hline \end{array} \text{ R. 8} \quad \Rightarrow \quad 8 = 20 - 1 \cdot 12 \quad \text{Eq.2}$$

$$8 \overline{)12} \begin{array}{l} 1 \\ \hline \end{array} \text{ R. 4} \quad \Rightarrow \quad 4 = 12 - 1 \cdot 8 \quad \text{Eq.3}$$

Using these  
equations we get:

$$12 = 172 - 1 \cdot 20 \quad \text{Eq.1}$$

$$8 = 20 - 1 \cdot 12 \quad \text{Eq.2}$$

$$4 = 12 - 1 \cdot 8 \quad \text{Eq.3}$$

$$4 = 12 - 1 \cdot 8 \quad \text{Eq.3}$$

$$4 = 12 - 1 \cdot (20 - 1 \cdot 12) \quad \text{Eq.2}$$

$$4 = 2 \cdot 12 - 1 \cdot 20 \quad \text{Simp.}$$

$$4 = 2 \cdot (172 - 8 \cdot 20) - 1 \cdot 20 \quad \text{Eq.1}$$

$$4 = 2 \cdot 172 + (-17) \cdot 20 \quad \text{Simp.}$$

So  $x^* = 2$  and  $y^* = -17$

$$\text{Solve } 172x + 20y = 1000$$

$$4 = 2 \cdot 172 + (-17) \cdot 20$$

- Find  $p$  such that  $c = dp$ .

$$d = \gcd(172, 20) = 4$$

$$c = 1000$$

$$\text{so } 1000 = 4 \cdot 250.$$

$$\text{Solve } 172x + 20y = 1000$$

$$4 = 2 \cdot 172 + (-17) \cdot 20$$

- Then  $x_0 = x^*p$  and  $y_0 = y^*p$  are particular solutions since  $c = dp = a(x^*p) + b(y^*p)$ .

$$1000 = 4 \cdot 250 = [2 \cdot 172 + (-17) \cdot 20] \cdot 250$$

$$1000 = 172 \cdot (500) + 20 \cdot (-4250)$$

So a particular solution is

$$x_0 = 500 \text{ and } y = -4250.$$

Solve  $172x + 20y = 1000$

- Then all solutions are  $x = x_0 + (b/d)t$  and  $y = y_0 - (a/d)t$  where  $t$  is an integer.

From the equation  $172x + 20y = 1000$ , we see that  $a = 172$  and  $b = 20$ .

From our previous work,  $x_0 = 500$ ,  $y_0 = -4250$ , and  $d = 4$ .

So the solutions, in integers, are

$$x = 500 + 5t \text{ and } y = -4250 - 43t$$

where  $t$  ranges over the integers.

## Example

Find all *positive* solutions to the Diophantine equation  $172x + 20y = 1000$ .

We just saw that all solutions to this equation are of the form  $x = 500 + 5t$  and  $y = -4250 - 43t$  where  $t$  ranges over the integers. So we need to find those values of  $t$  for which

$$x = 500 + 5t > 0 \text{ and } y = -4250 - 43t > 0.$$

Find all *positive integer solutions* to the equation

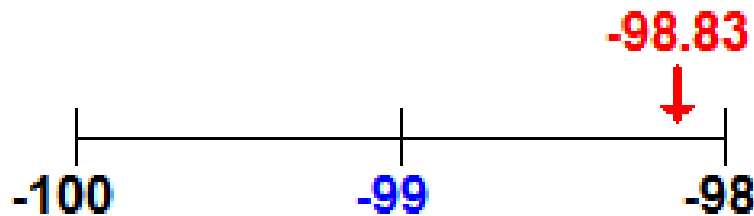
$$172x + 20y = 1000.$$

All solutions are  $x = 500 + 5t$  and  $y = -4250 - 43t$ .

$$x = 500 + 5t > 0 \Rightarrow t > -100.$$

$$y = -4250 - 43t > 0 \Rightarrow t < -98.83\dots$$

Since  $t$  must be an *integer*,  $t \leq -99$ .



So  $-100 < t \leq -99$ .

Find all *positive* integer solutions to the equation

$$172x + 20y = 1000.$$

All solutions are  $x = 500 + 5t$  and  $y = -4250 - 43t$ .

We just found that  $-100 < t \leq -99$ .

Since  $t$  must be an integer,

$-100 < t \leq -99 \Rightarrow t = -99$ . So there is only one positive solution to the Diophantine equation, namely

$$x = 500 + 5t = \dots = 5 \text{ and}$$

$$y = -4250 - 43t = \dots = 7.$$