Section 3. Linear Diophantine Equations

Note. In this section, we define linear Diophantine equations. We give necessary and sufficient conditions for the existence of integer solutions to such equations. We consider more general Diophantine equations, which are studied in more detail in later sections.

Note. Dudley introduces linear Diophantine equations with the following problem:

> In a corral there are cowboys and an odd number of horses. There are 20 legs in all. How many legs belong to horses?

With h as the number of horses and c as the number of cowboys (both positive integers), we need solution(s) to the equation $4h + 2c = 20$. Of course there are infinitely many solutions using *real numbers*, but it is not immediately obvious that there are *positive integer* solutions (well, it *is* here since the numbers are small, but in general it might not be so obvious). This is an example of a linear Diophantine equation. We will explore it again below.

Definition. An equation of the form $ax + by = c$, where a, b, and c are integers, is a *linear Diophantine equation*. A *solution* to the equation is a pair of integers x and y.

Note. Other types of Diophantine equations are of the form $x^2 + y^2 = z^2$ (considered in Section 18), $x^4 + y^4 = z^4$ (considered in Section 19), and $x^2 - 2y^2 = 1$ (considered in Section 20). In each case, we seek integer solutions x, y, and z.

Note. Diophantus is sometimes called the "father of algebra." He presented his work on algebraic equations and number theory in his *Arithmetica*. Though his mathematical work is known, details about his life are vague at best; for example, the dates of when he lived (circa 200 CE–circa 284 CE) are rough estimates. In *Arithmetica* he considers three types of quadratic equations: $ax^2 + bx = c$, $ax^2 = bx + c$, and $ax^x + c = bx$. The reason for this is that he would not allow the use of negative numbers (in fact negative numbers become a widely accepted part mathematics due to the development of the theory of equations only in the 16th century, largely due to work by Tartaglia and Cardano; see my online notes for Introduction to Modern Algebra [MATH 4127/5127] on A Students Question: Why The Hell Am I In This Class? for some details... complex numbers also attain a level of acceptance at this time). So he would only accept positive, rational solutions to these equations. He considers polynomials in x that can take on a value that is a perfect square or perfect cube. Diophantus introduced an algebraic symbolism that used an abbreviation for the unknown and the powers of the unknown. You might get an appreciation for the difficulty of arithmetic work in Diophantus' time; remember that the numerals which we use, the "Arabic numerals," were not used until after the 1,000 CE. Other works by Diophantus include "On Polygonal Numbers," "The Porisms" (a collection of lemmas), and "Preliminaries to the Geometric Elements." *Arithmetica* was translated from Greek into Latin in the 1400s and this lead to the spread of Diophantus' ideas. It was a 1621 copy by Bachet from which Pierre de Fermat studied and in the margins of his copy in which he wrote that he found a proof that there are no positive integer solutions x, y, x to the equation $x^n + y^n = z^n$ when integer n is greater than 2 (this lead to "Fermat's Last

Theorem," which remained unproved from the mid 1600s to the late 1900s; we'll discuss this more in Section 17). You can read *Arthmetica* online at: *Diophantus of Alexandria, A Study in the History of Greek Algebra*, 2nd Edition, by Sir Thomas L. Heath (Cambridge University Press, 1910) (accessed 7/5/2021).

Diophantus of Alexandria (circa 200–circa 284)

The image is from Greatest Greeks webpage. The biographical information is from MacTutor History of Mathematics Archive page on Diophantus. Both accessed 7/5/2021.

Note. Not every linear Diophantine equation has an integer solution. For example, $2x + 4y = 5$ has no solution since $2x + 4y$ is even and 5 is not. We now return to the horses and cowboys problem stated at the beginning of this section. We required positive integers h and c such that $4h + 2c = 20$. We can rearrange this to get $h = (10 - c)/2$. Since we require *positive* integer solutions, we see that we can take c to be between 1 and 9. Also, c must be even so that h is an integer. This gives us the four solutions (c, h) of $(2, 4)$, $(4, 3)$, $(6, 2)$, and $(8, 1)$. But in the given problem, we required that "there are cowboys [plural; at least 2] and an

odd number of horses." Of the four solutions, the only one that satisfies these two conditions is $(c, h) = (4, 3)$. To answer the posed question "How many legs belong to horses?," we see that we have $4h = 4 \times 3 = 12$ legs.

Note. We want an organized way to determine if a linear Diophantine equation has a solution, and when it does we want to find the solutions. In our first result, we show that if a linear Diophantine equation has one solution then in has infinitely many solutions. By "solution," we mean a solution using integers.

Lemma 3.1. If $x = x_0$ and $y = y_0$ is a solution of $ax+by = c$, then so is $x = x_0+bt$ and $y = y_0 - at$ for any integer $t \in \mathbb{Z}$.

Note. We now give necessary and sufficient conditions for a linear Diophantine equation to have a solution.

Lemma 3.2. If $(a, b) \not| \, c$ then $ax + by = c$ has no solutions, and if $(a, b) \,|\, c$ then $ax + by = c$ has a solution.

Note 3.3.A. If the linear Diophantine equation $ax + by = c$ has a solution, then by Lemma 3.2 we know that $(a, b) \,|\, c$. We denote $(a, b) = d$ so that we can then divide both sides of $ax + by = c$ to create a new linear Diophantine equation (since the numbers involved will remain integers by the divisibility conditions). Since

$d \mid a$ then $a = da'$, since $d \mid b$ then $b = db'$, and since $d \mid, c$ then $c = cc'$ (for some integers a', b', and c'). Then $ax + by = c$ becomes $a'x + b'y = c'$ where $(a', b') = 1$ by Theorem 1.1. So if a linear Diophantine equation has solutions, then we can find the solutions by considering an equation whose coefficients are relatively prime (and in this equation the coefficients are smaller in absolute value). Lemma 3.1 gives infinitely many solutions which we show below (in Lemma 3.3) are all of the solutions.

Exercise 3.3(c). Find all solutions of $14x + 35y = 91$.

Lemma 3.3. Suppose that $(a, b) = 1$ and $x = x_0$, $y = y_0$ is a solution of $ax+by = c$. Then all solutions of $ax + by = c$ are given by $x = x_0 + bt$, $y = y_0 - at$ where $t \in \mathbb{Z}$.

Note. Notice from Note 3.3.A that if we start with equation $ax + by = c$ (which has a solution) then we can modify the to get $a'x+b'y = c'$ where $(a', b') = 1$, which then has solutions $x = x_0 + b't = x_0 + (b/(a, b))t$, $y = y_0 - a't = x_0 - (a/(a, b))t$ where $x = x_0$, $y = y_0$ is a solution of $a'x + b'y = c'$. This observation allows us to combine Lemmas 3.1, 3.2, and 3.3 to get the following.

Theorem 3.1. The linear Diophantine equation $ax + by = c$ has no solutions if $(a, b) \not| c$. If $(a, b) \mid c$, then there are infinitely many solutions,

$$x = r + \frac{b}{(a, b)}t, \ y = s - \frac{a}{(a, b)}t \text{ where } t \in \mathbb{Z}$$

and $x = r$, $y = s$ is some solution.

Note. We are still left with the problem of finding some solution to $ax + by = c$ on which we can base the general solution. We will use congruences in Section 5 to find such a solution $x = r$, $y = s$.

Revised: 7/5/2021