Summary: The Euclidean Algorithm and Linear Diophantine Equations

The main goals of this chapter are to develop:

- The Euclidean Algorithm[1] to efficiently compute greatest common divisors;
- A method for quickly determining when an equation of the form $ax + by = c$ has integer solutions (x, y).
- A method for quickly finding a single solution (x, y) to an equation of the form $ax + by = c$ (when there are solutions).
- A method for determining all solutions to an equation of the form $ax + by = c$ starting from a single solution.

In the end, we are able to find all solutions to any linear diophantine equation.

Before addressing the Research Questions we will first prove a lemma. Without the lemma, we would end up reproving this fact several times in slightly different contexts in the Research Questions below.

Lemma 2.1 *Suppose $a, b, c, d, n \in \mathbf{Z}$. If $n \mid a$ and $n \mid b$, then $n \mid (ac + bd)$.*

Proof. Since $n \mid a$, there exists an integer a_1 such that $na_1 = a$. Similarly since $n \mid b$, there exists $b_1 \in \mathbf{Z}$ such that $nb_1 = b$. Thus,

$$\begin{aligned} ac + bd &= na_1c + nb_1d \\ &= n(a_1c + b_1d). \end{aligned}$$

Thus, $n \mid (ac + bd)$. $\square$

The key observation that makes the Euclidean Algorithm work is the subject of Research Question 1.

Theorem 2.2 (RQ1) *Suppose that a and b are positive integers, and let q and r be integers such that $a = qb + r$ and $0 \leq r < b$. (The existence of q and r is guaranteed by the Division Algorithm.) Then $\gcd(a, b) = \gcd(b, r)$.*

[1] The *Euclidean Algorithm* was published by Euclid in his treatise on geometry, *Elements*, during the third century B.C. The Euclidean Algorithm is the oldest algorithm on record to be presented in general terms, as opposed to earlier algorithms for arithmetic operations which are given as a series of examples. Moreover, the term *algorithm* (for its modern usage) was first employed in the 1950s to describe the Euclidean Algorithm.

Proof. To simplify notation, we let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(b, r)$. Our strategy in this proof will be to show two things: (1) $d_1 \leq d_2$, and (2) $d_2 \leq d_1$. From this, the only possible conclusion is that $d_1 = d_2$, which is exactly what we want to prove.

Since $d_2 = \gcd(b, r)$, it follows that $d_2 \mid b$ and $d_2 \mid r$. By Lemma 2.1, this implies that d_2 divides

$$bq + r \cdot 1 = qb + r = a.$$

Since d_2 is a common divisor of a and b and $d_1 = \gcd(a, b)$, it follows that $d_2 \leq d_1$.

To show that the second required inequality holds, we reorganize the equation $a = qb+r$ and then use the same approach as in the first part of the proof. Specifically, since $d_1 = \gcd(a, b)$ and $a - qb = r$, we have

$$\begin{aligned} r &= a - qb \\ &= a \cdot 1 - bq. \end{aligned}$$

Using an argument analogous to the one above employing Lemma 2.1, it follows that $d_1 \mid r$, which in turn implies that $d_1 \leq d_2$.[2] Thus we have established both of the required inequalities. □

Recall from the lab that we can reverse the steps of the Euclidean Algorithm to find one solution to the linear diophantine equation

$$ax + by = \gcd(a, b). \tag{2.1}$$

For the record, we will state the existence of this solution formally.

Lemma 2.3 (GCD Trick) *If a and b are integers which are not both 0, then there exist integers x and y such that*

$$ax + by = \gcd(a, b).$$

If $x = x_0$ and $y = y_0$ is a solution to equation (2.1), then it is easy to see that $x = kx_0$ and $y = ky_0$ is a solution to the equation

$$ax + by = k \gcd(a, b), \tag{2.2}$$

where k is any integer. Thus it follows that any equation of this more general form will have a solution. The conjecture associated with Research Question 2 shows that *only* equations equivalent to equation (2.2) will have solutions.

Theorem 2.4 (RQ2) *In order for $ax + by = c$ to have solutions, c must be of the form $c = k \gcd(a, b)$ for some integer k.*

[2] You should fill in the gaps yourself to be sure that the cited argument really works in this case.

Proof. To simplify notation, let $d = \gcd(a, b)$. Then we have $d \mid a$ and $d \mid b$. By Lemma 2.1 we have that $d \mid (ax + by)$, and so $d \mid c$. Hence $c = k \gcd(a, b)$ for some integer k. □

Research Question 2 and the discussion which preceeds it can be phrased in the following way. Fix integers a and b (not both 0) and let $d = \gcd(a, b)$. We will refer to numbers of the form $ax + by$ with $x, y \in \mathbf{Z}$ as (integer) linear combinations of a and b. Then, the set of linear combinations of a and b is exactly the same as the set of multiples of d. Written in terms of sets, this statement becomes

$$\{ax + by \mid x, y \in \mathbf{Z}\} = \{kd \mid k \in \mathbf{Z}\}. \tag{2.3}$$

This formulation matches some of the computations you did in the lab where you computed many linear combinations $ax+by$ and found that the results were multiples of d.

The remainder of the chapter is devoted to finding a general form for *all* solutions to the linear diophantine equation $ax + by = k \gcd(a, b)$. This problem is attacked in a series of steps, starting with Research Question 3, which addresses the equation $ax + by = 1$, where $\gcd(a, b) = 1$.

Theorem 2.5 (RQ3) *Suppose that* $\gcd(a, b) = 1$ *and that* $x = x_0$ *and* $y = y_0$ *is a solution to the equation*

$$ax + by = 1.$$

Then all solutions to this equation are given by $x = x_0 + mb$ *and* $y = y_0 - ma$*, where* m *is any integer.*

Proof. The proof breaks into two parts. In the first part, we verify that the forms for x and y given above do indeed yield solutions to our equation. For the second part, we show that any solution to our equation must be of the form asserted above.

Suppose that $x = x_0 + mb$ and $y = y_0 - ma$ for some integer m where $ax_0 + by_0 = 1$. Then

$$\begin{aligned} ax + by &= a(x_0 + mb) + b(y_0 - ma) \\ &= (ax_0 + by_0) + (amb - bma) \\ &= 1 + 0 = 1. \end{aligned}$$

Thus we see that $x = x_0 + mb$ and $y = y_0 - ma$ provides a solution to our equation for any integer m.

Now, suppose that x and y satisfy $ax + by = 1$. Define $s = x - x_0$ and $t = y - y_0$, so that $x = x_0 + s$ and $y = y_0 + t$. Then we have

$$\begin{aligned} 1 &= ax + by \\ &= a(x_0 + s) + b(y_0 + t) \\ &= (ax_0 + by_0) + (as + bt) \\ &= 1 + (as + bt). \end{aligned}$$

Therefore it follows that $as + bt = 0$, and so we have

$$as = -bt. \tag{2.4}$$

At least one of a and b must be nonzero, or $\gcd(a, b)$ would not exist. Suppose that $b \neq 0$ (the case when $a \neq 0$ is similar).

Since $\gcd(a, b) = 1$, this means that s must be divisible by b by exercise 1.13 (or Lemma 2.9 below), so that $s = mb$ for some integer m. Plugging this into equation (2.4) above, we have $amb = -bt$, and thus $t = -am$. Therefore $x = x_0 + mb$ and $y = y_0 - ma$, which is the form required. □

Research Question 4 generalizes RQ3 to the equation $ax + by = d$, where $d = \gcd(a, b) \geq 1$.

Theorem 2.6 (RQ4) *Suppose that $d = \gcd(a, b) \geq 1$, and $x = x_0$ and $y = y_0$ is a solution to the equation*

$$ax + by = d.$$

Then all solutions to this equation are given by $x = x_0 + m(b/d)$ and $y = y_0 - m(a/d)$, where m is any integer.

Proof. We begin by noting that the two equations

$$ax + by = d \qquad \text{and} \qquad (a/d)x + (b/d)y = 1$$

have exactly the same set of solutions. Furthermore, $\gcd(a/d, b/d) = 1$ by exercise 1.14, so that the right-hand equation above is of the form covered in Research Question 3. Applying that result with the coefficients (a/d) and (b/d), we find that

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

as required. □

Research Question 5 addresses the most general linear diophantine equation that has solutions. Note that if $k = 1$, then we reduce to Research Question 4, and further if $d = 1$, then we reduce to Research Question 3.

Theorem 2.7 (RQ5) *Let a, b, and k be integers with a or b not equal to 0. Suppose that $d = \gcd(a, b)$, and $x = x_0$ and $y = y_0$ is a solution to $ax + by = d$. Then all solutions to the equation*

$$ax + by = kd,$$

are given by $x = kx_0 + m(b/d)$ and $y = ky_0 - m(a/d)$, where m is any integer.

Proof. The proof can be carried out in a manner similar to the proof of the conjecture associated with Research Question 3. The details are left to the reader. □

With the above work complete, we now have completely resolved the question of the nature of solutions to the equation

$$ax + by = c.$$

Here's a summary: If $c \neq k \gcd(a, b)$ for any integer k, then there are no solutions. If $c = k \gcd(a, b)$, then all solutions can be found by

1. Finding a single solution $x = x_0$ and $y = y_0$ to $ax+by = d$ (where $d = \gcd(a, b)$) using the reverse Euclidean Algorithm
2. Using this solution to find a single solution $x = kx_0$ and $y = ky_0$ to $ax+by = kd$
3. Setting $x = kx_0 + m(b/d)$ and $y = ky_0 - m(a/d)$ to obtain all solutions to the equation

Example 2.1 Let's solve $52x + 56y = 36$, first finding all integer solutions, and then finding all positive solutions. We begin by determining that $\gcd(52, 56) = 4$. Since $4 \mid 36$, we know that there are infinitely many solutions to our equation. Using the reverse Euclidean Algorithm (or by inspection), we find that

$$52(-1) + 56(1) = 4.$$

Thus we have $x_0 = -1$, $y_0 = 1$, and $k = 36/4 = 9$. Therefore the general solution is given by

$$x = 9 \cdot (-1) + m(56/4) = -9 + 14m$$

and

$$y = 9 \cdot 1 - m(52/4) = 9 - 13m,$$

where m is any integer.

With the general solution in hand, we can easily see that there are no solutions with both x and y positive because

$$x > 0 \implies -9 + 14m > 0 \implies m > 0$$

and

$$y > 0 \implies 9 - 13m > 0 \implies 0 \geq m.$$

Since these two conditions on m are mutually exclusive, there are no positive solutions to the equation $52x + 56y = 4$.

Solutions to Selected Exercises

Exercise 2.1 Repeat the above procedure to compute gcd(7920, 4536).

Solution. We start by computing gcd(7920, 4536), and as an added bonus, we'll also throw in (at no additional charge) a solution to the equation

$$7920x + 4536y = \gcd(7920, 4536). \tag{2.5}$$

Here's the gcd computation:

1. $7920 = 1 \cdot 4536 + 3384$.
2. $4536 = 1 \cdot 3384 + 1152$.
3. $3384 = 2 \cdot 1152 + 1080$.
4. $1152 = 1 \cdot 1080 + 72$.
5. $1080 = 15 \cdot 72 + 0$.

Thus we see that gcd(7920, 4536) = 72. Next we reverse the steps to find a solution to equation (2.5).

$$\begin{aligned}
72 &= 1152 - 1 \cdot 1080 \\
&= 1152 - 1 \cdot (3384 - 2 \cdot 1152) \\
&= -1 \cdot 3384 + 3 \cdot 1152 \\
&= -1 \cdot 3384 + 3 \cdot (4536 - 1 \cdot 3384) \\
&= 3 \cdot 4536 - 4 \cdot 3384 \\
&= 3 \cdot 4536 - 4 \cdot (7920 - 1 \cdot 4536) \\
&= -4 \cdot 7920 + 7 \cdot 4536
\end{aligned}$$

Therefore we see that $x = -4$ and $y = 7$ is a solution to equation (2.5).

□