Linear Equations and the Greatest Common Divisor

Given two whole numbers a and b, we are going to look at all the possible numbers we can get by adding a multiple of a to a multiple of b. In other words, we will consider all numbers obtained from the formula

$$ax + by$$

when we substitute all possible integers for x and y. Note that we are going to allow both positive and negative values for x and y. For example, we could take $a = 42$ and $b = 30$. Some of the values of $ax + by$ for this a and b are given in the following table:

	$x=-3$	$x=-2$	$x=-1$	$x=0$	$x=1$	$x=2$	$x=3$
$y=-3$	-216	-174	-132	-90	-48	-6	36
$y=-2$	-186	-144	-102	-60	-18	24	66
$y=-1$	-156	-114	-72	-30	12	54	96
$y=0$	-126	-84	-42	0	42	84	126
$y=1$	-96	-54	-12	30	72	114	156
$y=2$	-66	-24	18	60	102	144	186
$y=3$	-36	6	48	90	132	174	216

Table of Values of $42x + 30y$

Our first observation is that every entry in the table is divisible by 6. This is not surprising, since both 42 and 30 are divisible by 6, so every number of the form $42x + 30y = 6(7x + 5y)$ is a multiple of 6. More generally, it is clear that every number of the form $ax + by$ is divisible by $\gcd(a, b)$, since both a and b are divisible by $\gcd(a, b)$.

A second observation, which is somewhat more surprising, is that the greatest common divisor of 42 and 30, which is 6, actually appears in our table. Thus from the table we see that

$$42 \cdot (-2) + 30 \cdot 3 = 6 = \gcd(42, 30).$$

Further examples suggest the following conclusion:

The smallest positive value of $ax + by$ is equal to $\gcd(a, b)$.

There are many ways to prove that this is true. We will take a constructive approach, via the Euclidean algorithm, which has the advantage of giving a procedure for finding the appropriate values of x and y. In other words, we are going to describe a method of finding integers x and y that are solutions to the equation

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

Since, as we have already observed, every number $ax+by$ is divisible by $\gcd(a, b)$, it will follow that the smallest positive value of $ax + by$ is precisely $\gcd(a, b)$.

How might we solve the equation $ax + by = \gcd(a, b)$? If a and b are small, we might be able to guess a solution. For example, the equation

$$10x + 35y = 5$$

has the solution $x = -3$ and $y = 1$, and the equation

$$7x + 11y = 1$$

has the solution $x = -3$ and $y = 2$. We also notice that there can be more than one solution, since $x = 8$ and $y = -5$ is also a solution to $7x + 11y = 1$.

However, if a and b are large, neither guesswork nor trial and error is going to be helpful. We are going to start by illustrating the Euclidean algorithm method for solving $ax + by = \gcd(a, b)$ with a particular example. So we are going to try to solve

$$22x + 60y = \gcd(22, 60).$$

The first step is to perform the Euclidean algorithm to compute the $\gcd$. We find

$$\begin{aligned} 60 &= 2 \times 22 + 16 \\ 22 &= 1 \times 16 + \ 6 \\ 16 &= \ 2 \times 6 + \ 4 \\ 6 &= \ 1 \times 4 + \ 2 \\ 4 &= \ 2 \times 2 + \ 0 \end{aligned}$$

This shows that $\gcd(22, 60) = 2$, a fact that is clear without recourse to the Euclidean algorithm. However, the Euclidean algorithm computation is important because we're going to use the intermediate quotients and remainders to solve the equation $22x + 60y = 2$. The first step is to rewrite the first equation as

$$16 = a - 2b, \qquad \text{where we let } a = 60 \text{ and } b = 22.$$

We next substitute this value into the 16 appearing in the second equation. This gives (remember that $b = 22$)

$$b = 1 \times 16 + 6 = 1 \times (a - 2b) + 6.$$

Rearranging this equation to isolate the remainder 6 yields

$$6 = b - (a - 2b) = -a + 3b.$$

Now substitute the values 16 and 6 into the next equation, $16 = 2 \times 6 + 4$:

$$a - 2b = 16 = 2 \times 6 + 4 = 2(-a + 3b) + 4.$$

Again we isolate the remainder 4, yielding

$$4 = (a - 2b) - 2(-a + 3b) = 3a - 8b.$$

Finally, we use the equation $6 = 1 \times 4 + 2$ to get

$$-a + 3b = 6 = 1 \times 4 + 2 = 1 \times (3a - 8b) + 2.$$

Rearranging this equation gives the desired solution

$$-4a + 11b = 2.$$

(We should check our solution: $-4 \times 60 + 11 \times 22 = -240 + 242 = 2$.)

We can summarize the above computation in the following efficient tabular form. Note that the left-hand equations are the Euclidean algorithm, and the right-hand equations compute the solution to $ax + by = \gcd(a, b)$.

$$\begin{array}{rl|l}
a = & 2 \times b + 16 & 16 = a - 2b \\
b = 1 \times 16 + & 6 & 6 = b - 1 \times 16 \\
 & & \quad = b - 1 \times (a - 2b) \\
 & & \quad = -a + 3b \\
16 = & 2 \times 6 + 4 & 4 = 16 - 2 \times 6 \\
 & & \quad = (a - 2b) - 2 \times (-a + 3b) \\
 & & \quad = 3a - 8b \\
6 = & 1 \times 4 + 2 & 2 = 6 - 1 \times 4 \\
 & & \quad = (-a + 3b) - 1 \times (3a - 8b) \\
 & & \quad = -4a + 11b \\
4 = & 2 \times 2 + 0 &
\end{array}$$

Why does this method work? As the following table makes clear, we start with the first two lines of the Euclidean algorithm, which involve the quantities a and b, and work our way down.

$$\begin{array}{r|l}
a = \ q_1 b + r_1 & r_1 = a - q_1 b \\
b = q_2 r_1 + r_2 & r_2 = b - q_2 r_1 \\
 & \quad = b - q_2(a - q_1 b) \\
 & \quad = -q_2 a + (1 + q_1 q_2) b \\
r_1 = q_3 r_2 + r_3 & r_3 = r_1 - q_3 r_2 \\
 & \quad = (a - q_1 b) - q_3\big(-q_2 a + (1 + q_1 q_2) b\big) \\
 & \quad = (1 + q_2 q_3) a - (q_1 + q_3 + q_1 q_2 q_3) b \\
\vdots & \qquad\qquad \vdots
\end{array}$$

As we move from line to line, we will continually be forming equations that look like

$$\text{latest remainder} = \text{some multiple of } a \text{ plus some multiple of } b.$$

Eventually, we get down to the last nonzero remainder, which we know is equal to $\gcd(a, b)$, and this gives the desired solution to the equation $\gcd(a, b) = ax + by$.

A larger example with $a = 12453$ and $b = 2347$ is given in tabular form on top of the next page. As before, the left-hand side is the Euclidean algorithm and the right-hand side solves $ax + by = \gcd(a, b)$. We see that $\gcd(12453, 2347) = 1$ and that the equation $12453x + 2347y = 1$ has the solution $(x, y) = (304, -1613)$.

We now know that the equation

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

always has a solution in integers x and y. The final topic we discuss in this section is the question of how many solutions it has, and how to describe all the solutions. Let's start with the case that a and b are relatively prime, that is, $\gcd(a, b) = 1$, and suppose that (x_1, y_1) is a solution to the equation

$$ax + by = 1.$$

We can create additional solutions by subtracting a multiple of b from x_1 and adding the same multiple of a onto y_1. In other words, for any integer k we obtain a new solution $(x_1 + kb, y_1 - ka)$.[1] We can check that this is indeed a solution by computing

$$a(x_1 + kb) + b(y_1 - ka) = ax_1 + akb + by_1 - bka = ax_1 + by_1 = 1.$$

[1] Geometrically, we are starting from the known point (x_1, y_1) on the line $ax + by = 1$ and using the fact that the line has slope $-a/b$ to find new points $(x_1 + t, y_1 - (a/b)t)$. To get new points with integer coordinates, we need to let t be a multiple of b. Substituting $t = kb$ gives the new integer solution $(x_1 + kb, y_1 - ka)$.

$a = 5 \times b \quad + 718$	$718 = a - 5b$
$b = 3 \times 718 + 193$	$193 = b - 3 \times 718$
	$= b - 3 \times (a - 5b)$
	$= -3a + 16b$
$718 = 3 \times 193 + 139$	$139 = 718 - 3 \times 193$
	$= (a - 5b) - 3 \times (-3a + 16b)$
	$= 10a - 53b$
$193 = 1 \times 139 + 54$	$54 = 193 - 139$
	$= (-3a + 16b) - (10a - 53b)$
	$= -13a + 69b$
$139 = 2 \times 54 \quad + 31$	$31 = 139 - 2 \times 54$
	$= (10a - 53b) - 2 \times (-13a + 69b)$
	$= 36a - 191b$
$54 = 1 \times 31 \quad + 23$	$23 = 54 - 31$
	$= -13a + 69b - (36a - 191b)$
	$= -49a + 260b$
$31 = 1 \times 23 \quad + 8$	$8 = 31 - 23$
	$= 36a - 191b - (-49a + 260b)$
	$= 85a - 451b$
$23 = 2 \times 8 \quad + 7$	$7 = 23 - 2 \times 8$
	$= (-49a + 260b) - 2 \times (85a - 451b)$
	$= -219a + 1162b$
$8 = 1 \times 7 \quad + 1$	$1 = 8 - 7$
	$= 85a - 451b - (-219a + 1162b)$
	$= 304a - 1613b$
$7 = 7 \times 1 \quad + 0$	

So, for example, if we start with the solution $(-1, 2)$ to $5x + 3y = 1$, we obtain new solutions $(-1 + 3k, 2 - 5k)$. Note that the integer k is allowed to be positive, negative, or zero. Putting in particular values of k gives the solutions

$$\ldots (-13, 22),\ (-10, 17),\ (-7, 12),\ (-4, 7),\ (-1, 2),$$
$$(2, -3),\ (5, -8),\ (8, -13),\ (11, -18) \ldots .$$

Still looking at the case that $\gcd(a, b) = 1$, we can show that this procedure gives all possible solutions. Suppose that we are given two solutions (x_1, y_1) and (x_2, y_2) to the equation $ax + by = 1$. In other words,

$$ax_1 + by_1 = 1 \qquad \text{and} \qquad ax_2 + by_2 = 1.$$

We are going to multiply the first equation by y_2, multiply the second equation by y_1, and subtract. This will eliminate b and, after a little bit of algebra, we are

left with

$$ax_1y_2 - ax_2y_1 = y_2 - y_1.$$

Similarly, if we multiply the first equation by x_2, multiply the second equation by x_1, and subtract, we find that

$$bx_2y_1 - bx_1y_2 = x_2 - x_1.$$

So if we let $k = x_2y_1 - x_1y_2$, then we find that

$$x_2 = x_1 + kb \qquad \text{and} \qquad y_2 = y_1 - ka.$$

This means that the second solution (x_2, y_2) is obtained from the first solution (x_1, y_1) by adding a multiple of b onto x_1 and subtracting the same multiple of a from y_1. So every solution to $ax + by = 1$ can be obtained from the initial solution (x_1, y_1) by substituting different values of k into $(x_1 + kb, y_1 - ka)$.

What happens if $\gcd(a, b) > 1$? To make the formulas look a little bit simpler, we will let $g = \gcd(a, b)$. We know from the Euclidean algorithm method that there is at least one solution (x_1, y_1) to the equation

$$ax + by = g.$$

But g divides both a and b, so (x_1, y_1) is a solution to the simpler equation

$$\frac{a}{g}x + \frac{b}{g}y = 1.$$

Now our earlier work applies, so we know that every other solution can be obtained by substituting values for k in the formula

$$\left(x_1 + k \cdot \frac{b}{g},\ y_1 - k \cdot \frac{a}{g}\right).$$

This completes our description of the solutions to the equation $ax + by = g$, as summarized in the following theorem.

Theorem 1 (Linear Equation Theorem)**.** *Let a and b be nonzero integers, and let $g = \gcd(a, b)$. The equation*

$$ax + by = g$$

always has a solution (x_1, y_1) in integers, and this solution can be found by the Euclidean algorithm method described earlier. Then every solution to the equation can be obtained by substituting integers k into the formula

$$\left(x_1 + k \cdot \frac{b}{g},\ y_1 - k \cdot \frac{a}{g}\right).$$

For example, we saw that the equation

$$60x + 22y = \gcd(60, 22) = 2$$

has the solution $x = -4$, $y = 11$. Then our Linear Equation Theorem says that every solution is obtained from the formula

$$(-4 + 11k, 11 - 30k) \qquad \text{with } k \text{ any integer.}$$

In particular, if we want a solution with x positive, then we can take $k = 1$, which gives the smallest such solution $(x, y) = (7, -19)$.

In this chapter we have shown that the equation

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

always has a solution. This fact is extremely important for both theoretical and practical reasons, and we will be using it repeatedly in our number theoretic investigations. For example, we will need to solve the equation $ax + by = 1$ if we study cryptography. And we use this equation for theoretical study of factorization of numbers into primes.

Exercises

1. **(a)** Find a solution in integers to the equation

$$12345x + 67890y = \gcd(12345, 67890).$$

(b) Find a solution in integers to the equation

$$54321x + 9876y = \gcd(54321, 9876).$$

2. Describe all integer solutions to each of the following equations.

(a) $105x + 121y = 1$

(b) $12345x + 67890y = \gcd(12345, 67890)$

(c) $54321x + 9876y = \gcd(54321, 9876)$

3. The method for solving $ax + by = \gcd(a, b)$ described in this chapter involves a considerable amount of manipulation and back substitution. This exercise describes an alternative way to compute x and y that is especially easy to implement on a computer.

(a) Show that the algorithm described in Figure 1 computes the greatest common divisor g of the positive integers a and b, together with a solution (x, y) in integers to the equation $ax + by = \gcd(a, b)$.

(b) Implement the algorithm on a computer using the computer language of your choice.

(c) Use your program to compute $g = \gcd(a, b)$ and integer solutions to $ax + by = g$ for the following pairs (a, b).
(i) $(19789, 23548)$ (ii) $(31875, 8387)$ (iii) $(22241739, 19848039)$

(d) What happens to your program if $b = 0$? Fix the program so that it deals with this case correctly.

(e) For later applications it is useful to have a solution with $x > 0$. Modify your program so that it always returns a solution with $x > 0$. [*Hint.* If (x, y) is a solution, then so is $(x + b, y - a)$.]

(1)	Set $x = 1$, $g = a$, $v = 0$, and $w = b$.
(2)	If $w = 0$ then set $y = (g - ax)/b$ and return the values (g, x, y).
(3)	Divide g by w with remainder, $g = qw + t$, with $0 \leq t < w$.
(4)	Set $s = x - qv$.
(5)	Set $(x, g) = (v, w)$.
(6)	Set $(v, w) = (s, t)$.
(7)	Go to Step (2).

Figure 1: Efficient algorithm to solve $ax + by = \gcd(a, b)$

4. (a) Find integers x, y, and z that satisfy the equation

$$6x + 15y + 20z = 1.$$

(b) Under what conditions on a, b, c is it true that the equation

$$ax + by + cz = 1$$

has a solution? Describe a general method of finding a solution when one exists.

(c) Use your method from (b) to find a solution in integers to the equation

$$155x + 341y + 385z = 1.$$

5. Suppose that $\gcd(a, b) = 1$. Prove that for every integer c, the equation $ax + by = c$ has a solution in integers x and y. [*Hint.* Find a solution to $au + bv = 1$ and multiply by c.] Find a solution to $37x + 47y = 103$. Try to make x and y as small as possible.

6. Sometimes we are only interested in solutions to $ax + by = c$ using nonnegative values for x and y.

(a) Explain why the equation $3x + 5y = 4$ has no solutions with $x \geq 0$ and $y \geq 0$.

(b) Make a list of some of the numbers of the form $3x + 5y$ with $x \geq 0$ and $y \geq 0$. Make a conjecture as to which values are not possible. Then prove that your conjecture is correct.

(c) For each of the following values of (a, b), find the largest number that is not of the form $ax + by$ with $x \geq 0$ and $y \geq 0$.

(i) $(a, b) = (3, 7)$ (ii) $(a, b) = (5, 7)$ (iii) $(a, b) = (4, 11)$.

(d) Let $\gcd(a, b) = 1$. Using your results from (c), find a conjectural formula in terms of a and b for the largest number that is not of the form $ax + by$ with $x \geq 0$ and $y \geq 0$? Check your conjecture for at least two more values of (a, b).

(e) Prove that your conjectural formula in (d) is correct.

(f) Try to generalize this problem to sums of three terms $ax + by + cz$ with $x \geq 0$, $y \geq 0$, and $z \geq 0$. For example, what is the largest number that is not of the form $6x + 10y + 15z$ with nonnegative x, y, z?

This page intentionally left blank