Elementary Number Theory : §2

Henry Slayer | University of California, Santa Cruz

Linear Diophantine Equations

The Euclidean algorithm studies the relationships between numbers, comparing their parts, and measuring how two integers can be decomposed into smaller and smaller portions of themselves. This decomposition is governed by the greatest common divisor, which exists hand in hand with the least common multiple, as we have seen. Rising more or less naturally from the interplay between various integers, we encounter linear Diophantine equations. A linear Diophantine equation is an equation of the form

$$ax + by = c$$

For integers a, b, c, x, y. This probably isn't the first time that you've seen an equation of this form. It's really nothing more than a line in $\mathbf{R}^2$. However, our approach to these types of equations will likely be different from what's typically done in high school algebra or calculus courses. We are interested in three things

(i) Does $ax + by = c$ have integer solutions?

(ii) Provided it does, how do we find them?

(iii) Given (i) and (ii), can we generalize infinite families of integer solutions?

The answer to the first question is a blunt consequence of divisibility, and our method of solution will give us direction for the latter two questions.

Solubility of Linear Diophantine Equations

We find that solubility os $ax + by = c$ is a direct consequence of $GCD\,(a, b)$.

Theorem 1. *Let a, b, c, x, y be integers. Then, the equation $ax + by = c$ has integer solutions (x, y) if and only if $GCD\,(a, b) \,|\, c$.*

Proof. First, assume that $ax+by = c$ has an integer solution. By the properties of the greatest common divisor, $GCD\,(a, b) \,|\, ax$, $GCD\,(a, b) \,|\, by$, and so $GCD\,(a, b)$ must also divide c. Conversely, suppose that $GCD\,(a, b) \,|\, c$. In the penultimate line of Euclid's algorithm, when performed on a and b, we will obtain something that looks like

$$r_i = q_{i+1}(r_{i+1}) + GCD\,(a, b)$$

Pulling the quotient to one side, we obtain

$$r_i = q_{i+1}(r_{i+1}) = GCD\,(a, b)$$

Now, the left-hand side of the equation above, through the iterative process of back-substitution, can bring us back to a linear combination of our initial values a and b (as we will show in a subsequent example). Thus, for integers x_0, y_0,

$$ax_0 + by_0 = GCD\,(a, b)$$

As $GCD\,(a, b) \mid c$, this equation can be scaled to

$$ax + by = c$$

for integers x and y. □

The converse of the theorem above suggests a method for finding a particular solution to linear diophantine equations. This method is effective, and we do most of the work in the beginning, when we're seeking to determine if c is a multiple of the greatest common divisor.

Example 1. *Does* $763x + 129y = 1$ *have integer solutions? If so, find a particular solution* (x, y)*.*

Proof. We know that this equation will have integer solutions if 1 is a multiple of the greatest common divisor of 763 and 129. In this case, then, the greatest common divisor must be 1. So, we proceed by Euclid's algorithm.

$$\begin{align} 763 &= 5(129) + 118 \tag{1}\\ 129 &= 1(118) + 11 \tag{2}\\ 118 &= 10(11) + 8 \tag{3}\\ 11 &= 1(8) + 3 \tag{4}\\ 8 &= 2(3) + 2 \tag{5}\\ 3 &= 1(2) + 1 \tag{6}\\ 2 &= 2(1) + 0 \tag{7}\end{align}$$

The second-to-last line tells us that 763 and 129 have a greatest common divisor of 1, which means that we can find integer solutions for the equation above. To find a particular solution, all that we need to do is reverse the Euclidean algorithm, working our way back up by reverse-substitution. Because Euclid's algorithm gives us a system of equations, we can 'look up' to the line above, and make substitutions to bring ourselves closer to our initial values of a and *b*. Starting with the final line:

$$\begin{aligned}1 &= 3 - 2(1)\\ &= 3 - (8 - 2(3)) = 3(3) - 8 \qquad \textit{by line 5}\\ &= 3(11 - 8) - 8 = 3(11) - 4(8) \qquad \textit{by line 4}\\ &= 3(11) - 4(118 - 10(11)) = 43(11) - 4(118) \qquad \textit{by line 3}\\ &= 43(129 - 118) - 4(118) = 34(129) - 47(118) \qquad \textit{by line 2}\\ &= 43(129) - 47(763 - 5(129)) \qquad \textit{by line 1}\\ &= 278(129) - 47(763)\end{aligned}$$

So, our particular solution to the equation $736x + 129y = 1$ is $(-47, 278)$. □

This method is extremely effective for finding particular solutions to linear diophantine equations. However, the bookkeeping can certainly get a bit tangled, and it's easy to get lost in the line-by-line calculations. Be sure to check your work along the way.

Families of Solutions

So, we've determined that $ax + by = c$ is solvable, and we've found some integral solution (x_0, y_0), all thanks to the Euclidean algorithm. To characterize *all* solutions to a given linear diophantine equation, we turn our attention towards a clever use of *homogeneous* linear diophantine equations, which look like

$$ax + by = 0$$

So, suppose that $ax + by = c$ is satisfied by a particular solution (x_0, y_0). If we consider x and y to be 'general solution' terms, it follows, then, that

$$ax + by = ax_0 + by_0 = c$$

Which, in turn, means that

$$a(x - x_0) + b(y - y_0) = 0$$
$$a(x - x_0) = -b(y - y_0)$$

We interpret this equality to generate 'solution sets' for the linear diophantine form $ax + by = c$, provided that it is solvable. We'll prove the general case for one term, and the second follows by symmetry.

Because we have equality above, we know that $-b(y - y_0)$ must be a multiple of the $LCM\,(a, b)$. So, assume then that

$$a(x - x_0) = n \cdot LCM\,(a, b)$$

Which means

$$x = x_0 + \frac{n \cdot LCM\,(a, b)}{a}$$

Furthermore, the GCD/LCM product formula tells us that $\frac{LCM\,(a,b)}{a} = \frac{b}{GCD\,(a,b)}$. So, given $ax + by = c$, and a particular solution (x_0, y_0), we can generate all solutions for x by

$$x = x_0 + \frac{n \cdot b}{GCD\,(a, b)}$$

A similar argument justifies the following for y

$$y = y_0 - \frac{n \cdot a}{GCD\,(a, b)}$$

Where the sign has been flipped, and n is the same n as above (as $a(x - x_0) = -b(y - y_0) = n \cdot LCM\,(a, b)$.

Theorem 2. *Let a, b, c, x, y be integers. Then, the equation $ax + by = c$ has integer solutions when $GCD\,(a, b) \,|\, c$. Based on a particular solution (x_0, y_0), all solutions to this equation can be generated by*

$$x = x_0 + \frac{n \cdot b}{GCD\,(a, b)}, \qquad y = y_0 - \frac{n \cdot a}{GCD\,(a, b)}$$

Writing these expressions in terms of the GCD is more out of preference rather than necessity. The GCD arises naturally when we perform the Euclidean algorithm, and so it's favorable to capitalize on this construction's computational convenience.

We can extend our study of linear diophantine equations into three variables (and more!). The process is mostly the same, so we will simply conclude this section with an example.

Linear Diophantine Equations in 3 Variables

Extending into a 3-variable case can be a bit tricky. For equations of the form $ax + by + cz = d$, we need to work in parts, solving for pariwise sub-relationships that tie the three-variable dynamic together.

Example 2. *Let x, y, z be integers. Characterize all integer solutions to the equation $3x + 5y + 4z = 9$, if such integer solutions exist.*

Proof. The first thing that we want to do is ensure that the $GCD(a, b, c)$ is a divisor of 9. A quick look tells us that because 3 and 5 are prime, they share no common divisors, and neither divide 4. Thus, the three values are pairwise coprime, which means that $GCD(a, b, c) = 1$, and 1 certainly divides 9. So, we know that solutions certainly exist. In order to solve this equation, we're going to want to break it down into two smaller systems. We start by taking a look at $3x + 5y$. We know from solving two-variable LDE's that this linear combination will give us compound moves that are multiples of $GCD\,(a, b)$. So, we start by solving this subsystem for $GCD\,(3, 5) = 1$. We find (and the reader should be sure to check) that $(2, -1)$ is a particular solution to $3x + 5y = 1$, which means that if $3x + 5y = v$, x and y will be characterized by $(2v, -v)$. So, we store that information for later. It will come in handy.
Now that we've established a connection between 3 and 5, we can use that 'common ratio' back in our original equation, which becomes

$$v + 4z = 9$$

A quick glance tells us that $(1, 2)$ is a particular (v, z) solution, which implies that

$$v = 1 + 4n, \qquad z = 2 - n$$

Are our general solutions, which we obtained from the theorem proved earlier. Translating v into the language of x and y by what we had previously established,

$$x = 2v = 2 + 8n, \quad y = -v = -1 - 4n, \quad z = 2 - n$$

And so, we've obtained general sets of solutions for $3x + 5y + 4z = 9$, by first solving a smaller linear relationship, which we then used as a placeholder to shed light on the larger linear dynamics at play. □