Math From Scratch Lesson 19: Linear Diophantine Equations

W. Blaine Dowler

December 27, 2011

Contents

1 Definition **1**

2 Restrictions on z **1**

3 Solving the equation **2**
3.1 A Particular Solution 2
3.2 The General Solution 3

4 Next **4**

1 Definition

A linear diophantine equation is an equation of the form $ax+by=z$, where x, y and z are known and we must calculate values for a and b. Typically, $0 < z < x$ and $0 < z < y$.

2 Restrictions on z

For a solution to exist, we must have $z = k \cdot \gcd(x, y)$ for some integer value of k. To prove this, let $g = \gcd(x, y)$. Thus, $x = lg$ and $y = mg$. This leaves us with $ax + by = alg + bmg = (al + bm)\, g = z$. In the final equality, the left hand side $(al + bm)\, g$ is clearly divisible by g with zero remainder, so the right hand side must be as well.

3 Solving the equation

The solution, as we will see, will not be unique, but will instead be a family of solutions. First, though, we will use the Euclidean algorithm to find a particular solution.

3.1 A Particular Solution

Let us use a concrete example to illustrate the logic. Let us use the example

$$221a + 351b = 39$$

We previously proved that $\gcd(221, 351) = 13$ using the Euclidean algorithm as follows:

$$\begin{aligned} 351 \div 221 &= 1R130 \\ 221 \div 130 &= 1R91 \\ 130 \div 91 &= 1R39 \\ 91 \div 39 &= 2R13 \\ 39 \div 13 &= 3R0 \end{aligned}$$

We can rewrite these steps as follows:

$$\begin{aligned} 351 - 221 \cdot 1 &= 130 \\ 221 - 130 \cdot 1 &= 91 \\ 130 - 91 \cdot 1 &= 39 \\ 91 - 39 \cdot 2 &= 13 \end{aligned}$$

We can now use repeated substitution, starting with the bottom line, to replace remainders with subtractions. For example, we replace 39 in the last line with the left hand side of the previous equation to generate

$$91 - (130 - 91) \cdot 2 = 3 \cdot 91 - 2 \cdot 130 = 13$$

We now replace 91 with the second line above and collect like terms again:

$$3 \cdot (221 - 130) - 2 \cdot 130 = 3 \cdot 221 - 5 \cdot 130 = 13$$

In our final step, we substitute for 130 and rearrange:

$$3 \cdot 221 - 5 \cdot (351 - 221) = 8 \cdot 221 - 5 \cdot 351 = 13$$

Thus, $8 \cdot 221 - 5 \cdot 351 = 13$. However, we were asked to solve $351a + 221b = 39$. Well, $39 = 13 \cdot 3$, so we can multiply our entire equation by 3 and get

$$24 \cdot 221 - 15 \cdot 351 = 39$$

This is one solution to our problem, generated with a large number of simple steps of the kind computers excel at doing for us.

3.2 The General Solution

In the general solution to the equation $ax + by = z$, we need the following facts:

1. $\gcd(x, y) = g$
2. $x = lg$
3. $y = mg$
4. $z = ng$
5. There is always at least one particular solution that we can find by applying and then reversing the Euclidean algorithm to determine g, as with our example above.

Let us begin with our particular solution $a_0x + b_0y = z$. (In our prior example, $x = 351$, $y = 221$, $z = 39$, $a_0 = -15$ and $b_0 = 24$.) We now show that we can build the unique family of solutions using only information we have available.

A general solution is most easily found by transforming our particular solution in a manner which has no net result. If we let $a = a_0 + d$ and $b = b_0 + e$, then we can search for a relationship between d, e, and our other known quantities.

By substitution, we find

$$\begin{aligned} z &= ax + by \\ &= (a_0 + d)x + (b_0 + e)y \\ &= a_0x + b_0y + dx + ey \\ &= z + dx + ey \end{aligned}$$

Thus, $dx + ey = 0$, or $d = -\frac{ey}{x}$. Thus, our solution becomes $b = b_0 + e$ and $a = a_0 - \frac{ey}{x}$. Now, we must have closure for this expression to work. We also

insist that we have integer solutions: thus, $a_0 - \frac{ey}{x}$ must be an integer. a_0 is known to be an integer, so we are left with the condition that $\frac{ey}{x}$ is an integer. As $x = lg$ and $y = mg$, we have $\frac{ey}{x} = \frac{em}{l}$ must be an integer. We can guarantee that m is not divisible by l; if it were, then g would not have been the greatest common factor of x and y. Therefore, e is divisible by l. As $l = \frac{x}{g}$, we have $e = \frac{ux}{g}$ for some integer u. This integer is arbitrary; this is why we have infinite solutions.

We now directly have half of our general solution: $b = b_0 + \frac{ux}{g}$. To find the other half, we substitute our e into $a = a_0 + d = a_0 - \frac{ey}{x} = a_0 - \frac{uxy}{gx} = a_0 - \frac{uy}{g}$.

Finally, for the equation $ax + by = z$, where z is a multiple of $\gcd(x, y) = g$, we have infinitely many solutions

$$a = a_0 - \frac{uy}{g}$$

and

$$b = b_0 + \frac{ux}{g}$$

for some particular a_0, b_0 (which can always be found with the Euclidean algorithm) and for some arbitrary $u \in \mathbb{Z}$.

4 Next

Now, finally and at long last, we are ready to tackle the Chinese Remainder Theorem in April. In May we'll cover totients, and in June we'll cover the popular RSA encryption algorithm in full mathematical detail.