Introduction to Diophantine Equations

Tom Davis
tomrdavis@earthlink.net
http://www.geometer.org/mathcircles
September 7, 2006

Abstract

In this article we will only touch on a few tiny parts of the field of linear Diophantine equations. Some of the tools introduced, however, will be useful in many other parts of the subject.

1 Whole Numbers

In number theory, we are usually concerned with the properties of the integers, or whole numbers: $Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Let us begin with a very simple problem that should be familiar to anyone who has studied elementary algebra.

• Suppose that dolls sell for 7 dollars each, and toy train sets sell for 18 dollars. A store sells 25 total dolls and train sets, and the total amount received is 208 dollars. How many of each were sold?

The standard solution is straight-forward: Let x be the number of dolls and y be the number of train sets. Then we have two equations and two unknowns:

$$\begin{aligned} x + y &= 25 \\ 7x + 18y &= 208 \end{aligned}$$

The equations above can be solved in many ways, but perhaps the easiest is to note that the first one can be converted to: $x = 25 - y$ and then that value of x is substituted into the other equation and solved:

$$\begin{aligned} 7(25 - y) + 18y &= 208 \\ 175 - 7y + 18y &= 208 \\ -7y + 18y &= 208 - 175 \\ 11y &= 33 \\ y &= 3 \end{aligned}$$

Then if we substitute $y = 3$ into either of the original equations, we obtain $x = 22$, and it is easy to check that those values satisfy the conditions in the original problem.

Now let's look at a more interesting problem:

• Suppose that dolls sell for 7 dollars each, and toy train sets sell for 18 dollars. A store sells only dolls and train sets, and the total amount received is 208 dollars. How many of each were sold?

This time there is only one equation: $7x + 18y = 208$. We probably learned in algebra class that you need as many equations as unknowns to solve problems like this, so at first it seems hopeless, but there is one additional key piece of information: the number of dolls and the number of train sets must be *non-negative whole numbers*. With that in mind, let's see what we can do, ignoring for the moment the fact that we already have a solution, namely: $x = 22$ and $y = 3$.

Beginning from our original equation, we can do this:

$$\begin{aligned} 7x &= 208 - 18y \\ x &= \frac{208 - 18y}{7} = 29 - 2y + \frac{5 - 4y}{7}. \end{aligned}$$

At first, this seems like we haven't made any progress, but notice that since y has to be an integer, the value of $(29 - 2y)$ is a whole number, so also the fraction $(5 - 4y)/7$ also has to be a whole number. Let's call it a, and then do some arithmetic with the resulting equation:

$$\begin{aligned} a &= \frac{5 - 4y}{7} \\ 7a &= 5 - 4y \\ 4y &= 5 - 7a \\ y &= \frac{5 - 7a}{4} = 1 - a + \frac{1 - 3a}{4}. \end{aligned}$$

As before, we still don't have a solution, but things look better in a sense: the denominator in the fraction is smaller: it is now 4 instead of 7. As before, since we know that a is a whole number, we know that $1 - a$ is a whole number, and therefore $(1 - 3a)/4$ must be a whole number which we will call b, and we'll again repeat the same sort of algebraic manipulations:

$$\begin{aligned} b &= \frac{1 - 3a}{4} \\ 4b &= 1 - 3a \\ 3a &= 1 - 4b \\ a &= \frac{1 - 4b}{3} = -b + \frac{1 - b}{3}. \end{aligned}$$

The same reasoning as before tells us that $(1 - b)/3$ must be a whole number, so we call it c:

$$\begin{aligned} c &= \frac{1 - b}{3} \\ 3c &= 1 - b \\ b &= 1 - 3c. \end{aligned}$$

Now we've actually made some progress. No matter *what* integer value c takes, b will be an integer! Let's substitute that value of b back into the previous equation:

$$a = \frac{1 - 4b}{3} = \frac{1 - 4(1 - 3c)}{3} = \frac{-3 + 12c}{3} = -1 + 4c.$$

Now substitute this value of a to obtain y:

$$y = \frac{5-71}{4} = \frac{5-7(-1+4c)}{4} = \frac{12-28c}{4} = 3-7c.$$

Finally, we can substitute this value of y into the original equation to obtain x:

$$x = \frac{208-18y}{7} = \frac{208-18(3-7c)}{7} = \frac{154+126c}{4} = 22+18c.$$

Our solution looks a little different from what we obtained in the first problem, but here it is:

$$\begin{aligned} x &= 22+18c \\ y &= 3-7c \end{aligned}$$

If $c = 0$ we obtain the same solution we did previously: $x = 22$ and $y = 3$, but note that *any* integer value of c will yield another solution. We can see that positive values of c will yield negative values of y, but if $c = -1$, we obtain another solution: $x = 4$ and $y = 10$. It's easy to check that both (x, y) pairs are valid solutions to the original problem. If c is smaller, -2 or less, then the x values become negative, so there are no additional solutions.

When an equation of this sort is solvable by this method, there is no limit to the number of steps that need to be taken to obtain the solution. In the example above, we needed to introduce integers a, b and c, but other equations might require more or fewer of these intermediate values.

2 Linear Diophantine Equations

What we have just solved is known as a Diophantine equation – an equation whose roots are required to be integers. Probably the most famous Diophantine equation is the one representing Fermat's last theorem, finally proved hundreds of years after it was proposed by Andrew Wiles:

If $n > 2$, there are no non-trivial[1] solutions in integers to the equation:

$$x^n + y^n = z^n.$$

There are many, many forms of Diophantine equations, but equations of the sort that we just solved are called "linear Diophantine equations": all the coefficients of the variables are integers.

Let's look a little more closely at the equation we just solved: $7x + 18y = 208$. If the only requirement were that the roots be integers (not necessarily non-negative integers), then our solution: $x = 22 + 18c$ and $y = 3 - 7c$ represent an infinte set of solutions, where every different integer value of c generates another solution.

[1] The "trivial" solutions are those where x or y is zero.

A more geometric view of the problem is this: If we were to graph the equation $7x + 18y = 208$, the solutions are places where the graph passes through points that have integer coordinates. In Figure 1 a portion of that line is plotted, and the points where the graph has integer coordinates are indicated and labeled.

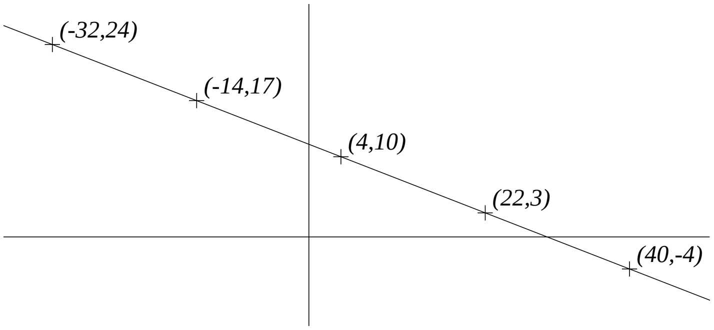

Figure 1: Graph of $7x + 18y = 208$

Notice that all the points with integer coordinates are evenly spaced along the line. In fact, if we begin at any point and add 18 to the x-coordinate and at the same time subtract 7 from the y-coordinate, we arrive at another point on the graph with integer coordinates. A quick examination of the original equation should make it obvious why this is the case. The equation is:

$$7x + 18y = 208.$$

If we add 18 to the x value, we increase the left side by $7 \cdot 18$. If we subtract 7 from the y value, we decrease the left side by the same amount: $18 \cdot 7$. The net effect is to leave the left side unchanged.

Notice that this line has a negative slope and happens to cut through the first quadrant (quadrant I) and intersect some points with integer coordinates there. This may or may not be the case for the graphs of other linear Diophantine equations. Lines with positive slopes can have an infinite number of solutions where both are positive, and there are equations where there are none. It's easy to construct such equations with whatever characteristics you wish.

Does every equation of the form:

$$ax + by = c,$$

where a, b and c are integers have a solution (x, y), where x and y are also integers?

The answer is no. For example, what if a and b are even and c is odd? The left side must be even, and if the right side is odd, there is no possibility of a solution with integer values. Similarly, if a and b are both multiples of 3 and c is not, the left side will be a multiple of 3 and the right side is not, so again, there are no possible integer solutions.

In fact, if the greatest common divisor (GCD) of a and b does not divide c, then there are no integer solutions. The amazing thing, however, is that if the GCD of a and b also divides c, then there are an infinite number of integer solutions, and we will see why that is the case later on.

Note also that another observation we made about our particular problem will also apply to a general linear Diophantine equation; namely, that if (x, y) is an integer solution to:

$$ax + by = c$$

then so will be $(x + bk, y - ak)$ where k is any integer. If we substitute $x + bk$ for x and $y - ak$ for y, we obtain:

$$\begin{aligned} a(x + bk) + b(y - ak) &= c \\ ax + abk + by - abk &= c \\ ax + by &= c, \end{aligned}$$

so if (x, y) is a solution, then so also is $(x + bk, y - ak)$.

3 Reducing Fractions

Now we will jump to a problem that at first glance is totally unrelated to linear Diophantine equations, but will turn out to be very similar. Let's begin with a very ugly problem:

Reduce the following fraction to lowest terms:

$$\frac{179703941}{215237573}.$$

Recall that to reduce a fraction to lowest terms, you search for numbers that are common factors of the numerator and denominator and if such numbers exist, the fraction can be simplified by dividing both numerator and denominator by that common number. For example, in the fraction $48/66$ both the numerator and denominator have a factor of 6, so we have:

$$\frac{48}{66} = \frac{6 \cdot 8}{6 \cdot 11} = \frac{8}{11}.$$

It's easy to check that the 8 and 11 in the fraction $8/11$ have no other integer common factors, so $8/11$ is reduced to its simplest possible form.

With a computer, or with a heck of a lot of effort by hand or even with a calculator, we can search for common factors of the numerator and denominator of our original problem, but that could require a great amount of effort. In fact, you will need to test hundreds of possible factors before you arrive at the following:

$$\frac{179703941}{215237573} = \frac{185071 \cdot 971}{185071 \cdot 1163} = \frac{971}{1163},$$

and even then, a bit more work must be done to assure that 971 and 1163 have no common factors.

What we would like to do is have a method to find the GCD (greatest common divisor) of the numerator and denominator, and then eliminate that from the numerator and denominator, yielding the fraction reduced to simplest form.

Let's try the following approach, which, except for some slightly ugly arithmetic, should seem quite familiar:

$$215237573 = 179703941 \cdot 1 + 35533632.$$

Notice that if some number does divide 215237573 and 179703941 then it must also divide 35533632. That means that:

$$\mathrm{GCD}(215237573, 179703941) = \mathrm{GCD}(179703941, 35533632).$$

Thus we have reduced the size of the numbers in our problem.

We can continue in the same way:

$$\begin{aligned} 179703941 &= 35533632 \cdot 5 + 2035781 \\ 35533632 &= 2035781 \cdot 17 + 925355 \\ 2035781 &= 925355 \cdot 2 + 185071 \\ 925355 &= 185071 \cdot 5 + 0. \end{aligned}$$

In every case, any number that divides the two leftmost numbers in the equations above must also divide the rightmost, and in the final line, we observe that 185071 must be the GCD of those numbers. Once we know that 185071 divides the numerator and denominator and in fact is the largest number to do so, we can divide the numerator and denominator of our original fraction by that number to obtain the form $971/1163$ as the simplest form.

This method to obtain the GCD of any two numbers is known as Euclid's algorithm.

4 Euclid's Algorithm and Diophantine Equations

Now let's use the Euclidean algorithm on two of the numbers from the original Diophantine equation we solved in Section 1: $7x + 18y = 208$.

$$\begin{aligned} 18 &= 7 \cdot 2 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

In this example, the final number is 1, so the GCD of 18 and 7 is 1 (in other words, 18 and 7 are relatively prime), but the interesting thing to note is that the numbers in the GCD calculation: $18, 7, 4, 3, 1$ are the same numbers that we got as denominators and as the coefficients of the variables in the numerators in the fractions when we were solving the Diophantine equation $7x + 18y = 208$. The only oddball numbers were the constants in the numerators, and that's not surprising: we never used the number 208 when we were using the Euclidean algorithm to find the GCD of 18 and 7. If you check the arithmetic calculations that are being done in each case, it will be clear why the numbers generated in both examples must be the same.

Suppose that the original Diophantine equation had had a 1 instead of the 208. To make sure you understand the technique we used to solve our Diophantine equation it would be a good exercise to solve the following equation by yourself before reading on:

$$7x + 18y = 1$$

Here's the solution (but just the equations: the textual arguments are omitted):

$$\begin{aligned}
7x + 18y &= 1 \\
x &= \frac{1 - 18y}{7} = -2y + \frac{1 - 4y}{7} \\
a &= \frac{1 - 4y}{7} \\
y &= \frac{1 - 7a}{4} = -a + \frac{1 - 3a}{4} \\
b &= \frac{1 - 3a}{4} \\
a &= \frac{1 - 4b}{3} = -b + \frac{1 - b}{3} \\
c &= \frac{1 - b}{3} \\
b &= 1 - 3c
\end{aligned}$$

The nice thing about the 1 in place of the 208 is that it remains constant throughout the calculation, whereas the 208 was reduced as various of the denominators divided it evenly. In *this* calculation, all the other coefficients are the same as the numbers generated in the straight-forward calculation of the GCD of 7 and 18.

To complete the solution, we need to back-substitute the $b = 1 - 3c$ and after a few steps we obtain: $x = -5 + 18c$ and $y = 2 - 7c$, where c is an arbitrary integer. (Obviously this equation will have no solutions where both x and y are positive.)

Thus when you do a GCD calculation of a and b, and that GCD turns out to be 1, you've done a lot of the work toward solving the Diophantine equation

$$ax + by = 1.$$

So if we can do the Euclidean algorithm, we can find with almost no effort other than a little arithmetic the coefficients we need to solve a linear Diophantine equation of the form $ax + by = 1$. Of course we'd like to be able to solve equations where the 1 is replaced by an arbitrary number c, but that is actually not too difficult.

As as example, let's find solutions for $7x + 18y = 208$ assuming that we've solved $7x + 18y = 1$. The solutions for the latter equation are $x = -5 + 18c$ and $y = 2 - 7c$, where c is an arbitrary integer. An easy solution is simply to set $c = 0$ and obtain $x = -5$ and $y = 2$ as a particular solution. But if we multiply x and y by 208, then the left side will be increased by a factor of 208 so if we increase the right side by the same factor, we'll have an (x, y) pair that satisfies our original equation $7x + 18y = 208$.

Thus a solution is this: $x = -5 \cdot 208 = -1040$ and $y = 2 \cdot 208 = 416$. It's easy to plug these numbers in to check that they are valid.

But we also noticed that adding any multiple of 18 to x while at the same time adding that same multiple of -7 to y will yield the other solutions, so the general solution to our original problem is: $x = -1040 + 18k$ and $y = 416 - 7k$. If $k = 58$, for example, this yields the solution $x = 4$ and $y = 10$.

We have seen that if we have any solution to one of these linear Diophantine equations, we can obtain all the others by adding constant multiples of the opposite coefficients to the given solution, all we really need is one solution.

In the previous examples, once we got to the point where we had $b = 1 - 3c$, we back-substituted and carefully kept track of the coefficient of c in the calculations. But since *any* solution will generate all the others, why not let $c = 0$? Then we just need to track a single number.

5 Putting It All Together

Let's use the techniques above, but in their most simplified form, to solve another Diophantine equation. Here's the problem:

• In a pet shop, rats cost 5 dollars, guppies cost 3 dollars and crickets cost 10 cents. One hundred animals are sold, and the total receipts are 100 dollars. How many rats, guppies and crickets were sold?

If r, g and c represent the number of rats, guppies and crickets, respectively, we've got two equations (but three unknowns):

$$\begin{aligned} r + g + c &= 100 \\ 5r + 3g + .1c &= 100 \end{aligned}$$

To turn the problem into a purely integer problem, multiply the second equation by 10:

$$\begin{aligned} r + g + c &= 100 \\ 50r + 30g + c &= 1000 \end{aligned}$$

If we subtract the first equation from the second we obtain the familiar looking linear Diophantine equation in two variables:

$$49r + 29g = 900.$$

Luckily, the GCD for 49 and 29 is 1 which divides 900 so there will be solutions (although possibly not solutions where all the values are non-negative.

(This problem is probably much easier to solve using "guess and check" techniques: we know that the number of crickets must be a multiple of 10, so you could just try 0, 10, 20, ..., 100 of them.)

Let's find the GCD of 49 and 29, using the Euclidean algorithm:

$$\begin{aligned}
49 &= 29 \cdot 1 + 20 \\
29 &= 20 \cdot 1 + 9 \\
20 &= 9 \cdot 2 + 2 \\
9 &= 2 \cdot 4 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}$$

Since we've used the variable c for the number of crickets, and g for the number of guppies, let's use variables i, j, k, et cetera for the integer values of fractions that we get as we step through the solution of the Diophantine equation. We will a particular solution to the simpler equation:

$$49r + 29g = 1$$

and then multiply both r and g by 900 for a solution to the original problem.

Without doing any calculations, but just reading the values obtained from the Euclidean algorithm used to calculate the GCD of 49 and 29 and the variables i, j, k and l as the integer values of fractions, we can just write down the relationships among them (expressed both ways). For the purposes of finding a solution to the equation, only the expressions on the right are important. Note how the numbers in the fractions (other than the 1, of course) are exactly the same as the numbers on the left in the execution of the Euclidean algorithm to find the GCD of 49 and 29 above.

$$\begin{array}{ll}
r = \dfrac{1 - 29g}{49} & g = \dfrac{1 - 49r}{29} \\[2ex]
i = \dfrac{1 - 20r}{29} & r = \dfrac{1 - 29i}{20} \\[2ex]
j = \dfrac{1 - 9i}{20} & i = \dfrac{1 - 20j}{9} \\[2ex]
k = \dfrac{1 - 2j}{9} & j = \dfrac{1 - 9k}{2} \\[2ex]
l = \dfrac{1 - k}{2} & k = 1 - 2l
\end{array}$$

From the last line, clearly $k = 2l$ for arbitrary integers l, so just set $l = 0$ to obtain a particular solution. If $l = 0$, then $k = 1$. If $k = 1$ then $j = -4$. If $j = -4$, then $i = 9$. If $i = 9$ then $r = -13$. And if $r = -13$, then $g = 22$.

It's easy to check our work; namely, that $r = -13$ and $g = 22$ is a solution to:

$$49r + 29g = 1.$$

To obtain a particular solution to the original equation, multiply by 900: $r = -11700$ and $g = 19800$. From previous considerations, we know that the general solution to the original equation will be:

$$\begin{aligned} r &= -11700 + 29k \\ g &= 19800 - 49k \end{aligned}$$

We're looking for non-negative values of r and g, so divide 29 into 11700 and we find that if $k = 404$ we obtain the values $r = 16$ and $g = 4$. If $k = 403$ or $k = 405$, either r or g is negative.

Since there are 100 total animals, $c = 80$, and it's easy to check that $r = 16$, $g = 4$ and $c = 80$ solves the problem.