Parabola Volume 49, Issue 2 (2013)

Linear Diophantine Equations

David Angell [1]

Many popular and well–known puzzles can be approached by setting up and solving equations. Frequently, however, it will be necessary to find solutions which are not just any old real numbers, but integers. Here are two examples.

- *The absent–minded bank teller*. Shane went to the bank and asked the teller to pay him a certain amount of money, in dollars and cents, from his account. When paying out the money, however, the bank teller accidentally switched the numbers of dollars and cents. After buying an ice cream for $\$2.55$, Shane found that he had left exactly four times what he had asked for. How much had he asked for?

- *The monkey and the coconuts*. Five sailors washed up on a desert island collect a pile of coconuts before going to sleep. During the night one of them gets up, divides the pile into five equal parts and throws one leftover coconut to the monkey, hides one of the five parts and puts the other four parts back into one pile. The other castaways, one at a time, do exactly the same. In the morning they share out the remaining coconuts and find that they divide exactly into five equal parts. How many coconuts were there?

To begin the first problem, we could let x be the number of dollars and y the number of cents Shane wanted. Then the amount he asked for was $100x + y$ cents, the amount he received was $100y + x$ cents, and so

$$4(100x + y) + 255 = 100y + x \ ;$$

we can now collect terms,

$$399x - 96y = -255 \ ,$$

and cancel common factors, simplifying the equation to

$$133x - 32y = -85 \ . \tag{1}$$

If we seek real numbers x, y to satisfy this equation, it is ridiculously simple: let x be anything you like, then calculate y from the equation. However, the problem of the bank teller only makes cents – sorry, makes sense – if x and y are non–negative integers less than 100. Because of the restriction, (1) is called a **linear Diophantine equation** in two variables. Some of the most famous difficult problems in number theory involve Diophantine equations of higher degree, that is, involving squares, cubes or even exponentials.

[1] Dr David Angell is a pure mathematician and associate lecturer in the School of Mathematics and Statistics at the University of New South Wales.

- *Pythagorean triples*: find all positive integers x, y, z which form the side lengths of a right–angled triangle: that is, solve $x^2 + y^2 = z^2$ in positive integers.
- *Fermat's Last Theorem*: prove that if $n \geq 3$ then the equation $x^n + y^n = z^n$ has no solution in non–zero integers.
- *Mordell's equation*: solve in integers $x^2 + 2 = y^3$.
- *Catalan's conjecture*: the only consecutive positive powers greater than the first are 8 and 9. That is, the only solution of $x^m - y^n = 1$ with x, y positive integers and $m, n \geq 2$ is $x = 3$, $m = 2$, $y = 2$, $n = 3$.

It's not just puzzles, however! Some very important applications of mathematics involve Diophantine equations.

- *RSA cryptography*: working out how to decode your own encrypted messages requires solving the equation

$$ex - (p-1)(q-1)y = 1 \, ,$$

  where e, p, q are known integers and x, y are to be found.
- Balancing formulae for chemical reactions can be accomplished by using Diophantine equations – the article at `pubs.acs.org/doi/abs/10.1021/ed045p731` gives an exposition of this.
- In `www.cs.helsinki.fi/u/gurtov/papers/per_paper.pdf`, Diophantine equations are applied to the design and analysis of peer–to–peer computing networks.

The term *Diophantine equation* commemorates the Greek mathematician Diophantus (third century A.D.?), who lived and worked in the city of Alexandria (now in Egypt), and wrote a treatise on solving various kinds of equations. In some ways it is rather odd to refer to "Diophantine equations", as it is the solutions which are restricted, not the equations; however the term is widely used and probably cannot now be changed! The higher degree Diophantine equations can be exceedingly difficult to solve[2], and in this article we shall just explain how to completely solve the relatively straightforward linear Diophantine equations.

So, we consider an equation

$$ax + by = c \, ,$$

where a, b, c are given integers and we wish to find all possible solutions in integers x, y. The first question is whether or not there are any solutions at all. Suppose that a and b have a common factor $g > 1$. If g is not a factor of c then the equation has no

[2]But for a few ideas you might like to read my article *Beginning algebraic number theory*, which appeared in *Parabola Incorporating Function* volume 41, issue 1, and is available online at `http://www.parabola.unsw.edu.au/vol41_no1/vol41_no1_2.pdf`.

solution, because the left-hand side is a multiple of g and the right-hand side is not. For a very simple example,

$$12345678x + 98765432y = 123456789$$

has no solution because, regardless of the values of x and y, the left-hand side is even and the right-hand side odd. For a (slightly) harder case,

$$2013x - 3102y = 1$$

has no solution since the left-hand side is a multiple of 3 and the right-hand side isn't. Notice by the way that in this example the coefficient b is negative: this is no problem at all.

On the other hand, suppose that every common factor of a and b is also a factor of c. Then we can divide both sides by the greatest common factor, leaving a case in which the (new) coefficients on the left-hand side have no common factor except 1. This is, in fact, exactly how we derived (1) from the previous equation: we observed that 399 and 96 have a common factor of 3, which is also a factor of -255 on the right-hand side, so we cancelled the 3. Another example: to solve the equation

$$4455x + 6677y = 8899$$

we would notice that the coefficients on the left-hand side have a common factor of 11 (easy!) and no more (a bit harder) and would divide out the 11 to give

$$405x + 607y = 809 \ .$$

It is true (though not by any means obvious) that once the left-hand side coefficients have no common factor, the equation is sure to have a solution in integers. Here is the relevant result.

Theorem. *Solution of linear Diophantine equations in two variables*. Suppose that a and b are integers with no common factor, and c is any integer. Then

- the equation $ax + by = c$ has integer solutions x, y;
- if $x = x_0$, $y = y_0$ is one specific solution of the equation, then all solutions are given by the formulae
$$x = x_0 - bt \ , \quad y = y_0 + at \ , \tag{2}$$
where t is an integer.

We won't prove this theorem, but will show by means of an example how to find a solution x_0, y_0. Once this is done, finding the complete solution is easy – all we have to do is substitute known numbers into the formulae (2). So, let's solve the "bank teller equation":

$$133x - 32y = -85 \ .$$

The main step is to apply the **Euclidean algorithm** to the left-hand side coefficients. This means, divide the larger by the smaller to give a quotient and remainder; then do

the same with the previous divisor and the remainder; and so on. In this example we have

$$\begin{aligned} 133 &= 4 \times 32 + 5 \\ 32 &= 6 \times 5 + 2 \\ 5 &= 2 \times 2 + 1 \, . \end{aligned}$$

(Make sure you are clear on the pattern here – note how the original remainder 5 moves to the left in each subsequent equation.) The 1 at the end confirms that our original numbers 133 and 32 have no common factor – if we didn't get a 1, we would have to go back to the previous step, find common factors, and see whether or not they are also factors of the right-hand side.

Next, we run the Euclidean algorithm "backwards" in order to write 1 as a multiple of 133 plus a multiple of 32. First rewrite all the divisions so as to make the remainder the subject:

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ 2 &= 32 - 6 \times 5 \\ 5 &= 133 - 4 \times 32 \end{aligned}$$

and then substitute each remainder into the previous equation, expanding and collecting terms at each step:

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2 \times (32 - 6 \times 5) \\ &= 5 - 2 \times 32 + 12 \times 5 \\ &= -2 \times 32 + 13 \times 5 \\ &= -2 \times 32 + 13 \times (133 - 4 \times 32) \\ &= -2 \times 32 + 13 \times 133 - 52 \times 32 \\ &= 13 \times 133 - 54 \times 32 \, . \end{aligned}$$

Finally, multiply both sides by the number -85 from equation (1), and collect terms on the right-hand side in such a way that the coefficients 133 and 32 are not altered:

$$\begin{aligned} -85 &= -85 \times 13 \times 133 + 85 \times 54 \times 32 \\ &= -1105 \times 133 + 4590 \times 32 \, . \end{aligned}$$

Now let's look at our situation. We seek x and y such that

$$133x - 32y = -85 \, ;$$

and we have just found that

$$133 \times (-1105) - 32 \times (-4590) = -85 \, .$$

If you look carefully at these two equations it should be clear that one possible solution is $x = -1105$, $y = -4590$; these can be our x_0 and y_0, and then from (2) the complete solution of our equation is

$$x = -1105 + 32t\ , \quad y = -4590 + 133t\ , \quad \text{where } t \text{ is an integer.}$$

Often a formula such as this will be the end of the problem; however, for the "bank teller" puzzle there is one more requirement: x and y should both be non–negative and less than 100. We have to try to find a value of t which will accomplish this. Looking at y first, we need

$$0 \leq -4590 + 133t < 100\ ,$$

and a bit of work turns this into

$$34.5 \leq t < 35.3\ ;$$

since t has to be an integer there is only one possibility, $t = 35$, giving the value $y = 65$. Does this give an admissible value for x? If not, the puzzle has no solution; however, we calculate

$$x = -1105 + 32t = -1105 + 32 \times 35 = 15\ ,$$

which is fine. So the **answer** to the puzzle is that Shane asked the bank teller for $\$15.65$.

A few of the questions in the problem section of this issue can be solved by means of Diophantine equations. We'll conclude this article by summarising the solution procedure. Given integers a, b, c, we wish to find integer solutions x, y of the equation $ax + by = c$.

1. Cancel from the equation all possible common factors of a, b, c. If the left-hand side coefficients still have a common factor which is not a factor of the right-hand side, then the equation has no solution. Otherwise, proceed. **Note** that from here on a, b, c refer to the values after cancelling any common factors – these may not be the same as the original values of a, b, c.

2. Apply the Euclidean algorithm to a, b: keep going until you end up with 1 as the final remainder.

3. Run the Euclidean algorithm "backwards" in order to write 1 as a multiple of a plus a multiple of b.

4. Multiply both sides by c, and collect terms in such a way that we now have c written as a multiple of a plus a multiple of b.

5. By comparing with the equation obtained at the end of step 1, write down a specific solution $x = x_0$, $y = y_0$.

6. Use (2) to write down the general solution for x and y in terms of an integer t. **Note** that the a and b in the formula will be those obtained after the cancellation in step 1, and possibly not the given a and b.

7. If necessary, choose appropriate value(s) of t in order to satisfy any additional conditions in the problem.

If you spend a bit of time learning and mastering this procedure, you will find that Diophantine equations form a useful technique for solving a wide variety of puzzles.