1. Use Euclid's algorithm to write $a/b = (a_0, a_1, \ldots, a_n)$.

2. Since a/b is in lowest terms, $a = \pm p_n$ and $b = \pm q_n$. Since $p_n q_{n-1} - p_{n-1} q_n = \pm 1$, it follows that, with some selection of signs, $x_0 = \pm c q_{n-1}$, $y_0 = \pm c p_{n-1}$ is a solution of the Diophantine equation. Thus, using the recursive definitions given in Chapter 14, calculate p_{n-1} and q_{n-1} and pick the signs so that x_0, y_0 is a solution.

3. If t is any integer, $x = x_0 + bt$, $y = y_0 - at$ is another solution of the Diophantine equation.

4. There are no integer solutions other than those mentioned in (3) above. For if $ax + by = c = ax_0 + by_0$, then $a(x - x_0) = b(y_0 - y)$ and b is a factor of $x - x_0$, since $\gcd(a, b) = 1$. Hence, for some integer t, $x = x_0 + bt$.

Example: Solve $25x + 55y = 50$.

First we get the gcd of 25 and 55 by using Euclid's algorithm:

$$25/55 = 0 + \frac{1}{55/25} = 0 + \frac{1}{2 + 5/25} = 0 + \frac{1}{2 + 1/5} = (0, 2, 5).$$

The gcd is the last divisor, namely, 5. (It is merely a coincidence that the last partial quotient is also 5.) We note that 5 divides 50 and so the equation does have integer solutions. We factor out the 5, obtaining $5x + 11y = 10$. We calculate the penultimate convergent $p_1/q_1 = (0, 2) = 1/2$. With the right signs, one solution is $x_0 = \pm 10 \times 2$ and $y_0 = \pm 10 \times 1$. Indeed, we can take $x_0 = -20$ and $y_0 = 10$. The general solution is $x = -20 + 11t$, $y = 10 - 5t$, where t is any integer.

Sometimes we want only positive solutions. In that case we must have $x_0 + bt > 0$ and $y_0 - at > 0$. In the above example this would require an integer t such that $1 < 20/11 < t < 10/5 = 2$, which is impossible.

Exercises

1. Solve the Diophantine equation $101x + 753y = 100,000$. (There are two positive integer solutions.)

2. Solve the Diophantine equation $158x + 57y = 20,000$. (There are two positive integer solutions.)

3. Solve the Diophantine equation $91x + 221y = 1053$. (There are no positive integer solutions.)

4. Show that the following Diophantine equation has a unique solution in positive integers: $17x + 19y = 320$.

5. The Sultana used to divide her maids into two companies, one which would follow her five abreast and the other which would follow her seven abreast – both in rectangular formation. These companies would consist of different numbers of maids on each of nine different days. What is the smallest number of maids the Sultana could have had?

6. Show that, if a and b are positive integers, then $ax + by = c$ has no solutions in positive integers when $[-x_0/b] \geq [y_0/a]$. (Here x_0 and y_0 are the solutions described above, and $[z]$ is the greatest integer not exceeding z.)

17

Quadratic Surds

Let d be a positive nonsquare integer. Using the Fundamental Theorem of Arithmetic, it is not hard to show that $\sqrt{d}$ is irrational. This was first proved by Theaetetus in about 400 BC.

If a and $b \neq 0$ are integers, the expression $(a+\sqrt{d})/b$ is called a *quadratic surd.* Note that if a' and b' are integers, and $(a+\sqrt{d})/b = (a'+\sqrt{d})/b'$ then $a = a'$ and $b = b'$. The proof is left as an exercise.

In this chapter we study continued fraction expansions of quadratic surds. These expansions can be used to solve quadratic Diophantine equations, such as the 'Pell equation' $x^2 - dy^2 = 1$.

To begin with an example, suppose that $x = (1, 1, 1, \ldots)$. Then $x = 1 + 1/x$ and hence $x^2 - x - 1 = 0$, with the result that $x = \frac{1}{2}(1+\sqrt{5})$. (We cannot take the other root of the equation since x is positive.) This is a quadratic surd. Indeed, it is a very famous one known as 'the golden ratio'. It is the ratio of the side to the base in the triangles obtained by connecting the five points of the Pythagorean star.

As another example, suppose that $y = (1, 1, 2, 1, 2, 1, \ldots)$. To evaluate this continued fraction, let $x = (1, 2, 1, 2, 1, \ldots)$. Then $y = 1 + 1/x$. Furthermore, $x = 1 + \frac{1}{2+1/x}$, so that $2x^2 - 2x - 1 = 0$ and hence $x = \frac{1}{2}(1+\sqrt{3})$. Thus $y = \sqrt{3}$.

Generalizing from these two examples, it is easily shown that any continued fraction which is ultimately periodic represents a quadratic surd. Less obvious is the converse of this statement, namely, that every quadratic surd has a continued fraction expansion which is ultimately periodic. This was first proved by Lagrange in about 1770. We shall prove the special case:

Theorem 17.1. *If d is a positive integer which is not a perfect square, the continued fraction expansion of $\sqrt{d}$ is ultimately periodic.*

Proof: We define sequences of integers a_n and b_n and a sequence of rationals r_n as follows, where $[\rho]$ denotes the greatest integer in ρ:

$$a_0 = 0,\ r_0 = 1,\ b_n = \left[\frac{\sqrt{d}+a_n}{r_n}\right],\ a_{n+1} = b_n r_n - a_n,\ r_{n+1} = (d_n - a_{n+1}^2)/r_n.$$

Then it is easily verified that

$$\frac{\sqrt{d}+a_n}{r_n} = b_n + \cfrac{1}{b_{n+1} + \cfrac{1}{b_{n+2} + \ddots}},$$

in particular,

$$\sqrt{d} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \ddots}}$$

and hence $b_{n+1} > 0$. It also follows by mathematical induction that the r_n are integers, once it is realized that

$$r_{n+2} = r_n - b_{n+1}^2 r_{n+1} + 2b_{n+1}a_{n+1}.$$

Let $x_n = (\sqrt{d}+a_n)/r_n$ and let t_n be its conjugate $(-\sqrt{d}+a_n)/r_n$. From Chapter 14 we know that

$$\sqrt{d} = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$

Taking conjugates, we obtain

$$-\sqrt{d} = \frac{t_n p_{n-1} + p_{n-2}}{t_n q_{n-1} + q_{n-2}}.$$

Solving for t_n, we obtain

$$t_n = \left(-\frac{q_{n-2}}{q_{n-1}}\right)\left(\frac{\sqrt{d}+p_{n-2}/q_{n-2}}{\sqrt{d}+p_{n-1}/q_{n-1}}\right).$$

As n increases, the second factor tends to 1. The q's are positive, so, for sufficiently large n, $t_n < 0$. Now $x_n > 1$ so, for sufficiently large n,

$$\frac{2\sqrt{d}}{r_n} = x_n - t_n > 1$$