and hence $r_n > 0$ and $2\sqrt{d} > r_n$. Since $t_n < 0$, it then follows that $a_n < \sqrt{d}$ while $x_n > 1$ implies $a_n > -\sqrt{d}$. Since

$$2\sqrt{d} > r_n > 0,$$

$$\sqrt{d} > a_n > -\sqrt{d},$$

there are only a finite number of possibilities for $x_n = (\sqrt{d} + a_n)/r_n$ and so the simple continued fraction must repeat.

Exercises

1. Find the continued fraction expansions of $\sqrt{2}$ and $\sqrt{10}$.

2. Find the quadratic surd which is represented by the periodic continued fraction $(a, b, c, a, b, c, \ldots)$.

3. Fill in the details in the proof of the above theorem.

4. Show that for nonsquare d, the continued fraction expansion of $\sqrt{d}$ is of the form $\sqrt{d} = (a_0, \overline{a_1, \ldots, a_{n-1}, 2a_0})$, with the part under the bar periodic.

5. For d as in Exercise 4, show that $p_{n-1}^2 - dq_{n-1}^2 = \pm 1$, where p_{n-1}/q_{n-1} is the $(n-1)$th convergent of $\sqrt{d}$. (Hint: show that

$$\sqrt{d} = \frac{\alpha_n p_{n-1} - p_{n-2}}{\alpha_n q_{n-1} - q_{n-2}}$$

where $\alpha_n = \sqrt{d} + a_0$.)

6. Find a positive integer solution to the equation $x^2 - 61y^2 = \pm 1$.

7. Prove that in $\frac{a+\sqrt{d}}{b}$, the positive integers a and b are uniquely determined.

Note that Exercises 4 and 5 are more difficult.

18

Pythagorean Triangles and Fermat's Last Theorem

A *Pythagorean triangle* is a right triangle all of whose sides have integer lengths. For example, let ABC be a triangle with a right angle at vertex C. Suppose that the sides AC and BC have lengths 5 and 12, respectively. Then the hypotenuse has length $\sqrt{5^2 + 12^2} = 13$. Since all three sides have integer lengths, this is a Pythagorean triangle.

Note that if k is any positive integer, the triangle with sides of lengths $5k, 12k$ and $13k$ is a Pythagorean triangle too. This triangle is just a magnification of the previous one and so it is not very interesting. However, it does suggest that it would be worthwhile to find all the Pythagorean triangles whose gcd is 1. These are called *primitive* Pythagorean triangles. It is easy to show that if x, y and z are the sides of a right triangle, then $\gcd(x, y, z) = \gcd(x, y) = \gcd(y, z)$. In what follows we shall assume that this gcd is equal to 1.

We shall use the following result:

Lemma 18.1. *If m and n are nonnegative integers such that* $\gcd(m, n) = 1$ *and mn is a square, then both m and n are squares.*

Professor Tournesol discovered an amusing proof of this theorem while he was in jail for having failed the president's son. The prisoners were put in a long row of cells. At first all the doors were unlocked, but then the jailor walked by and locked every second door. He walked by again and stopped at every third door, locking it if it was unlocked, but unlocking it if it was locked. On his next round he stopped at every fourth door, locking it if it was unlocked, unlocking it if it was locked, and so on. Professor Tournesol soon realised that the mth cell would be unlocked in the end just in case

m had an odd number of divisors. Now, if d divides m then so does m/d and it would seem that the divisors of m come in pairs. Unless...'what if $d = m/d$?', thought the professor, 'then the divisor d does not pair off with another, and $d = m/d$ just in case m is a square.'

Let $\tau(x)$ be the number of divisors of a positive integer x. Then $\tau(x)$ is odd just in case x is a square. Now, if $\gcd(m, n) = 1$ then a typical divisor of mn is of the form dg where d divides m and g divides n. Thus $\tau(mn) = \tau(m)\tau(n)$. If mn is a square then $\tau(mn)$ is odd, and hence both $\tau(m)$ and $\tau(n)$ are odd. Thus m and n are both squares. QED.

In order to solve the Diophantine equation $x^2+y^2 = z^2$ with $\gcd(x, y, z) = 1$, first note that x and y are not both odd. For if $x = 2a+1$ and $y = 2b+1$ then $x^2+y^2 = 4(a^2+b^2+a+b)+2$ which is not a square, since squares of odd numbers have the form $4(c^2+c)+1$ and squares of even numbers have the form $4c^2$. Since $\gcd(x, y) = 1$, it follows that x and y are not both even either. Hence exactly one of x and y is even. Without loss of generality, let us say that $y = 2y'$ and that x is odd. Then x^2 is also odd and y^2 is even. It follows that $z^2 = x^2 + y^2$ is odd and thus z is odd. Since x and z are both odd, $\frac{1}{2}(z + x)$ and $\frac{1}{2}(z - x)$ are both integers. Moreover, their gcd is 1, since any factor which divides them both also divides their sum z and their difference x. But $\gcd(x, z) = 1$.

Since $x^2 + y^2 = z^2$, we have $\frac{1}{2}(z + x)\frac{1}{2}(z - x) = y'^2$. From Professor Tournesol's discovery it follows that there are positive integers u and v with $\gcd(u, v) = 1$ such that $\frac{1}{2}(z + x) = u^2$ and $\frac{1}{2}(z - x) = v^2$. This gives $z = u^2 + v^2$, $x = u^2 - v^2$ and $y = 2y' = 2uv$. Note that u and v are not both odd, since z is not even. The above may be summarized as follows:

Theorem 18.2. *Let x, y and z be positive integers. Then $x^2 + y^2 = z^2$ with y even and $\gcd(x, y, z) = 1$ if and only if, for some positive integers u and v, not both of which are odd, with $u > v$ and $\gcd(u, v) = 1$,*

$$x = u^2 - v^2, \ y = 2uv, \ \textit{and} \ z = u^2 + v^2.$$

The suffiency of the above condition (that is, the 'if' part of the theorem) was known to the Mesopotamians about 4000 years ago (Neugebauer).

The eighth problem in the second book of the *Arithmetica* of Diophantus is to express 16 as a sum of two rational squares. Fermat (1601–1665) had a copy of this book and he enjoyed writing notes in its margins. Unlike Diophantus, Fermat was only interested in (positive) integer solutions to the equations in the *Arithmetica*. Fermat knew that the square of an integer can often be expressed as a sum of two positive integer squares. In the margin beside the problem about expressing 16 as a sum of two squares, Fermat wrote: