> On the other hand it is impossible to separate a cube into two cubes, or a biquadratic into two biquadratics, or generally *any power except a square into two powers with the same exponent.* I have discovered a truly marvellous proof of this, which, however, the margin is not large enough to contain' (p. 145, Heath's translation of the *Arithmetica*).

Fermat's assertion is called his 'Last Theorem', although, until quite recently, it would have been safer to call it a 'conjecture'. It is now believed that Fermat only proved the special case when the power $n = 4$, and the 'theorem' remained an open problem for 350 years, though many special cases were proved in that period. The complete theorem was finally proved by Andrew Wiles of Princeton University in 1994. His proof depended on the work of many other mathematicians, notably on a crucial result by K. A. Ribet, as well as ideas from G. Y. Taniyama, G. Shimura, B. Mazur and G. Frey, among others, and the last minute collaboration of Richard Taylor.

Fermat himself showed that $z^4 - x^4 = w^2$ has no solution in positive integers, and from this it follows at once that $x^4 + y^4 = z^4$ has no solution in positive integers (*Oeuvres* I, p. 340 and *Arithmetica*, 2nd edn., p. 293). We shall give a proof of this, due to Euler, which uses Fermat's *method of descent* (from a larger to a smaller solution):

Theorem 18.3. *There are no positive integers x, y and z such that*

$$x^4 + y^4 = z^2.$$

Proof: To obtain a contradiction, suppose there are such integers. Let us take such a triple with the product xy minimized. Then $\gcd(x, y) = 1$. Since x^2, y^2 and z are the sides of a primitive Pythagorean triangle, exactly one of x and y is even. Without loss of generality, let us say that x is even. By our previous theorem, there are positive integers u and v, not both odd, with $\gcd(u, v) = 1$, such that $x^2 = 2uv$ and $y^2 = u^2 - v^2$. Since $v^2 + y^2 = u^2$ and y is odd, v must be even. Since $\gcd(2v, u) = 1$ and $2vu = x^2$, it follows that $2v$ and u are squares (recall Professor Tournesol). Thus $u = c^2$ for some positive integer c.

Again by our above theorem, there are positive integers s and t, not both odd, with $\gcd(s, t) = 1$, such that $v = 2st$ and $u = s^2 + t^2$. Since $2v$ is a square, so is $2v/4 = v/2 = st$. Thus there are positive integers a and b such that $s = a^2$ and $t = b^2$.

The fact that $u = s^2 + t^2$ implies that $a^4 + b^4 = c^2$. Moreover, $(ab)^2 = st = v/2 < 2uv = x^2 \leq (xy)^2$ so that $ab < xy$. But this contradicts the minimality of xy.

Exercises

1. Prove that if a triangle has sides of lengths x, y and z, and $x^2+y^2 = z^2$ then the triangle has a right angle.

2. Show that if x, y and z are integers such that $x^2 + y^2 = z^2$ then $\gcd(x, y, z) = \gcd(x, z)$.

3. How many primitive Pythagorean triangles are there with hypotenuse < 50?

4. Show that if m and n are positive integers with $\gcd(m, n) = 1$ and mn is a cube then m is a cube.

5. Show that if u, v, u' and v' are positive integers such that $u^2 - v^2 = u'^2 - v'^2$ and $2uv = 2u'v'$ then $u = u'$ and $v = v'$.

6. Solve the Diophantine equation $x^{28} + y^{28} = z^{28}$.

7. Find all Pythagorean triangles with perimeter 1716.

19

What Is a Calculation?

At the second International Congress of Mathematicians (Paris, 1900), David Hilbert (1862–1943) presented a list of 23 problems, which he hoped would occupy mathematicians in the 20th century. We shall only talk about three of these problems here, as they concern the foundations of mathematics.

1. Prove or disprove the Continuum Hypothesis (Chapter 12).

2. Show that arithmetic, described as an axiomatic system, is consistent, that is, that it does not admit a proof that $0 = 1$. (As Paul Erdös would say, if such a proof were ever to be discovered, the universe would vanish.)

3. Find an effective method or 'algorithm', as it is now called, for deciding whether a given polynomial Diophantine equation (with integer coefficients) is solvable (in integers). (For the origin of the word 'algorithm', see Part I, Chapter 22.)

This last problem is actually Hilbert's Problem 10. Today we know that these three problems cannot be solved in the way Hilbert had intended. Kurt Gödel showed in 1938 that the Continuum Hypothesis cannot be proved and Paul Cohen showed in 1964 that it cannot be disproved either! The existence of mathematical statements that can be neither proved nor disproved had already been established by Gödel in 1931. It followed from his argument that the consistency of any formal system of arithmetic cannot be proved, unless we allow a method of proof which is more powerful than