Fermat’s Last Theorem
A Theorem at Last!

C S Yogananda

After more than three centuries of effort by some of the best mathematicians, Gerhard Frey, J-P Serre, Ken Ribet and Andrew Wiles have finally succeeded in proving Fermat’s assertion that the equation $X^n + Y^n = Z^n$ has no solutions in non-zero integers if $n \geq 3$. Each of the four mathematicians made a decisive contribution with Wiles delivering the coup de grace. The proof, as it finally came to be, is in some sense a triumph for Fermat.

When Pierre de Fermat died in 1665 he had not published a single mathematical work (except for an anonymous appendix to a book written by a colleague). His mathematical discoveries were contained in his correspondence with other mathematicians of his time, notably, Pascal, Frénicle de Bessy and Father Mersenne. He also left behind a few unpublished manuscripts and marginal notes in the books studied. We have to be grateful to his son Samuel for whatever we know of Fermat’s work. Samuel de Fermat went through his father’s papers and books in addition to soliciting letters written by his father from his correspondents in order to publish them. Among Fermat’s possessions was a copy of the Latin translation, by Bachet, of Diophantus’ Arithmetic in which Fermat had made a number of marginal notes.

The first work Samuel chose to publish, in 1670, was a new edition of Bachet’s Diophantus with an appendix containing forty eight marginal notes made by Fermat. The second of these notes appears alongside problem 8 in Book II of Arithmetic: “... given a number which is square, write it as a sum of two other squares”. Fermat’s note states, in Latin, that “on the other hand, it is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as sum of two fourth powers or, in general, for any number which is a power
"On the other hand, it is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as a sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers. I have a truly marvellous demonstration of this proposition which this margin is too narrow to contain". Thus, it was in 1670 that the world learnt of what has come to be termed Fermat's Last Theorem (FLT): The equation

\[ X^n + Y^n = Z^n \]

has no solutions in non-zero integers if \( n > 3 \). Fermat himself had given a proof of this assertion for \( n = 4 \) using infinite descent, a method he invented, and Euler proved the case \( n = 3 \). Thus to prove FLT we need to show that \( X^p + Y^p = Z^p \) has no solutions in non-zero integers whenever \( p \) is a prime greater than 3 (do you see why?).

After more than three centuries of effort by some of the best mathematicians, Gerhard Frey, J-P Serre, Ken Ribet and Andrew Wiles have finally succeeded in proving Fermat's assertion, each of them making a decisive contribution with Wiles delivering the coup de grace. The proof, as it finally came to be, is in some sense a triumph for Fermat. Elliptic curves and infinite descent play significant roles and it was Fermat who pioneered the use of elliptic curves in solving diophantine equations and it is to him that we owe the method of infinite descent.

**Diophantine Equations**

The chief work of Diophantus of Alexandria (c. 250 A.D) known to us is the *Arithmetic*, a treatise in thirteen books, or *Elements*, of which only the first six have survived. This work consists of about 150 problems, each of which asks for the solution of a given set of algebraic equations in positive rational numbers, and so equations for which we seek integer (or rational) solutions are referred to as diophantine equations. The most familiar example we know is \( X^2 + Y^2 = Z^2 \) whose solutions are *Pythagorean triples*; \((3, 4, 5), (5, 12, 13)\) are examples of such triples. If, instead, we ask for solutions, in integers, of \( X^2 + Y^2 = 3Z^2 \) we get an example of a