The story of Fermat's last theorem

In case you didn't know, Maths is fun! There have always been some people who do it for fun rather than for a living. One such was the Frenchman Pierre de Fermat (1601–1665), who amused himself throughout his life with problems in number theory. He recorded his findings either by writing letters to friends, or by making notes in the margin of his copy of the classic *Arithmetica* by Diophantus. These notes were only discovered after his death. Usually, he only gave a rough sketch of the reasoning for his assertions. Most, but not all, of them have turned out to be correct, and several of them are now recognized as important theorems. However, the most famous one of all remained an unsolved problem, tantalising mathematicians, for more than 300 years.

As we all know, there are plenty of examples of positive integers x, y, z such that $x^2 + y^2 = z^2$, for instance, $3^2 + 4^2 = 5^2$. But, try as you will, you won't find two cubes that add to another cube. More generally, Fermat claimed to know that there are *no* cases of integers x, y, z such that $x^n + y^n = z^n$ for any $n \geq 3$. He wrote in his *Arithmetica* that he "had a truly marvellous demonstration which this margin is too narrow to contain". The mathematical world took to calling the statement "Fermat's last theorem", but it was more appropriate to call it the "Fermat conjecture", since nobody knew whether it was true.

Elsewhere, Fermat did provide a sketch of a correct proof for the particular case $n = 4$. Nearly a century elapsed before there was any more progress: then Euler proved the case $n = 3$ (which, curiously, turns out to be harder than $n = 4$). Nearly another century elapsed before the ideas of Sophie Germain, Dirichlet and Lamé settled the cases $n = 5$ and $n = 7$. But none of these methods could be extended to general values of n. Cauchy thought he had seen a way forward, but Kummer demonstrated that there was a basic flaw in his approach. Kummer went on to develop methods that proved the conjecture for many more particular values of n.

In 1908 a German industrialist, Paul Wolfskehl, bequeathed a prize of 100,000 marks for a successful proof (though nothing for a disproof!). As a result, hundreds of attempts poured in, year after year, mostly from amateurs. They all turned out to contain fallacies, usually of quite an elementary nature, but sometimes quite subtle.

At last, in the 1990's, the British mathematician Andrew Wiles succeeded in giving a proof that has stood up to rigorous scrutiny by specialists in the field. But this bare statement is a gross oversimplification, both of the reliance on earlier work and of the drama of the final stages!

As with most of the big theorems in mathematics, Wiles's proof builds heavily on previous results and ideas. Indeed, part of its achievement is the way it succeeds in combining deep results from a variety of subject areas. In the 1950's, two Japanese mathematicians, Taniyama and Shimura formulated a bold conjecture, namely that "every elliptic curve over the rationals is modular" (needless to say, all the ingredients of this statement have precise definitions). A German, Gerhard Frey, had the idea that this conjecture, if true, would imply Fermat's last theorem. He got part of the way to proving this, and his proof was completed an American, Ken Ribet. But the general view was that the Taniyama-Shimura conjecture was just as hard to prove as Fermat's theorem itself.

Wiles, now at Princeton, USA, thought differently. He resolved to prove the conjecture. Furthermore, he resolved to prove it on his own, not discussing his ideas with other

mathematicians. Seven lonely years followed, including long periods without progress. But the time came in 1993 when he was confident that his proof was at last complete. Did he announce "the proof of Fermat's last theorem"? No! At a conference in Cambridge, he gave a short series of lectures with the innocuous title "Modular forms, elliptic curves and Galois representations". As the lectures progressed, people realized that important new work was being presented, but the ultimate goal was still unclear. A packed audience attended the last lecture. Keeping up the suspense, Wiles outlined an impressive array of new results, but the final conclusion remained concealed until the last moment, when Wiles quietly finished by writing "This proves Fermat's last theorem". The story spread immediately to the news media, and for once the news of a mathematical discovery appeared on the front pages of newspapers.

The next stage was for the detailed written version of Wiles's work – which was long and complicated – to be subjected to scrutiny by referees. Before long, it emerged that there was a serious snag: buried away in the detail was an unproved assumption, with no obvious remedy. The publicity had been premature! Relenting from his policy of working on his own, Wiles invited another English mathematician, Richard Taylor, to join him. Months went by without progress. Relief eventually came in the form of a sudden blinding insight: an earlier method, abandoned by Wiles some years previously, could be revived and combined with later methods to overcome the problem.

The finally approved proof appeared in 1995 in two papers in *Annals of Mathematics*, volume 141. The main paper, by Wiles only, is 109 pages long. The second one, by Taylor and Wiles, is another 20 pages; it establishes certain results essential for the main paper. Furthermore, both papers presuppose a large amount of earlier research literature before you start – the longer one has a list of 84 references. So the Wiles-Taylor proof is also a bit too long to write in the margin! It is also completely inaccessible to all but advanced specialists in a certain kind of number theory.

If Fermat really had a "truly marvellous demonstration", it was certainly nothing like this! Elliptic curves and modular forms had not been thought of at that time. Wiles has duly received the Wolfskehl prize, as well as the highest mathematical honour, the Fields Medal. But it would still be a great achievement if anyone could produce a substantially shorter and simpler proof, whether or not "marvellous".

Did Fermat really prove it? In the light the subsequent history, and of other inaccuracies in Fermat's work, it seems very likely that his alleged proof contained a fallacy, probably one of the same ones that appeared in the attempts of later people. But we will never know for sure.

Two books giving the full story are:

Fermat's Last Theorem by Simon Singh (Fourth Estate, 1997).

Fermat's Last Theorem by Amir D. Aczel (Four Walls Eight Windows, 1996).

Simon Singh also produced a rather good TV documentary on it for *Horizon*, a rare example of maths being made the subject of a TV programme.