THE ABEL PRIZE 2016

A glimpse of the Laureate's work

Alex Bellos

Fermat's Last Theorem – the problem that captured Andrew Wiles' imagination as a boy, and that he proved three decades later – states that:

> *There are no whole number solutions to the equation $x^n + y^n = z^n$ when n is greater than 2.*

The theorem got its name because the French amateur mathematician Pierre de Fermat wrote these words in the margin of a book around 1637, together with the words: "I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain." The tantalizing suggestion of a proof was fantastic bait to the many generations of mathematicians who tried and failed to find one. By the time Wiles was a boy Fermat's Last Theorem had become the most famous unsolved problem in mathematics, and proving it was considered, by consensus, well beyond the reaches of available conceptual tools.

The proof that Andrew Wiles discovered in 1994 was certainly not the one that Fermat was thinking of when he scribbled in his margin. (It is now accepted that the Frenchman was mistaken in believing he had a proof.) Wiles' work builds on two concepts that were introduced to mathematics in the eighteenth and nineteenth centuries: elliptic curves and modular forms.

An elliptic curve is an equation of the form $y^2 = x^3 + ax + b$, where a and b are constants. Mathematicians began to study these equations in order to calculate the distances planets moved along their elliptical paths. By the beginning of the nineteenth century, however, they were of interest for their own properties, and the subject of work by Niels Henrik Abel among others.

Modular forms are a much more abstract kind of mathematical object. They are a certain type of mapping on a certain type of graph that exhibit an extremely high number of symmetries.

Elliptic curves and modular forms had no apparent connection with each other. They were different fields, arising from different questions, studied by different people who used different terminology and techniques. Yet in the 1950s two Japanese mathematicians, Yutaka Taniyama and Goro Shimura, had an idea that seemed to come out of the blue: that on a deep level the fields were equivalent. The Japanese suggested that every elliptic curve could be associated with its own modular form, a claim known as the Taniyama-Shimura conjecture, a surprising and radical proposition no one had any idea how to prove.

In 1984 the German mathematician Gerhard Frey for the first time linked the truth of Fermat's Last Theorem to the truth of the Taniyama-Shimura conjecture. The theorem, as we saw above, says that there are no whole number solutions to $x^n + y^n = z^n$ when n is greater than 2. Frey showed that if you assume this statement is *false*, you can create an elliptic curve so weird that it seems to have no associated modular form. Two years later the American Ken Ribet proved that Frey's hunch was correct: if Fermat's Last Theorem is false, there is an elliptic curve that has no

associated modular form, in other words, the Taniyama-Shimura conjecture is *also* false.

Frey and Ribet's work also implied the contrapositive argument, that if the Taniyama-Shimura conjecture is true, then Fermat's Last Theorem cannot be false, which means it must also be true. From that moment, in order to prove Fermat's Last Theorem all that was needed was to prove the Taniyama-Shimura conjecture.

Still, no one knew how to achieve this feat, and there was no suggestion that it would be any easier than proving Fermat's Last Theorem. Perhaps the equivalence of the theorem and the conjecture meant that both were impossible? Andrew Wiles, a specialist in both elliptic curves - the subject of his PhD - and modular forms, had at least the right background to engage with the problem. And after eight intense years of study, Wiles proved that the conjecture was true.

Wiles's original and audacious proof is considered one of the greatest triumphs of contemporary mathematics. Its outline is as follows: each elliptic curve has a sequence of numbers that defines it, as does each modular form. Wiles showed that every sequence belonging to an elliptic curve could be exactly matched with the sequence belonging to a modular form. To do this he devised a toolkit based on the work of the 19th century mathematician Évariste Galois, who discovered the symmetries that arise from the solutions of certain equations.

Proof of the Taniyama-Shimura conjecture, a result now known as the modularity theorem, meant that Wiles had also proved Fermat's Last Theorem, thus bringing to a close a chapter of mathematical history that began 350 years previously. Yet more than settling an old and famous riddle, the impact of the modularity theorem on mathematics has been immense. Wiles demonstrated a fundamental structural connection between elliptic curves and modular forms, a rich and important result within number theory with many deep consequences. He also devised a powerful conceptual toolkit that has been used over the past two decades by other mathematicians in spectacular ways.