Sir Andrew John Wiles,
Abel Prize Laureate 2016

Hanc marginis exiguitas non caperet

”Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.”

Pierre de Fermat

(It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.)

Pierre de Fermat

This is the famous comment, written by Pierre de Fermat around 1637 in his copy of Diophantus' book Arithmetica. Fermat was a French lawyer with a passion for mathematics. The statement he refers to, known as Fermat's Last Theorem (it was not his last assertion, but the last one to be proved), or just FLT, is one of history's longest lasting puzzles, easy to formulate but equally difficult to crack. Numerous great mathematical thinkers have taken up the challenge, but for more than 350 years all attempts to find a rigorous proof of the statement have failed. However, it was not all in vain: a large amount of knowledge has been created on the roads into the many blind alleys, and on the one successful road toward the final solution.

Very few people believe that Fermat actually had a proof of the theorem. One can be fairly certain that it would have been extremely difficult or even impossible to provide a complete proof of the assertion using the mathematical tools and techniques on hand in the 17th century. Even for a brilliant mathematician like Pierre de Fermat, the proof of FLT given by Andrew Wiles would have been highly inaccessible had he been given the possibility to read it. In 1637 it would still be centuries before the concepts of elliptic curves and modular forms were to emerge.

Today Fermat's marginal comment is phrased:

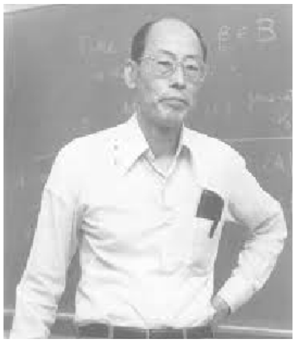
> *The equation $x^n + y^n = z^n$, where $n > 2$ has no non-trivial integer solutions.*

Notice that Fermat requires the exponent n to be greater than 2. For $n = 2$ the statement is false, since the equation $x^2 + y^2 = z^2$ has many non-trivial integer solutions, the most famous being $3^2 + 4^2 = 5^2$. But why is the statement true for $n \geq 3$? Is there a mysterious connection between powers and sums of powers? Or are there just too few integers?

Among the first 10,000 numbers there are 2,691 sums of two squares, 100 squares and 42 numbers that are both a square and a sum of squares. In contrast, there are only 202 sums of two cubes, 21 cubes and, according to FLT, none of these are sums of cubes. The two properties, being a sum of cubes and being a cube itself, are so rare that it is unlikely

that any number would be both. Nevertheless, according to Wiles' work, the reason for the lack of concurrence between powers and sums of power is much more subtle.

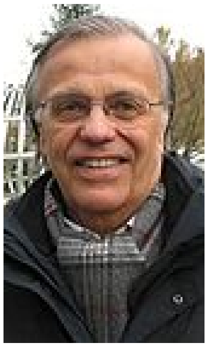
Yutaka Taniyama



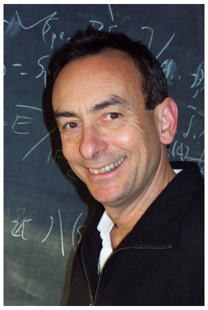
Goro Shimura

Andre Weil

In the 1950s, two young Japanese mathematicians, Yutaka Taniyama and Goro Shimura, were studying certain sequences of numbers. They considered the number of solutions of a type of equations, called elliptic curves, and compared them with specific expressions of a class of functions, called modular forms. Taniyama and Shimura discovered that the sequences of numbers were very similar and concluded that this could not be a coincidence. They conjectured that there was a deeper connection between elliptic curves and modular forms, producing two identical sequences of numbers in apparently different mathematical subfields. About 10 years later these ideas were considered in a publication by the influential French mathematician André Weil. The conjecture was promptly hailed as hot stuff, now under the name of the Taniyama-Shimura-Weil conjecture (TSW for short). In spite of numerous attempts to crack the puzzle, no one managed to come up with a proof.



Gerhard Frey



Ken Ribet

Then, in the mid 1980s, the German mathematician Gerhard Frey asserted that if TSW was true, then FLT would follow as a consequence. Frey suggested that if FLT was false, then there would exist a semi-stable elliptic curve that was not modular. However, the TSW conjecture says the opposite, that all elliptic curves are modular. So when Ken Ribet a few years later proved Frey's assertion, the only obstacle to proving FLT was to prove the TSW conjecture. Many experts considered this to be a challenge for the distant future. But Andrew Wiles dug into the problem anyway, and within the next seven years he came up with a proof. He kept his discoveries hidden from the mathematical community, but during a conference in Cambridge in the summer of 1993 there were rumours of an upcoming sensation. Tension built up, and the number of curious colleagues in the audience increased during the lecture series Wiles gave. In his final lecture he concluded that Fermat's Last Theorem had finally got a proof.