Fermat's Last Theorem, a Theorem at Last

Keith Devlin, Fernando Gouvêa, and Andrew Granville

After defying all attempts at a solution for 350 years, Fermat's Last Theorem finally took its place among the known theorems of mathematics in June of this year.

On June 23, during the third of a series of lectures at a conference held at the Newton Institute in Cambridge, British mathematician Dr. Andrew Wiles, of Princeton University, sketched a proof of the Shimura-Taniyama-Weil conjecture for semi-stable elliptic curves. As Kenneth Ribet, of the University of California at Berkeley, showed some years ago, Fermat's Last Theorem is a corollary of this result.

In the years since Fermat made his famous marginal note in his copy of Diophantus' *Arithmetica*, asserting, without proof, that equations of the form

$$x^n + y^n = z^n$$

have no integer solutions for values of the exponent n greater than 2, many mathematicians, professionals and amateurs alike, have tried to find a proof. Every few years, the newspapers report yet another purported solution, which is subsequently found to be lacking in some way.

To understand why Wiles has succeeded where so many before him have failed, one needs to know something of the recent history of the problem.

To number theorists, until the last decade the question seemed completely unassailable, despite a number of significant advances that had been made as a result of attempts to solve it, among them the 19th century work of Kummer on cyclotomic fields and ideal theory.

More recently, there was Gerd Faltings' 1983 proof of the Mordell Conjecture, which implied that for each exponent, the Fermat equation could have at most a finite number of solutions. But, despite much simpler proofs of Vojta and Bombieri, it seems unlikely that such methods can be modified to show that there really are no solutions.

Wiles' approach comes from a somewhat different direction, and rests on an amazing connection, established during the last decade, between the Last Theorem and the theory of elliptic curves, that is, curves determined by equations of the form

$$y^2 = x^3 + ax + b,$$

where a and b are integers.

The path that led to the June 23 announcement began in 1955 when the Japanese mathematician Yutaka Taniyama proposed that there should be a connection between elliptic curves and another well-understood class of curves, known as modular curves. One should be able to establish a connection between any given elliptic curve and a modular curve, and this connection would "control" many of the properties of the initial curve.

Taniyama's conjecture was made more precise in 1968 by Andre Weil, who showed how to determine the exact modular curve that should be connected to a given elliptic curve.

In 1971 the first significant evidence in favor of this abstract understanding of equations was given by Goro Shimura, a Japanese mathematician at Princeton University, who showed that it works for a very special class of equations. As a result, Taniyama's proposal eventually became known as the Shimura-Taniyama-Weil conjecture.

Additional evidence in support of the conjecture came from the fact that its nature allowed for a substantial amount of numerical testing by computer: all curves that were examined seemed to be modular.

But so far, no one knew of any connection between this very abstract conjecture and Fermat's Last Theorem. Things changed dramatically in 1986 when Gerhard Frey, from Saarbrucken, discovered a most surprising and innovative link between the two. What he realized was that if $c^n = a^n + b^n$, then it seemed unlikely that one could understand the elliptic curve given by the equation

$$y^2 = x(x - a^n)(x + b^n)$$

in the way proposed by Taniyama. Following an appropriate re-formulation by Jean-Pierre Serre in Paris, Kenneth Ribet in Berkeley strengthened Frey's original concept to the point where it was possible to prove that the existence of a counter example to the Last Theorem would lead to the existence of an elliptic curve which could not be modular, and hence would contradict the Shimura-Taniyama-Weil conjecture.

This is the point where Wiles entered the picture. Using and developing powerful new methods of Barry Mazur(Harvard), Matthias Flach (Heidelberg), Victor Kolyvagin (Steklov Institute), and others, Wiles eventually succeeded in establishing the Shimura-Taniyama-Weil conjecture for an important class of elliptic curves (those with square-free "conductors"), which includes those relevant to proving Fermat's Last Theorem.

For the Cambridge conference, Wiles had announced his lectures, a series of three given on successive days, with the highly unspecific title "Modular Froms, Elliptic Curves, and Galois Representations." Prior to his lectures, he refused to give a hint as to what they might contain. Even though, by the third talk, many in the audience had guessed he might have cracked Fermat's Last Theorem, few dreamt that he could have proved so much more, and there was an audible gasp as he wrote the final result on the black board.

Given the history of attempts to prove the Last Theorem, readers will doubtless view this latest announcement with some initial skepticism. But it should be stressed that Wiles's work is not a chain of reasoning as strong as its weakest link. Instead it is a bedrock of ideas, solid and rigid, a rich and profound theory that will hold up even if a few detail need altering. Considering the enormous complexity of this work it will, of course, take time to be absolutely certain that there are no hidden flaws, but the experts feel confident that even any necessary changes will be possible. Many of these experts were

attending Wiles' talks, and from what he said and the way he said it, they were satisfied that the techniques are, in essence, sound. The situation is a bit like building a bridge across a chasm. Most attempts to solve the Last Theorem made by amateurs are like a single span consisting of many short pieces of wire tied together. One small flaw and the entire structure collapses. Wiles' solution is much more like a solid concrete and steel bridge, erected on firm foundations laid down by many others. It may contain many small cracks, but the bridge itself still stands, and the road crew can come along later to fill in the cracks. Of course, even solidly built bridges do fall down occasionally, but the nature of Wiles' work, which involves many appreciable, profound new ideas, suggests that this is not such a bridge.

Taking the bridge metaphor a step further, one might ask what is to be found on the other side? Well, it is likely that the proof of the whole of the Shimura-Taniyama-Weil conjecture is at hand, and the consequences are breathtaking. The face of number theory will be altered in a way that we cannot even guess right now.

The story of Fermat's Last Theorem is one of the most delightful in mathematics, and if it had to finally be resolved then perhaps it was best to be as the motivation for such a startling result.

Certainly, the method used to obtain the solution is of far more importance to mathematics than the Last Theorem itself. Indeed, had it not entered the mathematical world the way it had, as a cryptic note by one of the most powerful number theorists the world has ever seen, and had it not resisted all attempts at solution for so many years, the Last Theorem would have merited little more than a footnote to textbook accounts of Pythagoras' Theorem. But the Wiles result, and the work of the many other mathematicians that paved the way, is sure to have enormous impact in many parts of mathematics.

The next issue of FOCUS will include a much more detailed account of Wiles' new proof.

The Technical Details

Shortly after Wiles finished his lecture, Dr. Kenneth Ribet, of the University of California at Berkeley, wh was in the audience, sent out the following summary to his colleagues at Berkeley, where the excitement it created led to its rapid appearance on the Internet. The message is reproduced here with his permission.

I imagine that many of you have heard rumors about Wiles's announcement a few hours ago that he can prove Taniyama's conjecture for semistable elliptic curves over Q. This case of the Taniyama conjecture implies Fermat's Last Theorem, in view of the result that I proved a few years ago. (I proved that the "Frey elliptic curve" constructed from a possible solution to Fermat's equation cannot be modular, i.e., satisfy Taniyama's Conjecture. On the other hand, it is easy to see that it is semistable.

The method of Wiles borrows results and techniques from lots and lots of people. I mention a few: Mazur, Hida, Flach, Kolyvagin, yours truly, Wiles himself (older papers by Wiles), Rubin… The way he does it is roughly as follows. Start with a mod p representation of the Galois group of Q which is known to be modular. You want to prove that its lifts with a certain property are modular. This means that the canonical map from Mazur's universal deformation ring to its "maximal Hecke algebra" quotient is an isomorphism. To prove a map like this is an isomorphism, you can give some sufficient conditions based on commutative algebra. Most notably, you have to bound the order of a comology group which looks like a Selmer group for Sym^2 of the representation attached to the modular form. The techniques for doing this come from Flach; and then the proof went on to use Euler systems a la Kolyvagin, except in some new geometric guise.

If you take an elliptic curve over Q , you can look at the representation of Gal on the 3-division points of the curve. If you're lucky, this will be known to be modular, because of results of Jerry Tunnell (on base change). Thus, if you're lucky, the problem I described above can be solved (there are most definitely some hypotheses to check), and then the curve is modular. Basically, being lucky means that the image of the representation of Galois on 3-division points is GL(2,Z/3Z) .

Suppose that you are unlucky, i.e., that your curve E has a rational subgroup of order 3. Basically by inspection, you can prove that if it has a rational subgroup of order 5 as well, then it can't be semistable. (You look at the four non-cuspidal rational points of $X_0(15)$.) So you can assume that E[5] is "nice." Then the idea is to find an E' with the same 5-division structure, for which E'[3] is modular. (Then E' is modular, so E'[5] = E[5] is modular.) You consider the modular curve X which parameterizes elliptic curves whose 5-division points look like E[5] . This is a twist of X(5) . It's therefore of genus 0, and it has a rational point (namely, E), so it's a projective line. Over that you look at the irreducible covering which corresponds to some desired 3-division structure. You use Hilbert irreducibility and the Cebotarev density theorem (in some way that hasn't yet sunk in) to produce a non-cuspidal rational point of X over which the covering remains irreducible. You take E' to be the curve corresponding to this chosen rational point of X.

-Ken Ribet, June 23, 1993, Cambridge, England

Dr. Andrew Granville, of the University of Georgia, spent the last six months at the Newton Institute at Cambridge, and attended the lectures at which Wiles sketched his new proof. Dr. Fernando Gouvêa, a collaborator with, and former student of, Mazur, is on the faculty at Colby College. Dr. Keith Devlin is the Dean of Science at Saint Mary's College of California, and the editor of FOCUS