Progress on Fermat's Famous Math Problem

One of the most famous unsolved problems in mathematics is now placed firmly in the mainstream of modern math

For 300 years, mathematicians have struggled to solve a seemingly simple conjecture. The problem, known as Fermat's last theorem, stood just outside the mainstream of mathematics research, however, and the powerful tools that mathematicians have developed to deal with other problems were useless against it.

Now, following an intensive bout of research by an international group of mathematicians, Fermat's last theorem has been shown to depend on a "structural conjecture" in number theory. This conjecture has to do with theories that have been developed extensively over the last 30 years. As a consequence, Fermat's theorem has been removed from its position as an isolated possibility and now is viewed as just another consequence of a very general statement giving deep insight into an extensive network of mathematical objects. "There are now very good reasons to believe Fermat's last theorem," says Barry Mazur of Harvard University.

The result is particularly significant, mathematicians say, because it means that Fermat's theorem can also give insight into the structural conjecture, which is central to modern number theory. In addition, although it will make no difference to the body of mathematics whether the actual Fermat theorem is proved true or false, the equations that make up Fermat's last theorem are turning out to be immensely important. Number theorists now realize that these equations are intimately related to major problems. So there have been good reasons why mathematicians have worked on the Fermat equations.

Although Fermat's last theorem had appeared until recently as an isolated problem, it has a long history of inducing mathematicians to develop other theories in order to solve it. It has also captured the imagination of math hobbyists. Math departments throughout the country regularly get false proofs of it from amateur mathematicians.

Pierre Fermat, a 17th-century French judge and mathematician, proposed his last theorem in a casual way. He wrote the theorem in the margin of a book and noted also that he had a marvelous proof of it. But, he wrote, the margin, unfortunately, was too small for him to give any details.

Fermat's marginal note was discovered after his death but, although mathematicians searched his papers for the proof, they never found it. Ever since, the theorem has stumped countless mathematicians and has become one of the most famous unsolved problems in the history of mathematics. Some mathematicians said it was an unimportant problem anyway and a waste of their time to work on it. Others deluded themselves into thinking they had proved it. Still others gave up in frustration.

"There are now very good reasons to believe Fermat's last theorem."

Historians of mathematics believe that Fermat got the idea for his theorem when he read a French edition of a Greek text by Diophantus. He came to a section in which Diophantus stated the Pythagorean theorem—the fact that the sum of the squares of two sides of a right triangle equals the square of the hypotenuse. Diophantus noted that there are whole numbers x, y, and z for which the equation $x^2 + y^2 = z^2$ is true. For example, $3^2 + 4^2 = 5^2$.

So Fermat suggested a variation of Diophantus' statements. Although there are infinitely many solutions to the Pythagorean equation, Fermat wrote, he has a wonderful proof that there are no solutions to the equation $x^n + y^n = z^n$ when n is greater than 2.

It is, says Mazur, "a very strange conjecture. No one can reconstruct Fermat's proof and no one can find a counterexample." In fact, Mazur adds, mathematicians cannot even decide why the theorem is important.

Nonetheless, it intrigued many mathematicians, although it irritated others. Fermat himself proved that it is true for n equal to 3. And in the early 18th century, Karl Friedrich Gauss, one of the giants in the fields of mathematics and physics, was goaded by his colleagues into working on the problem. He showed it is true for n equal to 4 but failed to solve it in general. The Paris Academy offered a prize for a proof of the theorem, but Gauss wrote that it was not a problem he wanted to work on, adding that it is of virtually no importance to the rest of mathematics. "I confess that Fermat's theorem as a problem has very little interest for me, because I could easily lay down a multitude of such propositions, which one could neither prove nor dispose of," he wrote.

In the 19th century, the German mathematician Ernst Edward Kummer did much of his best work on problems related to Fermat's last theorem but Kummer did not regard the theorem itself as important. Fermat's theorem, he said, "is to be sure more a curiosity than a pinnacle of science."

In 1908, another German, P. Wolfkehl, offered what was at the time a very large sum of money to anyone who proved the theorem. He specified that before the money is paid out, the proof must be published and its veracity ascertained by the German academy of sciences in Göttingen. Wolfkehl's prize fell in value to almost nothing in the post–World War I inflation, much to the delight of those who regarded the theorem as a joke, but it now has risen in value again and is worth DM 10,000 or about $5,500. Curiously enough, the prize is only to be awarded for a proof that the theorem is true—nothing is to go to a person who proves it false.

Yet at the same time that some mathematicians expressed doubts that the theorem was worth their while to work on, they got a series of partial results. In 1983, Gerd Faltings, who is now at Princeton University, resolved the Mordell conjecture, an outstanding problem in number theory and, as a direct consequence, showed that if there are any solutions to Fermat's equations, there are only a finite number of them for each exponent. Samuel Wagstaff of Purdue University and Jonathan Tanner of the University of Pennsylvania showed, using a computer, that the theorem is true for, exponents n up to 150,000.

But, of course, none of these partial results says much about the theorem in general. Even if there are no more than a finite number of solutions for each exponent, it takes only one solution to disprove Fermat's theorem. And even though the theorem is true for n up to 150,000 it is very conceivable that if it were false, it would be false for much larger numbers than 150,000.

The current program to reduce Fermat's last theorem to the structural conjecture had its beginning a few years ago when Gerhard Frey of the University of the Saarlands in Germany began looking at what he describes as "very simple equations" for elliptic curves—a category of curves that are of

great interest to mathematicians because they provide ways of resolving a number of difficult problems. Frey says that he was not thinking of Fermat's theorem when he began his work. In fact, he says, "I never was very interested in Fermat's theorem."

So Frey started with a solution to a very simple equation. The equation was $a + b = c$, where a, b, and c are integers. Then he attached to this solution an elliptic curve, which is, in general, an equation of the form $y^2 = x^3 + c_2x^2 + c_1x + c_0$, where c_0, c_1, and c_2 are constants. In this case, Frey's equation was $y^2 = x(x - a)(x - c)$. At this point, says Frey, he realized that what he was doing had some connection with Fermat's last theorem. "It was easy to translate Fermat's last theorem into a conjecture about elliptic curves."

To do this, Frey supposed that Fermat's theorem is false—that there is a number, say it is a prime number p, and integers a, b, and c, for which $a^p + b^p = c^p$. The associated elliptic curve is $y^2 = x(x - a^p)(x - c^p)$. Now, Frey remarks, Fermat's last theorem is in the domain of elliptic curves, where there are "a lot of conjectures and a lot of tools. The problem with Fermat's theorem has been that there was no mathematical structure to help you deal with it."

But once Frey wrote down the elliptic curve that would follow if Fermat's theorem were false, he and others who studied it were struck by how peculiar it was. Kenneth Ribet of the University of California at Berkeley explains, "if you know anything about elliptic curves and you start studying that one, you notice that it has some peculiar properties." The curve "is a little bizarre. It makes you feel a little queasy," Ribet remarks. It is so strange, in fact, that your instincts will tell you that it "shouldn't exist," Ribet says.

This meant that if it could be proved that the curve in fact could not exist, then Fermat's theorem could not be false. It would therefore be proved true.

Frey began to work on this new approach to Fermat's theorem. He started by viewing the surface of solutions of the elliptic curve associated with the Fermat equations. This surface looks like the surface of a doughnut with one point removed. Then he assumed a standard conjecture that says that if this elliptic curve exists, its doughnut-shaped surface can be covered in a special way by the upper half of the complex plane. It is as though the sheet of the half plane can be wrapped around the doughnut in a particular way that preserves angles and certain mapping functions.

Now Frey could begin to compute what doughnuts there are that can be covered by the upper half plane in this way. The idea is to show that the doughnut that comes from the elliptic curve derived from Fermat's theorem cannot exist. If that were so, then the curve cannot exist. And if that were so, then the solution to the Fermat equations cannot exist. And if no solution could exist, then Fermat's last theorem is true.

It looked very promising, but Frey could not quite fill in all the gaps in his proof. On New Year's Day in 1985, at a conference in Germany, he presented his manuscript to the mathematical community, confident that others could help him complete the argument. "He was hoping people would tell him that the facts he needed were known," Ribet explains. Instead, that mathematicians told him that it was an interesting argument but that the facts are not known.

Yet mathematicians felt that somehow they could patch up the proof. Many had ideas, but nothing seemed to do the trick. Then Jean-Pierre Serre, of the College of France in Paris, pointed out that Frey's ideas meshed very well with a variety of conjectures that he had made, some of which were so strong that if they could be proved true, Fermat's last theorem would automatically follow, independent of the standard conjecture on which Frey made it hang. Serre's weakest conjecture, which he called epsilon—the mathematical symbol for a very small quantity—would complete Frey's argument and would show that Fermat's theorem follows from the standard conjecture.

Despite its belittling name, neither Serre nor anyone else could prove epsilon. Finally, Ribet did it with what Mazur describes as a "beautiful idea." Ribet has lectured on his result at Berkeley and has passed out his manuscript to numerous colleagues. Although his manuscript has met with favorable responses, Ribet still demurs a bit when he is asked about his proof. "It is a very complicated argument and it uses a lot of heavy machinery that few have studied very carefully," he explains. For now, Ribet is "telling mathematicians I believed I've proved it. But when I do this, I push a manuscript into their hands and say I would really like to have their comments."

Mazur explains that the structural conjecture in number theory, to which Fermat's theorem is now tied, is like the keystone of a cathedral. "Important intuitions in number theory depend on it and there are very convincing reasons to believe it is solid. In contrast, Fermat's last theorem is an ornament like a glass sliver in a chandelier inside the building."

According to Ribet, there previously was "no philosophical evidence" for Fermat's theorem. The tie to the structural conjecture means that the theorem "is now a consequence of something people feel *must* be true. It is linked with something people really believe."

Bettmann Archive

Pierre Fermat *wrote that the margin of the book was too small for his proof.*

The result, of course, still depends on the truth of the standard conjecture. So the question is, How reasonable is that conjecture? Number theorists say they have deep and convincing reasons to believe it, although they have no proof that it is true. "There is no practitioner who doesn't assume it from time to time. By now, if one is in the field, it is in one's central nervous system," Mazur says. If someone were to come up with a proof that the conjecture is wrong, says Ribet, "it would be a real shocker. The flag would be at half-mast at mathematics centers."

Fermat, however, could not have known of the standard conjecture and certainly could never have devised a proof like the one put forth by Frey, Serre, and Ribet. Did he have some other, simpler, proof? Mathematicians think not. Instead, they believe he made an understandable error and thought that algebraic integers, which are solutions to algebraic equations, have a prime number factorization theorem like the ordinary integers do. If that were the case, Fermat would have had a "proof." But the proof would have broken down by the time he got to exponent 23. Mathematicians assume he never got that far.

In the end, not only does the standard conjecture bear on Fermat's theorem, but Fermat's theorem also says something about the standard conjecture. Since the conjecture now makes very concrete predictions about equations, mathematicians can begin to test it in new ways. The story of Fermat's last theorem, then, does not end with this proof. It may have barely begun. ■

GINA KOLATA