A Taylor-made Plug for Wiles' Proof

Nigel Boston

Nigel Boston obtained his undergraduate degree at Cambridge University and his Ph.D. at Harvard under the direction of Barry Mazur. After a year in Paris and two years at Berkeley, he moved to Urbana, Illinois, in 1990. He has been there ever since, except for six months back in Cambridge, during which Wiles dropped his bombshell. Boston has been picking up the pieces ever since, some of which are presented here.

The aim of this article is to give undergraduates and their teachers some information with which to better understand the recent events regarding Fermat's Last Theorem. It is a problem that has tantalized amateurs and professionals alike for more than 350 years, that has led to the development of a lot of mathematics, and that has fooled many people into thinking they have solved it. In June 1993, Professor Andrew Wiles of Princeton University announced at a conference in Cambridge, England, that he had indeed managed to solve it. Because of the stature of the mathematicians involved and because of the solid methods used, many believed that a correct proof had finally been discovered. Over the months, however, doubts crept in and a gap was finally announced in November 1993. Then in October 1994, out of the blue, two manuscripts were released to the mathematical community. The longer one was in large part what Wiles had originally done, with a change towards the end, allowing him to complete the argument using the second manuscript, which is joint work with Richard Taylor. Over the ensuing months, the proof has been examined by many people and has held up to this intense scrutiny.

In this article I discuss the history of the problem, the modern attack on it via elliptic curves and modular forms, what Wiles' approach has been, and what he has accomplished. I hope to put the reader in a position to understand what all the furor has been about and to judge the final outcome. For further details, the interested reader should consult Gouvêa [1], Ribet [2], or Rubin and Silverberg [3].

History

Over the centuries many people have studied Pythagorean triples, that is, triples (x, y, z) of positive integers such that $x^2 + y^2 = z^2$. The example $3^2 + 4^2 = 5^2$ is commonly used in word problems to make sure the numbers come out nicely. The example $4961^2 + 6480^2 = 8161^2$ was known to the Babylonians around 1500 B.C.

All such triples can be described. If (x, y, z) is a Pythagorean triple, so is (dx, dy, dz) for any positive integer d, so it is enough to find a procedure that generates the *primitive* Pythagorean triples—those whose greatest common divisor is 1. The process is briefly as follows. At least one of x and y is even, say x. Write $(x/2)^2 = (z^2 - y^2)/4 = [(z + y)/2][(z - y)/2]$ and then use the fact (a consequence of unique factorization) that if two positive integers have no common factor and their product is a square, then both integers are squares. This leads to $x = 2rs$, $y = r^2 - s^2$, $z = r^2 + s^2$, where r and s are integers. All primitive Pythagorean triples are obtained by plugging in values of r and s.

About 1637, Pierre de Fermat wrote in the margin of his copy of Diophantus' *Arithmetica* that he had a wonderful proof that $x^n + y^n = z^n$ has no solutions in positive integers if $n > 2$ but that the margin was too small to hold the proof. Some people believe he really had a proof, but in his later correspondence regarding the cases $n = 3, 4$ he never refers to it. If he had been mistaken in his claim, would he have bothered to cross out his marginal scribbling? He certainly could not have foreseen that shortly after his death his son would publish it in Fermat's collected works and that countless mathematicians would fret over it for years to come.

Fermat himself handled the case of $n = 4$. He showed in fact that $x^4 + y^4 = z^2$ has no solutions in positive integers by noting that (x^2, y^2, z) is then a Pythagorean triple, by applying the above parametrization of such triples twice, and by thus obtaining a solution of the original equation with smaller z. But suppose we started with the solution with smallest z! This contradiction provides the first example of what is now known as the *method of infinite descent*.

This reduces the problem to the case where n is an odd prime, since every $n > 2$ is divisible by 4 or an odd prime, and if n is divisible by m, then an nth power is certainly an mth power. The case of $n = 3$ was done by Euler around about 1753, although he left out some details. Gauss gave the first complete proof. The idea is to write $x^3 = z^3 - y^3 = (z - y)(z - \omega y)(z - \omega^2 y)$, where ω is a complex cube root of 1. Because the collection of polynomials in ω with integer coefficients has a unique factorization property, the equation is solved by proceeding as with the Pythagorean triples.

In general, we would like to proceed by writing $x^n = \prod_i (z - \zeta^i y)$, where ζ is a complex nth root of 1, but the collection of polynomials in ζ with integer coefficients does not always have the desired unique factorization property. In 1847, Lamé announced to the French academy that he had proved Fermat's Last Theorem, but he had overlooked this particular trap. Shortly thereafter, Kummer showed that enough is true for Fermat's Last Theorem to hold for *regular* prime exponents p, i.e., ones that do not divide the numerators of any of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$. These numbers are defined by $x/(e^x - 1) = \sum B_n x^n/n!$. For instance, $B_{12} = -\frac{691}{2730}$, so 691 is not regular.

Since then, many ingenious ways have been found to prove Fermat's Last Theorem for various other values of n, but not for all n. So far it has definitely been proven for all $n < 4{,}000{,}000$. This sounds very convincing until you realize, for instance, that $x^4 + y^4 + z^4 = t^4$, which was conjectured by Euler to have no solutions in positive integers, defied computer attacks until 1987, when Noam Elkies discovered that it has infinitely many (unproportional) solutions. Its smallest solution is $95800^4 + 217519^4 + 414560^4 = 422481^4$. The next stage of our story is to forge a link with geometry which makes the existence of a counterexample to Fermat's Last Theorem very doubtful.

Elliptic Curves

Let f be a cubic polynomial with integer coefficients and with distinct roots. The equation $y^2 = f(x)$ defines an *elliptic curve* E (so named because they arise in computing the arc length of an ellipse). If K is any field, we can consider the set $E(K) = \{(x, y) \in K^2 : y^2 = f(x)\} \cup \{\infty\}$, where we simply throw in an extra point ∞. Figure 1 shows $E(\mathbf{R})$ in the case $f = x^3 - x$.

The point ∞ should be thought of as joining together the two ends going to infinity so that $E(\mathbf{R})$ is actually a union of two circles. This sits inside $E(\mathbf{C})$ ($\mathbf{C}$

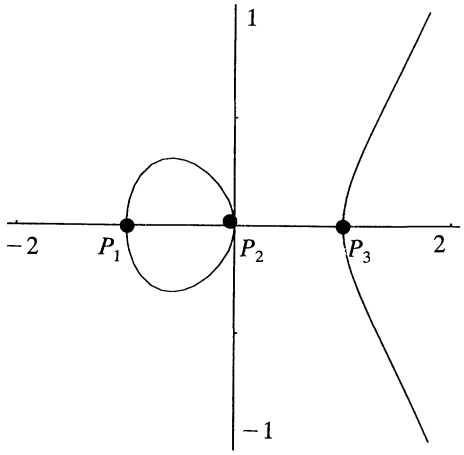

Figure 1

being the complex numbers), which is in fact topologically a torus, i.e., a product of two circles. Since you can add two points on a circle (by adding angles) to get another point on the circle, the torus has a similar rule of addition; that is, it is a *group*. This rule works for all $E(K)$, so that they are also groups. The rule is that ∞ is the zero for this addition and that $P+Q+R$ is zero if and only if P, Q, R are collinear. The tangent at a point is considered to intersect the curve twice there, so if P_1, P_2, P_3 are the three points where the tangent line is vertical then P_i, P_i, ∞ are collinear, and hence $2P_i$ is zero.

For n a positive integer, let $E[n] = \{P \in E(\mathbf{C})\colon nP = 0\}$, a subgroup of $E(\mathbf{C})$. For instance, $E[2] = \{\infty, P_1, P_2, P_3\}$. Since the group of points P of the circle such that $nP = 0$ is isomorphic to $\mathbf{Z}/n$, the integers modulo n (think of clock arithmetic), it follows that $E[n]$ is isomorphic to the product of $\mathbf{Z}/n$ with itself.

A complex number is called *algebraic* if it is a root of a polynomial with rational coefficients; for example, $\sqrt{2}$ is algebraic but π is not. The algebraic numbers form a field, and we let $G_{\mathbf{Q}}$ denote the group of all automorphisms of this field (i.e., maps from the field to itself respecting the field operations). For example, complex conjugation is in $G_{\mathbf{Q}}$. In fact, $G_{\mathbf{Q}}$ is a complicated, infinite group, whose structure we would love to understand better, because this would allow us to solve many problems in number theory.

Points in $E[n]$ have coordinates that are algebraic numbers, and applying any map in $G_{\mathbf{Q}}$ to these coordinates produces another element of $E[n]$. We therefore have, for each n, a map $\rho_n\colon G_{\mathbf{Q}} \to \mathrm{Aut}(E[n])$, the group of automorphisms of $E[n]$, which is isomorphic to $GL(2, \mathbf{Z}/n)$, the group under multiplication of invertible 2-by-2 matrices with entries in $\mathbf{Z}/n$. This is an example of a *Galois representation*, the key object of study by Wiles, Kenneth Ribet, and others.

The way elliptic curves and their Galois representations enter the picture is via a 1985 observation of Gerhard Frey. Suppose Fermat's Last Theorem is false. Then there is an odd prime p and integers u, v, w with no common factor, such that $u^p + v^p + w^p = 0$. (Set, e.g., $p = n$, $u = x$, $v = y$, $w = -z$.) By relabeling, if necessary, we can arrange for u to be one less than a multiple of 4 and v to be even. The Frey elliptic curve is defined to be $y^2 = x(x - u^p)(x + v^p)$. The fundamental idea behind the attack via elliptic curve theory, due to Frey, is to show that the Frey curve associated to a counterexample to Fermat's Last Theorem would have

such peculiar properties that its existence would lead to a contradiction. The curve, and thus the counterexample to Fermat's Last Theorem, then cannot exist!

Now, there are other ways to produce Galois representations ρ: $G_{\mathbf{Q}} \to GL(2, \mathbf{Z}/n)$. They are produced, for instance, by certain kinds of so-called modular forms. A representation produced this way is called *modular*. Elliptic curves E for which the associated Galois representations ρ_n are all modular are then said to be *modular* elliptic curves. (Modular elliptic curves can also be characterized as those elliptic curves that can be parametrized by certain modular functions.) In 1955, Yutaka Taniyama conjectured the statement (later put on a solid footing by Goro Shimura) that *all elliptic curves E defined over the rational numbers are modular*, and despite much investigation, no counterexamples to this conjecture have been found.

In 1986, Ribet considered the possible "types" of modular form that could produce a given representation ρ. He showed that if the Galois representation ρ_p for the Frey curve were modular, then it would be possible to produce it using a modular form of "type" $(2, 2)$. But there are no modular forms of this type, so Frey's curve cannot be modular! Frey's curve, if it exists, would constitute a counterexample to the Taniyama-Shimura conjecture.

Ribet's work was the first to show that a counterexample to Fermat's Last Theorem would violate some qualitative principle. This now provided the impetus for Wiles, an expert in elliptic curves and modular forms, to begin his eight years of secretive work in his attic, trying to prove a strong enough form of the Taniyama-Shimura conjecture to include Frey's curve, and thus reach the contradiction that would prove Fermat's Last Theorem.

Wiles' Work

In 1993, Wiles showed that for certain elliptic curves E (in particular, he thought, for the Frey curve), if the associated Galois representation ρ_3 is an onto map, then E is modular. He originally had a problem reaching the same conclusion in all the cases when ρ_3 is not onto, but he had his work typed up in May 1993 (with the amusing typo "Fermat's lost theorem"), sent it off to be checked by a few trusted people, and only then realized the trick that would take care of the remaining cases.

The idea (following Barry Mazur) is to fix an elliptic curve E and a positive integer m and to consider representations σ: $G_{\mathbf{Q}} \to GL(2, \mathbf{Z}/3^m)$, which on composition with the natural map (reducing matrix entries modulo 3) $GL(2, \mathbf{Z}/3^m) \to GL(2, \mathbf{Z}/3)$ yield the ρ_3 associated to E. For example, the ρ_{3^m} produced by E is such a representation. Among these representations will be modular ones and ones produced by elliptic curves. These two types share certain features, which are taken to define *admissible* σ. Pictorially,

$$\{\text{modular } \sigma\} \subseteq \{\text{admissible } \sigma\}$$

$$\subseteq$$

$$\{\sigma \text{ from elliptic curves}\}$$

Wiles' idea is to show that every admissible σ is in fact modular, so that in particular the ρ_{3^m} produced by E is modular. If this holds for all m, then in fact E is modular and we are done.

The result that the set of modular σ actually equals the set of admissible σ is reduced by some clever commutative algebra to proving an inequality, namely that the size of a so-called Selmer group related to the curve is at most a number coming from a special value of a so-called L-function related to the curve. Number theorists have had much experience with inequalities of this kind arising in other contexts and have a general conjecture covering them all, called the Bloch-Kato conjecture. Progress on this conjecture is being made steadily. This explains why, after the gap was announced, the proof was still regarded by some as close to being done. Of course, over the eight years, Wiles developed ingenious tools to attack this case of the conjecture, tools he thought sufficient for the job, but in any case tools that will be very useful for mathematicians in years to come. A 1991 preprint of Matthias Flach seemed to hold the key, and Wiles expertly generalized Flach's so-called Euler systems, but the gap apparently doomed this approach. In early 1994, he doubled back to an earlier idea of showing that certain rings are so-called complete intersection rings and, with the help of Taylor, completed the proof.

The Status

Wiles gave a course in Princeton in the spring of 1993, in which he announced his proof. Unfortunately, all but Nicholas Katz had dropped the course and so were not there to witness that historic moment! Katz and other confidants looked through Wiles' work and believed enough of it for him to go public. On June 23, 1993, at the Newton Institute in Cambridge, England, to a packed audience, most of whom had been tipped off about the amazing developments in his lectures the previous two days, as cameras flashed, Wiles announced that he had proven Fermat's Last Theorem. The next week at the Institute was far from normal. We were assailed by cameramen, requests for interviews, phones ringing off the hook, and celebrations.

It appeared that Wiles hoped to have a manuscript ready for public viewing in the fall. He submitted his work to *Inventiones Mathematicae*, and a team of referees began to pick it apart. Some errors were found and taken care of. Then rumors of an unfixable gap started circulating and in November 1993 Wiles officially confirmed this.

Some events have clouded the water. Marilyn vos Savant of "Ask Marilyn" fame wrote a book in three weeks, misleadingly claiming to have consulted leading mathematicians in the field and coming up with reasons why the proof is false based more on her lack of understanding of the area than on fact. Wiles was asked to model for another kind of Gap (jeans; he declined) and appeared in *People* magazine's 1993 end-of-year issue as one of the 25 most intriguing people of the year. Around April 1, 1994, hoaxes appeared saying that Elkies had found a counterexample and that Wiles' graduate students had fixed the gap.

In the spring of 1994, Wiles gave a series of talks at Princeton on his work. He did not get into the details of the proof, but at least produced Chapter 1 of his paper. At the same time, his former student Taylor, now a lecturer at Cambridge University, was visiting Princeton. Thus began their joint effort, culminating in the release of the manuscripts on October 25, 1994. The manuscripts have been submitted to the *Annals of Mathematics* for publication and have been received with enthusiasm by the experts, who have yet to find fault with them. In fact, this new approach is shorter than the old and many further improvements have been suggested recently. Thus there is hope that at long last a reasonably concise, albeit advanced, proof of Fermat's Last Theorem will soon be available.

References

1. Fernando Gouvêa, "A marvelous proof," *American Mathematical Monthly* 101:3 (1994) 203–222.
2. Kenneth Ribet, Galois representations and modular forms, *Bulletin of the American Mathematical Association* 32 (1995) in press.
3. Karl Rubin and Alice Silverberg, A report on Wiles' Cambridge lectures, *Bulletin of the American Mathematical Society* 31:1 (1994) 15–38.

———o———

A Prophet in his Own Land

"At first I thought I was just being slow," Wiles said. "It can be very hard to tell at first whether you're just being blind to something or whether there really is an obstacle—it's very hard to tell the difference.... There are people who have spent 30 years on one problem. You get caught in problems, trapped in them. I knew the danger, psychologically.... I was very tired,... I'd been working very hard, and I needed someone to check every statement I made.... I wanted to make sure that I had completely explored the ideas that I had and that I hadn't missed something obvious."

...

"I was sitting at my desk one morning really trying to pin down why the Flach method wasn't working when, in a flash, I saw that what was making it not work was exactly what would make a method I'd tried three years before work. It was totally unexpected. I didn't quite believe it." He dashed down from the attic to tell his wife. Although his enthusiasm was infectious, Dr. Wiles said, "I actually think she didn't believe me."

—Gina Kolata, How a gap in the Fermat proof was bridged, New York Times, January 31, 1995, pp. C1, C9.