NEWS ITEM FOR THE "NOTICES OF THE AMERICAN MATHEMATICAL SOCIETY"

Kenneth A. Ribet

Suppose that p, u, v, and w are integers, with $p > 1$. If $u^p + v^p + w^p = 0$, then $uvw = 0$.

Professor Andrew Wiles of Princeton University deduced this form of Fermat's Last Theorem at the conclusion of a series of three lectures during the June, 1993 workshop on Iwasawa theory, autmorphic forms, and p-adic representations at the Isaac Newton Institute for Mathematical Sciences in Cambridge, UK. Wiles had given his series a suggestive, but ambiguous, title—"Elliptic curves, modular forms, and Galois representations"—so that the audience had little inkling how the lectures would conclude. Persistent rumors had been circulating for days; the tension mounted as the series proceeded. The third lecture was attended by more than sixty mathematicians, a fair number of them carrying cameras to record the event.

In this last lecture, Wiles announced that he had proved Taniyama's conjecture—an enormously important conjecture in arithmetical algebraic geometry—for a large class of elliptic curves over $\mathbb{Q}$. These are the so-called "semistable" elliptic curves, those with square-free conductor. Most people in the audience knew that Fermat's Last Theorem would be a consequence of this result. Although Fermat's Last Theorem holds great fascination for amateurs and professionals alike, the Taniyama conjecture is ultimately of much greater significance for modern mathematics.

Yutaka Taniyama's conjecture, to the effect that every elliptic curve over $\mathbb{Q}$ is modular, was first proposed in somewhat tentative form at the Tokyo-Nikko conference in the mid 1950s. Its statement was refined through the efforts of G. Shimura and A. Weil; it has been known, variously, as Weil's conjecture, the Shimura-Taniyama conjecture, and so on. In its usual formulation, this conjecture associates objects of representation theory (modular forms) to objects of algebraic geometry (elliptic curves). It states that the L-series of an elliptic curve over $\mathbb{Q}$, which measures the behavior of the curve mod p for all primes p, can be identified with an integral transform of the Fourier series derived from a modular form. Taniyama's conjecture is a particular case of the "Langlands philosophy," a web of interrelated conjectures made by R. P. Langlands and his colleagues.

Although the Langlands conjectures require a substantial background in automorphic forms, Taniyama's conjecture has been rephrased in such a way that only complex-analytic maps appear [7]. One considers elliptic curves over $\mathbb{Q}$ up to $\overline{\mathbb{Q}}$-isomorphism: they are those compact Riemann surfaces of genus one which may be defined by polynomial equations with *rational* coefficients. Taniyama's conjecture states that for each such surface S, there is a congruence subgroup Γ of $\mathbf{SL}(2, \mathbb{Z})$ and a non-constant analytic map $\Gamma\backslash\mathcal{H} \to S$, where $\mathcal{H}$ is the complex upper half-plane.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

The Fermat-Taniyama connection grew out of a 1985 Oberwolfach lecture by G. Frey, who pointed out that a non-trivial solution to $a^p + b^p = c^p$ (with p an odd prime) permits one to write down a semistable elliptic curve which does not appear to satisfy Taniyama's conjecture [2, 3]. Frey's curve is the elliptic curve E given by the deceptively simple cubic equation $y^2 = x(x - a^p)(x + b^p)$. (It might be necessary to effect a preliminary adjustment of (a, b, c) before writing down the curve.) In a manuscript which he distributed in Oberwolfach, Frey outlined an incomplete proof that his curve was not modular, i.e., that one has the implication "Taniyama $\Rightarrow$ Fermat." He expected that his proof would be completed by experts in the theory of modular curves.

Frey begins with the observation that once E is modular, so is its group $E[p]$ of p-division points. This means that $E[p]$, viewed as an algebraic group over $\mathbb{Q}$, can be embedded in the Jacobian of the algebraic curve over $\mathbb{Q}$ canonically associated with an appropriate quotient $\Gamma\backslash\mathcal{H}$. A pair of conjectures, which Serre formulated after learning of Frey's construction, imply then that $E[p]$ is associated with a specific congruence subgroup $\Gamma_0(2)$ of $\mathbf{SL}(2, \mathbb{Z})$ (see [10, 11]). This is absurd because the Jacobian of $\Gamma_0(2)\backslash\mathcal{H}$ is zero.

In Serre's conjectures, I recognized a generalization of a problem that I had formulated while reading B. Mazur's article [5]. I succeeded in proving the conjectures in July, 1986, approximately one year after they were made [8, 9]. My announcement that I had proved "Taniyama $\Rightarrow$ Fermat" convinced the mathematical community that Fermat's Last Theorem must be true: we all expected that Taniyama's conjecture would someday be a theorem. It was generally accepted, however, that a proof of Taniyama's conjecture was far from imminent.

Oblivious to the received idea that Taniyama's conjecture was inaccessible, Wiles began working on his proof as soon as he learned that Fermat was a consequence of the conjecture. The proof would ultimately incorporate results and techniques from his previous works (including joint articles with J. Coates and with Mazur), and from the publications of G. Faltings, R. Greenberg, H. Hida, V. Kolyvagin, Mazur, K. Ribet, K. Rubin, J. Tilouine, to cite just a few names. A major stumbling block for Wiles was removed after he received a preprint by M. Flach (see [1]).

The following paragraphs outline the proof that Wiles sketched in his Cambridge lectures. The details of the proof are contained in a 200-page manuscript, which Wiles intends to release to the mathematical public in the coming weeks.

To show that a semisimple elliptic curve $E/\mathbb{Q}$ is modular, Wiles fixes an odd prime ℓ, which in practice is taken to be 3 or 5. Associated to E is the ℓ-adic representation $\rho_\ell\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}(2, \mathbb{Z}_\ell)$ gotten by considering the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the ℓ-power division points of E. (For background, the reader may consult any of the recent texts on elliptic curves, such as [12].) The elliptic curve E satisfies Taniyama's conjecture if and only if ρ_ℓ is "modular" in the sense that it is associated to a weight-two cuspidal eigenform in the usual way. The representation ρ_ℓ "looks and feels" modular in that it has the right determinant and satisfies some necessary local conditions at ℓ and other ramified primes.

Roughly speaking, Wiles proves that a representation like ρ_ℓ is modular if it "looks and feels" modular and reduces mod ℓ to a representation $\overline{\rho}_\ell\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}(2, \mathbb{F}_\ell)$ which is (1) surjective and (2) itself modular. Condition (2) means that $\overline{\rho}_\ell$ lifts to *some* representation which is modular; in other words, we want ρ_ℓ to be congruent to some modular representation. (In many cases, we can replace "surjective" by "irreducible" in studying $\overline{\rho}_\ell$.)

Wiles's argument is couched in the language of Mazur's deformation theory [6]. Wiles considers deformations of a representation $\overline{\rho}$ satisfying (1) and (2), restricting his attention to those deformations that could plausibly be related to cusp forms of weight two. (He requires the determinant of the deformation to be the cyclotomic character, and imposes a local condition at the prime ℓ. For example, if $\overline{\rho}$ is supersingular, he demands that the deformation be associated with a Barsotti-Tate group, locally at ℓ.) Wiles shows that the universal such deformation is modular, thereby verifying a conjecture of Mazur. To do this, he must show that a certain structural map φ of local rings, a priori a surjection, is in fact an isomorphism. It is here that Wiles uses the ideas of Mazur, Hida, Tilouine, Flach, Kolyvagin and others. To prove the injectivity of φ, Wiles was led to study the analogue of the classical Selmer group for the symmetric square of a modular lift ρ of $\overline{\rho}$, bounding it by techniques derived from those of Kolyvagin and Flach. (In many cases, Wiles calculates precisely the order of this Selmer group.)

After proving this key theorem, Wiles shows that E is modular. He examines first the case $\ell = 3$. A theorem of J. Tunnell [13], which incorporates results of H. Saito-T. Shintani and Langlands [4], shows that $\overline{\rho}_3$ satisfies (2) whenever it satisfies (1). It follows that E is modular whenever $\overline{\rho}_3$ is surjective.

A tantalizing problem, raised by Wiles at the close of his second lecture, is posed by the case where $\overline{\rho}_3$ is *not* surjective. Suppose, for example, that $\overline{\rho}_3$ is reducible: can we still win the endgame? Wiles explained his amazing solution to this problem in the third lecture. Using the Hilbert irreducibility theorem and the Cebotarev density theorem, he constructs an auxiliary semistable elliptic curve E' whose mod 3 representation satisfies (1) and whose mod 5 representation is isomorphic to $\overline{\rho}_5$. The construction succeeds because the modular curve $X(5)$ has genus zero. Applying his key theorem once, Wiles shows that E' is modular. Therefore $\overline{\rho}_5$ is modular, since it may be viewed as coming from E'. After a second application of the key theorem, this time to ρ_5, Wiles deduces that E is modular!

Wiles's proof of Taniyama's conjecture represents an enormous milestone for modern mathematics. On the one hand, it illustrates dramatically the power of the abstract "machinery" we have amassed for dealing with concrete Diophantine problems. On the other, it brings us significantly closer to the goal of tying together automorphic representations and algebraic varieties.

References

1. M. Flach, *A finiteness theorem for the symmetric square of an elliptic curve*, Invent. Math. **109** (1992), 307–327.
2. G. Frey, *Links between stable elliptic curves and certain diophantine equations*, Annales Universitatis Saraviensis **1** (1986), 1–40.
3. ———, *Links between solutions of $A - B = C$ and elliptic curves*, Lecture Notes in Math. **1380** (1989), 31–62.
4. R. P. Langlands, *Base change for* $\mathbf{GL}(2)$, Annals of Math. Studies, vol. 96, Princeton University Press, Princeton, 1980.
5. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. **47** (1977), 33–186.
6. ———, *Deforming Galois representations*, Galois groups over $\mathbb{Q}$, MSRI Publications., vol. 16, Springer-Verlag, Berlin and New York, 1989, pp. 385–437.
7. ———, *Number theory as gadfly*, Am. Math. Monthly **98** (1991), 593–610.
8. K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
9. ———, *From the Taniyama-Shimura Conjecture to Fermat's Last Theorem*, Annales de la Faculté des Sciences de l'Université de Toulouse **11** (1990), 116–139.

10. J-P. Serre, *Lettre à J-F. Mestre*, 13 août 1985, Contemporary Mathematics **67** (1987), 263–268.
11. ———, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.
12. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1986.
13. J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. AMS (new series) **5** (1981), 173–175.