A 2020 View of Fermat's Last Theorem

Kenneth A. Ribet

Fermat's Last Theorem (FLT) was formulated in the seventeenth century and proved only about twenty-five years ago. The theorem is a compelling topic because of the simplicity of its statement (and the complexity of its proof) and because it gave rise to entire subjects within mathematics as researchers probed the problem in previous centuries.

I spoke about this subject at the 1994 Joint Math Meetings in Cincinnati. As the audience gathered, there was palpable tension in the ballroom because of the gap in the proof of FLT that Andrew Wiles had announced in June 1993. After speaking for 30 minutes about the mathematics behind the proof, I projected a statement that Wiles had made at the end of 1993. Here is the key passage:

> …the final calculation of a precise upper bound for the Selmer group in the semistable case (of the symmetric square representation associated to a modular form) is not yet complete as it stands….

Although there was no guarantee in January 1994 that there would be a happy end to the story, the gap that Wiles alluded to in his statement was repaired by an article written by Richard Taylor and Andrew Wiles the following fall. The complementary manuscripts by Wiles [12] and Taylor–Wiles [11] were published together in the *Annals of Mathematics* in 1995, more or less at the same time that elements of the proof of FLT were being explained to large audiences at a conference at Boston University.[1]

It is important to recall that the full proof depended on hundreds (if not thousands) of pages of difficult prior work as well as the two new articles in the *Annals*. In addition to my 1990 article on Serre's conjecture [7], the argument outlined by Wiles appealed to the main theorem of Langlands's book *Base Change for GL(2)* [5], an irreducibility result in Barry Mazur's "Eisenstein ideal" article [6], and much more. (My 1995 article [8] sketches some of the mathematical tools that were used in the proof.)

The work of Wiles and Taylor–Wiles established the modularity of elliptic curves over the field of rational numbers. (In [7], I had proved that FLT would follow from this modularity.) Their new techniques led to a series of spectacular developments, including Serre's modularity conjecture [9], which was proved in 2009 by Khare and Wintenberger [2,3], and most of the conjecture of Fontaine and Mazur [1]. (For some cases of the proof, see, e.g., [4].)

It might be natural to guess that these and other developments in the Langlands program would allow for a vast overhaul of the proof that was completed in 1994. Indeed, there is no shortage of examples of major theorems whose initial proofs were simplified considerably by subsequent analysis. Are we now able to present a proof of Fermat's Last Theorem that is substantially more efficient than the quarter-century old version?

Certainly it is possible to formulate what looks like a succinct argument: FLT is a direct consequence of Serre's modularity conjecture [9] (which is now a theorem as mentioned above). Appealing to Serre's conjecture in this way has the technical advantage that the auxiliary (Frey) elliptic curve used in Wiles's argument disappears almost immediately after it is introduced. All we need to say is that if $a^p + b^p = c^p$ (with a, b, and c nonzero integers and p a prime ≥ 5), then the mod p Galois representation attached to the elliptic curve with equation $y^2 = x(x - a^p)(x + b^p)$ is an irreducible Galois representation that furnishes a counterexample to Serre's conjecture.

This one-sentence proof is not a clean simplification of the argument that was presented over a full week at the 1995 Boston University conference. The irreducibility of the Galois representation still relies on Mazur's theorem from [6]. More importantly, the proof of Serre's conjecture uses all of the ingredients that went into the original proof of FLT, plus quite a few more. (In particular, Khare and Wintenberger used Taylor's work on potential modularity [10] to establish Serre's modularity conjecture.)

Thus the question remains: is the proof simpler in 2020 than it was in 1995? As one writes on social media, "it's complicated." I will detangle some of the issues in Denver.

Kenneth A. Ribet is a professor of mathematics at the University of California, Berkeley. His email address is ribet@berkeley.edu.

The reader will not be surprised to learn that 20/20 vision is referred to as 6/6 vision in countries that use the metric system.

[1]*This proof is summarized on a t-shirt that one can obtain from* https://promys.org/resources/fermats-tshirts.

DOI: https://dx.doi.org/10.1090/noti1999

References

[1] Fontaine J-M and Mazur B. Geometric Galois representations. In *Elliptic curves, modular forms, & Fermat's last theorem* (*Hong Kong, 1993*), Ser. Number Theory, I. Int. Press, Cambridge, MA, 1995, pp. 41–78. MR1363495

[2] Khare C and Wintenberger J-P. Serre's modularity conjecture. I. *Invent. Math.*, **178**(3):485–504, 2009. MR2551763

[3] Khare C and Wintenberger J-P. Serre's modularity conjecture. II. *Invent. Math.*, **178**(3):505–586, 2009. MR2551764

[4] Kisin M. The Fontaine-Mazur conjecture for GL_2. *J. Amer. Math. Soc.*, **22**(3):641–690, 2009. MR2505297

[5] Langlands RP. *Base Change for GL(2)*, volume **96** of Annals of Mathematics Studies. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1980. MR0574808

[6] Mazur B. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (**47**):33–186 (1978), 1977. With an appendix by Mazur and M. Rapoport. MR0488287

[7] Ribet KA. On modular representations of $\mathrm{Gal}(\bar{Q}/Q)$ arising from modular forms. *Invent. Math.*, **100**(2):431–476, 1990. MR1047143

[8] Ribet KA. Galois representations and modular forms. *Bull. Amer. Math. Soc. (N.S.)*, **32**(4):375–402, 1995. MR1322785

[9] Serre J-P. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{Q}/Q)$. *Duke Math. J.*, **54**(1):179–230, 1987. MR0885783

[10] Taylor R. Remarks on a conjecture of Fontaine and Mazur. *J. Inst. Math. Jussieu*, **1**(1):125–143, 2002. MR1954941

[11] Taylor R and Wiles A. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, **141**(3):553–572, 1995. MR1333036

[12] Wiles A. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, **141**(3):443–551, 1995. MR1333035

Kenneth A. Ribet

Credits

Author photo is by Kate Awtrey, Atlanta Convention Photography.