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 $\geq 5$), then the mod $p$ Galois representation attached to the elliptic curve with equation $$y^2 = x(x - ap)(x + bp)$$
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.
References


Credits

Author photo is by Kate Awtrey, Atlanta Convention Photography.

Kenneth A. Ribet