
MR1474977 (99d:11067a)
Darmon, Henri (3-MGL); **Diamond, Fred** (4-CAMB);
Taylor, Richard **[Taylor, Richard L.]** (4-OX)
Fermat's last theorem.
Current developments in mathematics, 1995 (*Cambridge, MA*), 1–154, *Internat. Press, Cambridge, MA*, 1994.
11G18 (11D41 11F80 11G05)

Journal | Article | Doc Delivery

MR1605752 (99d:11067b)
Darmon, Henri (3-MGL); **Diamond, Fred** (1-MIT);
Taylor, Richard **[Taylor, Richard L.]** (1-HRV)
Fermat's last theorem.
Elliptic curves, modular forms & Fermat's last theorem (*Hong Kong*, 1993), 2–140, *Internat. Press, Cambridge, MA*, 1997.
11G18 (11D41 11F80 11G05)

Journal | Article | Doc Delivery

References: 0 | **Reference Citations: 3** | **Review Citations: 3**

Fermat's last theorem has served as a muse of number theory for nearly four centuries. It has given rise to a rich tapestry of diverse disciplines of mathematics. Still, the muse has not revealed all the secrets yet. There are more realms revolving around this theme that will undoubtedly serve as a focus of research for many centuries to come.

This article is a detailed exposition of the proof of Fermat's last theorem. (The second paper is a corrected and updated version of the first.) In a span of 150 pages, the authors do an excellent job of gathering together the relevant ideas from number theory, representation theory and commutative algebra that are needed in the proof. It begins with a highly readable introduction explaining the main ideas in a brief historical context.

Mazur's work on determining the rational points of the modular curves $X_0(l)$ and $X_1(l)$, with

l prime, is used as an “indicator” of a “philosophy” of rational points. Indeed, rational points on modular curves correspond to elliptic curves with cyclic subgroups or points of order l defined over the rational numbers. Such moduli interpretation of Diophantine questions has proved extremely useful.

In 1986, Frey had the insight that given a solution $a^l + b^l = c^l$ to the Fermat equation of degree l, we can without loss of generality suppose that $a^l \equiv -1 \pmod 4$ and $b^l \equiv 0 \pmod{32}$ and consider the elliptic curve defined by $y^2 = x(x-a^l)(x+b^l)$. This curve E is semistable and for $l > 7$, the action of the absolute Galois group $G_{\mathbf{Q}}$ on the l-division points of E gives rise to an irreducible representation $\overline{\rho}_{E,l}$. Mazur’s results described above imply that $\overline{\rho}_{E,l}$ is actually surjective and isomorphic to $\mathrm{GL}_2(\mathbf{F}_l)$, by combining results of Serre, in the case under discussion.

Shortly after this step, Serre made a careful study of representations $\overline{\rho}$ of $G_{\mathbf{Q}}$ into $\mathrm{GL}_2(\mathbf{F}_l)$. He made precise predictions on when such representations arise from modular forms mod l. Applying this to Frey’s construction above, the prediction is that $\overline{\rho}_{E,l}$ should come from a modular form mod l of weight 2 and level 2. Such modular forms can be lifted to classical modular forms of weight 2 and level 2 and these correspond to holomorphic differentials on the modular curve $X_0(2)$. Since the latter curve has genus 0, there are no such differentials. Thus, Serre’s conjectures imply Fermat’s last theorem.

Ribet subsequently discovered a “lowering of the level” principle and, assuming the Shimura-Taniyama conjecture, established Fermat’s last theorem. This reduces the problem of Fermat to showing that $\rho_{E,l}$ is modular, in the sense of Serre, for every prime l. Invoking the Chebotarev density theorem, we can make a further reduction. Namely, it suffices to show that $\rho_{E,l}$ is modular for some prime l. For then we would have a modular form f such that the pth Fourier coefficient $a_p(f)$ is equal to $\mathrm{Tr}(\rho_{E,l}(\mathrm{Frob}_p))$ for all but finitely many primes p. (As we shall see below, Wiles works primarily with $l = 3$ and also $l = 5$.) The modularity of E then follows from first invoking the Eichler-Shimura theorem to associate an elliptic curve E_f to the modular form f and then invoking Faltings’ isogeny theorem (earlier, Tate’s conjecture) to deduce that E and E_f are isogenous. (To be accurate, one does not need to use Faltings’ theorem since in the case of nonintegral j-invariant, which is what is needed here, Serre had already established Tate’s conjecture.) As is now well known, it is the semistable case of the Shimura-Taniyama conjecture that Wiles proves. His starting point is the $G_{\mathbf{Q}}$-action on the 3-division points of the Frey curve E defined above. By an application of the Langlands-Tunnell theorem, this representation $\overline{\rho}$ is modular in the sense that it arises from a modular form mod 3.

The main theorem of Wiles shows that that all lifts to representations over complete Noetherian local $\mathbf{Z}_l$-algebras R whose restriction to the decomposition group at l is the same as $\overline{\rho}$ are modular. This is proved by an ingenious application of commutative algebra and analytic number theory involving symmetric square L-functions. Since $\rho_{E,l}$ is one such representation, the theorem implies the Shimura-Taniyama conjecture in this (semistable) case.

The paper under review is divided into five parts. The first and second parts form a basic review of known material with the former having fewer prerequisites than the latter. The second part reviews the relevant theory of Galois cohomology and the deformation theory of Mazur. The third part forms the core of the paper. It gives the detailed proof of the main theorem of Wiles. In particular, it establishes the isomorphism criterion involving complete intersections. The fourth part focuses on Hecke algebras and discusses in detail the use of the symmetric square L-function to establish the isomorphism criterion of Section 3. Finally, Section 5 deals with the commutative algebra proper, complete intersections in particular, and the treatment given it by Faltings and Lenstra.

In summary, the authors give a very readable exegesis of the main theorem of Wiles. It can be recommended for serious graduate study.

{For the entire collection containing the first paper see MR 98d:00016. For the entire collection containing the second paper see MR 99d:11002.}

{For the entire collection see 99d:11002}

Reviewed by *M. Ram Murty*

© *Copyright American Mathematical Society 1999, 2003*