# How the proof of FLT worked!

Sachin Kumar
University of Waterloo, Faculty of Mathematics

June 2023

**Theorem (Fermat's).** $a^n + b^n = c^n$ has no non-trivial positive integer solutions for all $n \in \mathbb{Z}$, where $n > 2$ and $abc \neq 0$.

*Proof.* The proof follows a program formulated around 1985 by Frey and Serre [F, S]. By classical results of Fermat, Euler, Dirichlet, Legendre, and Lamé, we may assume that $n = p$, an odd prime $\geq 11$. Suppose $a, b, c \in \mathbb{Z}$, $abc \neq 0$, and $a^p + b^p = c^p$. Without loss of generality we may assume $2 \mid a$ and $b \equiv 1 \pmod 4$. Frey [F] obsserved that the elliptic curve $E : y^2 = x(x - a^p)(x + b^p)$ has the following remarkable properties: $E$ is semistable with conductor $N_E = \prod_{\ell \mid abc} \ell$ and $\overline{\rho}_{E,p}$ is unramified outside $2p$ and is flat at $p$. By the modularity theorem of Wiles and Taylor-Wiles [W, T-W], then is an eigenform $f \in \mathcal{S}_2(\Gamma_0(N_E))$ such that $\rho_{f,p} = \rho_{E,p}$. A theorem of Mazur implies $\overline{\rho}_{E,p}$ is irreducible, so Ribet's theorem [R] produces a Hecke eigenform $f \in \mathcal{S}_2(\Gamma_0(2))$ such that $\rho_{g,p} \equiv \rho_{f,p} \pmod{\wp}$ for some $\wp \mid p$. But $X_0(2)$ has genus 0, so $\mathcal{S}_2(\Gamma_0(2)) = 0$. This is a contradiction, hence there exists no non-trivial integer solutions. □

## References

[F] Frey, G.: Links between stable elliptic curves and certain Diophantine equations. *Ann. Univ. Sarav.* **1** (1986.) 1 - 40.

[R] Ribet. K.: On modular representations of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) arising from modular forms. *Invent. math.* **100** (1990), 431-476.

[S] Serre, J.-P.: Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$), *Duke Math. J.* **54** (1987), 179-230.

[T-W] Taylor, R. L., Wiles, A.: Ring theoretic properties of certain Hecke algebras. *Annals of Math.* **141** (1995), 553-572.

[W] Wiles, A.: Modular elliptic curves and Fermat's Last Theorem. *Annals of Math.* **141** (1995), 443-551.