Andrew Wiles on Fermat's Last Theorem

dr/dx • 7 Sep 2025

He writes until the chalk dust erases his fingerprints.
The object does not change:

$$\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p),$$

odd, absolutely irreducible, semistable. Determinant $\overline{\chi}_p$.
Everything lives inside this cage. He demands deformation theory to carry the weight.

Minimal deformation problem

Fix S, the finite set of places.
For each $\ell \in S$ he prescribes a local deformation condition $\mathcal{D}_\ell$.
Finite flat at p, unramified outside S, ordinary if necessary.

Define the functor:

$$\mathcal{D} : \mathsf{CNL}_{\mathbb{Z}_p} \to \mathsf{Sets}, \quad A \mapsto \{\rho_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(A) \text{ lifting } \bar{\rho},\ \rho_A|_{G_\ell} \in \mathcal{D}_\ell\}.$$

This functor is representable by a complete Noetherian local $\mathbb{Z}_p$-algebra $R_{\min}$.
He stares at the hull:

$$R_{\min} \cong \mathbb{Z}_p[[X_1, \ldots, X_d]]/(f_1, \ldots, f_r).$$

Each f_i is an obstruction. Each generator is a wall between him and Fermat.

Hecke algebra comparison

He moves to the Hecke side.
For modular forms of level N, weight 2, let T denote the Hecke algebra generated by T_ℓ for $\ell \nmid N$ and U_ℓ for $\ell \mid N$.
Localize at the maximal ideal $\mathfrak{m}$ corresponding to $\bar{\rho}$:

$$T_\mathfrak{m} \subset \mathrm{End}_{\mathbb{Z}_p}(H^1(X_1(N), \mathbb{Z}_p)).$$

The universal property gives a natural surjection:

$$R \twoheadrightarrow T.$$

He knows: if $R \cong T$, then every semistable elliptic curve is modular.
If every semistable elliptic curve is modular, Fermat's Last Theorem is dead.

Tangent space calculation

He presses into the tangent spaces.
Compute the Zariski tangent space:

$$t_R = \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{m}_R/\mathfrak{m}_R^2, \mathbb{F}_p) \cong H^1_{\mathcal{F}}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}),$$

where $\mathrm{ad}^0\bar{\rho}$ denotes the adjoint representation of trace zero matrices.

He compares to the cotangent space on the Hecke side:

$$t_T \cong \frac{\mathfrak{m}_T}{\mathfrak{m}_T^2}.$$

The numerical criterion demands equality of length:

$$\dim_{\mathbb{F}_p} t_R = \dim_{\mathbb{F}_p} t_T.$$

Every time he calculates, the inequality is off by one.
The criterion resists.

Cohomology labyrinth

He calculates local conditions.
For $\ell \neq p$ not dividing N:

$$H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, \mathrm{ad}^0\bar{\rho}) = \ker\bigl(H^1(\mathbb{Q}_\ell, \mathrm{ad}^0\bar{\rho}) \to H^1(I_\ell, \mathrm{ad}^0\bar{\rho})\bigr).$$

At p:

$$H^1_f(\mathbb{Q}_p, \mathrm{ad}^0\bar{\rho}) = \ker\bigl(H^1(\mathbb{Q}_p, \mathrm{ad}^0\bar{\rho}) \to H^1(\mathbb{Q}_p, \mathrm{ad}^0\bar{\rho} \otimes B_{\mathrm{cris}})\bigr).$$

The global Selmer group:

$$H^1_{\mathcal{F}}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}) = \ker\left(H^1(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}) \to \prod_v H^1(\mathbb{Q}_v, \mathrm{ad}^0\bar{\rho})/H^1_{\mathcal{F}}(\mathbb{Q}_v, \mathrm{ad}^0\bar{\rho})\right).$$

Every dimension formula fails to reconcile.

Iwasawa interlude

He mutters through Iwasawa theory.
Take $\mathbb{Q}_\infty = \bigcup_n \mathbb{Q}(\mu_{p^n})$.
$\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$.
The Iwasawa algebra:

$$\Lambda = \mathbb{Z}_p[[\Gamma]].$$

The Selmer group over $\mathbb{Q}_\infty$ is Λ-torsion.
Characteristic power series:

$$\mathrm{char}_\Lambda H^1_{\mathcal{F}}(\mathbb{Q}_\infty, T) = f(T),$$

with λ, μ invariants encoded.

He tests congruences between modular forms by comparing λ-invariants.
The data refuse to line up cleanly.

Non-minimal deformations

The compulsive shift: abandon minimality.
Allow ramification at auxiliary primes Σ.
Define the enlarged deformation problem with local conditions loosened.

The surjection extends:

$$R_\Sigma \twoheadrightarrow T_\Sigma.$$

He then patches across Σ.

Patching modules

Define:

$$M_\Sigma = H^1(X_\Sigma, \mathbb{Z}_p)_\mathfrak{m},$$

cohomology of modular curves at auxiliary level.
Construct inverse system:

$$M = \varprojlim_\Sigma M_\Sigma.$$

M becomes a balanced module: depth equals dimension.
He proves Gorenstein property, then complete intersection:

$$\mathrm{depth}(R) = \dim(R).$$

Now the numerical criterion is satisfied.

Congruence modules

He isolates the congruence module:

$$C = \frac{T}{\mathfrak{m}T} \cong \frac{H^0(X, \omega^{\otimes 2})}{\mathfrak{m}}.$$

Its annihilator controls the failure of $R = T$.
But patching forces C to vanish.
The alignment is exact.

Final collapse

He writes it as the theorem he cannot deny:

$$R \cong T.$$

Isomorphism of complete intersections.
Every semistable elliptic curve is modular.
Fermat's Last Theorem collapses into corollary.

$$R = T.$$