18.783 Elliptic Curves
Lecture 25

Andrew Sutherland

December 12, 2023

Fermat's last theorem

Conjecture (Fermat 1637)

The equation $x^n + y^n = z^n$ *has no integer solutions with* $xyz \neq 0$ *and* $n > 2$.

Suppose (a, b, c, n) is a counterexample to the conjecture.

If $d = \gcd(a, b, c) > 1$ then $(a/d, b/d, c/d, n)$ is also a counterexample.
We thus assume $\gcd(a, b, c) = 1$, which forces a, b, c to be pairwise coprime.

If n is divisible by $2 < m < n$ then $(a^{n/m}, b^{n/m}, c^{n/m}, m)$ is also a counterexample. It thus suffices to consider the case $n = 4$ and the case where n is an odd prime.

Fermat treated $n = 4$, so we assume n is an odd prime and replace z with $-z$ to obtain

$$x^n + y^n + z^n = 0,$$

which we wish to show has no solutions with $x, y, z \in \mathbb{Z}_{\neq 0}$ pairwise coprime.

Chronology of progress

1637	Fermat makes his conjecture and proves it for $n = 4$.
1753	Euler proves FLT for $n = 3$ (his proof has a fixable error).
1800s	Sophie Germain proves FLT for $n \nmid xyz$ for all $n < 100$.
1825	Dirichlet and Legendre complete the proof for $n = 5$.
1839	Lamé addresses $n = 7$.
1847	Kummer proves FLT for all primes $n \nmid h(\mathbb{Q}(\zeta_n))$, called regular primes. This leaves 37, 59, and 67 as the only open cases for $n < 100$.
1857	Kummer addresses 37, 59, and 67, but his proof has gaps.
1926	Vandiver fills the gaps and addresses all irregular primes $n < 157$.
1937	Vandiver and assistants handle all irregular primes $n < 607$.
1954	Lehmer, Lehmer, and Vandiver introduce techniques better suited to mechanical computation and use a computer to address all $n < 2521$.
1954-1993	Computers verify FLT for all $n < 4,000,000$.

This work is all based on results in algebraic number theory and has no direct connection to elliptic curves.

The Frey-Hellegouarch curve

In his 1972 PhD thesis Hellegouarch considers the elliptic curve over $\mathbb{Q}$

$$E_{a,b,c} : y^2 = x(x - a^p)(x + b^p)$$

associated to a solution to the Fermat equation

$$a^p + b^p + c^p = 0$$

for some prime $p > 3$. Proving FLT amounts to showing that no such $E_{a,b,c}$ exists.

In 1984 Frey suggested that any such $E_{a,b,c}$ could not be modular.

Serre gave a more precise formulation of Frey's suggestion known as the epsilon conjecture that involves modular forms and their associated Galois representations.

Serre's epsilon conjecture was proved by Ribet in the late 1980's, meaning that the modularity of elliptic curves over $\mathbb{Q}$ (even just in the semistable case) would imply FLT.

Why the Frey-Hellegouarch curve should not exist

The discriminant of $E_{a,b,c}$ is

$$\Delta(E_{a.b,c}) = -16(0-a^p)^2(0+b^p)^2(a^p+b^p)^2 = -16(abc)^{2p},$$

which is very close to its minimal discriminant

$$\Delta_{\min}(E_{a,b,c}) = 2^{-8}(abc)^{2p}.$$

The elliptic curve $E_{a,b,c}$ has good reduction at all primes $\ell \nmid abc$ and multiplicative reduction at $\ell | abc$. It follows that $E_{a,b,c}$ is semistable with conductor

$$N_{E_{a,b,c}} = \prod_{\ell | abc} \ell,$$

which is dramatically smaller than $\Delta_{\min}(E_{a,b,c})$ (recall that $p > 4,000,000$), and would appear to be incompatible with Szpiro's conjecture $\Delta_{\min}(E) \le c_\epsilon N_E^{6+\epsilon}$.

Galois representations

Definition

Let $E/\mathbb{Q}$ be an elliptic curve and let ℓ be a prime. The mod-ℓ Galois representation

$$\bar{\rho}_{E,\ell}\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut}(E[\ell]) \simeq \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

is defined by $\bar{\rho}(\sigma) := \Big((x:y:z) \mapsto (\sigma(x):\sigma(y):\sigma(z))\Big) \in \operatorname{Aut}(E[\ell])$.
We similarly define for each prime power ℓ^n

$$\bar{\rho}_{E,\ell^n}\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut}(E[\ell^n]) \simeq \operatorname{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}).$$

The ℓ-adic Galois representation is the continuous homomorphism

$$\rho_{E,\ell}\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{Aut}(T_\ell(E)) \simeq \operatorname{GL}_2(\mathbb{Z}_\ell),$$

Here $T_\ell(E) := \varprojlim_n E[\ell^n]$ is the ℓ-adic Tate module and $\mathbb{Z}_\ell := \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}$ is the ring of ℓ-adic integers.

Frobenius elements

The value of $\bar{\rho}_{E,\ell^n}(\sigma)$ depends only on the restriction of σ to the ℓ^n-torsion field $K := \mathbb{Q}(E[\ell^n])$, which we note is a Galois extension of $\mathbb{Q}$.

Let S be a finite set of primes that includes ℓ and the primes of bad reduction for E.

For each prime $p \notin S$ we may fix a prime $\mathfrak{p}|p$ of K above p and consider the Frobenius element $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$, which is the inverse image of the p-power Frobenius automorphism of the residue field $\mathbb{F}_p := \mathcal{O}_K/\mathfrak{p}$ under the canonical isomorphism

$$\begin{aligned}\{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\} =: D_{\mathfrak{p}} &\xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p) = \langle x \mapsto x^p \rangle \\ \sigma &\mapsto \left(\bar{x} \mapsto \overline{\sigma(x)}\right).\end{aligned}$$

The Frobenius elements $\sigma_{\mathfrak{p}}$ for $\mathfrak{p}|p$ form a conjugacy class σ_p of $\mathrm{Gal}(K/\mathbb{Q})$.

Frobenius elements

For which prime $p \notin S$ we have

$$\operatorname{tr} \rho_{E,\ell^n}(\sigma_p) \equiv a_p \bmod \ell^n \qquad \text{and} \qquad \det \rho_{E,\ell^n}(\sigma_p) \equiv p \bmod \ell^n,$$

which uniquely determines the trace of Frobenius $a_p \in \mathbb{Z}$ once we have $\ell^n > 4\sqrt{p}$.

The ℓ-adic Galois representation $\rho_{E,\ell}$ determines the Dirichlet coefficients a_p of the L-function $L(E,s)$ for all but the finitely many primes $p \in S$. By the Faltings-Tate theorem, this uniquely determines the isogeny class of E.

Thus for every prime $\ell \neq p$ the ℓ-adic Galois representation of $E/\mathbb{Q}$ uniquely determines its isogeny class and therefore its L-function $L(E,s)$.

This includes the values of a_p at $p \in S$, even though we excluded them.

Modular Galois representations

We call any continuous homomorphism $\rho\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\mathbb{Z}_\ell)$ an ℓ-adic Galois representation, whether it is associated to an elliptic curve or not, and similarly define mod-ℓ Galois representations $\bar{\rho}\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Definition

An ℓ-adic Galois representation ρ is modular (of weight k and level N) if there is a modular form $f_\rho = \sum a_n q^n \in S_k(\Gamma_1(N))$ with $a_n \in \mathbb{Z}$ such that

$$\operatorname{tr} \rho(\sigma_p) = a_p$$

for all primes $p \nmid \ell N$, and we similarly call $\bar{\rho}\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ modular if

$$\operatorname{tr} \bar{\rho}(\sigma_p) \equiv a_p \bmod \ell$$

for all primes $p \nmid \ell N$.

Serre's modularity conjecture

Definition

Let $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the automorphism corresponding to complex conjugation.
A mod-ℓ Galois representation $\bar{\rho}$ is odd if $\det \rho(c) = -1$, and irreducible if its image does not fix any one dimensional subspace of $(\mathbb{Z}/\ell\mathbb{Z})^2$, equivalently, its image is not conjugate to a group of upper triangular matrices.

For any elliptic curve $E/\mathbb{Q}$ the mod-ℓ Galois representation $\bar{\rho}_{E,\ell}$ is necessarily odd, and irreducible for $\ell \neq 2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163$, by Mazur's isogeny theorem.

Conjecture (Serre)

Every odd irreducible Galois representation $\bar{\rho}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *is modular.*

Serre's ϵ-conjecture and Ribet's level lowering theorem

Serre gave a more precise formulation of his conjecture that associates an optimal weight and optimal level to each odd irreducible mod-ℓ Galois representation. For mod-ℓ Galois representations $\bar{\rho}_{E,\ell}$ the optimal weight is 2 (provided we pick $\ell \nmid N_E$).

For the Frey-Helleougarch curve $E_{a,b,c}$ the optimal level is 2.
But there are no nonzero modular forms of weight 2 and level 2, because

$$\dim S_2(\Gamma_1(2)) = \dim S_2(\Gamma_0(2)) = g(X_0(2)) = 0.$$

Theorem (Ribet)

Let ℓ be prime, let E be an elliptic curve of conductor $N = mN'$, where m is the product of all primes $p|N$ such that $v_p(N) = 1$ and $v_p(\Delta_{\min}(E)) \equiv 0 \bmod \ell$. If E is modular and $\bar{\rho}_{E,\ell}$ is irreducible, then $\bar{\rho}_{E,\ell}$ is modular of weight 2 and level N'.

Corollary

The elliptic curve $E_{a,b,c}$ is not modular.

The modulatiry lifting theorem of Taylor and Wiles

Given a representation $\rho_0\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, a representation $\rho_1\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ whose reduction modulo ℓ is equal to ρ_0 is called a lift of ρ_0. More generally, if R is a suitable ring with a reduction map to $\mathbb{Z}/\ell\mathbb{Z}$, and $\rho_1\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ has reduction ρ_0, then we say that ρ_1 is a lift of ρ_0 (to R). A deformation of ρ_0 is an equivalence class of lifts of ρ_0 to the ring R, which is sometimes called the deformation ring.

Building on work by Mazur, Hida, and others that established the existence of certain universal deformations $\rho_{\mathbb{T}}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T})$, where $\mathbb{T}$ is a certain Hecke algebra, Taylor and Wiles were able to show that if ρ_0 is modular, then *every* lift of ρ_0 satisfying a specified list of properties is modular (this is an example of an "$R = \mathbb{T}$" theorem).

Theorem (Taylor-Wiles)

Let $E/\mathbb{Q}$ be a semistable elliptic curve. If $\overline{\rho}_{E,\ell}$ is modular, then $\rho_{E,\ell}$ is also modular (and therefore E is modular).

The proof of Fermat's last theorem

Theorem (Langlands-Tunnel)

Let E be an elliptic curve over $\mathbb{Q}$. If $\overline{\rho}_{E,3}$ is irreducible, then it is modular.

Theorem (Wiles)

Let $E/\mathbb{Q}$ be a semistable elliptic curve for which $\overline{\rho}_{E,5}$ is irreducible. There exists a semistable elliptic curve $E'/\mathbb{Q}$ such that $\overline{\rho}_{E',3}$ is irreducible and $\overline{\rho}_{E',5} \simeq \overline{\rho}_{E,5}$.

Lemma

No semistable elliptic curve $E/\mathbb{Q}$ admits a rational 15-isogeny.

Theorem (Wiles)

Let $E/\mathbb{Q}$ be a semistable elliptic curve. Then E is modular.

Proof: To the board!