18.783 Elliptic Curves **Spring 2015**
Lecture #26 **05/14/2015**

26 Fermat's Last Theorem

In our final lecture we give an overview of the proof of Fermat's Last Theorem. Our goal is to explain exactly what Andrew Wiles [14], with the assistance of Richard Taylor [13], proved, and why it implies Fermat's Last Theorem; this implication is a consequence of prior work by several other mathematicians, including, most notably, Richard Frey, Jean-Pierre Serre, and Ken Ribet. We will say very little about the details of Wiles' proof, which are beyond the scope of this course, but we will at least outline its main components.

26.1 Fermat's Last Theorem

In 1637, Pierre de Fermat famously wrote in the margin of his copy of Diophantus' *Arithmetica* that the equation

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

has no integer solutions with $xyz \neq 0$ for all $n > 2$, and claimed to have a proof of this fact. As with most of Fermat's work, he never published this claim (mathematics was Fermat's hobby, not his profession; he was actually a lawyer). Fermat's marginal comment was apparently discovered only after his death, when his son Samuel was preparing to publish Fermat's mathematical correspondence, but it soon became well known and appears as a comment in later versions of *Arithmetica*.

Fermat did prove the case $n = 4$, using a descent argument. It then suffices to consider only cases where n is an odd prime, since if $p|n$ and (x_0, y_0, z_0) is a solution to $x^n + y^n = z^n$, then $(x_0^{n/p}, y_0^{n/p}, z_0^{n/p})$ is a solution to $x^p + y^p = z^p$.

A brief chronology of the progress made toward proving Fermat's Last Theorem prior to Wiles' work is given below.

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 $n < 4,000,000$.

All of the results above are based on work in algebraic number theory, none of it uses elliptic curves. The first person to suggest a connection between elliptic curves and Fermat's Last Theorem was Yves Hellegouarch. In his 1972 doctoral thesis [5], Hellegouarch associates to any non-trivial solution (a, b, c) of $x^p + y^p = z^p$ with p an odd prime, the elliptic curve

$$E_{a,b,c}\colon \qquad y^2 = x(x - a^p)(x + b^p).$$

Without loss of generality we assume that $\gcd(a, b, c) = 1$, in which case a, b, c must be pairwise relatively prime, and that $a \equiv 3 \bmod 4$ and $b \equiv 0 \bmod 2$ (note that p is odd so we multiply both sides by -1 if necessary to achieve this). Proving Fermat's Last Theorem then amounts to showing that no such elliptic curve $E_{a,b,c}$ can exist.

Hellegouarch did not make much progress with this, but in 1984 Gerhard Frey suggested that the elliptic curve $E_{a,b,c}$, if it existed, could not possibly be modular [4]. Shortly thereafter, Jean-Pierre Serre [10] reduced Frey's conjecture to a much more precise statement about modular forms and Galois representations, known as the *epsilon conjecture*, which was proved by Ken Ribet a few years later [9]. With Ribet's result in hand, it was then known that the modularity conjecture, which states that every elliptic curve over $\mathbb{Q}$ is modular, implies Fermat's Last Theorem: it guarantees that $E_{a,b,c}$, and therefore the solution (a, b, c) to $x^p + y^p = z^p$, cannot exist. But at that time (late 1980s) no one expected the modularity conjecture to be proved any time soon; indeed, the fact that it implies Fermat's Last Theorem was rightly taken as evidence of how difficult it would be to prove.

26.2 A strange elliptic curve

To get a sense of what makes the elliptic curve $E_{a,b,c}$ so strange that one might question its very existence, let us compute its discriminant:

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

As explained in the last lecture, the definition of the L-series of an elliptic curve E requires us to determine the minimal discriminant of E and the type of reduction we get (additive, split multiplicative, or non-split multiplicative) at each prime which divide it. It turns out that the discriminant Δ is not quite minimal, the minimal discriminant is actually

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

which differs from Δ only at the prime 2. Let us verify this for primes $\ell > 3$. Multiplying out the equation for $E_{a,b,c}$ yields $y^2 = x^3 - (a^p - b^p)x^2 - (ab)^p x$, and if we put $d = a^p - b^p$ and $e = (ab)^p$ and convert this equation to short Weierstrass form we obtain

$$y^2 = x^3 - 27(d^2 + 3e)x - 27d(d^2 + 9e),$$

with discriminant $\Delta' = -2^4 3^{12}(abc)^p$. It follows from Theorem 14.13 that we can remove a prime $\ell > 3$ from Δ' if and only if $d^2 + 3e$ is divisible by ℓ^4 and $d^2 + 9e$ is divisible by ℓ^6. Now d and e must be relatively prime, since a and b are, but if $d^2 + 3e$ and $d^2 + 9e$ were both divisible by ℓ than d and e would both be divisible by ℓ, which is a contradiction.

On the other hand, the conductor $N_{a,b,c}$ of $E_{a,b,c}$ is much smaller than $\Delta_{a,b,c}$; in fact,

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

is squarefree. This implies that $E_{a,b,c}$ is semistable, meaning that it does not have additive reduction modulo any prime $\ell | \Delta_{\min}$. We can easily verify this for odd primes ℓ by checking whether the cubic $x(x - a^p)(x + b^p)$ has a triple root when reduced modulo ℓ; recall from

Lecture 25 that this is the only case where we get additive reduction (the singularity on the reduced curve is a cusp rather than a node). When $\ell|a$ we get $x^2(x+b^p) \bmod \ell$ with $b \not\equiv 0 \bmod \ell$ because $a \perp b$. The case $\ell|b$ is similar, and when $\ell|c$ we have $b \equiv - \bmod \ell$ and $x(x-a^p)^2 \bmod \ell$ has only a double root because $a \perp c$.

For the elliptic curve $E_{a,b,c}$ the ratio $\Delta_{a,b,c}/N_{a,b,c}$ grows exponentially with p. But it is very unusual (conjecturally impossible) for the minimal discriminant of an elliptic curve to be so much larger than its conductor. Szpiro's conjecture, which is closely related to the ABC conjecture, states that we for every $\epsilon > 0$ there is a constant c_ϵ such that

$$\Delta_{\min}(E) \le c_\epsilon N_E^{6+\epsilon}$$

holds for every elliptic curve $E/\mathbb{Q}$. This cannot possibly be true for $E_{a,b,c}$ if p is sufficiently large. This does not directly imply that $E_{a,b,c}$ cannot be modular, but it does suggest that there is something very strange about this elliptic curve. We should note that even if Szpiro's conjecture is proved, one would need an effective version with an explicit value for c_ϵ in order to prove that $E_{a,b,c}$ cannot exist.[1]

Before leaving this discussion, let us note that since $E_{a,b,c}$ is semistable (since $N_{a,b,c}$ is squarefree), so in order to prove Fermat's Last Theorem it is not necessary to prove the full modularity conjecture; it is enough to show that every semistable elliptic curve $E/\mathbb{Q}$ is modular, which is precisely what Wiles did.

26.3 Galois representations

Let E be an elliptic curve over $\mathbb{Q}$, let ℓ be a prime, and let $K = \mathbb{Q}(E[\ell])$ be the extension of $\mathbb{Q}$ obtained by adjoining the coordinates of all the points in $E[\ell]$ to ℓ. Then K is a Galois extension of $\mathbb{Q}$ (it is either the splitting field of the ℓth division polynomial, or a quadratic extension of it), and the Galois group $G := \mathrm{Gal}(K/\mathbb{Q})$ acts on the ℓ-torsion subgroup $E[\ell]$ via its action on the coordinates of each point. This yields a group representation

$$\rho\colon G \to \mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

Let S be the finite set of primes consisting of ℓ and all the primes of bad reduction for E. Every prime $p \notin S$ is unramified in K; as explained in Lecture 21, this means that the principal ideal $p\mathcal{O}_K$ factors into a product of distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ in $\mathcal{O}_K$ (the ring of integers of K). The Galois group G acts on the set $\{\mathfrak{p}_i\}$, and the *decomposition group* D_p is defined as the kernel of this action (the subgroup that acts trivially). For each prime $\mathfrak{p}$ dividing $p\mathcal{O}_K$ we get a surjective homomorphism $D_\mathfrak{p} \twoheadrightarrow \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$, where $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ is the residue field at $\mathfrak{p}$, which is a cyclic extension of $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. Because p is unramified, this homomorphism is actually an isomorphism. Recall that the Galois group $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ has a canonical generator, the Frobenius automorphism $x \mapsto x^p$, and we let $\mathrm{Frob}_\mathfrak{p}$ of $D_\mathfrak{p}$ denote the element of $D_\mathfrak{p}$ that is mapped to $x \mapsto x^p$ by the isomorphism $D_\mathfrak{p} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$. For different choices of $\mathfrak{p}$ dividing $p\mathcal{O}_K$ we get conjugate elements $\mathrm{Frob}_\mathfrak{p}$ (and every conjugate of $\mathrm{Frob}_\mathfrak{p}$ arises in this way), and we let Frob_p denote this conjugacy class in G; we typically speak of the *Frobenius element* Frob_p as an element of G that represents this conjugacy class, with the understanding that is determined only up to conjugacy.

[1] Mochizuki has recently announced a proof of the ABC conjecture which is in the process of being reviewed (as of this writing it has yet to be accepted by the mathematical community); but even if his proof holds up, it does not give an effective version of Szpiro's conjecture.

Thus for each prime $p \notin S$ we get a Frobenius element $\mathrm{Frob}_p \in G$, and may consider its image $A_p := \rho(\mathrm{Frob}_p) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ under the Galois representation ρ. The characteristic polynomial of A_p (which depends only on the conjugacy class of Frob_p) is

$$\det(\lambda I - A_p) = \lambda^2 - (\operatorname{tr} A_p)\lambda + \det A_p,$$

where $\operatorname{tr} A_p \equiv a_p \bmod \ell$ and $\det A_p \equiv p \bmod \ell$. Here a_p is the pth coefficient of the L-series of E, equivalently, the trace of the Frobenius endomorphism of the reduction of E modulo p (which is a prime of good reduction because $p \notin S$).

For any positive integer n we can similarly consider the Galois representation

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

For primes $p \notin S$ with $4\sqrt{p} \leq \ell^n$, the value of the integer $a_p \equiv \operatorname{tr} \rho(\mathrm{Frob}_p) \bmod \ell^n$ is uniquely determined. Note that this holds no matter which prime ℓ we pick.

The above discussion applies not only to $\mathbb{Q}(E[\ell^n])$, but to any Galois extension K of $\mathbb{Q}$ that contains $\mathbb{Q}(E[\ell^n])$. Even if the extension $k/\mathbb{Q}$ is ramified at primes outside of S, the image of $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ under ρ depends only on the restriction of the automorphism σ to $\mathbb{Q}(E[\ell^n])$, so given a Galois representation $\rho(\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(E[\ell^n])$ we can determine $a_p \bmod \ell^n$ for any $p \notin S$, even when p is ramified in K.

We now define the *ℓ-adic Tate module*

$$T_\ell(E) = \varprojlim_n E[\ell^n]$$

as the projective limit of the inverse system

$$E[\ell] \xleftarrow{[\ell]} E[\ell^2] \xleftarrow{[\ell]} \cdots \xleftarrow{[\ell]} E[\ell^n \xleftarrow{[\ell]} E[\ell^{n+1}] \xleftarrow{[\ell]} \cdots,$$

whose connecting homomorphisms are multiplication-by-ℓ maps. The elements of $T_\ell(E)$ are infinite sequences of points $(P_1, P_2, P_3, \ldots)$ with $P_n \in E[\ell^n]$ such that $\ell P_{n+1} = P_n$.

If we then put $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we obtain the *ℓ-adic Galois representation*

$$\rho_{E,\ell}\colon G_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell),$$

where $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$ is the ring of ℓ-adic integers, which contains $\mathbb{Z}$ as a subring.[2] For any $p \notin S$ we then have $\operatorname{tr} \rho_{E,\ell}(\mathrm{Frob}_p) = a_p$, as elements of $\mathbb{Z}$. The representation $\rho_{E,\ell}$ thus determines the coefficients a_p of the L-series $L_E(s)$ at all good primes p (all but finitely many). By the Tate-Faltings Theorem (Theorem 25.36), this is more than enough to uniquely determine E up to isogeny, which then determines the entire L-series of E, including the Euler factors at bad primes.

We also have the *mod-ℓ Galois representation*

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

which is equivalent to composing $\rho_{E,\ell}$ with the map from $\mathrm{GL}_2(\mathbb{Z}_\ell)$ to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ that reduces each matrix coefficient modulo ℓ.

[2] You can view elements of Z_ℓ as infinite sequences of integers $(a_1, a_2, a_3, \ldots)$ with $a_n \equiv a_{n+1} \bmod \ell^n$, and ring operations defined coordinate-wise. We embed $\mathbb{Z}$ in $\mathbb{Z}_\ell$ via the map $a \mapsto (a, a, a, \ldots)$. Note that the ring $\mathbb{Z}_\ell$ has characteristic 0, but we can reduce any element modulo ℓ (or ℓ^n).

26.4 Serre's modularity conjecture

Let us now forget about elliptic curves for a moment and consider an arbitrary (continuous)[3] ℓ-adic Galois representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. We say that ρ is *modular* (of weight k and level N) if there exists a modular form $f_\rho = \sum a_n q^n$ in $S_k^{\mathrm{new}}(\Gamma_0(N))$ with $a_n \in \mathbb{Z}$ such that

$$\operatorname{tr}\rho(\mathrm{Frob}_p)) = a_p$$

for all primes p that do not divide ℓN (note that the set $\{p : p|\ell N\}$ is exactly analogous to the set S we defined earlier). Similarly, if we have a mod-ℓ representation $\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we say that $\overline{\rho}$ is modular if

$$\operatorname{tr}\overline{\rho}(\mathrm{Frob}_p) \equiv a_p \bmod \ell$$

for all primes p not dividing ℓN.

Let $c \in G_{\mathbb{Q}}$ be the automorphism corresponding to complex conjugation. We say that a Galois representation ρ is *odd* if $\det\rho(c) = -1$. This is necessarily the case if $\rho = \rho_{E,\ell}$ is a Galois representation associated to an elliptic curve. One way to see this is to base change E to $\mathbb{C}$ and view it as an elliptic curve over $\mathbb{C}$ that is isomorphic to a torus $\mathbb{C}/L$ for some lattice $L = [1,\tau]$. For a suitable choice of basis $\{P, Q\}$ for the ℓ^n-torsion subgroup of $\mathbb{C}/L$ in which P has real coordinates, complex conjugation fixes P and sends Q to $-Q$ (this is easy to see when $\operatorname{re}\tau = 0$ and it is true in general). Since we already know that every $f = \sum a_n q^n$ in $S_k^{\mathrm{new}}(\Gamma_0(N))$ with $a_n \in \mathbb{Z}$ gives rise to an elliptic curve (see Theorem 25.35), this constraint also applies to Galois representations associated to modular forms (at least when the weight k is 2).

We want to impose a further constraint on the Galois representations we will consider that is not always satisfied by the representation $\overline{\rho}_{E,\ell}$ associated to an elliptic curve $E/\mathbb{Q}$, but which usually is (and always is for $\ell > 163$). We say that a Galois representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is *irreducible* if its image does not fix any of the one-dimensional subspaces of $(\mathbb{Z}/\ell\mathbb{Z})^2$; equivalently, if its image is conjugate to a subgroup of the upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (a *Borel* subgroup, under the terminology introduced in Problem Set 13).

In 1975 Serre made the following remarkable conjecture, which he refined in [10].

Theorem 26.1 (Serre's modularity conjecture)**.** *Every odd irreducible Galois representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is modular.*

Moreover, Serre gave a precise recipe for what the optimal weight and level of the corresponding modular form f_ρ should be. In the case of the curve $E_{a,b,c}$ arising from a solution $a^p + b^p = c^p$ to Fermat's equation, Serre's recipe gives the weight $k = 2$ and the level $N = 2$. But if Serre's conjecture is true (including the recipe for the weight and level), then the mod-ℓ Galois representation $\overline{\rho}_{E_{a,b,c},\ell}$ associated to $E_{a,b,c}$ cannot possible be modular, simply because $S_2^{\mathrm{new}}(\Gamma_0(2))$ has dimension zero (the genus of $X_0(2)$). This means that $E_{a,b,c}$ cannot be a modular: if it were the existence of the modular form $f_{E_{a,b,c}}$ would imply that the representation $\rho_{E_{a,b,c},\ell}$, and therefore $\overline{\rho}_{E_{a,b,c},\ell}$, is modular.

Serre's conjecture is now a theorem, proved in 2008 by Khare and Wintenberger [6, 7], but this came long after the proof of Fermat's Last Theorem. However, Serre formulated a narrower conjecture, the *epsilon conjecture*, that is still strong enough to imply that $E_{a,b,c}$ cannot be modular, and Ribet proved the epsilon conjecture in 1986 [9].

[3] As pro-finite groups, both $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/Q)$ and $\mathrm{GL}_2(\mathbb{Z}_\ell)$ have a topology; every ℓ-adic Galois representation is required to be continuous with respect to this topology; if are not familiar with the pro-finite topology, don't worry, it has no impact on our discussion here.

26.5 The modularity lifting theorem

Ribet's theorem implies that the elliptic curve $E_{a,b,c}$ is not modular. The final and most difficult step is to show that if the elliptic curve $E_{a,b,c}$ exists, then in fact it *is* modular, yielding a contradiction. It then follows that no elliptic curves $E_{a,b,c}$ can exist, and therefore there are no solutions (a, b, c) to Fermat's equation $x^p + y^p = z^p$ for any odd prime p. Andrew Wiles, with the assistance of Richard Taylor,[4] proved the stronger statement that every semistable elliptic curve over $\mathbb{Q}$ is modular (recall that $E_{a,b,c}$ is semistable).

A key element of the proof is a technique now known as *modularity lifting*. Let E be an elliptic curve over $\mathbb{Q}$ and let ℓ be a prime. Wiles uses modularity lifting to show that if the mod-ℓ Galois representation $\overline{\rho}_{E,\ell}$ of semistable elliptic curve $E/\mathbb{Q}$ is modular, then the ℓ-adic representation $\rho_{E,\ell}$ is also modular, which in turn implies that E is modular.

Given a representation $\rho_0\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, a representation $\rho_1\colon G_S \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ whose reduction modulo ℓ is equal to ρ_0 is called a *lift* of ρ_0. More generally, if R is a suitable ring[5] with a reduction map to $\mathbb{Z}/\ell\mathbb{Z}$, and $\rho_1\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(R)$ is a representation whose reduction is equal to ρ_0, then we say that ρ_1 is a lift of ρ_0 (to R). Two lifts of ρ_0 are said to be *equivalent* if they are conjugate via an element in the kernel of the reduction map from $\mathrm{GL}_2(R)$ to $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. 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 proving the existence of certain *universal deformations*, Wiles was able to show that if ρ_0 is modular, then *every* lift of ρ_0 satisfying a specified list of properties is modular, and he was able to ensure that this list of properties is satisfied by the ℓ-adic representation $\rho_{E,\ell}$ associated to a semistable elliptic curve E.[6] We thus have the following theorem.

Theorem 26.2 (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).*

26.6 Proof of Fermat's Last Theorem

It remains only to find a modular representation $\rho_0\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ that we can lift to $\rho_{E,\ell}$. The obvious candidate is $\overline{\rho}_{E,\ell}$, for some suitable choice of ℓ. It is not clear that proving the modularity of $\overline{\rho}_{E,\ell}$ modular is necessarily any easier than proving the modularity of $\rho_{E,\ell}$, but thanks to work of Langlands and Tunnel on a special case of Langlands' Reciprocity Conjecture [2, Ch. 6], we have the following result for $\ell = 3$.

Theorem 26.3 (Langlands-Tunnel). *Let E be an elliptic curve over $\mathbb{Q}$. If $\overline{\rho}_{E,3}$ is irreducible, then it is modular.*

The only difficulty is that $\overline{\rho}_{E,3}$ is not always going to be irreducible. If E has a rational point of order 3, for example, $\overline{\rho}_{E,3}$ will definitely be reducible. More generally, this will be the happen whenever E admits a rational 3-isogeny. However, if E is semistable and $\overline{\rho}_{E,3}$ is reducible then $\overline{\rho}_{E,5}$ must be irreducible. The reason is that if both $\overline{\rho_{E,3}}$ and $\overline{\rho}_{E,5}$

[4] Wiles' retracted his initial proof due to a gap that was found. Richard Taylor helped Wiles to circumvent this gap, which was the last critical step required to obtain a complete proof; see [3] for an accessible account.

[5] A complete local Noetherian ring with residue field $\mathbb{F}_\ell$.

[6] This one sentence encompasses most of the proof and glosses over a massive amount of detail; unfortunately, in order to meaningfully say more than this we need to introduce a lot of additional material. We refer the interested reader to [2], which contains not only a detailed overview of the proof, but many chapters devoted to the background material needed to understand it.

were irreducible then E would admit a rational 15 isogeny and correspond to a non-cuspidal $\mathbb{Q}$-rational point on the modular curve $X_0(15)$. This modular curve does in fact have four non-cuspidal $\mathbb{Q}$-rational points, but it turns out that none of these points corresponds to a semistable elliptic curve.

Unfortunately there is no analog of the Langlands-Tunnel theorem for $\ell = 5$. Indeed, the case $\ell = 3$ is quite special: the group $\mathrm{PGL}(2, \mathbb{Z}/3\mathbb{Z}) \simeq S_4$ is solvable, something that is not true for any prime $\ell > 3$ (and the case $\ell = 2$ has other problems). So we would seem to be stuck. But Wiles very cleverly proved the following result, which is now known as the *3-5 trick*.

Theorem 26.4 (Wiles)**.** *Let $E/\mathbb{Q}$ be a semistable elliptic curve for which $\overline{\rho}_{E,5}$ is irreducible. Then there is another semistable elliptic curve $E'/\mathbb{Q}$ such that*

- *$\overline{\rho}_{E',3}$ is irreducible,*
- *$\overline{\rho}_{E',5} \simeq \overline{\rho}_{E,5}$.*

Now we are in business.

Theorem 26.5 (Wiles)**.** *Let $E/\mathbb{Q}$ be a semistable elliptic curve. Then E is modular.*

Proof. There are two cases. If $\overline{\rho}_{E,3}$ is irreducible then:

- $\overline{\rho}_{E,3}$ is modular, by the Langlands-Tunnel theorem,
- $\rho_{E,3}$ is modular, by the modularity lifting theorem,
- E is modular, since $f_E = f_{\rho_{E,3}}$.

On the other hand, if $\overline{\rho}_{E,3}$ is reducible, then:

- $\overline{\rho}_{E,5}$ is irreducible, because $X_0(15)$ has no non-cuspidal $\mathbb{Q}$-rational points that correspond to semistable elliptic curves,
- there exists a semistable $E'/\mathbb{Q}$ with $\overline{\rho}_{E',3}$ irreducible and $\overline{\rho}_{E'5} \simeq \overline{\rho}_{E,5}$, by the 3-5 trick,
- $\rho_{E',3}$ is modular, by the Langlands-Tunnel theorem,
- $\rho_{E',3}$ is modular, by the modularity lifting theorem,
- E' is modular, since $f_{E'} = f_{\rho_{E',3}}$,
- $\rho_{E',5}$ and therefore $\overline{\rho}_{E',5}$ is modular, since $f_{\rho_{E',5}} = f_{E'}$,
- $\overline{\rho}_{E,5} \simeq \overline{\rho}_{E',5}$ is modular,
- $\rho_{E,5}$ is modular, by the modularity lifting theorem,
- E is modular, since $f_E = f_{\rho_{E,5}}$.

Quod erat demonstrandum. □

Corollary 26.6. *$x^n + y^n = z^n$ has no integer solutions with $xyz \neq 0$ for $n > 2$.*

References

[1] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, Journal of the American Mathematical Society **14** (2001), 843–939.

[2] G. Cornell, J.H. Silverman, G. Stevens, *Modular forms and Fermat's Last Theorem*, Springer, 1998.

[3] G. Faltings, *The proof of Fermat's last theorem by R. Taylor and A. Wiles*, Notices of the American Mathematical Society **42** (1995), 743–746.

[4] G. Frey, *Links between stable elliptic curves and certain diophantine equations*, Annales Universitatis Saraviensis. Series Mathematicae **1** (1986), 1–40.

[5] Y. Hellegouarch, *Courbes elliptiques et équation de Fermat*. Thèse, Besançon, (1972).

[6] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, Inventiones Mathematicae **178** (2009), 485–586.

[7] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (II)*, Inventiones Mathematicae **178** (2009), 485–586.

[8] J.S. Milne, *Elliptic curves*, BookSurge Publishers, 2006.

[9] K. Ribet, *On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*, Inventiones Mathematicae **100** (1990), 431–476.

[10] J.-P. Serre, *Sur les représentationes modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*, Duke Mathematics Journal **54** (1987), 179–230.

[11] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer, 1994.

[12] A. Weil, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Mathematische Annalen **168** (1967), 149–156.

[13] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics **141** (1995), 553–572.

[14] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics **141** (1995), 443-551.

18.783 Elliptic Curves
Spring 2015