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 well beyond the scope of this course, but we will at least outline its main components.

Before discussing Fermat's Last Theorem, we first conclude our discussion of L-series of elliptic curves.

25.1 The L-series of an elliptic curve

In the previous lecture we defined the L-series $L_E(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ of an elliptic curve $E/\mathbb{Q}$, and its conductor N_E, and we said that E is *modular* if the function $f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n$ is a modular form of weight 2 for $\Gamma^0(N)$, where $q = e^{2\pi i\tau}$. The modularity conjecture of Taniyama, Shimura, and Weil[1] states that every $E/\mathbb{Q}$ is modular. This is now a theorem [2].

Theorem 25.1 (Modularity conjecture)**.** *Every elliptic curve $E/\mathbb{Q}$ is modular.*

When E is modular, the L-series of E and the modular form f_E necessarily coincide, and this implies that $L_E(s)$ has an analytic continuation and satisfies a functional equation, since this holds for the L-series of a modular form; see Theorem 24.20. But prior to the proof of the modularity conjecture, this was an open question known as the Hasse-Weil conjecture.

Theorem 25.2 (Hasse-Weil conjecture)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then $L_E(s)$ has an analytic continuation to a meromorphic function on $\mathbb{C}$, and*

$$\tilde{L}_E(s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s)$$

satisfies the functional equation

$$\tilde{L}_E(s) = w_e\tilde{L}_E(2-s),$$

where $w_e = \pm 1$.

The sign w_E in the functional equation is called the *root number* of E. If $w_E = -1$ then the functional equation implies that $\tilde{L}_E(s)$, and therefore $L_E(s)$, has a zero at $s = 1$; in fact it is not hard to show that $w_E = 1$ if and only if $L_E(s)$ has a zero of even order at $s = 1$.

The conjecture of Birch and Swinnerton-Dyer (BSD) relates the behavior of $L_E(s)$ at $s = 1$ to the rank of $E(\mathbb{Q})$. Recall that

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\mathrm{tor}} \times \mathbb{Z}^r,$$

where $E(\mathbb{Q})_{\mathrm{tor}}$ denotes the torsion subgroup of $E(\mathbb{Q})$ and r is the *rank* of E.

[1] Each of these mathematicians contributed to this conjecture; the relationship between the conductor and the level of the modular form that is included in our definition of modularity is due to Weil [12].

Conjecture 25.3 (Weak BSD conjecture)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of rank r. Then $L_E(s)$ has a zero of order r at $s = 1$.*

The strong version of the BSD conjecture makes a more precise statement, but a proof of even the weak version is enough to claim the million dollar Clay prize.

There is also the weaker parity conjecture, which relates the root number w_E in the functional equation to the parity of r.

Conjecture 25.4 (Parity conjecture)**.** *Let $E/\mathbb{Q}$ be an elliptic curve of rank r. Then the root number is given by $w_E = (-1)^r$.*

25.2 Modular elliptic curves

The relationship between elliptic curves and modular forms is remarkable and not at all obvious. It is reasonable to ask why people believed the modular conjecture in the first place. The most compelling reason is that every newform of weight 2 (a normalized eigenform of $S_2^{\text{new}}(\Gamma_0(N))$ for some N, see §24.6 in Lecture 24) gives rise to a modular elliptic curve.

Theorem 25.5 (Eichler-Shimura)**.** *Let $f = \sum a_n q^n$ be a weight 2 newform for $\Gamma_0(N)$ with $a_n \in \mathbb{Z}$. Then there exists an elliptic curve $E/\mathbb{Q}$ of conductor N for which $f_E = f$.*

See [8, V.6] for details of how to construct the elliptic curve given by the theorem.

The elliptic curve E whose existence is guaranteed by the Eichler-Shimura theorem is only determined up to isogeny.[2] This is due to the fact that isogenous elliptic curves E and E' over $\mathbb{Q}$ must have the same L-series, and therefore $f_E = f_{E'}$. It is easy to show that the a_p values in the L-series of E and E' must agree at every prime p at which both curves have good reduction (all but finitely many primes), and it turns out that in fact E and E' must have the same reduction type at every prime so their L-series are actually identical. The converse also holds, but this is not so easy to show. In fact, something even stronger is true [8, Thm. V.4.1].

Theorem 25.6 (Tate-Faltings)**.** *Let E and E' be elliptic curves over $\mathbb{Q}$ with L-series $L_E(s) = \sum a_n n^{-s}$ and $L_{E'}(s) = \sum a'_n n^{-s}$, respectively. If $a_p = a'_p$ for sufficiently many primes p of good reduction for E and E', then E and E' are isogenous.*

What "sufficiently many" means depends on the curves E and E', but the key point is that it is a finite number.

For any positive integer N, one can enumerate all the newforms in $S_2^{new}(\Gamma_0(N))$ with integral q-expansions; this is a finite list. It is also possible (but not easy) to enumerate all the isogeny classes of elliptic curves with conductor N; this is also a finite list. When this was done for various small values of N, it was found that the two lists matched perfectly in every case. Some explicit examples can be found in the Sage worksheet https://hensel.mit.edu:8002/home/pub/16/. It was examples like these that made the modularity conjecture truly compelling.

As noted above, the modularity conjecture has now been proved. It was Andrew Wiles who made the first real breakthrough that led to its proof. As a side benefit, this allowed him to the prove Fermat's Last Theorem, but for number theorists the proof of the modularity conjecture is far more significant in its implications.[3]

[2] There is an "optimal" representative for each isogeny class; see John Cremona's appendix to [1].

[3] It is worth noting that Gauss did not consider Fermat's Last Theorem an interesting problem, but I suspect he would have been quite taken with the modularity conjecture.

25.3 Fermat's Last Theorem

In 1637, 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 some of the progress made toward proving Fermat's Last Theorem prior to Wiles' work is given below.

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 to suggest a connection between elliptic curves and Fermat's Last Theorem was Yves Hellegouarch. In his 1972 doctoral thesis [6], 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

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

Without loss of generality we may assume that $\gcd(a, b, c) = 1$, with $a \equiv 3 \bmod 4$ and $b \equiv 0 \bmod 2$. 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 conjectured that the elliptic curve $E_{a,b,c}$, if it existed, could not possibly be modular [5]. Shortly thereafter, Jean-Pierre Serre reduced Frey's conjecture to a much more precise statement about modular forms and Galois representations, known as the *epsilon conjecture*, which was then proved in 1986 by Ken Ribet [9], showing that the Modularity Conjecture implies Fermat's Last Theorem.

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

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

This discriminant is not quite minimal; the minimal discriminant is $\Delta_{\min} = 2^{-8}(abc)^{2p}$. The key point is that $\Delta_{\min}$ grows exponentially with p, but the conductor $N_{a,b,c}$ of $E_{a,b,c}$ is much smaller; in fact it turns out that

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

where ℓ ranges over the prime divisors of abc.

But it is very unusual to have the minimal discriminant be so much larger than the conductor. In fact a conjecture of Szpiro states that for every $\epsilon > 0$ there is a constant C such that the minimal discriminant $\Delta_{\min}$ of any elliptic curve $E/\mathbb{Q}$ satisfies

$$\Delta_{\min} \leq C N_E^{6+\epsilon},$$

which would certainly not be true of $E_{a,b,c}$ for any sufficiently large p. Now the fact that the minimal discriminant of $E_{a,b,c}$ is so much larger than its conductor 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. To see the connection with modularity, we need to discuss Galois representations, which is the topic of the next section.

Before leaving this discussion, let us note that the conductor $N_{a,b,c}$ is squarefree, hence $E_{a,b,c}$ is semistable (meaning that it does not have additive reduction at any prime). To prove Fermat's Last Theorem it is not necessary to prove the modularity conjecture in its totality, it is enough to show that every semistable elliptic curve $E/\mathbb{Q}$ is modular, which is precisely what Wiles did.

25.4 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 $E[\ell]$. 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. Recall from Lecture 22 that this means that the principal ideal $p\mathcal{O}_K$ factors into a product of *distinct* prime ideals in the ring of integers $\mathcal{O}_K$. There is then an isomorphism between the decomposition group

$$D_{\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma\mathfrak{p} = \mathfrak{p}\}$$

and the Galois group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$, where $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ is the *residue field* of $\mathfrak{p}$. The unique element of $D_{\mathfrak{p}}$ corresponding to the Frobenius map $x \to x^p$ in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ is called a *Frobenius element*. We may get different Frobenius elements for different choices of $\mathfrak{p}$, but they are all conjugate under the action of $\mathrm{Gal}(K/\mathbb{Q})$. We let Frob_p denote the conjugacy class of Frobenius elements and call it "the" Frobenius element, keeping in mind that this "element" is really a conjugacy class.

For any prime $p \notin S$, the characteristic polynomial of $A_p = \rho(\mathrm{Frob}_p) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is

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

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 mod p.

We can similarly consider the representation

$$\rho\colon G \to \operatorname{Aut}(E[\ell^n]) \simeq \operatorname{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}),$$

for any positive integer n. For all primes $p \notin S$ with $4\sqrt{p} \le \ell^n$, the value of the integer $a_p \equiv \operatorname{tr}\rho(\operatorname{Frob}_p) \bmod \ell^n$ is uniquely determined. It does not matter which prime ℓ we pick, any ℓ will work.

The above discussion applies not only to the field K, but to any Galois extension of $\mathbb{Q}$ containing K. So let G_S to be the absolute Galois group of the maximal algebraic extension of $\mathbb{Q}$ that is unramified at all primes $p \notin S$, and let

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

be the ℓ-adic Tate module of E. We then have the *ℓ-adic Galois representation*

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

where $\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z}$ is the ring of ℓ-adic integers, which contains $\mathbb{Z}$ as a proper subring.[4] For any $p \notin S$ we then have $\operatorname{tr}\rho_{E,\ell}(\operatorname{Frob}_p) = a_p$, as elements of $\mathbb{Z}$. Thus the representation $\rho_{E,\ell}$ determines infinitely many prime index coefficients a_p of the L-series of E. By Theorem 25.6, this determines the isogeny class of E and therefore the entire L-series of E.

We also have the *mod-ℓ Galois representation*

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

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

25.5 Serre's modularity conjecture

Let us now forget the elliptic curve E and consider an arbitrary (continuous) ℓ-adic Galois representation $\rho\colon G_S \to \operatorname{GL}_2(\mathbb{Z}_\ell)$, where S is some finite set of primes that contains ℓ. We say that ρ is *modular* (of even weight k and level N) if there exists a modular form $f_\rho = \sum a_n q^n$ in $S_k^{\text{new}}(\Gamma_0(N)$ with $a_n \in \mathbb{Z}$ such that $\operatorname{tr}\rho(\operatorname{Frob}_p)) = a_p$ for all primes $p \notin S$. Similarly, if we have a mod-ℓ Galois representation $\rho\colon G_S \to \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we say that ρ is modular if $\operatorname{tr}\rho(\operatorname{Frob}_p) \equiv a_p \bmod \ell$ for all primes $p \notin S$.

Let $\sigma \in G_S$ denote the complex conjugation automorphism. We say that a Galois representation ρ is *odd* if $\rho(\sigma)$ is the scalar matrix $-\mathrm{Id}$, corresponding to multiplication by -1. We say that ρ is *irreducible* if its image does not fix any of the one-dimensional subspaces of $(\mathbb{Z}/\ell\mathbb{Z})^2$. In 1975 Serre made the following remarkable conjecture, which he refined in [10].

Theorem 25.7 (Serre's modularity conjecture)**.** *Every odd irreducible Galois representation $\rho\colon G_S \to \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is modular.*

[4] If you have not seen the ring of ℓ-adic integers before, think of its elements as formal power series in ℓ. Each integer $n \in \mathbb{Z}$ corresponds to a polynomial whose coefficients are given by writing n in base ℓ.

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, because the dimension of $S_2^{\text{new}}(\Gamma_0(2))$ is zero! 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 [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].

25.6 Wiles' proof

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 $E_{a,b,c}$ 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,[5] 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 lifiting 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 $\rho_0\colon G_S \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, 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[6] with a reduction map to $\mathbb{Z}/\ell\mathbb{Z}$, and $\rho_1\colon G_S \to \mathrm{GL}_2(R)$ 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.[7] Thus we have the following theorem.

Theorem 25.8 (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).*

It remains only to find a modular representation $\rho_0\colon G_S \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ 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

[5] Wiles' retracted his initial proof because it contained a gap. Richard Taylor helped Wiles to circumvent that gap; see [4].

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

[7] 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 [3], which contains not only a detailed overview of the proof, but many chapters devoted to the background material needed to understand it.

proving modularity for $\overline{\rho}_{E,\ell}$ modular is necessarily any easier than proving modularity for $\rho_{E,\ell}$, but thanks to work of Langlands and Tunnel on a special case of Langlands' Reciprocity Conjecture [3, Ch. 6], we can use the following result for $\ell = 3$.

Theorem 25.9 (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 be reducible. But in this case it is not hard to show that $\overline{\rho}_{E,5}$ must be irreducible, for if it were reducible then E would be isogenous to an elliptic curve $E'/\mathbb{Q}$ with a point of order 3 and a point of order 5, hence a point of order 15; but this is prohibited by Mazur's torsion theorem.

Unfortunately there is no analog of the Langlands-Tunnel theorem for $\ell = 5$. Indeed, the case $\ell = 3$ is quite special: the group $\mathrm{PGL}(2, \mathbb{Z}/\ell\mathbb{Z}) \simeq S_4$ is solvable, something that is not true for any $\ell > 3$ (the case $\ell = 2$ hs problems of its own). So we would seem to be stuck. But Wiles very cleverly proves the following theorem.

Theorem 25.10 (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*

(a) $\overline{\rho}_{E',3}$ is irreducible,

(b) $\overline{\rho}_{E',5} \simeq \overline{\rho}_{E,5}$.

Now we are in business. Suppose $E/\mathbb{Q}$ is a semistable elliptic curve. If $\overline{\rho}_{E,3}$ is irreducible then we can apply the Langlands-Tunnel theorem and Wiles' lifting theorem to prove that E is modular. On the other hand if $\overline{\rho}_{E,3}$ reducible, then $\overline{\rho}_{E,5}$ is irreducible, and we can apply Theorem 25.10 to obtain a semistable elliptic curve $E'/\mathbb{Q}$ for which $\overline{\rho}_{E',3}$ is irreducible, and by applying the Langlands-Tunnel theorem and Wiles' lifting theorem we can prove that E' is modular. But then $\overline{\rho}_{E',5}$ is modular, and by part(b) of the theorem, so is $\overline{\rho}_{E,5} \simeq \overline{\rho}_{E',5}$. Now we can apply Wiles' lifting theorem to $\overline{\rho}_{E,5}$, and we again find that E is modular. Q.E.D.

References

[1] Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure and Applied Mathematics Quarterly **2** (2006), 617–636.

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

[3] Gary Cornell, Joseph H. Silverman, Glenn Stevens, *Modular forms and Fermat's Last Theorem*, Springer, 1998.

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

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

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

[7] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture*, Inventiones Mathematicae **178** (2009), 485–586.

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

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

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

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

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

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

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

18.783 Elliptic Curves
Spring 2013