Formalizing Fermat, Lecture 4

Kevin Buzzard, Imperial College London

EPSRC TCC, 19th Feb 2026

Summary of where we are

We just beat Level 4.

So we proved the following theorem:

Theorem
Modulo results proved in the 1980s, statement B4 implies FLT.

What is B4?

Before I remind you of that, let me remind you of what it means for a 2-dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to be *hardly ramified*.

Hardly ramified: reminder

Let R be a coefficient ring (compact Hausdorff local ring) with odd residue characteristic ℓ, and say V/R is free of rank 2 with the product topology.

A continuous group homomorphism $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_R(V)$ (which I'm going to shorten to "R-representation") is *hardly ramified* if:

- $det(\rho) = \chi$ the ℓ-adic cyclotomic character;
- ρ is unramified outside 2 and ℓ;
- ρ is flat at ℓ;
- ρ at 2 has a rank 1 quotient where $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ acts via an unramified character whose square is trivial.

B4: reminder

We've proved B4 implies FLT modulo the 1980s.

What was B4?

B4: if $\ell \geq 5$ is prime, V is 2-dimensional over $R := \mathbb{Z}/\ell\mathbb{Z}$ and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_R(V)$ is continuous and hardly ramified, then ρ is reducible.

One-line summary of proof of B4 implies FLT: look at ℓ-torsion in the Frey curve, and use Mazur.

This is 1980s mathematics.

We're going to prove B4 (modulo 1980s) using newer techniques.

Level 5: from ℓ to 3

Wiles crucially used the prime 3 in his work.

Wiles proved facts about the Frey curve by analysing its 3-torsion.

In level 5, we will also move from ℓ to 3.

But the big question is: given a hardly ramified mod ℓ representation, how do we build a mod 3 representation?

The Frey curve has gone.

Lifting irreducible Galois representations

Definition of statement B5a: Let $\ell \geq 5$ be a prime, let $V/(\mathbb{Z}/\ell\mathbb{Z})$ be a 2-dimensional vector space, and let $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathit{Aut}_{\mathbb{Z}/\ell\mathbb{Z}}(V)$ be an irreducible hardly ramified $\mathbb{Z}/\ell\mathbb{Z}$-Galois representation.

(i.e., the thing which B4 says doesn't exist).

Then there exists a finite extension K of $\mathbb{Q}_\ell$ with integers $\mathcal{O}$ having maximal ideal $\mathfrak{m}$, a finite free $\mathcal{O}$-module $\mathcal{V}$ of rank 2, and a hardly ramified Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathit{Aut}_{\mathcal{O}}(\mathcal{V})$ such that ρ mod $\mathfrak{m}$ is isomorphic to (the base extension to $\mathcal{O}/\mathfrak{m}$ of) $\overline{\rho}$.

B5a slogan: "An irreducible hardly ramified $\mathbb{Z}/\ell\mathbb{Z}$-representation lifts to an ℓ-adic hardly ramified representation."

Note to those still thinking about the Tate curve:

The ℓ-adic Tate module of the Frey curve won't do, because (unlike the ℓ-torsion) it will be ramified at all primes dividing *abc*.

Spreading out hardly ramified representations

If you think that theorem B5a is surprising, then B5b is even more surprising.

Definition of statement B5b: Say $\ell \geq 5$ is a prime, $\mathcal{O}$ is the integers in a finite extension K of $\mathbb{Q}_\ell$, $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$, and $\mathcal{V}$ is a free rank 2 $\mathcal{O}$-module.

Say $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathit{Aut}_{\mathcal{O}}(\mathcal{V})$ is a hardly ramified representation and ρ mod $\mathfrak{m}$ is irreducible and has all traces in $\mathbb{Z}/\ell\mathbb{Z}$ (i.e., descends to $GL_2(\mathbb{Z}/\ell\mathbb{Z})$).

(Note that we just produced one of these in B5a.) Then

(i) there exists a number field $M \subset K$ and elements $t_p \in M$ for all $p \neq 2, \ell$ such that $\mathit{trace}(\rho(\mathit{Frob}_p)) = t_p$ for all $p \neq 2, \ell$ ("arithmetic elements have arithmetic traces");

and furthermore

(ii) for every maximal ideal P of the integer ring $\mathcal{O}_M$ with residue field of characteristic $p \neq 2$ there's a hardly ramified p-adic representation $\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_{M,P})$ satisfying $tr(\rho_P(\mathit{Frob}_q)) = t_q$ for all primes $q \neq 2, p, \ell$.

Spreading out hardly ramified representations

Slogan for B5b: an ℓ-adic hardly ramified representation "spreads out" into a compatible family of hardly ramified p-adic representations.

In the 1980s this was completely out of reach.

In the 1990s humans could prove results like this, under an additional assumption that the mod ℓ reduction of the representation came from a modular form.

The extraordinary thing about B5b is that it has no residual modularity hypothesis.

The modularity hypothesis is replaced by a "residual representation descends to $GL_2(\mathbb{Z}/\ell\mathbb{Z})$" hypothesis.

B5b enables us to move from ℓ to 3.

A word on compatible families

We all learn as undergraduates that "two finite-dimensional representations with the same trace are isomorphic."

This is true for representations of finite groups over fields of characteristic zero.

In characteristic p, or with infinite groups, you have to be careful about semisimplicity (as we'll see later).

But B5b is exhibiting a completely different phenomenon.

The 2-adic and 3-adic cyclotomic characters χ_2 and χ_3 are two totally different representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, to $\mathbb{Z}_2^\times$ and $\mathbb{Z}_3^\times$.

Their kernels are the disjoint fields $\mathbb{Q}(\mu_{2^\infty})$ and $\mathbb{Q}(\mu_{3^\infty})$.

And yet if $p \geq 5$ is a prime, $\chi_2(Frob_p) = p \in \mathbb{Z}_2^\times$ and $\chi_3(Frob_p) = p \in \mathbb{Z}_3^\times$.

So the traces are taking values in the integers of $\mathbb{Q}$ and are "the same".

For a "random" non-arithmetic element g of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\chi_2(g)$ and $\chi_3(g)$ will probably be totally unrelated.

This phenomenon is the beginning of the theory of motives.

3-adic hardly ramified representations

Here's a really strong theorem about hardly ramified 3-adic representations.

Definition of statement B5c: Say $\mathcal{O}$ is the integers in a finite extension K of $\mathbb{Q}_3$, $\mathcal{V}$ is a free rank 2 $\mathcal{O}$-module, and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathit{Aut}_{\mathcal{O}}(\mathcal{V})$ is a hardly ramified $\mathcal{O}$-representation.

Then $\rho \cong \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ where χ is the 3-adic cyclotomic character.

Boss theorem

Here's a summary of our B5 statements. All representations in the below are hardly ramified.

B5a: irreducible $\mathbb{Z}/\ell\mathbb{Z}$-representation lifts to an ℓ-adic one if $\ell \geq 5$.

B5b: Such an ℓ-adic representation spreads out to a compatible family.

B5c: 3-adic representation is an extension of trivial by cyclotomic.

Level 5 boss theorem: Statements B5a, B5b and B5c together imply FLT.

The shocking fact about the B5 theorems is that they are provable, even though none of them have the word "modular" in.

All 20th century theorems of this form had modularity assumptions.

So proving them will be 21st century mathematics.

But in this level we don't have to prove them.

We have to prove that they imply FLT.

Beating the level 5 boss

As usual, we only have to prove that B5a, B5b and B5c imply B4, which says that a hardly ramified $\mathbb{Z}/\ell\mathbb{Z}$-representation is reducible.

We prove it by contradiction, so say $\overline{\rho}$ is an irreducible hardly ramified $\mathbb{Z}/\ell\mathbb{Z}$-representation.

By B5a it lifts to a hardly ramified ℓ-adic representation ρ.

By B5b this lifted representation is part of a "compatible family" of hardly ramified P-adic Galois representations (ρ_P).

This family is indexed by P, the maximal ideals (not containing 2) of the integers $\mathcal{O}_M$ of a number field M.

Now let P now be a prime of $\mathcal{O}_M$ above 3.

By B5c we have that $tr(\rho_P(Frob_p)) = \chi(p) + 1 = p + 1$ for all $p \neq 2, 3$.

So by B5b $\rho(Frob_p)$ and hence (by B5a) its reduction $\overline{\rho}(Frob_p)$ also have trace $p + 1$ for all $p \neq 2, 3, \ell$.

Beating the level 5 boss

We have a continuous irreducible $\overline{\rho}$ acting on a 2-dimensional vector space over $\mathbb{Z}/\ell\mathbb{Z}$.

We just saw that B5a,b,c imply $\overline{\rho}(\mathit{Frob}_p)$ has trace $p+1$ for all $p \neq 2, 3, \ell$.

Because the image of $\overline{\rho}$ is finite, $\overline{\rho}$ factors through a finite Galois extension $\mathit{Gal}(L/\mathbb{Q}) \to \mathit{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

By the Cebotarev density theorem (known in 1980s), every element in $\mathit{Gal}(L/\mathbb{Q})$ is a Frobenius element Frob_p for some prime $p \neq 2, 3, \ell$.

So the irreducible $\overline{\rho}$ has the same trace as the representation $\chi + 1$.

The Brauer-Nesbitt theorem (known in 1980s) implies that $\overline{\rho} \cong \chi + 1$. (note that $\ell > 2$.)

But $\overline{\rho}$ is irreducible.

This contradiction completes the proof, and thus completes level 5 🎉.

The moral of level 5

The moral of level 5 is that profound theorems about p-adic Galois representations imply Fermat's Last Theorem.

What we need to now do in this course is to prove B5a, B5b and B5c.

B5c is by far the easiest.

The heart of the argument is an auxiliary lemma classifying mod 3 hardly-ramified representations.

The proof of the lemma is inspired by Tate's original argument from the 1970s that there are no irreducible mod 2 2-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ unramified outside 2.

The argument is harder than Tate's, because it needs deeper results relating discriminants and degrees of number fields. We'll do it next.

B5a and B5b are both consequences of one modularity lifting theorem.

We'll do them after.

Level 6: killing B5c

We have turned FLT into a 3-headed monster, with heads B5a, B5b, B5c.

In this level, we will chop off one of the heads.

Let B6 be the statement that B5a and B5b are true.

Level 6 boss theorem: B6 implies FLT modulo the 1980s.

Proof: We saw in level 5 that B5a, B5b and B5c imply FLT.

So all we have to do is to prove that B5c is true. Let's restate it.

Say $K/\mathbb{Q}_3$ is a finite extension with integers $\mathcal{O}$, and say $\mathcal{V}$ is a finite free rank 2 $\mathcal{O}$-module.

Say $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathit{Aut}_{\mathcal{O}}(\mathcal{V})$ is a hardly ramified $\mathcal{O}$-representation.

Then $\rho \cong \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ where χ is the 3-adic cyclotomic character (and $*$ may or may not be zero).

Reduction mod 3

We deduce this 3-adic result from a mod 3 result.

Let k be a *finite* field of characteristic 3, and say V/k is a rank 2 k-module.

Say $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_k(V)$ is hardly ramified.

Lemma

There's a choice of basis such that $\overline{\rho} \cong \begin{pmatrix} \overline{\chi} & * \\ 0 & 1 \end{pmatrix}$ *where* $\overline{\chi}$ *is the mod 3 cyclotomic character.*

In particular, irreducible mod 3 hardly ramified representations don't exist.

Note that k can be any finite field of characteristic 3, not just $\mathbb{Z}/3\mathbb{Z}$.

Recall that B4 claimed that irreducible hardly ramified representations to $GL_2(\mathbb{Z}/\ell\mathbb{Z})$ don't exist for any $\ell \geq 5$.

Our techniques here, however, are specific to 3, as you'll see.

Remaining goals for today

What's left for today then, is two classification theorems for hardly ramified representations.

Lemma

If k is finite of characteristic 3 and $\overline{\rho}$ is a hardly-ramified k-representation, then $\overline{\rho} \cong \begin{pmatrix} \overline{\chi} & * \\ 0 & 1 \end{pmatrix}$.

Theorem (B5c)

If $\mathcal{O}$ is the integers in a finite extension K of $\mathbb{Q}_3$ and ρ is a hardly ramified $\mathcal{O}$-representation, then $\rho \cong \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$.

We'll first show that the lemma implies B5c modulo the 1970s.

Then we'll spend the rest of the lecture proving the lemma modulo the 1980s.

This will finish level 6.

Hardly ramified base change

Side-quest: to relate the lemma on k-representations to B5c on $\mathcal{O}$-representations we need to check that the mod ℓ reduction of a hardly-ramified representation is hardly-ramified.

But let's go on a side quest and prove the correct theorem, which is that "hardly-ramified" is preserved under arbitrary base change.

So say R_1 and R_2 are two coefficient rings with the same odd residue characteristic ℓ.

Say $f : R_1 \to R_2$ is a continuous ring homomorphism.

Say $\mathcal{V}_1$ is an R_1-module which is R_1-free of rank 2, and $\rho_1 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_{R_1}(\mathcal{V}_1)$ is a hardly ramified R_1-representation.

Let $\mathcal{V}_2 := \mathcal{V}_1 \otimes_{R_1} R_2$; this is of course R_2-free of rank 2.

Say $\rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_{R_2}(\mathcal{V}_2)$ is $\rho_1 \otimes_{R_1} R_2$.

I claim that ρ_2 is also hardly ramified. Let's check the axioms.

Cyclotomic character

Recall that if R is a coefficient ring with residue characteristic ℓ then there's a unique ring homomorphism $\mathbb{Z}_\ell \to R$.

$det(\rho_1) : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to R_1^\times$ is cyclotomic via $\mathbb{Z}_\ell \to R_1$; $det(\rho_2) = det(\rho_1) \otimes_{R_1} R_2$.

So we just need to check that the map $\mathbb{Z}_\ell \to R_2$ is equal to the composite $\mathbb{Z}_\ell \to R_1 \to R_2$.

But this follows from uniqueness.

One axiom down.

Hardly ramified base change

The kernel of ρ_2 is at least as big as the kernel of ρ_1.

So if ρ_1 is unramified outside 2ℓ then so is ρ_2.

Two down, two to go.

Condition at 2

At 2 the hardly-ramified condition is the existence of a $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$-stable R_1-free rank 1 submodule $\mathcal{W}_1 \subseteq \mathcal{V}_1$ with an R_1-free rank 1 quotient $\mathcal{V}_1/\mathcal{W}_1$ on which $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ acts via an unramified character ψ whose square is 1.

Because everything is free, it all just tensors straight up to R_2.

In other words, $\mathcal{W}_1 \otimes_{R_1} R_2$ is an R_2-free rank 1 submodule with quotient $(\mathcal{V}_1 \otimes_{R_1} R_2)/(\mathcal{W}_1 \otimes_{R_1} R_2) \cong (\mathcal{V}_1/\mathcal{W}_1) \otimes_{R_1} R_2$ on which Galois is still acting by ψ.

That's 3/4 axioms done.

But the last one is a little deeper.

Flatness.

Say ρ_1 is flat at ℓ. We need that ρ_2 is flat at ℓ.

So (by definition) if J_2 is an open ideal of R_2 then we want ρ_2 mod $J_2 : \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to Aut_{R_2/J_2}(\mathcal{V}_2/J_2)$ to come from a finite free $\mathbb{Z}_\ell$-Hopf algebra.

The preimage of J_2 is an open ideal $J_1 \subseteq R_1$.

We thus have an injection $\overline{f} : R_1/J_1 \to R_2/J_2$ of *finite* rings with the discrete topology.

By definition of flatness, ρ_1 mod $J_1 : \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to GL_{R_1/J_1}(\mathcal{V}_1/J_1)$ comes from a finite free $\mathbb{Z}_\ell$-Hopf algebra.

We have a flat Galois action on the finite abelian group $\mathcal{V}_1/J_1 \cong (R_1/J_1)^2$ and we need to figure out if its base extension along $\overline{f}$ to $(R_2/J_2)^2$ is still flat.

Let's write $\overline{R}_1 = R_1/J_1$ and $\overline{R}_2 = R_2/J_2$; these are finite rings.

Flatness

We have a finite abelian group $\overline{\mathcal{V}}_1 \cong \overline{R}_1^2$ with a flat Galois action.

We want to understand what happens when we base change to $\overline{\mathcal{V}}_2 \cong \overline{R}_2^2$.

But recall that the definition of flatness doesn't care that the $\overline{R}_i$ are *rings*.

This is just about a Galois action on a *finite abelian group* coming from a Hopf algebra over $\mathbb{Z}_\ell$.

So write the $\overline{R}_1$-module $\overline{R}_2$ as a quotient of $\overline{R}_1^n$ for some natural n.

Then $\overline{\mathcal{V}}_2$ is a quotient of $\overline{\mathcal{V}}_1^n$.

Product of flat is flat; quotient of flat is flat, so we're done.

We've proved that hardly-ramified Galois representations base change!

p-adic representations

We also need a second side-quest, to show that another kind of modification of a hardly-ramified representation is still hardly-ramified.

Say p is an odd prime, K is a finite extension of $\mathbb{Q}_p$, and $\mathcal{O}$ is its ring of integers.

Say $\mathcal{V}$ is a free rank 2 $\mathcal{O}$-module, and $V = \mathcal{V} \otimes_{\mathcal{O}} K$.

If $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_{\mathcal{O}}(\mathcal{V})$ is hardly ramified, then we can base change the coefficient ring to get a continuous representation $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_K(V)$.

What do you think about the claim "ρ hardly ramified iff $\tilde{\rho}$ hardly ramified"?

This does *not make sense*.

Because K is not compact so it's not a coefficient ring.

p-adic representations

$\mathcal{O}$ the integers in $K/\mathbb{Q}_p$ finite.

ρ a hardly ramified $\mathcal{O}$-representation on $\mathcal{V}$; $\tilde{\rho} = \rho \otimes_{\mathcal{O}} K$ on $V := \mathcal{V} \otimes_{\mathcal{O}} K$.

Now say $\mathcal{V}' \subset V$ is any $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable $\mathcal{O}$-submodule of V which is $\mathcal{O}$-free of rank 2.

Then $\tilde{\rho}$ descends to $\rho' : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathit{Aut}_{\mathcal{O}}(\mathcal{V}')$.

We have $\rho \otimes_{\mathcal{O}} K \cong \tilde{\rho} \cong \rho' \otimes_{\mathcal{O}} K$.

I claim that ρ' is also hardly ramified.

Note that ρ' may not be isomorphic to ρ over $\mathcal{O}$, although they have the same trace.

Let me show you an example of this phenomenon.

Example

Say $\mathcal{O} = \mathbb{Z}_p$ and $K = \mathbb{Q}_p$.

Say $\Gamma \subseteq GL_2(\mathbb{Z}_p)$ is the matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $p \mid c$.

(check: this is a subgroup; it's the preimage of the upper-triangular matrices in $GL_2(\mathbb{Z}/p\mathbb{Z})$.)

Then Γ acts naturally on $\mathbb{Z}_p \oplus \mathbb{Z}_p = \mathcal{V}$, and the induced $\rho : \Gamma \to GL_2(\mathbb{Z}_p)$ is the inclusion.

The subspace $\mathcal{V}' := p\mathbb{Z}_p \oplus \mathbb{Z}_p$ is Γ-stable, and the induced $\rho' : \Gamma \to GL_2(\mathbb{Z}_p)$ sends $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $\begin{pmatrix} a & pb \\ c/p & d \end{pmatrix}$.

So ρ mod p is upper-triangular and ρ' mod p is lower-triangular (with different actions on the 1-d invariant subspaces). In particular they're not isomorphic.

Hardly ramified

We have hardly-ramified $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathit{Aut}_{\mathcal{O}}(\mathcal{V})$.

We have its base extension $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathit{Aut}_K(V)$ with $V = \mathcal{V} \otimes_{\mathcal{O}} K$.

We have $\mathcal{V}' \subset V$ another Galois-stable lattice, with associated $\mathcal{O}$-representation ρ'.

Let's check that the hardly-ramified conditions for ρ imply the hardly-ramified conditions for ρ'.

The first two are easy: $\mathit{det}(\rho) = \chi$ iff $\mathit{det}(\tilde{\rho}) = \chi$ iff $\mathit{det}(\rho') = \chi$.

And ρ unramified at ℓ iff $\tilde{\rho}$ unramified at ℓ iff ρ' unramified at ℓ.

The others need a little more thought.

Condition at p

Say ρ is flat at p.

We can multiply $\mathcal{V}'$ by a power of p without changing the isomorphism class of ρ'.

We can thus assume $p^N\mathcal{V} \subseteq \mathcal{V}' \subseteq \mathcal{V}$ for some $N \geq 1$.

Now say J is an open ideal of $\mathcal{O}$. We want to check that $\mathcal{V}'/J\mathcal{V}'$ is a flat $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module.

We know that $\mathcal{V}'/J\mathcal{V}'$ is a Galois-stable submodule of $\mathcal{V}/J\mathcal{V}'$.

And we know that $\mathcal{V}/J\mathcal{V}'$ is a Galois-stable quotient of $\mathcal{V}/p^nJ\mathcal{V}$.

And p^nJ is an open ideal of R, so $\mathcal{V}/p^nJ\mathcal{V}$ is flat.

And flatness transfers over to submodules and quotient modules.

So $\mathcal{V}'/J\mathcal{V}'$ is flat and we're done.

Condition at 2

Finally we need to check the condition at 2.

So say $\mathcal{V}$ has a $\mathcal{O}$-free rank 1 $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$-stable sub $\mathcal{W}$ with an $\mathcal{O}$-free rank 1 quotient $\mathcal{V}/\mathcal{W}$ where $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ acts via an unramified character ψ whose square is 1.

Then so does $V = \mathcal{V} \otimes_{\mathcal{O}} K$, namely $W := \mathcal{W} \otimes_{\mathcal{O}} K \subset \mathcal{V} \otimes_{\mathcal{O}} K$.

We see that $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$ acts via ψ on V/W.

Let $\mathcal{W}' := W \cap \mathcal{V}'$.

Then $\mathcal{W}'$ is $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$-stable, as both W and $\mathcal{V}'$ are.

And the quotient $\mathcal{V}'/\mathcal{W}'$ is nonzero, $\mathcal{O}$-finitely-generated and injects into $V/W \cong K$, so it's isomorphic to $\mathcal{O}$.

Galois acts on it via ψ so we're done!

Remaining goals for today

Let χ be the 3-adic cyclotomic character and $\overline{\chi}$ its mod 3 reduction.

Recall that we're proving the 3-adic and mod 3 classification theorems for hardly ramified representations:

Lemma (Mod 3 lemma)

If k is finite of characteristic 3 and $\overline{\rho}$ is a hardly-ramified k-representation, then $\overline{\rho} \cong \begin{pmatrix} \overline{\chi} & * \\ 0 & 1 \end{pmatrix}$.

Theorem (B5c)

If $\mathcal{O}$ is the integers in a finite extension K of $\mathbb{Q}_3$ and ρ is a hardly ramified $\mathcal{O}$-representation, then $\rho \cong \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$.

Let's now prove that the mod 3 lemma implies the theorem.

The reduction $\overline{\rho}$ is reducible.

$\mathcal{O}$ the integers in $K/\mathbb{Q}_3$ finite, ρ a hardly ramified $\mathcal{O}$-representation.

If $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$ then we've just seen that the reduction $\overline{\rho} = \rho/\mathfrak{m}$ of ρ is also hardly ramified (as it's a base change).

And $\mathcal{O}/\mathfrak{m}$ is a finite field of characteristic 3.

So by the mod 3 lemma (which we're assuming for now), $\overline{\rho} \cong \begin{pmatrix} \overline{\chi} & * \\ 0 & 1 \end{pmatrix}$.

In particular $\overline{\rho}$ is reducible.

Now let $\tilde{\rho} = \rho \otimes_{\mathcal{O}} K$.

I claim that $\tilde{\rho}$ is also reducible.

Indeed this follows from "Ribet's Lemma."

Ribet's Lemma

(2.1) **Proposition.** *Suppose that the K-representation ρ is simple but that its reductions are reducible. Let φ_1 and φ_2 be the characters associated to the reductions of ρ. Then G leaves stable some lattice $L \subset V$ for which the associated reduction is of the form* $\begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$ *but is not semi-simple.*

This is a theorem about 2-dimensional p-adic representations from Ribet's 1976 paper "A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$."

"simple" means "irreducible". $\phi_1 = 1$ and $\phi_2 = \chi$.

The lemma (which is a Proposition!) implies that there's some $\mathcal{O}$-free $\mathcal{V}' \subset V$ whose mod $\mathfrak{m}$ reduction is $\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$ with $* \neq 0$.

But $\mathcal{V}'$ is hardly ramified, so its mod $\mathfrak{m}$ reduction is too.

This contradicts the mod 3 lemma.

Any questions so far?

Reducibility

Hence $\tilde{\rho}$ is reducible, so there's some K-basis of V such that $\rho \cong \begin{pmatrix} \alpha_1 & * \\ 0 & \alpha_2 \end{pmatrix}$.

It's not hard to check that there is some lattice $\mathcal{V}'$ in V such that the corresponding $\mathcal{O}$-representation ρ' is also of this form.

So now α_1 and α_2 restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3)$, being subquotients of a flat representation, are flat.

But because p is odd, the "$e < p - 1$" hypothesis much loved by Fontaine and Raynaud in the 1970s, applies.

In particular, Fontaine's 1977 Asterisque book can be used to classify the 1-dimensional flat representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3)$ (and $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ for $\ell > 2$).

Answer: the only flat 1-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ are unramified representations and unramified twists of the cyclotomic character.

End of proof of B5c

We have α_1 and α_2 3-adic characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, with $\alpha_1(g)$ and $\alpha_2(g)$ the eigenvalues of $\tilde{\rho}(g)$.

Our condition at 2 shows that if g is in an inertia group at 2, then $\tilde{\rho}(g) \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. So both eigenvalues are 1.

Hence the α_i are unramified at 2 and so unramified outside 3.

By the Kronecker–Weber theorem, the α_i hence factor through the cyclotomic extension $\mathbb{Q}(\mu_{3^\infty})$.

So there isn't even any room for an unramified twist – the α_i must either be trivial or cyclotomic (I_3 surjects onto $Gal(\mathbb{Q}(\mu_{3^\infty})/\mathbb{Q})$.)

Their product is cyclotomic, so there's one of each.

Again by the mod 3 lemma, $\rho \cong \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ and B5c is proved.

Classifying mod 3 hardly ramified reps

It remains to prove the mod 3 lemma. Let's restate it.

We have k a finite field of characteristic 3, and V/k free rank 2.

We have $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_k(V)$ and V is finite with the discrete topology.

The claim is that $\overline{\rho} \cong \begin{pmatrix} \overline{\chi} & * \\ 0 & 1 \end{pmatrix}$.

This proof will take the rest of this lecture, and will finish level 6.

First note that, by definition of the topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\overline{\rho}$ factors through an injection $Gal(L/\mathbb{Q}) \hookrightarrow Aut_k(V)$ for L a finite Galois extension of $\mathbb{Q}$.

By our hardly ramified assumption, L is unramified outside 2 and 3.

We also know something about the behaviour of $\overline{\rho}$ at 2 (upper triangular) and 3 (flat).

We need to figure out how to translate these representation-theoretic facts to facts about the number field L.

Local analysis at 2

At 2 we know $\overline{\rho} \cong \begin{pmatrix} \psi\overline{\chi} & * \\ 0 & \psi \end{pmatrix}$

with ψ unramified and order 1 or 2, with $\overline{\chi}$ the mod 3 cyclotomic character (so also unramified at 2) and $*$ unspecified.

So the image of an inertia group I_2 is contained within $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

Note that k is finite but it might be *huge*.

However the maximal 3-torsion quotient of I_2 is cyclic! (known in the 1950s.)

In fact the general theorem is that an inertia subgroup I_p has a normal Sylow p-subgroup and the quotient is pro-cyclic (and isomorphic to $\prod_{\ell \neq p} \mathbb{Z}_\ell$.)

So the image of I_2 is a cyclic $\mathbb{Z}/3\mathbb{Z}$-vector space and thus either trivial, or cyclic of order 3.

In particular, L is *tamely ramified* at 2 (which just means that the image of I_3 in L has order coprime to 2).

Discriminant of a number field

If K is any number field with $[K : \mathbb{Q}] = n$, then there's an integer associated to K called its *discriminant*.

Let me remind you of its definition.

First, note that $K \cong \mathbb{Q}^n$ as a $\mathbb{Q}$-vector space.

If $\lambda \in K$ then multiplication by λ on K is K-linear and hence $\mathbb{Q}$-linear.

So, regarded as a linear endomorphism of a finite-dimensional $\mathbb{Q}$-vector space, it has a *trace* $tr(\lambda)$ in $\mathbb{Q}$.

Discriminant of a number field

K a number field of $\mathbb{Q}$-dimension n.

Let $\mathcal{O}_K$ be the integers of K (the elements which are zeros of monic polynomials with $\mathbb{Z}$ coefficients).

It's well-known that $\mathcal{O}_K \cong \mathbb{Z}^n$ as an abelian group, living in $K \cong \mathbb{Q}^n$.

Let $e_1, e_2, \ldots, e_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$.

Form the $n \times n$ matrix over $\mathbb{Q}$ whose (i, j) entry is $tr(e_i e_j)$.

Its determinant is the *discriminant* of L. It's independent of the choice of basis.

Facts about the discriminant

Now say K is a number field, assumed Galois over $\mathbb{Q}$, and with discriminant d.

Here are some facts.

d is an integer.

We say a prime p *ramifies* in K if the image of one (or all) inertia group(s) I_p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $Gal(K/\mathbb{Q})$ is nontrivial.

It's a fact that the primes dividing d are precisely the primes which ramify in K.

If the ramification is *tame* (that is, the image of I_p has order e prime to p) then the power of p dividing d is exactly $[K : \mathbb{Q}](e-1)/e$.

(This is well-known, and not hard: it follows from the statement that if $p\mathcal{O}_K = (P_1P_2\dots P_g)^e$ then $v_{P_i}(\mathcal{D}_K) = e-1$ where $\mathcal{D}_K$ is the *different* of $K/\mathbb{Q}$.)

(And the norm of the different is the discriminant.)

Back to mod 3 hardly ramified Galois representations

Back to k a finite field of characteristic 3 and $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_k(V)$ hardly ramified, so $\overline{\rho}$ factors through $\overline{\rho} : Gal(L/\mathbb{Q}) \hookrightarrow Aut_k(V)$.

Now $\overline{\rho}$ is unramified outside 2 and 3.

So the discriminant of L is an integer of the form $\pm 2^a 3^b$.

We have seen that $\overline{\rho}$ is tame at 2, and the image of I_2 has size either 1 or 3.

In particular L is tame at 2 with $e = 1$ or $e = 3$.

Hence a is either 0 or $2[L : \mathbb{Q}]/3$.

But what about b?

Local analysis at 3

At 3 we just have this weird condition that $\overline{\rho}$ is flat.

Note that $\overline{\rho}$ is definitely going to be ramified at 3 (as its determinant is).

Let's define a subgroup J_3 of $Gal(L/\mathbb{Q})$, the image of an inertia subgroup I_3 of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let's split the argument into two cases: the tame case and the wild case.

In other words, let's split into the cases where the finite group J_3 has order prime to 3 or a multiple of 3.

Local analysis at 3: the tame case

Say J_3 has order prime to 3.

Then J_3 must be *cyclic* (as it's a continuous image of $\prod_{\ell \neq 3} \mathbb{Z}_\ell$ in a finite group.)

And in particular it's abelian, of order coprime to the characteristic of k.

So, after replacing k with a finite extension k' if necessary, $\overline{\rho}|J_3$ is the direct sum $\phi_1 \oplus \phi_2$ of two characters taking values in $k'^{\times}$.

Now if $Frob_3$ is a Frobenius element in $Gal(L/\mathbb{Q})$, it is well-known that conjugation by $Frob_3$ acts as $x \mapsto x^3$ on J_3.

So $\overline{\rho}(Frob_3)(\overline{\rho}|J_3)(\overline{\rho}(Frob_3)^{-1})$ is $\phi_1^3 \oplus \phi_2^3$.

This is $(\overline{\rho}(Frob_3) \times \overline{\rho} \times \overline{\rho}(Frob_3)^{-1})|J_3$, so it's conjugate, and hence isomorphic, to $\overline{\rho}|J_3$.

So $\phi_1 \oplus \phi_2 \cong \phi_1^3 \oplus \phi_2^3$.

Local analysis at 3: the tame case

We're doing the tame case.

So we're assuming that J_3, a local inertia group at 3 in $Gal(L/\mathbb{Q})$, has order prime to 3.

We've seen that $\overline{\rho}|J_3 \cong \phi_1 \oplus \phi_2$ (over a finite extension k' of k.)

And hence that $\phi_1 \oplus \phi_2 \cong \phi_1^3 \oplus \phi_2^3$.

So we must either have $\phi_1 = \phi_1^3$ and $\phi_2 = \phi_2^3$, or $\phi_1 = \phi_2^3$ and $\phi_2 = \phi_1^3$.

In either case $\phi_1^9 = \phi_1$ and $\phi_2^9 = \phi_2$.

So $\phi_1^8 = \phi_2^8 = 1$.

So $|J_3| \leq 8$.

So if $3^b || disc(L)$ then $b \leq 7[L : \mathbb{Q}]/8$.

Local analysis at 3: the tame case

Upshot: if $\overline{\rho} : Gal(L/\mathbb{Q}) \hookrightarrow Aut_k(V)$ is hardly ramified and tame at 3, then

$$|disc(L)| \leq 2^{2[L:\mathbb{Q}]/3} 3^{7[L:\mathbb{Q}]/8}.$$

So $|disc(L)|^{1/[L:\mathbb{Q}]}$, the so-called *root discriminant* of L, is $\leq 2^{2/3}3^{7/8} < 4.16$.

Also, we know $det(\rho)$ is the mod 3 cyclotomic character, so $\mathbb{Q}(\zeta_3) \subseteq L$.

This implies that $[L : \mathbb{Q}]$ is even.

It also implies that there is no embedding $L \to \mathbb{R}$; we say L is "totally imaginary."

What do we do now? We have a bound for the root discriminant of L.

We look it up in a table.

Poitou's table

Discriminants des corps totalement imaginaires

n =	$\lvert d\rvert^{1/n} \geqslant$	Exemples connus $\lvert d\rvert^{1/n} =$	$\lvert d\rvert =$
2	1.722 119	1.732	3
4	3.254 561	3.289	117
6	4.557 067	4.796	23^3
8	5.659 362	5.786	$2^8\ 17^3$
10	6.600 341	6.841	$3^5\ 31^4$
12	7.412 879	7.774	$3^9\ 19^5$
14	8.122 437	8.468	$2^{14}\ 29^6$
16	8.748 418		
18	9.305 672		

This is part of a table in Poitou's 1977 paper "Sur les petits discriminants."

Turns out: small root discriminant implies small degree.

The table (and paper) implies that if $[L:\mathbb{Q}] \geq 6$ then $|disc(L)|^{1/[L:\mathbb{Q}]} > 4.557$.

So our result $|disc(L)|^{1/[L:\mathbb{Q}]} < 4.16$ implies $[L:\mathbb{Q}] \leq 4$ (recall it's even).

The tame case

Upshot: if $\overline{\rho}$ is a mod 3 hardly ramified representation which is furthermore tame at 3, then $\overline{\rho}$ factors through $Gal(L/\mathbb{Q})$ with $L/\mathbb{Q}$ finite and Galois of degree either 2 or 4. This is morally game over.

In particular, $Gal(L/\mathbb{Q})$ is abelian of order prime to 3, so (after possibly extending k to a larger finite field k'') $\overline{\rho}$ is a direct sum of two characters.

We know inertia at 2 has order 1 or 3, and now it can't have order 3, so these characters are unramified outside 3.

They're also tame at 3, because they have order 1, 2 or 4.

So the abelian extensions of $\mathbb{Q}$ cut out by these characters are unramified outside 3 and tame at 3.

The Kronecker–Weber theorem tells us that every abelian extension is contained within a cyclotomic extension.

The extra condition of being unramified outside 3 and tame at 3 implies that this extension is contained within $\mathbb{Q}(\zeta_3)$.

The tame case

So far: if $\overline{\rho}$ is tame at 3 then after base extension to some k'' we have $\overline{\rho} \cong \chi_1 \oplus \chi_2$ with both χ_i factoring through $Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q})$.

So they're either 1 or the mod 3 cyclotomic character $\overline{\chi}$.

Their product is $\overline{\chi}$, so $\overline{\rho} \cong 1 + \overline{\chi}$ over k''.

By Brauer-Nesbitt, $\overline{\rho} \cong 1 + \overline{\chi}$ over k as well.

So $\overline{\rho} \cong \begin{pmatrix} \overline{\chi} & * \\ 0 & 1 \end{pmatrix}$ (with $* = 0$) and we're done in the tame case.

The wild case

What are we doing?

We're trying to show that a mod 3 hardly-ramified representation $\overline{\rho}$ is conjugate to $\begin{pmatrix} \overline{\chi} & * \\ 0 & 1 \end{pmatrix}$.

We've done it assuming furthermore that $\overline{\rho}$ is tame at 3.

What about the wild case?

In his Stanford course last year, Taylor showed a low-level approach for controlling the ramification of $\overline{\rho}$ at 3 in the wild case.

We will just be lazy, and invoke Theorem A of the 1985 paper of Fontaine "Il n'y a pas de variété abélienne sur $\mathbb{Z}$".

This beautiful observation of Fontaine is what he used to prove that there is no nontrivial abelian scheme over $\mathbb{Z}$.

Global analysis

The corollary of Fontaine's theorem A tells us immediately that if k is a finite field of characteristic p and if $\overline{\rho} : Gal(L/\mathbb{Q}) \hookrightarrow Aut_k(V)$ is flat at p, and if $p^b || disc(L)$, then $b < p[L : \mathbb{Q}]/(p-1)$.

(in fact it tells us that if $p = (P_1 P_2 \dots P_g)^e$ then $v_{P_i}(\mathcal{D}_L) < ep/(p-1)$ and now use the fact that the norm of the different is the discriminant).

Upshot: if $\overline{\rho}$ is wild at 3, then $|disc(L/\mathbb{Q})|^{1/[L:\mathbb{Q}]} < 2^{2/3}3^{3/2} < 8.25$.

Back to Poitou

Discriminants des corps totalement imaginaires

n =	$\lvert d\rvert^{1/n} \geqslant$	Exemples connus $\lvert d\rvert^{1/n} =$	$\lvert d\rvert =$
2	1.722 119	1.732	3
4	3.254 561	3.289	117
6	4.557 067	4.796	23^3
8	5.659 362	5.786	$2^8\ 17^3$
10	6.600 341	6.841	$3^5\ 31^4$
12	7.412 879	7.774	$3^9\ 19^5$
14	8.122 437	8.468	$2^{14}\ 29^6$
16	8.748 418		
18	9.305 672		

$|disc(L/\mathbb{Q})|^{1/[L:\mathbb{Q}]} < 2^{2/3}3^{3/2} < 8.25$ implies $[L:\mathbb{Q}] \leq 14$.

Furthermore, this time we know that $[L:\mathbb{Q}]$ is a multiple of 2 (as $\mathbb{Q}(\zeta_3) \subseteq L$) and of 3 (as $\overline{\rho}$ is wild at 3 so 3 divides the size of $J_3 \subseteq Gal(L/\mathbb{Q})$).

So $[L:\mathbb{Q}] = 6$ or 12.

Mod 3 representations: the wild case

Set $G := Gal(L/\mathbb{Q})$, so G has order 6 or 12, and its index 2 subgroup $H := Gal(L/\mathbb{Q}(\zeta_3))$ has size 3 or 6.

We are trying to analyse $\overline{\rho} : G \hookrightarrow Aut_k(V)$.

Because $|H| = 3$ or 6, H has a unique subgroup P of order 3 (just do a case by case check).

So this subgroup P is *characteristic* in H (i.e., invariant under all automorphisms of H).

And because H has index 2 in G, H is normal in G, meaning that P is normal in G.

Mod 3 representations: the wild case

We have $\overline{\rho} : G \hookrightarrow Aut_k(V)$, and G has a normal subgroup P of order 3.

Because $\overline{\rho}$ is a mod 3 representation, the fixed points of P are positive-dimensional, and hence a line.

(this is a counting argument: V has order a multiple of 3, and P-orbits have size 1 or 3, with $\{0\}$ of size 1 so there are more of size 1.)

Because P is normal in G, G stabilises this line.

So $\overline{\rho} \cong \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}$.

Again, ϕ_1 and ϕ_2 have image in $k^\times$, so size prime to 3.

So they're unramified at 2, tame at 3, so must be 1 or $\overline{\chi}$ (we saw this before).

And their product is $\overline{\chi}$ so we have one of each.

If $\phi_1 = \overline{\chi}$ and $\phi_2 = 1$ then we're done!

So we have to rule out $\phi_1 = 1$ and $\phi_2 = \overline{\chi}$.

Mod 3 representations: the wild case

What's left?

We have a hardly ramified mod 3 $\overline{\rho} \cong \begin{pmatrix} 1 & * \\ 0 & \overline{\chi} \end{pmatrix}$, wild at 3, and we want a contradiction.

The image of $H = Gal(L/\mathbb{Q}(\zeta_3))$ is a subset of $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ so it must have order 3 (not 6).

So $|G| = 6$ and the image of a local decomposition group D_3 in $Gal(L/\mathbb{Q})$ is all of $Gal(L/\mathbb{Q})$.

In particular, the image of $\mathrm{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3)$ in $Aut_k(V)$ has order a multiple of 3.

We're seeking a contradiction, and we're about to get it using a sledgehammer.

Back to Ribet

Before completing the proof that M is semi-simple as a D-module, we summarize the properties of M that we will use:

(a) It is free of rank 2 over $\mathbf{F}$,

(b) D acts trivially on a 1-dimensional subspace X of M and via the character $\chi\,(=\chi^{k-1})$ on the quotient $Y=M/X$.

(c) M is the module attached to a finite flat group scheme $\mathscr{M}$ of type $(p, \ldots, p)$ over $\mathscr{R}$.

(4.4) **Theorem.** *The image of D in* Aut M *has prime-to-p order.*

The same paper of Ribet contains a theorem saying that this cannot happen.

D is a decomposition group at 3, M is our V, $\mathbb{F}$ is our k, $k = 2$, $\mathcal{R}$ is our $\mathbb{Z}_3$.

Ribet's proof is short but crucially uses Raynaud's 1974 $(p, p, \ldots, p)$ paper.

In particular it uses the deep fact that if $\ell > 2$ then a flat $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-module comes from a *unique* (up to isomorphism) Hopf algebra.

This contradiction finishes the proof of the mod 3 lemma and hence of level 6.