Formalizing Fermat, Lecture 1

Kevin Buzzard, Imperial College London

EPSRC TCC, 22nd Jan 2026

Preliminaries

Before I forget: *no lecture next week*.

Lectures Thursday 3–5 in Huxley 6M42 (if you're at Imperial) or via the EPSRC TCC (if you're in Oxford, Warwick, Bath, Bristol or Swansea), from today 22/1/2026 until 19/3/2026.

Except no lecture next week 29/1/2026 and also no lecture 5/3/2026 (when I'll be giving a summary of the course in the Oxford number theory seminar).

Formalizing Fermat

This course is inspired by an EPSRC-funded Lean project which I'm involved in.

But it will be a Lean-free course, focussing on number theory.

Lean has made me think about mathematics as a logic game.

So the course is a game, and the object of the game is to prove Fermat's Last Theorem.

My role is to walk you through the various levels of the game.

The boss of each level is a theorem of the form "this statement/these statements imply FLT".

The statements will initially be straightforward but will get more technical over time.

I have no feeling yet about how far I'll get, but at the very least I will get to "this modularity lifting theorem implies FLT", and I hope to talk about the proof of the modularity lifting theorem.

Formalizing Fermat

I'm giving the course, so I get to make the rules of the game.

And the rules are inspired by the objectives of the EPSRC-sponsored Lean project, so they may come across as quite esoteric.

One of the rules of the game is that I am allowed to *assume*, without proof, any theorem which was published in the 1980s or before.

Note: the Wiles and Taylor–Wiles papers which introduced modularity lifting theorems and proved FLT were published in the 1990s.

So I can't cheat and assume them.

The proof I'll give

I could just go through the Wiles/Taylor–Wiles papers and basically assume all the results in the references of those papers.

But instead I'm going to explain a more modern proof.

[Buzzword-alert] The original proof assumed the Langlands–Tunnell theorem (which needed non-Galois cubic base change), and Ribet's beautiful work on mod p level-lowering for modular forms.

The proof I'll present won't need either of these results, although it will need cyclic base change for GL_2 so in particular there is some harmonic analysis involved.

However all of the harmonic analysis needed was known in the 1980s so I'm going to skip it.

I'll say more about the details of the route in the next lecture.

Definitions

In contrast to 1980s proofs (which I'm going to skip), I will be quite pedantic about giving *definitions*.

In fact, in the first two levels I am going to be *extremely* pedantic about giving definitions.

In particular I hope that all the pre-1990s results which I'm going to skip in the course will at least be *unambiguously stated*.

Any questions before we start?

Then let's begin with level 0.

Level 0: statement of Fermat's Last Theorem.

(cut scene)

Number theorists seem to be torn on whether the natural numbers begin at 0 or at 1.

In this course, they'll begin at 0.

This level is a tutorial level, so there will be no boss battle.

The goal of level 0 is to *state* Fermat's Last Theorem.

So let's make the relevant definitions.

Definition of the natural numbers.

Definition: The natural numbers are defined in the following way:

*) 0 is a natural number;
*) If n is a natural number, its *successor* $S(n)$ is a natural number;
*) That's it.

In some foundations of mathematics (those allowing the calculus of inductive constructions), this is a perfectly valid definition and no more need be said.

But let me clarify what "That's it" means.

It means "you are allowed to define functions from the natural numbers by recursion, and you are allowed to prove theorems about the natural numbers by induction."

Definition of the natural numbers

*) 0 is a natural number;
*) If n is a natural number, its *successor* $S(n)$ is a natural number;
*) That's it (i.e., induction and recursion are valid).

Remark: Any two models of the natural numbers are uniquely isomorphic (here "isomorphism" means "preserves 0 and S").

The proof is the usual "universal property yoga": given two models, use recursion to define maps between them and induction to prove that the composites in each direction are the identity map.

But does a model exist?

Existence of a model of the natural numbers is an *axiom of mathematics*.

We will have no need to choose a concrete model for the natural numbers; all we'll need to know about them is the properties listed above.

API for the natural numbers

As any computer programmer knows, once you've made a new structure you need to make an Application Programming Interface (or API) for it.

So let's make a basic API for the natural numbers.

That is, let's make some basic definitions involving natural numbers.

API for the natural numbers

Notation.

We write $\mathbb{N}$ for the collection of all natural numbers.

We know 0 is a natural number (by definition), and this is expressed either as $0 \in \mathbb{N}$ or $0 : \mathbb{N}$ depending on your foundational beliefs.

The other thing we have by definition is $S : \mathbb{N} \to \mathbb{N}$ (the "successor" or "next number" function).

Definition: Small numbers (1,2,3).

We define $1 := S(0)$, $2 := S(1)$ and $3 := S(2)$.

Definition: Addition.

Addition is a function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, with notation $a + b$, and is defined recursively on the second variable by the following formulae:

$n + 0 := n$;
$n + S(x) := S(n + x)$.

Multiplication and exponentiation

Definition: Multiplication.

Multiplication is a function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with notation $a \times b$ or just ab, defined recursively on the second variable by $a \times 0 := 0$ and $a \times S(n) := (a \times n) + a$.

Definition: Exponentiation.

Exponentiation is a function $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with notation a^b, defined recursively on the second variable by $a^0 := 1$ and $a^{S(n)} := a^n \times a$.

Inequality and divisibility

Definition: Inequality.

“Less-than-or-equal-to” is a predicate on $\mathbb{N} \times \mathbb{N}$ with notation $a \leq b$.

It can be defined recursively (if you understand recursive predicates), but an easier definition is simply $a \leq b := \exists c, b = a + c$.

Definition: Divisibility.

Divisibility is a predicate on $\mathbb{N} \times \mathbb{N}$ with notation $a \mid b$.

It's defined as $a \mid b := \exists c, b = ac$.

We say “a divides b” or “b is a multiple of a” if $a \mid b$.

Remark: We don't need divisibility in this level, but we'll need it in the next level.

Statement of the theorem

One last definition:

Positivity.

We say that a natural number n is *positive* if $1 \leq n$.

And now we're finally ready to state the theorem.

Fermat's Last Theorem states that if $a, b, c, n \in \mathbb{N}$ are positive, and $3 \leq n$, then $a^n + b^n \neq c^n$.

With the emergence of the beast, that's the end of level 0.

(you'll have to imagine your own cut scene.)

The rest of the levels will be spent battling this beast.

The moral of level 0: it is possible to give a rigorous statement of Fermat's Last theorem on one side of A4 paper, assuming nothing more than the *axioms of mathematics* and the *rules of logic*.

It is somehow *really extraordinary* that all known proofs of this theorem involve thousands of pages of new definitions and theorems about these definitions.

Level 1: Reduction to the case $5 \leq n$ and n prime.

This is the first proper level, and the first level of a game is usually relatively straightforward.

My first goal in this level (and indeed the first main goal in all subsequent levels) is to show you boss of the level, so we know what we're up against.

In other words, I want to *state* the theorem we're going to be proving in the level.

The boss theorem in this and every other level will be of the form "this statement/these statements imply FLT."

We beat the boss, and thus we make the beast slightly weaker.

But I can't show you the level 1 boss yet, because the result involves concepts which we've not seen yet (5 and "prime").

5

Definition: $4 := S(3)$ and $5 := S(4)$.

Prime numbers

Definition: Prime numbers.

A natural number p is *prime* if $2 \leq p$ and if $p = ab$ with $a, b : \mathbb{N}$ then either $a = 1$ or $b = 1$.

Example: 2 is prime.

Proof: omitted (this was known in the 1980s).

Remark: the proof that 2 is prime is quite long, given only what we currently know (which is essentially nothing).

In fact we haven't talked about proofs at all so far in this course.

The main difficulty in the proof that 2 is prime, is ruling out things like $2 = 373234827364 \times 243823482768$.

The easiest way to rule this out, is to first prove (by induction) various lemmas relating inequalities and multiplication.

Tricky exercise: prove that 2 is prime, given only what we know.

Hint: try to find the right lemmas which will make it easy.

Meet the first boss.

We are now ready to write the mathematical statement involved in the level 1 boss.

Statement B1. There are no solutions to $a^p + b^p = c^p$ if a, b, c, p are positive naturals, p is prime, and $5 \leq p$.

The main result of this level is

Theorem (Boss of level 1)

Statement B1 implies FLT modulo results known in the 1980s.

An equivalent way of stating this theorem is its contrapositive:

Say there is a solution to $x^n + y^n = z^n$ with x, y, z positive naturals and $3 \leq n$.

Then there is a solution to $a^p + b^p = c^p$ with a, b, c positive naturals and $5 \leq p$ a prime number.

To prove this we are going to need a huge amount of extra API.

But this API is *theorems*, rather than definitions, so, by the rules of the course, we can assume them without proof.

More API for the natural numbers

The naturals satisfy the following theorems: for all $x, y, z \in \mathbb{N}$ we have

*) $0 + x = x + 0 = x$;

*) $x + (y + z) = (x + y) + z$;

*) $x + y = y + x$;

*) $1 \times x = x \times 1 = x$;

*) $x(yz) = (xy)z$;

*) $xy = yx$;

*) $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$.

(In other words, the naturals are a commutative semiring.)

Proof: exercise (this was known in the 1980s).

Hint: Essentially every result here is proved by induction; the art is working out what to induct on, and the order in which to prove the results.

If you'd like to do this exercise, I would recommend playing the *natural number game* (it's online).

Finite products

We need one more definition: a finite product (we only have binary products so far).

Say $a_0, a_1, a_2, \ldots$ are naturals (i.e., say $a : \mathbb{N} \to \mathbb{N}$ is a function).

For n a natural, we define the natural $\prod_{i<n} a_i$ (a *finite product*) recursively on n:

$\prod_{i<0} a_i := 1$, and $\prod_{i<S(n)} a_i := (\prod_{i<n} a_i) \times a_n$.

Remark If a is a constant function then we recover exponentiation.

Theorem: Every positive natural number is a finite product of prime numbers.

Proof omitted (this was known in the 1980s).

One natural proof is to first establish strong induction, and then use that.

A key intermediate lemma

Lemma

If $3 \leq n$ is a natural, then n is either a multiple of 3, of 4, or of a prime p with $5 \leq p$.

Proof.

By the previous result, n is a finite product of primes.

Case 1: all of the primes involved are 2, so $n = 2^t$ for some natural t.

Then either $n = 1$ or $n = 2$ or n is a multiple of 4 (proof by induction on t), and one can check that $3 \leq 1$ and $3 \leq 2$ are both false (although these claims are not obvious, as antisymmetry of $\leq$ is a little subtle).

Case 2: there is some prime $p \neq 2$ dividing n.

Case 2a: $p \in \{0, 1, 2, 3, 4\}$. Then one can check that $p = 3$.

Case 2b: $p \notin \{0, 1, 2, 3, 4\}$. Then one can check that $5 \leq p$.

In all cases we are done (the checks were known in the 1980s). □

Beating the first boss

Recall what we're trying to prove.

Assume we have x, y, z, n are positive naturals, $3 \leq n$ and $x^n + y^n = z^n$.

Our goal to manipulate this data until it we get a solution to $a^p + b^p = c^p$ with a, b, c positive and $5 \leq p$ prime.

The next key observation: if $d \mid n$ and we have a solution to $x^n + y^n = z^n$ in positive naturals, then, writing $n = dm$, we have a solution to $a^d + b^d = c^d$ in positive naturals, namely $a = x^m$, $b = y^m$ and $c = z^m$.

The proof of this needs $a^{dm} = a^{md}$ (commutativity of multiplication), $a^{md} = (a^m)^d$ (proof by induction on d) and the claim that a power of a positive number is positive (proof by induction on the power).

By the previous lemma, either $3 \mid n$, $4 \mid n$ or $p \mid n$ for some prime p with $5 \leq p$.

So we're done if we can rule out the existence of positive integer solutions to $a^3 + b^3 = c^3$ and $a^4 + b^4 = c^4$.

Finishing the first boss

We have reduced our first boss battle to proving the non-existence of positive integer solutions to $a^3 + b^3 = c^3$ and to $a^4 + b^4 = c^4$.

The first of these results is an old theorem of Euler, and the second is an even older theorem of Fermat.

In particular, they were both known in the 1980s, so we're done.

And that's the end of level 1.

(cut scene)

The moral of level 1

The moral of level 1 is that, in stark contrast to *stating* Fermat's Last Theorem (which can be done in under 1 side of A4 from the axioms of mathematics), proving even the *simplest* of things directly from the axioms of mathematics is a *huge* amount of work.

I am lucky enough to have been involved in the Lean community since 2017.

Back then, if we wanted to prove $(x + y)^2 = x^2 + 2xy + y^2$ we had to apply all the ring axioms by hand and it took 10 lines.

I've done projects with undergraduates whose goals were formalizing proofs of basic results such as non-existence of positive integer solutions to $a^4 + b^4 = c^4$ and these were *really* challenging to do in a theorem prover back then, involving several hundred lines of code.

The moral of level 1

Since then, things have got much better.

We have many tools that facilitate basic computations, and we have literally hundreds of thousands of lemmas proving many obvious things.

It is an extraordinary tribute to the strength of both the Lean community, and of the prover behind it, that I can even *contemplate* proving FLT modulo the 1980s.

Formalization of mathematics is still a very painful process.

But it's becoming easier every day, and with the advent of AI help it will get even easier.

Upgrade!

As a reward for beating level 1, we now gain a super-power: we can now assume the results taught in a typical undergraduate mathematics degree.

This is what me, a bunch of Imperial undergraduates, and a load of other like-minded people around the world were working on in the 2010s.

I'd like to thank all of those people for making the project of formalizing Fermat viable.

As a result of this upgrade, this course will now become a lot more normal.

Level 2: Frey packages

Before I can state the boss theorem of this level, I need to define a “Frey package”, which is a term I made up.

And to do this, we need integers and congruence.

The integers

Recall that a monoid is a group without inverses (i.e. they have a unit, multiplication, and the axioms are left/right identity and associativity).

The integers $\mathbb{Z}$ are defined to be the additive localization of the additive monoid $\mathbb{N}$ at the additive submonoid $\mathbb{N}$. The integers have a natural commutative ring structure.

Because the integers are a localization of the naturals, there's a canonical additive monoid homomorphism $\mathbb{N} \to \mathbb{Z}$, which can even be checked to be a semiring homomorphism.

Notation. The mathematical notation for this map is "no notation at all".

But it's there.

Congruences

To define a Frey package, I also need to be able to talk about congruence of integers modulo a natural, and coprimality.

Definition. We say that two integers x and y are *congruent* modulo a natural n, and write $x \equiv y$ mod n, if n, when considered as an integer via the invisible map, divides $x - y$.

Coprimality. We say that two integers are *coprime* if no prime divides both of them (invisible map blah blah blah).

Frey packages

Definition

A *Frey package* is the following data: Three nonzero pairwise-coprime integers a, b, c, with $a \equiv 3 \bmod 4$ and $b \equiv 0 \bmod 2$, and a prime $p \geq 5$, such that $a^p + b^p = c^p$.

Statement B2: There is no Frey package.

Theorem (Boss level)

Statement B2 implies FLT, modulo results from the 1980s.

By level 1 we just need to show that B2 implies B1 (no solutions to FLT for $p \geq 5$ prime).

Again we show the contrapositive: given a solution to $a^p + b^p = c^p$ with a, b, c positive naturals and $p \geq 5$ prime, we'll show how to make a Frey package.

Beating the level 2 boss

We have $a^p + b^p = c^p$ with $p \geq 5$ prime and a, b, c positive naturals. We want a solution to $a^p + b^p = c^p$ with a, b, c nonzero integers, pairwise coprime, $a \equiv 3 \bmod 4$ and $b \equiv 0 \bmod 2$.

First map a, b, c into the integers.

Next we achieve coprimality of a and b by observing that if any prime divides a and b then it divides $a^p + b^p$ and hence c^p and hence c, so can be factored out.

We then observe (easy check) that this implies pairwise coprimality of a, b, c.

By parity precisely one of a, b, c is now even; if it's a then swap a and b; if it's c then swap b and c and change both signs (this is OK because p is odd). This ensures that b is even and a, c are odd.

Because a is odd, it's 1 or 3 mod 4; if it's 1 mod 4 then just change the signs of all three of a, b, c.

We're done! Note that life is much easier when we assume undergraduate mathematics without mention. Let's romp on to level 3.

Level 3: Frey curves

Level 3 of a game is a good time for a big reveal.

Wiles' work is sometimes sold as proving a profound theorem relating elliptic curves to modular forms.

Big reveal: the proof I'll explain in this course will not mention modular forms at all.

They are there, but we'll never need to use them, as they appear in no theorem statements, and all the facts we need about them were known in the 1980s.

We will however need elliptic curves (in several places, including now).

Elliptic curves

Let K be a field.

Definition An *elliptic curve over* K is five elements a_1, a_2, a_3, a_4, a_6 of K such that $-(a_1^2+4a_2)^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(2a_4+a_1a_3)^3-27(a_3^2+4a_6)^2+9(a_1^2+4a_2)(2a_4+a_1a_3)(a_3^2+4a_6) \neq 0$.

If you imagine that a_n has “degree n” then the left hand side of the mess above (called the *discriminant* Δ_E of the elliptic curve E) has degree 12.

The advantage of this definition of elliptic curve is that it is valid in all characteristics and it needs no algebraic geometry at all.

It also hammers home the idea that the *actual underlying mathematical definition* of an object is irrelevant, and all that matters is the API.

The arithmetic of elliptic curves

The meaning of the definition is the following.

If K is a field and $E := (a_1, a_2, a_3, a_4, a_6)$ is an elliptic curve over K, we associate a polynomial $f_E \in K[X, Y]$ to E called the *defining polynomial* of E, and it's $f_E := Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6)$.

One can check that the "discriminant non-zero" hypothesis on an elliptic curve implies that there is no point $(x, y) \in K^2$ such that all three of the polynomials f_E, $\partial f_E/\partial X$ and $\partial f_E/\partial Y$ vanish when evaluated at $(X, Y) = (x, y)$.

So if you know some algebraic geometry, the non-vanishing discriminant condition says that f_E cuts out a *smooth* curve in affine 2-space (and indeed the corresponding projective curve is also smooth, and has a rational point $[0 : 1 : 0]$).

Example

Let's do a family of examples (which will be relevant later).

Recall the defining polynomial of an elliptic curve $E := (a_1, a_2, a_3, a_4, a_6)$ is $f_E(X, Y) = Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6)$, so you can recover E from $f_E(X, Y)$.

Now K be a field, and say α, β, γ are three elements of K.

Let's try to make an elliptic curve with defining polynomial $Y^2 - (X - \alpha)(X - \beta)(X - \gamma)$.

We multiply out and see we need to set $a_1 = a_3 = 0$, $a_2 = -(\alpha + \beta + \gamma)$, $a_4 = \alpha\beta + \beta\gamma + \gamma\alpha$ and $a_6 = -\alpha\beta\gamma$.

Substituting into that ghastly discriminant equation, we check that it simplifies to $16(\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 \neq 0$.

So if K doesn't have characteristic 2 and if α, β, γ are pairwise distinct, this defines an elliptic curve.

Points

Say E is an elliptic curve over K (we write "say E/K is an elliptic curve" for short).

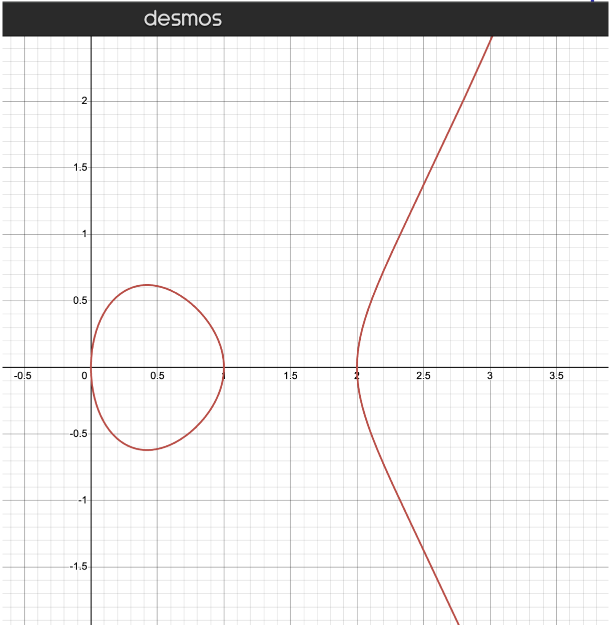
Its K*-points*, or just its *points*, are the solutions to $f_E(X, Y) = 0$ in K^2 with one extra point, traditionally called the "point at infinity", or just "∞" for short.

But that's a silly confusing name in our context, so let's just call it 0.

Notation: $E(K)$ is the K-points of E.

Example: if α, β, γ are three distinct real numbers and $E/\mathbb{R}$ is the elliptic curve with defining polynomial $f_E(X, Y) = Y^2 - (X - \alpha)(X - \beta)(X - \gamma)$ then the real points of E are just the points on the graph $f_E(X, Y) = 0$, plus a random extra point called 0.

Example $Y^2 = X(X-1)(X-2)$



Base change for elliptic curves

Say E is an elliptic curve over a field K.

Say L is another field, equipped with a field homomorphism $K \to L$.

Then E gives rise to an elliptic curve over L, by simply applying the field homomorphism to the five numbers (and noting that the discriminant can't become zero because maps of fields are injective).

We call this new elliptic curve E_L.

Abuse of notation: if E is an elliptic curve over K and if L is a field and a K-algebra, then we say the *L-points of E* are the L-points of E_L.

We write $E(L)$ for the L-points of E.

There is an obvious ("canonical") map $E(K) \to E(L)$ (send 0 to 0).

More generally if L and M are K-fields (i.e. K-algebras which are fields) and $\phi : L \to M$ is a K-algebra morphism then ϕ induces a map $\phi_* : E(L) \to E(M)$ sending a solution (x, y) in L to $(\phi(x), \phi(y))$, and sending 0 to 0.

An involution on the points of an elliptic curve.

Let me describe an involution on the points on an elliptic curve (which you might have guessed from the picture).

Recall: the K-points of $E = (a_1, a_2, a_3, a_4, a_6)$ are 0 and the K-solutions (x, y) to $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

If (x, y) is a K-solution then we can ask if there are any other K-solutions with the same X coordinate.

This is asking about roots of quadratic equation in Y; we know $Y = y$ is a solution to $Y^2 + a_1xY + a_3Y - (x^3 + a_2x^2 + a_4x + a_6) = 0$. The other root of this quadratic is $Y = -y - a_1x - a_3$ (because the sum of the roots must be $-a_1x - a_3$).

We can thus define an involution $-$ on $E(K)$ by $-0 := 0$ and $-(x, y) := (x, -y - a_1x - a_3)$.

The group law on an elliptic curve

Say K is a field and E/K is an elliptic curve.

Theorem

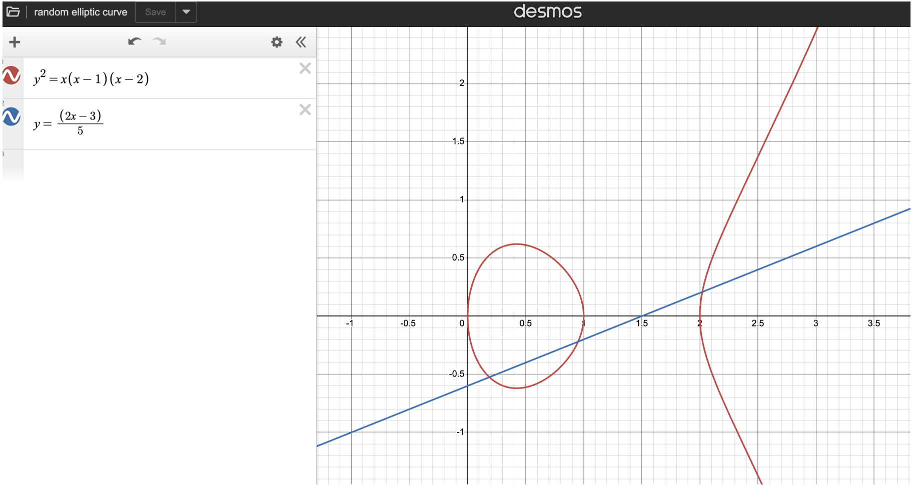
There exists one and only one way to put an additive abelian group structure on $E(K)$, with the following properties:
(i) 0 is the additive identity element;
(ii) the additive inverse of P is $-P$;
(iii) three distinct non-zero points in $E(K)$ sum to zero iff they are collinear.

Proof: Existence of a group law with these properties was known in the 1980s.

Uniqueness: the equations above tell you how to compute $P+Q$ for every pair (P,Q) other than $P+P$ for $0 \neq P$, and group theory tells you that $P+P$ must be the unique point on the curve which isn't $P+Q$ for any other Q :-)

Remark: the hard work is associativity (which can be done by a huge computer calculation).

Summing to zero



$y^2 = x(x-1)(x-2)$

$y = \frac{(2x-3)}{5}$

Functoriality

If E/K is an elliptic curve and L is a K-field then $E(L) := E_L(L)$ is now a group.

If L and M are K-fields and $\phi : L \to M$ is a K-algebra morphism then the induced map $\phi_* : E(L) \to E(M)$ is a group homomorphism (because $\phi : L^2 \to M^2$ sends collinear points to collinear points).

This construction $\phi \mapsto \phi_*$ is functorial (it sends the identity to the identity and composites to composites).

So it sends field isomorphisms to group isomorphisms.

In particular, if L is a K-field and $\phi : L \cong L$ is a K-algebra isomorphism then $\phi_* : E(L) \cong E(L)$ is an additive abelian group isomorphism.

Functoriality also implies that we have an action of the multiplicative group $Aut_K(L)$ of K-algebra automorphisms of L, on the additive abelian group $E(L)$.

The elliptic curve attached to a Frey package.

Recall that a *Frey package* is a prime $p \geq 5$ and pairwise coprime nonzero integers a, b, c with $a \equiv 3 \bmod 4$, b even, and $a^p + b^p = c^p$.

Given a Frey package, the associated *Frey curve* is the elliptic curve over $\mathbb{Q}$ with defining polynomial $Y^2 - X(X - a^p)(X + b^p)$.

We'd better check that this is an elliptic curve (that is, that the discriminant is nonzero).

By the earlier calculation, and the fact that $2 \neq 0$ in $\mathbb{Q}$, this boils down to checking that 0, a^p and $-b^p$ are distinct rational numbers.

By assumption $a, b, c \neq 0$, so certainly $a^p \neq 0$ and $-b^p \neq 0$.

Finally, note that $a^p - (-b^p) = c^p \neq 0$, so $a^p \neq -b^p$.

Hence the Frey curve associated to a Frey package is indeed an elliptic curve.

Absolute Galois groups.

Say K is a field.

Let $\overline{K}$ denote a separable closure of K.

Reminder: this is a separable algebraic field extension of K, which is separably closed, meaning that any positive degree $f \in \overline{K}[X]$ which is coprime to its derivative df/dX, has a root in $\overline{K}$.

Such things exist (if you believe in algebraic closures of fields, they're just a subfield of the algebraic closure).

Remark: we'll only care about the case $K = \mathbb{Q}$ in this lecture, and in this case a model for $\overline{\mathbb{Q}}$ is the algebraic numbers in $\mathbb{C}$.

NB in constrast to the naturals, $\overline{K}$ as a K-algebra is typically only unique up to non-unique isomorphism.

Let $Gal(\overline{K}/K)$ denote the group of K-algebra automorphisms of the K-field $\overline{K}$ (this is a measure of the failure of $\overline{K}$ to be unique up to unique isomorphism).

The mod p Galois representation attached to an elliptic curve.

Now say K is a field and E/K is an elliptic curve.

We have seen how an automorphism of a K-field L gives rise to a group automorphism of $E(L)$.

In particular, we have an action of $Gal(\overline{K}/K)$ on $E(\overline{K})$ by additive abelian group isomorphisms.

If n is a natural number and $E(\overline{K})[n]$ denotes the n-torsion subgroup of $E(\overline{K})$ (that is, the subgroup of points P such that $nP = 0$), then we get an induced action of $Gal(\overline{K}/K)$ on $E(\overline{K})[n]$.

We call this “the mod n Galois representation associated to E/K.”

Note: it depends on a choice of $\overline{K}$ so it is in some sense not as well-defined as you might think.

Why representation?

A representation of a group is usually an action of a group on a vector space.

If $n = p$ is a prime number, then $E(\overline{K})[p]$ is naturally a vector space over the field $\mathbb{Z}/p\mathbb{Z}$, and abelian group isomorphisms $E(\overline{K})[p] \cong E(\overline{K})[p]$ are linear maps for this vector space structure.

So $E(\overline{K})[p]$ really does admit a representation of the group $Gal(\overline{K}/K)$ in the undergraduate sense.

Meet the boss of level 3

Say (a, b, c, p) is a Frey package and E is the associated Frey curve.

Say $\overline{\mathbb{Q}}$ is any separable closure of $\mathbb{Q}$.

Say $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut(E(\overline{\mathbb{Q}})[p])$ is the associated mod p Galois representation.

Statement B3: For any Frey package and for any separable closure of $\mathbb{Q}$, the representation ρ above is reducible.

Recall that a representation of a group G on a vector space V is *reducible* if there's some subspace $0 < W < V$ which is G-stable, i.e. $\rho(g)(w) \in W$ for all $g : G$ and $w \in W$.

Theorem (Level 3 Boss)

Statement B3 implies FLT modulo the 1980s.

Summary of where we are

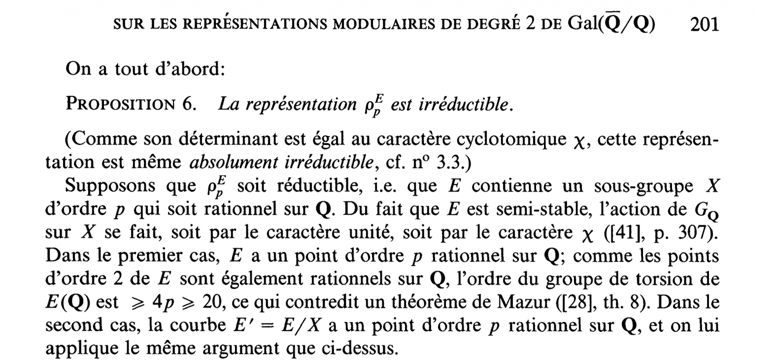
Statement B3 says "a certain mod p representation ρ coming from a Frey package is reducible".

We have already proved in level 2 that statement B2 implies FLT, and B2 is the statement "there is no Frey package".

So all we have to do to beat the level 3 boss is to deduce that there is no Frey package from statement B3, using only results known in the 1980s.

So it will suffice to show that we can derive a contradiction from the claim that ρ is reducible, using only results from the 1980s.

An old paper of Serre



SUR LES REPRÉSENTATIONS MODULAIRES DE DEGRÉ 2 DE $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ 201

On a tout d'abord:

PROPOSITION 6. *La représentation ρ_p^E est irréductible.*

(Comme son déterminant est égal au caractère cyclotomique χ, cette représentation est même *absolument irréductible*, cf. n° 3.3.)

Supposons que ρ_p^E soit réductible, i.e. que E contienne un sous-groupe X d'ordre p qui soit rationnel sur $\mathbf{Q}$. Du fait que E est semi-stable, l'action de $G_{\mathbf{Q}}$ sur X se fait, soit par le caractère unité, soit par le caractère χ ([41], p. 307). Dans le premier cas, E a un point d'ordre p rationnel sur $\mathbf{Q}$; comme les points d'ordre 2 de E sont également rationnels sur $\mathbf{Q}$, l'ordre du groupe de torsion de $E(\mathbf{Q})$ est $\geqslant 4p \geqslant 20$, ce qui contredit un théorème de Mazur ([28], th. 8). Dans le second cas, la courbe $E' = E/X$ a un point d'ordre p rationnel sur $\mathbf{Q}$, et on lui applique le même argument que ci-dessus.

This is Serre's 1987 Duke paper "Sur les représentations modulaires de degré 2 de $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$".

Proposition 6 is a proof that the representation is irreducible, which is the opposite of reducible, giving us the contradiction we seek.

(cut scene music)

The moral of level 3

To try and figure out what just happened, let me say something about Serre's proof.

Using a delicate arithmetic argument, Serre shows that if ρ is reducible then one can manipulate the Frey curve until it becomes a curve $Y^2 = (X-\alpha)(X-\beta)(X-\gamma)$ over $\mathbb{Q}$ whose p-torsion over $\overline{\mathbb{Q}}$ contains not just a nontrivial vector subspace stabilised by $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ but a non-zero *point* fixed by this Galois group.

By Galois theory, the coordinates of this point must be rational.

But in 1977 a ground-breaking 154-page paper of Barry Mazur showed that no elliptic curve over $\mathbb{Q}$ of the form $Y^2 = (X-\alpha)(X-\beta)(X-\gamma)$ can have a $\mathbb{Q}$-point of prime order $p \geq 5$.

Mazur's proof uses a bunch of technical arithmetic geometry, including a large chunk of Grothendieck's theory from the 1960s (itself many hundreds of pages, most of which is not in Lean's mathematics library).

Use of Mazur's paper

All known proofs of FLT start in this way, assuming Mazur's result.

Note that Mazur's paper is longer than the Wiles and Taylor–Wiles papers.

Lean's mathematics library has enough machinery to *state* the main theorem of Mazur's paper.

Formalizing the proof in Mazur's paper is not in the remit of the EPSRC grant; in 2029 I will be looking at the state of AI autoformalization tools (and currently have no feeling for how good they will be).

Mazur's work represents one of several highly nontrivial bottlenecks in the way of a full formalization of FLT.

The bottleneck I am working on is the modularity lifting theorem machinery (another technique used in every known proof of FLT), and the reason I am giving this course is that it will help me plan an assault on it.