# Formalising Fermat

K. Buzzard, Imperial College London

7th September 2022, AITP

# Before we start

Thanks to the organisers for inviting me to speak, and thank you all for coming.

# Introduction

Freek Wiedijk maintains a list of 100 mathematical challenges for formalisers.

98 of them are now formalised!

Some are mathematically completely trivial (for example, the irrationality of $\sqrt{2}$).

Most of the others are mathematics at undergraduate/masters level.

What I learnt in the last 5 years: this does not imply “trivial to formalise in a theorem prover”.

# Introduction

One trick to get undergraduate level mathematics formalised: teach undergraduate mathematicians how to formalise.

Example: the 98th theorem on the list to be formalised is the “Fair games theorem”, formalised by Imperial College undergraduate Kexing (Jason) Ying in Lean, and Shinnar and Trager in Coq.

Of the two remaining unformalised theorems on the list, one is the isoperimetric inequality (the largest area you can make with a string of fixed length is a circle); certainly there’s no obstruction to formalising a proof of this in e.g. Lean.

And then there’s Fermat’s Last Theorem.

# Fermat’s Last Theorem

Either Fermat’s Last Theorem (FLT) was put on the list as some kind of joke, or the person who suggested it was completely ignorant of the nature of the proof.

Note: the list was apparently compiled in the mid-90s, at around the same time FLT was proved by Wiles and Taylor.

The shortest known proof, if written out in full (assuming all of undergraduate mathematics), would occupy many thousands of book/journal pages.

The amount of mathematics involved in the shortest known proof of FLT is perhaps a couple of orders of magnitude more than the mathematics needed to prove all the other 99 statements put together.

# Overview

An overview of the talk:

- What is Fermat’s Last Theorem?
- What does the proof *look like*?
- Tentative first steps towards a computer formalisation.

# What is Fermat's Last Theorem?

The equation

$$a^2 + b^2 = c^2$$

turns out to have lots of interesting solutions in positive integers.

For example $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $8^2 + 15^2 = 17^2$,$\ldots$.

There is even a formula for the general solution in positive integers.

A polynomial equation with integer coefficients is known as a *Diophantine equation* (named after Diophantus of Alexandria).

To *solve* the equation is to find one, or all, of the solutions in naturals, integers, or rational numbers.

# What is Fermat's Last Theorem?

On the last slide we saw several solutions to the Diophantine equation $a^2 + b^2 = c^2$.

However it's much harder to find solutions in positive integers to $a^3 + b^3 = c^3$, and indeed Euler proved centuries ago that there were none.

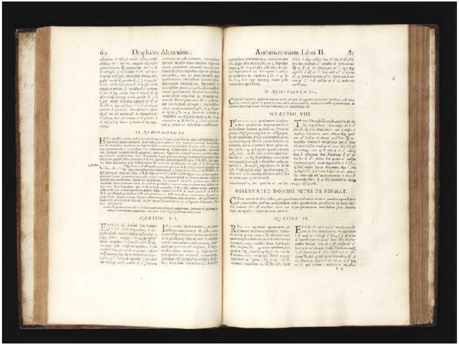
Fermat himself proved that there were no positive integer solutions to $a^4 + b^4 = c^4$.

You can probably see where this is going.

# What is Fermat's Last Theorem?

Fermat conjectured around 375 years ago that if $n \geq 3$ then there were no solutions to the Diophantine equation $a^n + b^n = c^n$ in positive integers $a$, $b$ and $c$.

He wrote in his copy of Diophantus' book "I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain".



60 Diophanti Alexandrini.

Arithmeticorum Liber II. 61

QVÆSTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

QVÆSTIO IX.

## What is Fermat’s Last Theorem?

Fermat’s claim was only discovered after his death, by his son.

It is widely believed that Fermat did *not* have a correct proof of the result at the time.

350 years later Wiles announced a proof; there was a gap, but he fixed it a year later in joint work with Taylor.

# Why is it so hard?

Recall the question is about showing that there are no solutions to $a^n + b^n = c^n$ in positive integers.

Dividing by $c^n$, and setting $x = a/c$ and $y = b/c$, we must equivalently show that the only *rational* solutions to $x^n + y^n = 1$ for $n \geq 3$ are the obvious ones with $x = 0$ or $y = 0$.

If we regard $n$ as being fixed, then we can think of Fermat as infinitely many Diophantine equations in two variables.

So what is the state of the art regarding rational solutions to Diophantine equations in two variables?

# Diophantine equations in two variables

A measure of the difficulty of a two-variable Diophantine equation is the *degree* of the equation.

Example: the degree of $x^n + y^n = 1$ is $n$.

Degree one (i.e., linear) equations, like $37x + 59y = 100$ are trivial to solve in rational numbers.

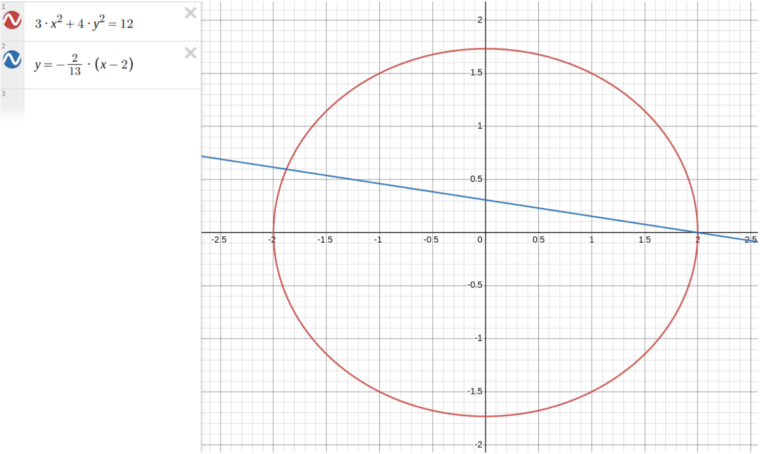
Degree two equations like $3x^2 + 4y^2 = 12$ were well-understood over 100 years ago.

There is an algorithm to figure out if one solution exists.

If you can find one solution, you can write down all the solutions.

For example, $(x, y) = (2, 0)$ is a solution to $3x^2 + 4y^2 = 12$.

A line with rational slope through this point hits the curve at a second rational point.



1 $3 \cdot x^2 + 4 \cdot y^2 = 12$

2 $y = -\frac{2}{13} \cdot (x-2)$

3

Substituting the linear equation into the quadratic gives a quadratic in one variable, with one known rational solution, hence the other solution is rational. But the argument is geometric. This is the beginning of algebraic geometry.

# Degree 3 equations

Degree 3 equations in two variables are currently only conjecturally understood, from a Diophantine perspective.

One big open problem in the area is the Birch and Swinnerton-Dyer conjecture.

The conjecture states "a cubic equation $E$ with one rational solution has infinitely many rational solutions if and only if $L(E,1)=0$ where $L(E,s)$ is a certain complex function attached to the equation".

The conjecture was made in the 60s. It was only proved that $L(E,1)$ made sense in 2000, as a consequence of extensions of Wiles' work. The conjecture is still open.

# Equations of higher degree

In general a two-variable Diophantine equation of degree higher than 3 only has *finitely many* rational solutions.

This is a profound 1984 theorem of Faltings (which won him the Fields Medal).

No algorithm is known for computing these solutions, so it doesn't help with FLT, which is a much more precise statement ("these are all the solutions", not "there are only finitely many").

So this is why FLT is hard.

# Interlude

In 2019, Balakrishnan, Dogra, Mueller, Tuitman and Vonk found all the rational solutions to a certain important quartic curve in two variables (the modular curve $X_s(13)$, a.k.a. $y^4 + 5x^4 - 6x^2y^2 + 6x^3 + 26x^2y + 10xy^2 - 10y^3 - 32x^2 - 40xy + 24y^2 + 32x - 16y = 0$).

The result had important consequences in arithmetic, and was published in the Annals of Mathematics.

The proof makes essential use of calculations in `magma`, an unverified closed-source computer algebra system using fast unrefereed algorithms.

It would be difficult, but certainly not impossible, to port everything over to an unverified open source system such as `sage`.

Nobody has any plans to do this. Hence part of the proof remains secret. Nobody in the mathematics community really minds.

# The proof

Although the statement of FLT just involves natural numbers, all known proofs involve a *vast* amount of technical machinery, and structures far more complicated than those we teach to undergraduates.

Unlike the proof of the odd order theorem (a statement about finite groups, whose proof is hundreds of pages of lemmas about finite groups and the occasional use of the complex numbers), all known proofs of Fermat's Last Theorem involve a great deal of analysis, geometry, topology, algebra and arithmetic.

# Formalising the proof

People have formalised large proofs before.

However they were typically large proofs about *mathematically simple objects* (spheres, planar graphs, finite groups. . . ).

Formalising a proof of FLT will involve having a very good API for some seriously complicated mathematical objects.

Can theorem provers even handle this kind of thing?

# The Liquid Tensor Experiment

In July of this year, Johan Commelin, Adam Topaz and others finished a Lean formalisation of the Clausen–Scholze “fundamental theorem of liquid vector spaces”.

This is a full formalisation of a theorem proved by humans in 2019.

The mathematical objects involved are complicated. The proof is intricate; it was 85K lines of code plus liberal use of Lean’s maths library ($10^6$ LOC).

This story makes me believe that it should be *possible* to formalise Wiles’ proof in Lean, or at least to start.

# Why Lean?

Lean has a solid mathematics library `mathlib` containing the foundations of analysis, geometry, algebra, topology and arithmetic, all in one place.

`mathlib` covers most of an undergraduate degree and a lot of relevant MSc-level material, and would be an essential prerequisite.

Furthermore, Lean's community contains professional mathematicians who know the material.

What about other ITPs?

# Coq

Coq uses essentially the same type theory as Lean.

Thus there is no theoretical obstruction to beginning a formalisation of FLT in Coq.

A major concern I had about the system several years ago was “setoid hell” but apparently this has been solved.

# Coq

A practical concern I have is that the my perception of the model it has for mathematics development is:

- `ssreflect`, a large library of constructive algebra;
- Several important smaller projects doing things like analysis or elliptic curves.

The proof of FLT is classical and needs lots of analysis, topology, algebra, geometry and arithmetic *all functioning concurrently*.

# The HOL systems

Isabelle/HOL has AFP, which also contains a huge amount of undergraduate mathematics.

However I do have concerns about formalising a proof of FLT in a HOL system.

I believe that the weaker logic (HOL instead of DTT) will cause a great deal of inconvenience.

Datapoint: Bordg, Li and Paulson formalised schemes (basic building blocks of modern algebraic geometry) in Isabelle/HOL, but they could not use Isabelle/HOL's rings because of issues around the lack of dependent types.

Nobody has a clue whether their new alternative development of ring theory can be used to do advanced commutative algebra, and AFAIK nobody is trying to find out.

# The univalent systems

As far as I can see, the univalence axiom is of no help in a proof of FLT.

Note also that all known proofs of FLT use classical mathematics.

# State of the art

So where are we right now with regards to formalising Fermat?

The modern proof of Fermat's Last Theorem looks like this.

Start with a fixed counterexample, so $a^n + b^n = c^n$.

Consider the Diophantine equation $Y^2 = X(X - a^n)(X + b^n)$.

Now apply a profound theorem of Mazur from the 1970s with a 100+ page proof using heavy algebraic geometry, which we are a long way from formalising, to give us an *irreducible Galois representation*.

Right now: let's just assume Mazur's result.

# State of the art

Next step: from the Galois representation, you build a “mod *p* modular form”.

Chris Birkbeck is developing the classical theory of modular forms in Lean (so will soon be able to *state* the result which Wiles needed).

To get the modular form from the Galois representation, you need deep theorems of Langlands on harmonic analysis, and I don’t understand these well enough to supervise a project in this area.

So again we save most of this for later.

The route from analysis to algebraic geometry comes via Serre’s “GAGA principle”, which is currently being formalised by my PhD student Jujian Zhang.

# State of the art

Given the mod $p$ modular form, you now apply profound results of Wiles and others which can be summarised as special cases of “the 2-dimensional case of the Langlands Philosophy”, and get a contradiction.

This involves a lot more algebraic geometry.

It is feasible to start building some of the proof of the Langlands philosophy in the 2-dimensional case (especially the commutative ring theory).

Unfortunately, the proofs in the 2-dimensional case need the Langlands philsophy in the 1-dimensional case.

Another name for the 1-dimensional Langlands philosophy is “class field theory”.

# State of the art

Class field theory: the main theorems were proved in at the end of the 19th century.

Amelia Livingston has been working on group and Galois cohomology, an essential tool for class field theory, as part of her PhD.

María Inés de Frutos Fernández is starting to work on local class field theory, a prerequisite for the global results.

# State of the art

Assuming cohomological facts from class field theory (1-d Langlands philosophy), Lean would be ready to start on the proofs of the necessary facts from the 2-d Langlands philosophy.

This is the topic of a grant proposal which I am in the process of writing.

Freek Wiedijk's PhD student Michail Karatarakis is working on *stating* the hard theorems of Wiles and Taylor which we will need.

Perhaps worth noting: the shortest known route to the proof is not the one which Wiles and Taylor took, but the main players are still the same (Galois representations, modular forms).

# Summary

We are a long way from a fully formalised proof of FLT.

There is a route to a formalisation in Lean which I can see.

Likely outcome: within 5 years we could have *reduced* the proof to several highly nontrivial statements about 20th century mathematical objects.