Diophantine equations

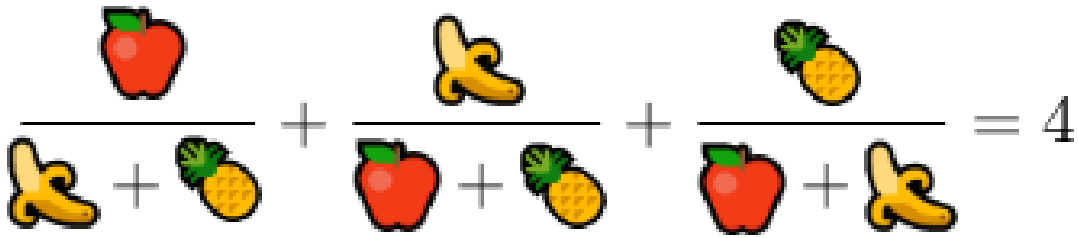
David Ang

University College London

Monday, 20 May 2024

A friendly problem

95% of people cannot solve this!



Can you find values for  ,  , and  ?

Let's write:

- a for **a**pple
- b for **b**anana
- c for ananas **c**omosus

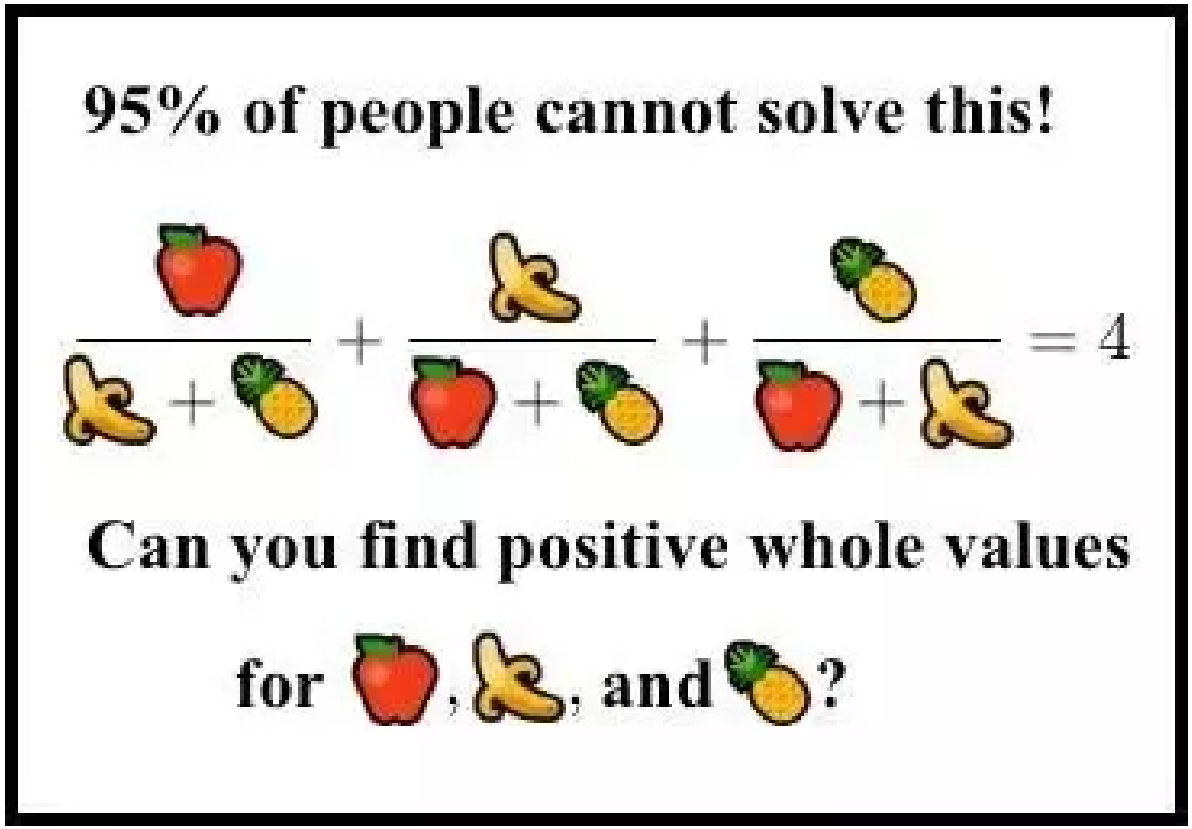
Real values:

- $a = 2 + \sqrt{3}$
- $b = 1$
- $c = 0$

Integer values:

- $a = 11$
- $b = 4$
- $c = -1$

A fiendish problem



Smallest positive whole values:

- $a =$ 154476802108746166441951315019919837485664325669565431700026634898253202035277999
- $b =$ 368751317941299998271978115652254748254929799689719709962831374716372246340555 79
- $c =$ 437361267792869725786125260237139015281653755816161361862143799337842346777 2036

Diophantine equations

A **Diophantine equation** is a polynomial equation in two or more unknown variables with *integer* coefficients.

Examples

$$X - 2Y - 3Z = 4 \qquad 2X^2 - 3XY + 4Y^2 - 5X + 6Y - 7 = 0$$

$$3X^3 + 4Y^3 + 5Z^3 = 0 \qquad X^4 + Y^4 = Z^4 \qquad Y^2 = X^5 + 1$$

To **solve** a Diophantine equation means to find its *integer* solutions:

- Is there an integer solution?
- Can we write down an integer solution?
- Are there infinitely many integer solutions?
- Can we generate new integer solutions from old ones?
- Is there a way to write down all integer solutions?
- Can we describe the distribution of integer solutions?

Fermat's last theorem

In 1637, Pierre de Fermat claimed the following theorem.

Conjecture (Fermat's last theorem)

The only integer solutions to $X^n + Y^n = Z^n$ for some $n > 2$ satisfy $XYZ = 0$.

"I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."

In 1995, Andrew Wiles published the first complete proof, which involved *very advanced* 20th century mathematics.

I think Fermat was mistaken.

Why are Diophantine equations so difficult?

Hilbert's tenth problem

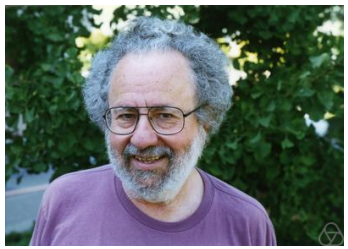
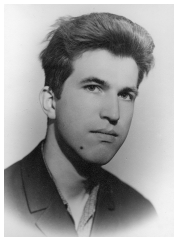
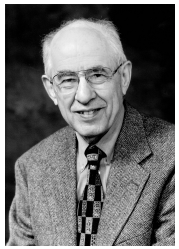
In 1900, David Hilbert published a list of 23 unsolved problems ranging over all areas of mathematics.

Question (Hilbert)

Is there an algorithm to solve *any* Diophantine equation?

Answer (Davis, Matiyasevich, Putnam, Robinson)

No.


We have to get creative!

Overview

Diophantine equations become more difficult to solve with more variables, so we will focus on two or three variables.

Diophantine equations can also be classified by their degree, and the approaches to solve them typically depend on the degree.

For the rest of the talk, we will consider the following examples:

- Linear equations
  - $aX + bY = c$ for fixed $a, b, c \in \mathbb{Z}$
- Quadratic equations
  - $X^2 + aY^2 = b$ for fixed $a, b \in \mathbb{Z}$
- Cubic equations
  - $X^3 + Y^2Z = aZ^3$ for fixed $a \in \mathbb{Z}$

Ultimately we will develop ideas leading to Fermat's last theorem.

Linear equations

Observe that an integer solution gives a solution modulo n for any $n \in \mathbb{N}$.

Question

Is there an integer solution to $15X + 21Y = 35$?

Answer

No, because $15X + 21Y \equiv 0 \mod 3$, but $35 \equiv 2 \mod 3$.

Theorem (Bézout's identity)

There is an integer solution to $aX + bY = c$ *iff* $\gcd(a, b) \mid c$.
Furthermore, there is an algorithm to determine all of its solutions.

For a proof, refer to MATH0006 Algebra 2.

Bézout's identity

Question

Can we write down an integer solution to $15X + 21Y = 36$?

Answer

Yes, because 36 is divisible by $\gcd(15, 21) = 3$. By the division algorithm:

$$\begin{aligned} 21 &= 1 \cdot 15 + 6 && \text{divide 21 by 15} \\ 15 &= 2 \cdot 6 + 3 && \text{divide 15 by 6} \end{aligned}$$

By reversing the division algorithm:

$$\begin{aligned} 3 &= 15 - 2 \cdot 6 && \text{substitute 3} \\ &= 15 - 2 \cdot (21 - 1 \cdot 15) && \text{substitute 6} \\ &= 3 \cdot 15 - 2 \cdot 21 && \text{rearrange} \end{aligned}$$

Thus $X = \frac{36}{3} \cdot 3 = 36$ and $Y = \frac{36}{3} \cdot -2 = -24$ works!

Quadratic equations

Can we do something similar for quadratic equations $X^2 + Y^2 = b$?

Question

Is there an integer solution to $X^2 + Y^2 = 7^5$?

Answer

No, because $X^2, Y^2 \equiv 0, 1 \mod 4$, but $7^5 \equiv 3 \mod 4$.

Theorem (Sum of two squares theorem)

There is an integer solution to $X^2 + Y^2 = b$ iff b is not divisible by a prime congruent to 3 modulo 4 with odd exponent.

For a proof, refer to MATH0034 Number Theory.

Sum of two squares theorem

Question

Can we write down an integer solution to $X^2 + Y^2 = 5^3$?

Answer

Yes, because 5 is a prime congruent to 1 modulo 4. In particular, 5^3 is not divisible by any prime congruent to 3 modulo 4 with odd exponent. In the ring of Gaussian integers $\mathbb{Z}[i]$:

$$5^3 = X^2 + Y^2 = (X + iY)(X - iY)$$

By *unique factorisation in* $\mathbb{Z}[i]$, write $X \pm iY = (W \pm iZ)^3$. Then:

$$5^3 = ((W + iZ)(W - iZ))^3 = (W^2 + Z^2)^3$$

Now $W = 2$ and $Z = 1$ is an integer solution to $W^2 + Z^2 = 5$. Moreover:

$$X + iY = (W + iZ)^3 = (W^3 - 3WZ^2) + i(3W^2Z - Z^3)$$

Thus $X = W^3 - 3WZ^2 = 2$ and $Y = 3W^2Z - Z^3 = 11$ works!

Number rings

Can we do something similar for quadratic equations $X^2 + aY^2 = b$?

Question

Is there an integer solution to $X^2 + 2Y^2 = 7^2$?

Answer

Consider the number ring $R := \mathbb{Z}[\sqrt{-2}]$. Factorise:

$$7^2 = X^2 + 2Y^2 = (X + \sqrt{-2}Y)(X - \sqrt{-2}Y)$$

By unique factorisation in R, write $X \pm \sqrt{-2}Y = (W \pm \sqrt{-2}Z)^2$. Then:

$$7^2 = ((W + \sqrt{-2}Z)(W - \sqrt{-2}Z))^2 = (W^2 + 2Z^2)^2$$

There are no integer solutions to $W^2 + 2Z^2 = 7$!

Note that $W^2 + 2Z^2 > 0$, so it is easy to rule out solutions.

Failure of unique factorisation

Solving the quadratic equation $X^2 + aY^2 = b$ seems to rely on unique factorisation in the ring $R := \mathbb{Z}[\sqrt{-a}]$, but this might fail.

Examples

- In $R = \mathbb{Z}[\sqrt{-5}]$, we have $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.
- In $R = \mathbb{Z}[\sqrt{10}]$, we have $10 = 2 \cdot 5 = \sqrt{10} \cdot \sqrt{10}$.

The solution is to replace $X + \sqrt{-a}$ with the **ideal**

$$\langle X + \sqrt{-a} \rangle := \{(X + \sqrt{-a})r : r \in \mathbb{Z}[\sqrt{-a}]\},$$

which has unique factorisation into **prime ideals** if $a \not\equiv 3 \mod 4$.

The failure of unique factorisation into *primes* is measured by the **ideal class group** $\mathrm{Cl}(R)$. For some $\mathrm{Cl}(R)$, a similar argument still works!

For more details, refer to MATH0035 Algebraic Number Theory.

Cyclotomic rings

In the 19th century, Ernst Kummer proved Fermat's last theorem for many exponents using this approach.

Theorem (Kummer)

If p is a regular odd prime, then the only integer solutions to $X^p + Y^p = Z^p$ satisfy $XYZ = 0$.

Proof.

Consider the **cyclotomic ring** $R := \mathbb{Z}[\zeta_p]$, where $\zeta_p := e^{\frac{2\pi i}{p}}$. Then:

$$Z^p = X^p + Y^p = (X + Y) \cdot (X + \zeta_p Y) \cdot (X + \zeta_p^2 Y) \cdot \cdots \cdot (X + \zeta_p^{p-1} Y)$$

A "similar" argument still works if p is a regular prime! □

Say that a prime p is **regular** if it does not divide the size of $\mathrm{Cl}(R)$, which conjecturally accounts for 61% of all primes.

Rational projective plane

Observe that $X^n + Y^n = Z^n$ is **homogeneous** of degree n.

In particular, this *almost* gives a correspondence:

$$\begin{array}{rcl} \{(X,Y,Z) \in \mathbb{Z}^3 : X^n + Y^n = Z^n\} & \leftrightsquigarrow & \{(x,y) \in \mathbb{Q}^2 : x^n + y^n = 1\} \\ (X,Y,Z) & \mapsto & (\frac{X}{Z}, \frac{Y}{Z}) \\ (xz, yw, wz) & \leftarrow\!\shortmid & (\frac{x}{w}, \frac{y}{z}) \end{array}$$

This correspondence is not quite bijective:

- Both (X,Y,Z) and $(\lambda X, \lambda Y, \lambda Z)$ map to $(\frac{X}{Z}, \frac{Y}{Z})$.
- Where does $(X,Y,0)$ map to?

Both of these issues can be fixed by working in the **projective plane**.

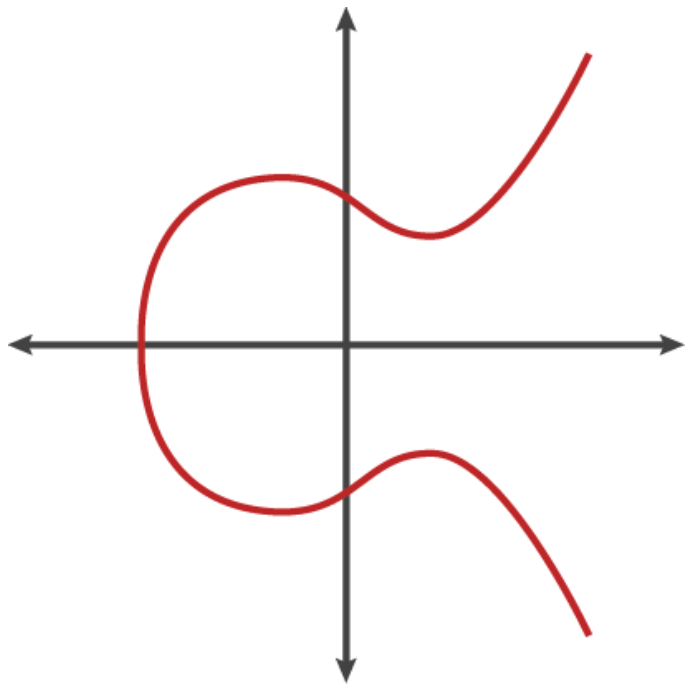
- Replace the left hand side with equivalence classes up to scaling.
- Supplement the right hand side with "points at infinity".

For more details, refer to MATH0076 Algebraic Geometry.

Fermat curves

By working in the projective plane, the integer solutions of $X^n + Y^n = Z^n$ are *essentially* the rational solutions of $x^n + y^n = 1$.

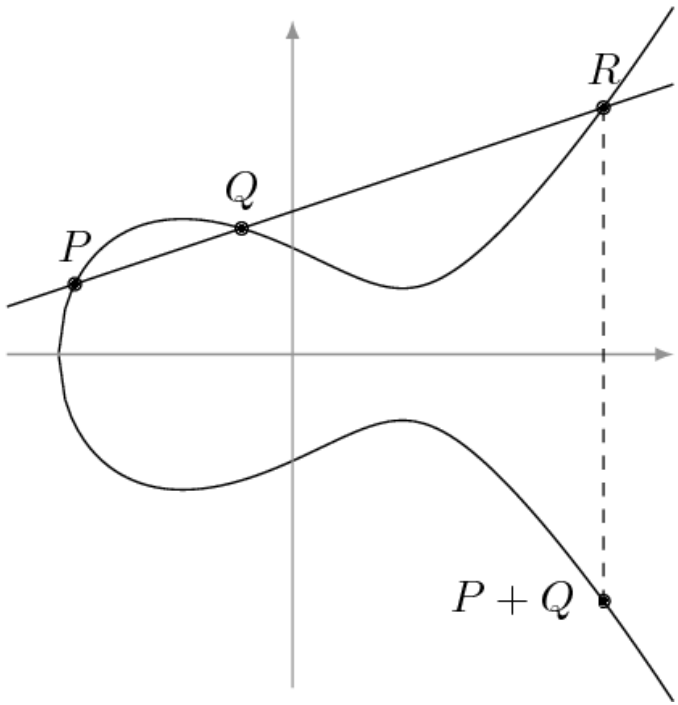
The cubic equation $x^3 + y^3 = 1$ defines an object in algebraic geometry called an **elliptic curve** that lives in the projective plane.

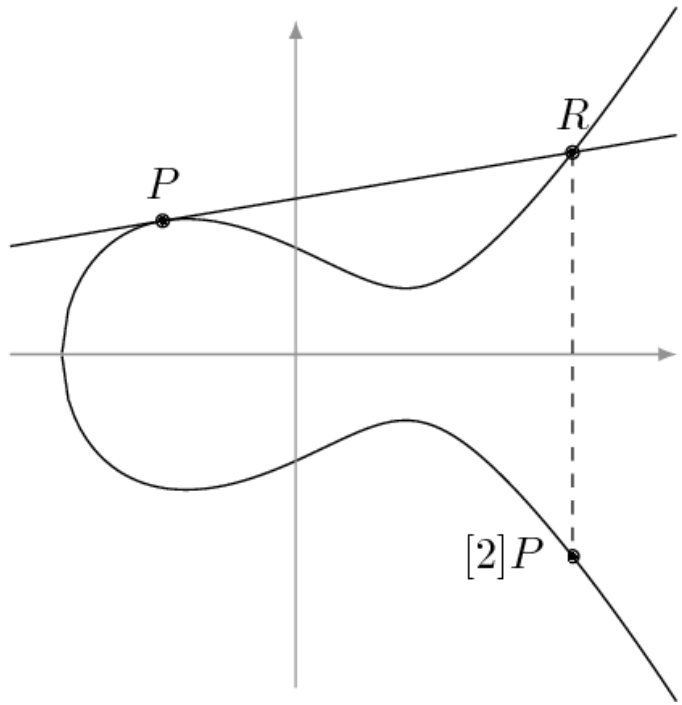


Elliptic curves

The set of rational solutions of an elliptic curve forms an abelian group:

$$P + Q + R = 0 \iff P, Q, R \text{ are collinear}$$





This gives a way to generate new rational solutions from old ones!

Cubic equations

Question

Can we write down two rational solutions to $x^3 - y^2 = 4$?

Answer

This defines an elliptic curve, with an obvious solution $x = 2$ and $y = 2$.
The tangent of $e(x, y) = x^3 - y^2 - 4$ at the point $(x, y) = (2, 2)$ is:

$$\frac{\partial e}{\partial x}(2) \cdot (x - 2) + \frac{\partial e}{\partial y}(2) \cdot (y - 2) = 0$$

This simplifies as $y = 3x - 4$, which substitutes into $e(x, y) = 0$ to yield:

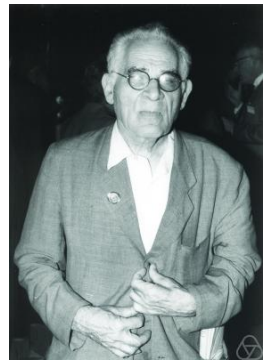
$$0 = x^3 - (3x - 4)^2 - 4 = (x - 2)^2(x - 5)$$

Thus $x = 5$ and $y = 3(5) - 4 = 11$ works!

In fact, *adding* the solution $x = 2$ and $y = 2$ to itself repeatedly generates the *only* infinite family of rational solutions to $x^3 - y^2 = 4$.

Mordell's theorem

In 1922, Louis Mordell classified the abstract group structure of rational solutions of elliptic curves.



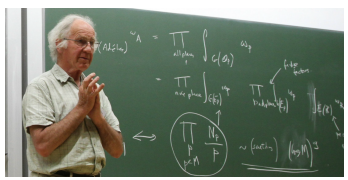
Theorem (Mordell)

The rational solutions of an elliptic curve can be generated by a finite set of initial rational solutions.

Associated to an elliptic curve E is a complex-analytic function $L_E(s)$.

Conjecture (Birch, Swinnerton-Dyer)

An elliptic curve E has infinitely many rational solutions iff $L_E(1) = 0$.

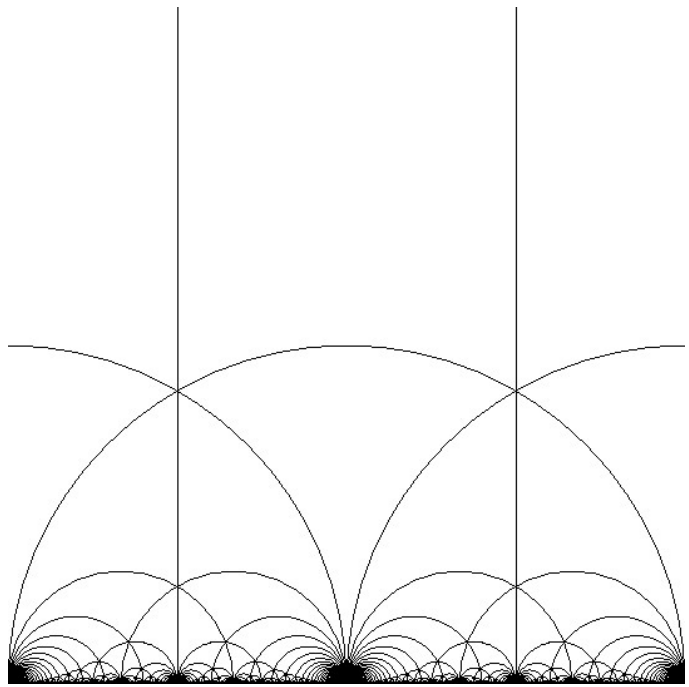


For more details, refer to MATH0036 Elliptic Curves.

Modular forms

Andrew Wiles proved Fermat's last theorem by contradiction.

This requires classifying certain highly-symmetric functions on the upper half $\mathcal{H}$ of the complex plane called **modular forms**.



Newforms

The modular forms of interest are the so-called **level N newforms**.

These are functions $f : \mathcal{H} \to \mathbb{C}$ satisfying the **modular condition**:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 \cdot f(z)$$

for any $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = 1$ and $N \mid c$.

Theorem (Valence formula)

For fixed N, there are finitely many level N newforms.

In fact, there are *no* level N newforms for:

$$N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60\}$$

For more details, refer to MATH0104 Modular Forms.

Modularity theorem

Also associated to a modular form f is a complex-analytic function $L_f(s)$.

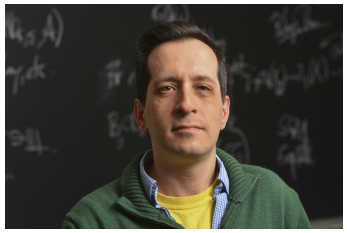
Call an elliptic curve E **modular** if there is a level N newform f such that $L_E(s) = L_f(s)$ for some N.

Theorem (Wiles)

For squarefree N, all elliptic curves are modular.

Theorem (Breuil, Conrad, Diamond, Taylor)

All elliptic curves are modular.



Fermat's last theorem

Fermat's last theorem can now be deduced from the modularity theorem.

Assume for a contradiction that $X^n + Y^n = Z^n$ has an integer solution not satisfying $XYZ = 0$. Consider the elliptic curve E given by:

$$y^2 = x(x - X^n)(x + Y^n)$$

This is called the **Frey curve** associated to the triple (X, Y, Z).

The modularity theorem says that E corresponds to a level N newform f.

Theorem (Ribet)

f can be "level-lowered" to a level 2 newform.

There are no level 2 newforms, hence a contradiction!

Formalising Fermat

My PhD supervisor Kevin Buzzard started a massive project to teach the modularity theorem to a computer.

This means *formally* defining all the relevant objects (elliptic curves, modular forms) and *rigorously* verifying all the details of the proof.

`https://imperialcollegelondon.github.io/FLT/`

This is a *huge* amount of work, and we need *all* the help we can get!

To get started, check out MATH0109 Theorem Proving in Lean!