Fermat's Last Theorem and the Modular Method

Philippe Michaud-Rodgers

University of Warwick Postgraduate Seminar

04.11.2020

Table of Contents

Table of Contents

Statement of Fermat's Last Theorem

Theorem (Wiles + many others! 1995)

The equation

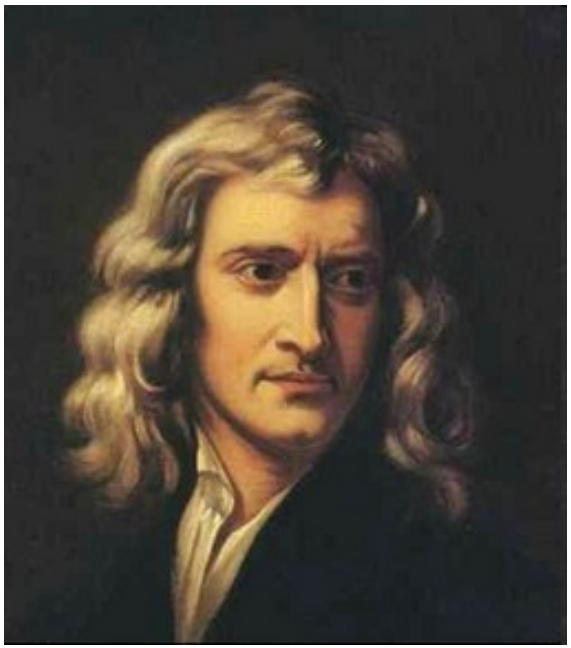
$$x^n + y^n = z^n,$$

with $n \geq 3$, has no non-trivial solutions for integers x, y, z.

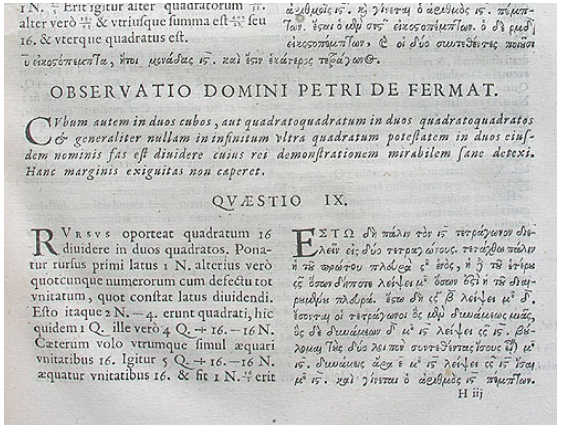
By a *non-trivial* solution, we mean that $xyz \neq 0$.

Fermat's Little Margin

- Pierre de Fermat:



- His Margin:



OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

"I have discovered a truly remarkable proof of this result which this margin is too small to contain."

First Observations

- If $n = p \cdot m$ and (x, y, z) satisfies $x^n + y^n = z^n$, then

$$(x^m)^p + (y^m)^p = (z^m)^p.$$

- $n = 3$ (Euler, 1770) and $n = 4$ (Fermat, 1670): elementary.

So enough to prove:

FLT

The equation

$$x^p + y^p = z^p,$$

with $p \geq 5$, prime, has no non-trivial solutions for integers x, y, z.

Outline of Argument

- Suppose $x^p + y^p = z^p$.
- Associate to (x, y, z) an "elliptic curve", E.
- Associate to E a "level N_p newform", f.
- Observe that there are no newforms at level N_p.

Aim: Understand this.

Table of Contents

Definition of a Modular Form

- Let $H = \{\tau \in \mathbb{C} : \mathrm{im}(\tau) > 0\}$. This is the *upper half plane*.

Definition

A "level N" modular form (of weight 2) is a holomorphic function $f : H \to \mathbb{C}$ satisfying:
(i) for $z \in H$,

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

whenever $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$, $N|c$;
(ii) Another technical condition.

- f has a *Fourier* or *q-expansion*:

$$f = \sum_{n=0}^{\infty} c_n q^n, \text{ where } c_n \in \mathbb{C}, q = e^{\frac{2\pi i}{z}}.$$

Newforms: Definition

- A *newform at level N* is a special type of level N modular form.
- It has a q-expansion

$$f = \sum_{n=1}^{\infty} c_n q^n.$$

- A newform is *rational* if $c_i \in \mathbb{Q}$ for all i (then in fact $c_i \in \mathbb{Z}$ for all i), and irrational otherwise.
- Newforms at level 38:

$$f_1 = q - q^2 + q^3 + q^4 - q^6 - q^7 + \cdots$$
$$f_2 = q + q^2 - q^3 + q^4 - 4q^5 - q^6 + 3q^7 + \cdots$$

Absence of Newforms

Fact

There are no newforms at levels

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60.$$

Table of Contents

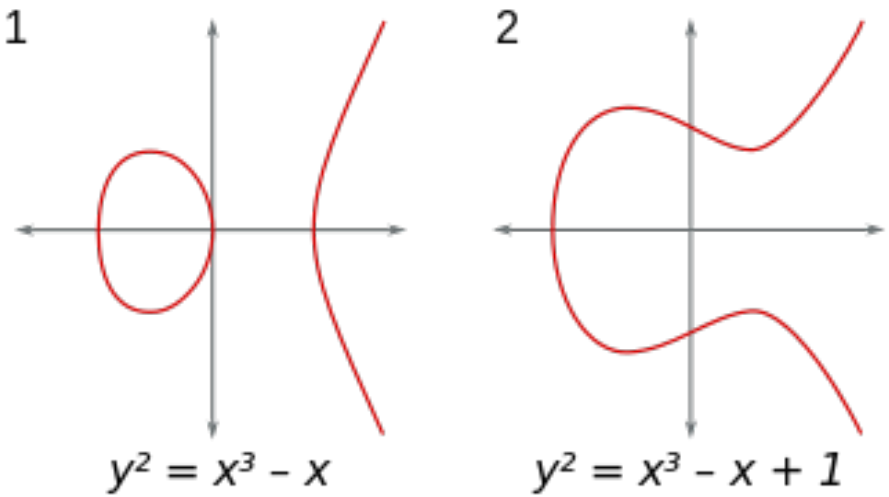
What is an Elliptic Curve?

Definition

An elliptic curve over $\mathbb{Q}$ is a curve given by an equation

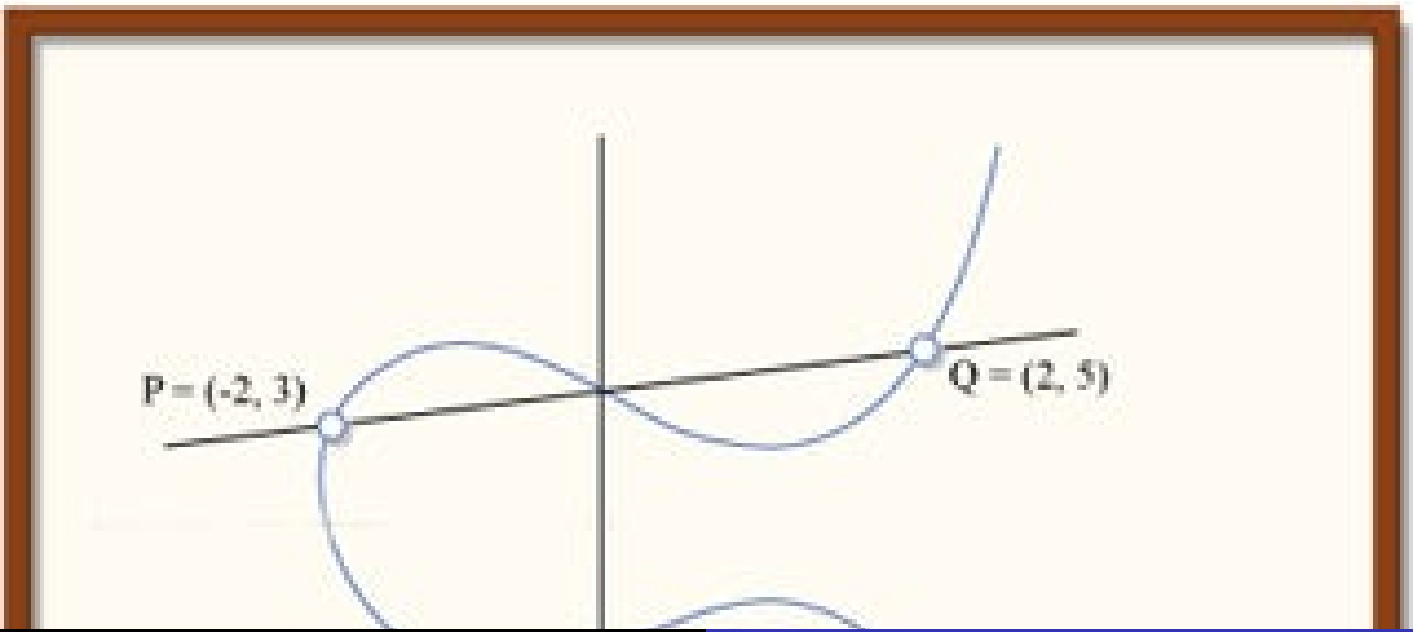
$$Y^2 = X^3 + AX^2 + BX + C,$$

where $A, B, C \in \mathbb{Q}$. It is smooth.



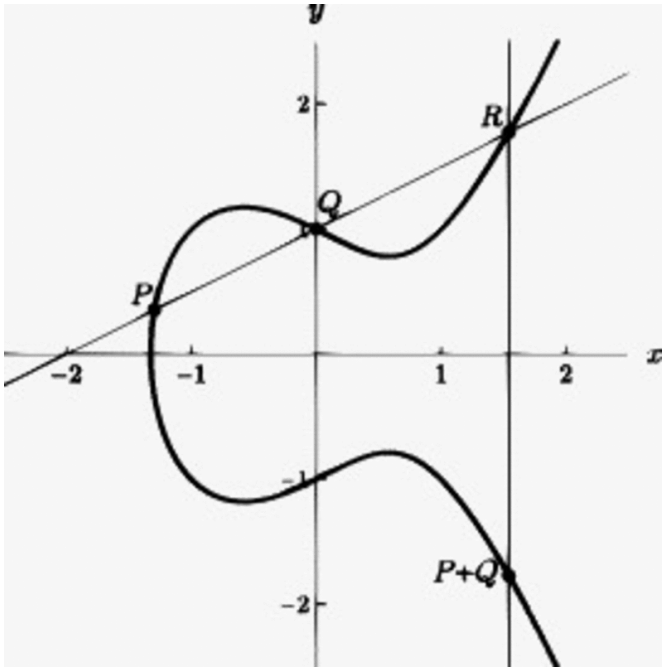
Rational Points

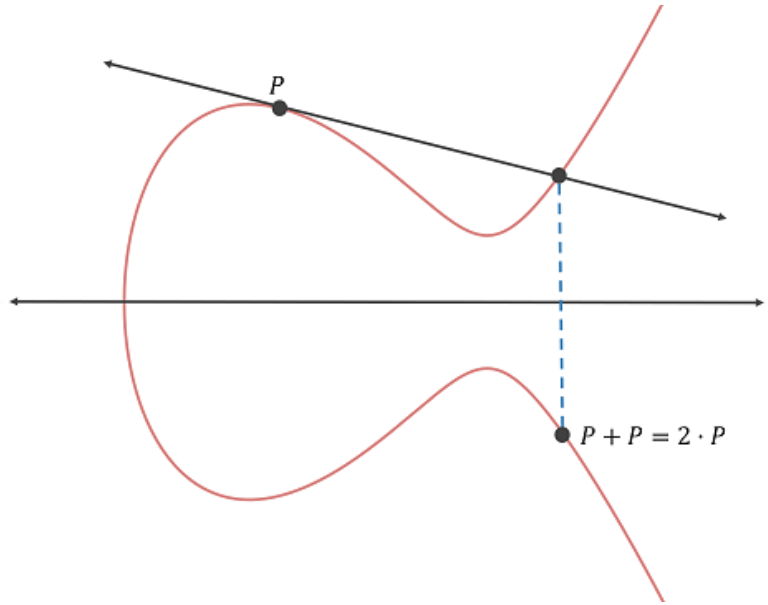
- $E : Y^2 = X^3 + AX^2 + BX + C$.
- A point $P = (x, y)$ is a *rational point* on E if P lies on E, and $x, y \in \mathbb{Q}$.
- We write $E(\mathbb{Q})$ for the set of rational points.
- Example: $Y^2 = X^3 + 17, \quad (2, 5) \in E(\mathbb{Q})$



$E(\mathbb{Q})$ is a group!

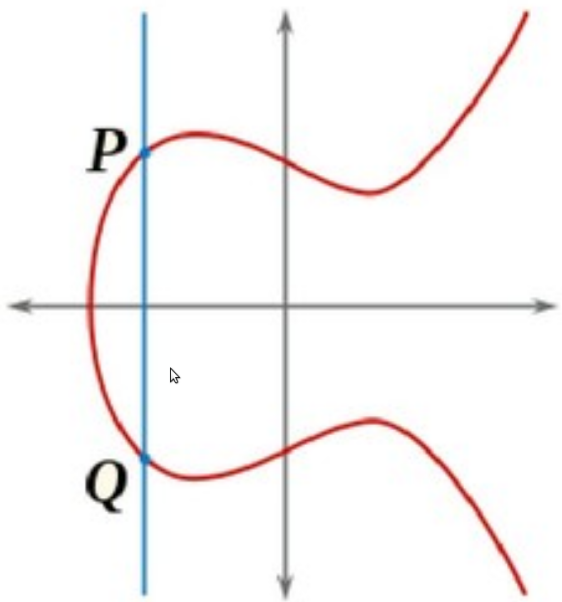
- Let $P, Q \in E(\mathbb{Q})$. Then $P \oplus Q \in E(\mathbb{Q})$. What is $P \oplus Q$?



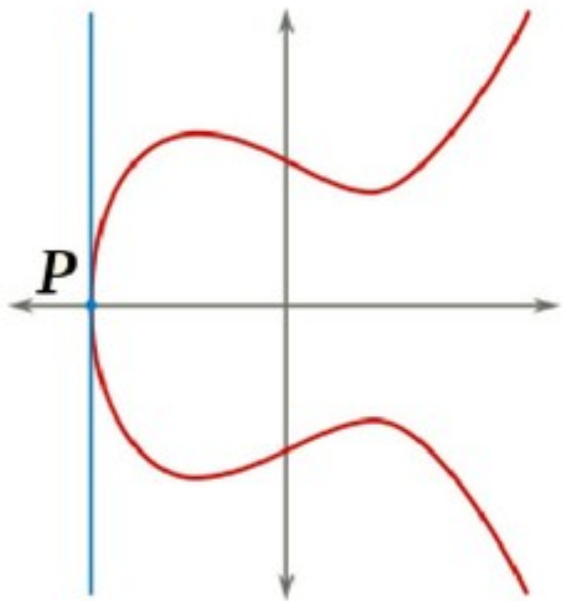


Group Law Continued

What is the identity in the group? It is 0 (or ∞):



$P + Q = 0$



$2P = 0$

Group Structure

- $E(\mathbb{Q})$ is an *abelian* group (clear).
- $E(\mathbb{Q})$ is a finitely generated abelian group (Mordell-Weil)
- Everything I have said works if you replace $\mathbb{Q}$ by a number field K, e.g. $K = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt[3]{19}), \ldots$.

Three Important Quantities

$$E : Y^2 = X^3 + AX^2 + BX + C = (X - e_1)(X - e_2)(X - e_3)$$

Discriminants

The *Discriminant* of E is the discriminant of $X^3 + AX^2 + BX + C$.
This is $\Delta_E = [(e_1 - e_2)(e_2 - e_3)(e_1 - e_3)]^2$.
The *minimal discriminant of* E, $\Delta_{\min,E}$, is the smallest discriminant "under transformations".

Conductor

The conductor of E is

$$N_E = \prod_{p|\Delta_{\min,E}} p^{e(p)},$$

where $e_p > 0$ depends on the *reduction type* of E at p.

Reduction of an Elliptic Curve

$E : Y^2 = X^3 + AX^2 + BX + C, \quad p$ prime, $A, B, C \in \mathbb{Z}$.

- We can *reduce* E *mod* p, and write $\widetilde{E}$.
- View $\widetilde{E}$ as a curve over $\mathbb{F}_p$, and write $\widetilde{E}(\mathbb{F}_p)$ for its $\mathbb{F}_p$ points.
- If $p \nmid N$, then $\widetilde{E}$ is itself an elliptic curve over $\mathbb{F}_p$ (other reduction types possible).
- Set $a_p(E) = p + 1 - \#\widetilde{E}(\mathbb{F}_p)$.

Example: Let $E : Y^2 = X^3 + 5X^2 + 9X + 25$ and $p = 5$.
Then $N_E = 2^9 \cdot 313$ and $\widetilde{E} : Y^2 = X^3 - X$.
$\widetilde{E}(\mathbb{F}_5) = \{\infty, (\overline{0}, \overline{0}), (\overline{1}, \overline{0}), (\overline{2}, \overline{1}), (\overline{2}, \overline{-1}), (\overline{-1}, \overline{0}), (\overline{-2}, \overline{2}), (\overline{-2}, \overline{2})\}$.
So $a_5(E) = 5 + 1 - 8 = -2$.

Elliptic Curves Recap

- $E : Y^2 = X^3 + AX^2 + BX + C$.
- $E(\mathbb{Q})$ is a finitely generated abelian group.
- We associate an integer N to E, called the conductor.
- For each prime $p \nmid N$, we have an $a_p(E)$.

Table of Contents

Eichler-Shimura

- Recall: a level N rational newform is a holomorphic function $f : H \to \mathbb{C}$ with q-expansion

$$f = \sum_{n=1}^{\infty} c_n q^n, \qquad \text{where } c_i \in \mathbb{Z}, q = e^{\frac{2\pi i}{z}}.$$

Eichler-Shimura

Let f be a level N rational newform. Then we can associate to f an elliptic curve E_f over $\mathbb{Q}$ of conductor N, so that for all primes $p \nmid N$:

$$c_p = a_p(E).$$

Modularity

Modularity Theorem (Wiles, Taylor + Wiles, Breuil + Conrad + Diamond + Taylor)

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Then E is *modular*. Meaning we can associate a level N rational newform $f_E = \sum c_n q^n$ to E satisfying $c_p = a_p(E)$ for any $p \nmid N$.

So we have maps **(BLACK BOX 1)**

$$\{\text{Level } N \text{ rational newforms}\} \leftrightarrows \{\text{Elliptic Curves } /\mathbb{Q} \text{ of Conductor } N\}$$

Arises mod p

- Let E be an elliptic curve of conductor N.
- Let $f = \sum c_n q^n$ be a newform of level N'.

Definition

Let p be a prime. We say E *arises modulo* p from f if for all primes $l \nmid pNN'$,

$$c_l \equiv a_l(E) \pmod{p}.$$

- This is a natural definition given what we saw above.
- Note that here N and N' can differ.

Level-Lowering

(BLACK BOX 2)

Level-Lowering Theorem (Ribet)

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and let $p \geq 5$ be prime. (Suppose E has no *rational p-subgroups*.) Then E arises mod p from a newform f at level N_p, where

$$N_p = \frac{N}{\prod_{q \| N, p | \mathrm{ord}_q(\Delta_{\min})} q}$$

- If E satsifies hypotheses and there are no newforms at level N_p, then this gives a contradiction.

Rational p-subgroups and Mazur's theorem

- Recall: $E(K)$ is a group for fields K.
- The 'p' in p-subgroup means the subgroup has order p.
- 'Rational' means the subgroup is rational, not necessarily the points.

e.g. $\{(\sqrt{2}, 0), (-\sqrt{2}, 0)\}$ is rational even though its elements are not rational.

(BLACK BOX 3)

Mazur's Theorem

Let $E : Y^2 = f(X)$ be an elliptic curve over $\mathbb{Q}$ of conductor N and let $p \geq 5$. Suppose N is squarefree and that f has 3 rational roots. Then E has no rational p-subgroups. (So can level-lower)

Table of Contents

The Frey Curve

Recall FLT:

FLT

The equation $x^p + y^p = z^p$, with $p \geq 5$, prime, has no non-trivial solutions for integers x, y, z.

Suppose (x, y, z) is a solution and define the *Frey Curve*

$$E : Y^2 = X(X - x^p)(X + y^p)$$

This is an elliptic curve.

- We want to show that E cannot exist.
- First check E has no rational p-subgroups.
- Then level-lower to reach a contradiction.

Frey Curve Computations

- Frey Curve $E : Y^2 = X(X - x^p)(X + y^p)$.
- Minimal discriminant: $\Delta_{\min} = 2^{-8}(xyz)^{2p}$.
- Conductor:

$$N = 2 \prod_{p|xyz, \text{odd}} p.$$

  Note that N is dependent on x, y, z.
- N is squarefree, and $X(X - x^p)(X + y^p)$ has three rational roots.
- So, by Mazur (Black Box 3), we can level-lower.

Level-Lowering the Frey Curve

- We level lower (Black Box 2): E arises modulo p from a newform f at level N_p.
- Recall:

$$\Delta_{\min} = 2^{-8}(xyz)^{2p}, \quad N = 2 \prod_{p|xyz,\text{odd}} p, \quad N_p = \frac{N}{\prod_{q\|N, p|\text{ord}_q(\Delta_{\min})} q}$$

- So $N_p = 2$.
- But! There are no newforms at level 2, a contradiction.

Hoorah!

Table of Contents

The Modular Method

- The Modular Method (level-lowering a Frey curve) can be applied to other Diophantine equations.
- Usually we do find newforms at the level N_p.
- There are lots of techniques to try and eliminate them.
- The Modular Method can often be combined with other methods.

Other Diophantine Examples

The Modular Method has been used extensively to solve or partially solve:

- The Generalised Fermat Equation: $Ax^n + By^n = Cz^n$.
- Other *signatures*: $Ax^p + By^p = Cz^2$, $Ax^p + By^p = Cz^3$.
- Lebesgue-Nagell equation: $x^2 + D = y^n$, $D \in \mathbb{Z}$.
- Perfect Powers in Fibonacci and Lucas sequences: $y^k = F_n$, $y^k = L_n$.
- Fermat's Last Theorem over totally real fields: e.g. $K = \mathbb{Q}(\sqrt{d}), d \geq 0$.

Thank you for listening! :)