Modular method for solving Diophantine equations

Marta Dujella

University of Basel

November 9, 2020

Some Diophantine Equations

Goal: present a method of solving Diophantine equations of certain type.

Theorem (Wiles 1995, "Fermat's Last Theorem")

Suppose that p/geq5 is a prime number. Then the equation

$$x^p + y^p + z^p = 0$$

has no solutions in $\mathbb{Q}$ with $xyz \neq 0$.

More generally:

Theorem (Wiles ($r = 0$); Ribet ($r \geq 2$); Darmon, Merel ($r = 1$))

Suppose $p \geq 5$ prime. Then the equation

$$x^p + 2^r y^p + z^p = 0$$

has no solutions with $xyz = 0$ and x, y, z pairwise coprime except $r = 1$ and $(x, y, z) = \pm(-1, 1, -1)$.

Fermat's Last theorem

Suppose that

$$a^p + b^p + c^p = 0 \tag{1}$$

has a solution for $a, b, c \in \mathbb{Q}$ with $abc \neq 0$. We can assume that $p \geq 5$, $a, b, c \in \mathbb{Z}$, $\gcd(a, b, c) = 1$ and that

$$b \equiv 0 \pmod 2 \quad \text{and} \quad a \equiv -1 \pmod 4.$$

This means we can define the following elliptic curve over $\mathbb{Q}$:

$$E : y^2 = x(x - a^p)(x + b^p) \tag{2}$$

By studying properties of E, one can see that E behaves strangely. **Idea**: Show that E cannot exist! **How**?

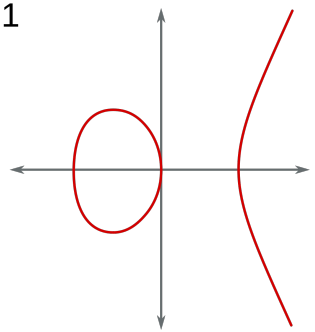
- Show that E is not *modular*
- Prove that all elliptic curves are modular

Elliptic curves - Weirstrass equation

Definition

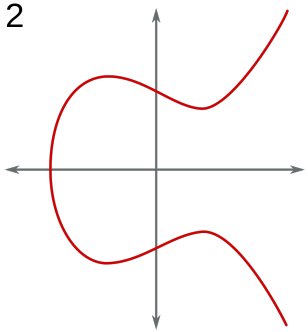
An elliptic curve E over a field K is a smooth, projective, algebraic curve of genus 1, with a specified point $\mathcal{O} \in E(K)$.

1



$y^2 = x^3 - x$

2



$y^2 = x^3 - x + 1$

Every elliptic curve E can be written as a projective curve satisfying a Weirstrass equation:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

If $\mathrm{char}(K) \neq 2$, E can be given by

$$y^2 = x^3 + ax^2 + bx + c = f(x) \text{ (with } \mathcal{O} = [0 : 1 : 0]).$$

Elliptic curves - Discriminant

$$E : y^2 = x^3 + ax^2 + bx + c = f(x)$$

E smooth $\iff$ f has no multiple roots in $\overline{K}$ $\iff$ $\mathrm{Disc}(f) \neq 0$
Discriminant of E is

$$\Delta(E) = 16\,\mathrm{Disc}(f) = 16(a^2b^2 - 4a^3c - 4b^3 - 27c^2 + 18abc).$$

If $f(x) = (x - e_1)(x - e_2)(x - e_3)$, then $\Delta(E) = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2$.

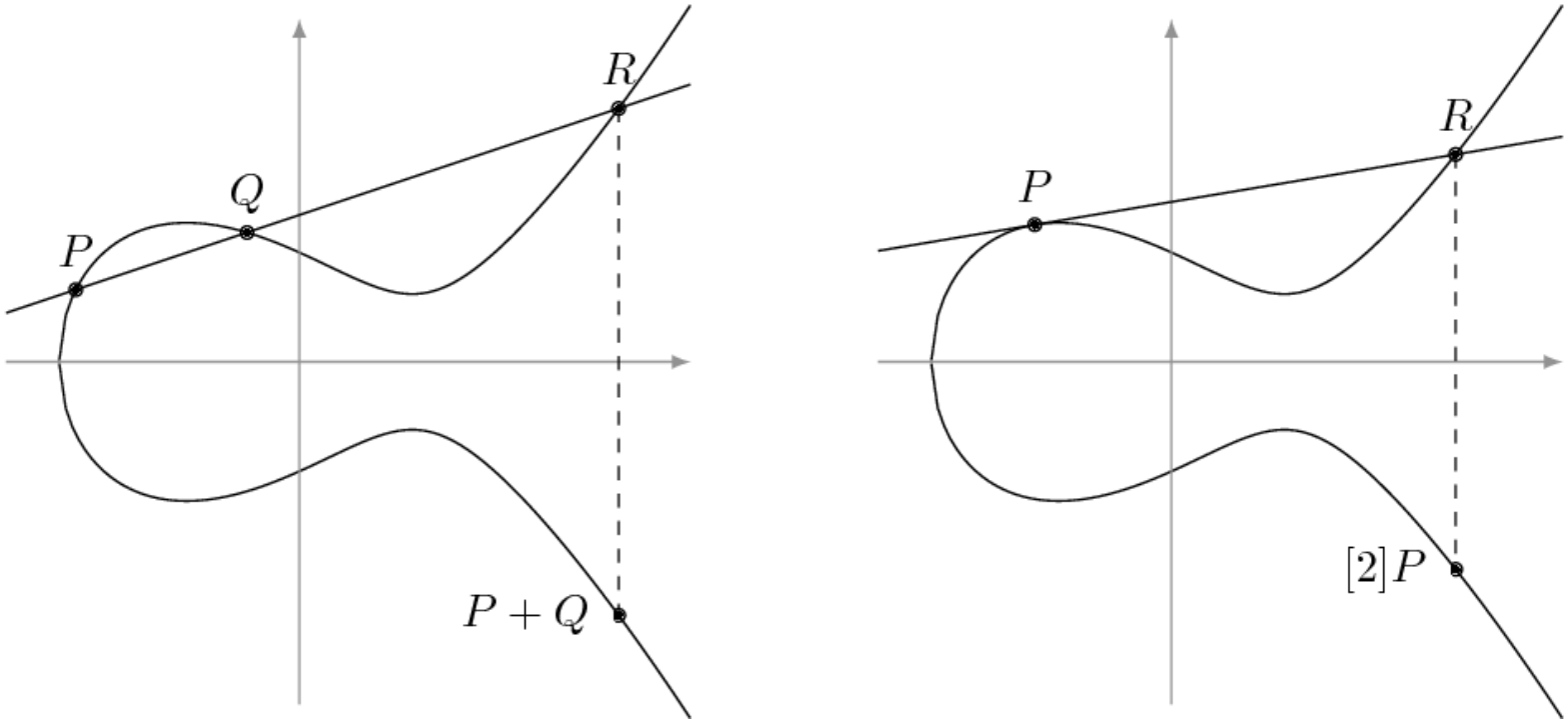
Example

Let $E : \ y^2 = x(x - A)(x + B)$, with $A, B, C := A + B \neq 0$. Then E is an elliptic curve with discriminant

$$\Delta(E) = 16A^2B^2(A + B)^2 = 16(ABC)^2$$

Elliptic curves - group law

We can define an operation (addition) on an elliptic curve E by a process of chords and tangents:



With this operation $(E, +)$ is an abelian group. What is known about its structure?

Elliptic curves - Group structure

Theorem (Mordell - Weil)

If K is a number field, then $E(K)$ is a finitely generated abelian group.

$$E(K) \cong E(K)^{tors} \times \mathbb{Z}^r$$

For $K = \mathbb{Q}$ all possibilities for the torsion of $E(K)$ are known, by Mazur's theorem.

Elliptic curves - Reduction modulo p

Consider an elliptic curve E over $\mathbb{Q}$. We can make a change of coordinates so that all $a_i \in \mathbb{Z}$ and $|\Delta(E)|$ is **minimal**.
This is a minimal model for E and $\Delta_{min} := \Delta(E)$ is the **minimal discriminant**.
We can look at this equation modulo some prime p. We get a curve $\bar{E}$ over $\mathbb{F}_p$,

$$\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}.$$

Could be **singular**! Depending on the type of curve E we have cases:

1. **Good reduction** - if E is non-singular ($\Leftrightarrow p \nmid \Delta(E)$)
2. **Bad reduction** - if E is singular ($\Leftrightarrow p \mid \Delta(E)$), with subcases:
   a. **Additive reduction** - if E has a cusp
   b. **Multiplicative reduction** - if E has a node

If E has everywhere good or multiplicative reduction, then E is semistable.

Conductor of an elliptic curve

$$N = \prod_{p \text{ prime}} p^{f_p(E)},$$

$$\text{where} \quad f_p(E) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2 & \text{if } E \text{ has additive reduction at } p \text{ and } p \neq 2, 3. \end{cases}$$

For $p = 2, 3$ $f_p(E)$ more complicated, but $f_p(E) \geq 2$ if E has additive reduction p.

N stores information about reduction of E at all primes (finer than Δ_{min}).

E is semistable if and only if the conductor N of E is squarefree.

An important example

Example

Let $E : y^2 = x(x - A)(x - B)$ with $A, B \in \mathbb{Z}$, $\gcd(A, B) = 1$ and $A \equiv -1 \pmod 4$, $B \equiv 0 \pmod{32}$. Set $C := A + B$.

$$\Delta_{min} = \frac{(ABC)^2}{256}, \quad N = \prod_{\substack{p \text{ prime} \\ p \mid ABC}} p$$

Newforms

Definition

A newform of level N is a normalized modular form in $S_2^{new}(N)$ that is a simultaneous eigenvector for all Hecke operators.

Facts about newforms:

- A newform is given by its q expansion

$$f = q + \sum_{n \geq 2} c_n q^n$$

- There are finitely many newforms of level N ($N \in \mathbb{N}$), and there are exact formulas for number of newforms of level N
- $K = \mathbb{Q}(c_2, c_3, \dots)$ is a totally real finite extension of $\mathbb{Q}$
- The Fourier coefficients c_n are algebraic integers

Theorem

There are no newforms at levels 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60.

The modularity theorem

A newform f is rational if all $c_n \in \mathbb{Q}$, otherwise it is irrational.

Theorem

There is a bijection:

$$\textit{rational newforms of level } N \leftrightarrow \textit{isogeny classes of elliptic curves over } \mathbb{Q} \textit{ of conductor } N$$

$$f = q + \sum_{n \geq 2} c_n q^n \mapsto E_f$$

such that $c_p = a_p(E) = p + 1 - \#E_f(\mathbb{F}_p)$ *for all primes* $p \nmid N$.

Elliptic curve is **modular** if it is in the image of the map above.

The Modularity Theorem: All elliptic curves over $\mathbb{Q}$ are modular.

Reminder:

- We now know the Frey curve

$$E : y^2 = x(x - a^p)(x + b^p)$$

  is modular (supposing it exists) $\implies$ there is a rational newform associated to E

- Still have to show that it cannot be modular ("behaves strangely")
- **Note**: level N = conductor of E depends on a, b, c, p
- **Idea**: relate E to a newform of level that doesn't depend on the solution

Level-lowering

Let $E/\mathbb{Q}$ be an elliptic curve, of conductor N and minimal discriminant Δ_{min}, and let p be a prime. Define

$$N_p = N/\prod_{\substack{q||N \\ p|ord_q(\Delta)}} q.$$

If $f = q + \sum_{n\geq 2} c_n q^n$ is a newform of level N', we say that E **arises from** f **mod** p ($E \sim_p f$) if there is an ideal $\mathfrak{P} \mid p$ of $\mathcal{O}_K$ such that $c_\ell \equiv a_\ell(E) \pmod{\mathfrak{P}}$ for all but finitely many primes ℓ.

Theorem (Ribet 1990, "Level-lowering theorem")

Let E be an elliptic curve defined over $\mathbb{Q}$ and $p \geq 5$ prime. Suppose that E has no p-isogenies over $\mathbb{Q}$ and that it is **modular**.
Then there exists a newform of level N_p such that $E \sim_p f$.

Fermat's Last Theorem - revisited

Now we have all the ingredients needed for the proof of FLT.
Suppose that $a, b, c \in \mathbb{Z}, p \geq 5$ prime satisfying

$$a^p + b^p + c^p = 0, \quad abc \neq 0.$$

Without loss of generality $\gcd(a, b, c) = 1, b \equiv 0 \pmod 2$ and, $a \equiv -1 \pmod 4$.
Define an elliptic curve over $E : y^2 = x(x - a^p)(x + b^p) \implies$ defined over $\mathbb{Q}$
We have seen that for an elliptic curve of this form
$(A = a^p, B = b^p, C = A + B = -c^p)$

$$\Delta_{min} = \frac{(abc)^{2p}}{256}, \quad N = \prod_{\ell | ABC} l = \prod_{\ell | abc} l$$

We can apply Ribet's theorem because:

- E is modular by the modularity theorem
- E has no p-isogenies (due to Mazur, because $p \geq 5$ and $\#E(\mathbb{Q})[2] = 4$)

Fermat's Last Theorem - continued

Calculating N_p from Ribet's theorem, we get

$$N_p = \prod_{\ell | abc} \ell \Big/ \prod_{\substack{q||N \\ p|ord_q(\Delta_{min})}} q = 2$$

By Ribet, there exists a newform f of level 2 such that $E \sim_p f$.
But, there are **no newforms at level 2**.
Contradiciton!

Further applications

Theorem (Wiles ($r = 0$); Ribet ($r \geq 2$); Darmon, Merel ($r = 1$))

Suppose $p \geq 5$ prime. Then the equation

$$x^p + 2^r y^p + z^p = 0$$

has no solutions with $xyz = 0$ and x, y, z pairwise coprime except $r = 1$ and $(x, y, z) = \pm(-1, 1, -1)$.

General recipe for modular method

Study a Diophantine equation, suppose it has a solution and associate an elliptic (Frey) curve E to this solution so that it has properties:

- The coefficients of E depend on the solution of the Diophantine equation
- Δ_{min} is of the form $C \cdot D^p$, so that C does not depend on the solutions but only on the equation itself
- E has multiplicative reduction at primes dividing D
- Primes dividing D can be removed when we write down $N_p \to N_p$ depends only on the equation
- Only finitely many possibilities for N_p
- For each N_p, only finitely many newforms of level N_p
- Applying Ribet's, Mazur's and modularity theorem we get a finite list of possible f-s such that $E \sim_p f$.