Introduction to the modular method

Nicolas Billerey

Laboratoire de mathématiques Blaise Pascal
Université Clermont Auvergne

Barcelona
February 3, 2020

Table of contents

Table of contents

Generalized Fermat Equations (GFE)

- Let A, B and C be coprime non-zero integers.
- We are interested in the following diophantine problem : find all sextuples (x, y, z, p, q, r) of integers such that $p,\ q,\ r \geq 2$ and

$$Ax^p + By^q = Cz^r.$$

- This is a widely open problem, despite lots of efforts by many mathematicians, starting with old Greeks.
- In this lecture : survey a tiny, yet important part of this long story, focusing mainly on the case

$$A = B = C = 1 \quad \text{and} \quad p = q = r.$$

Solutions and signatures

Given p, q, $r \geq 2$, consider the Generalized Fermat Equation

$$Ax^p + By^q = Cz^r. \tag{1}$$

Definition

- We call a solution any triple (x, y, z) of integers satisfying (1).
- A solution is said primitive if $\gcd(x, y, z) = 1$.
- The triple (p, q, r) is called the signature.

In solving Eq. (1), the problem is completely different according to whether

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1, = 1 \text{ or } < 1.$$

Fixed signature

- For any integer $p \geq 4$, the equation

$$AX^p + BY^p = CZ^p$$

  defines a smooth, projective curve of genus $\frac{(p-1)(p-2)}{2} \geq 2$.
- By Faltings' proof of Mordell's conjecture, it has only finitely many rational points.
- Applying Faltings' result in a subtle way, Darmon and Granville obtained the following.

Theorem (Darmon-Granville)

Let $p, q, r \geq 2$ be integers such that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. Then, there exist only finitely many primitive solutions to the Generalized Fermat Equation

$$Ax^p + By^q = Cz^r.$$

Varying signatures : general expectations

abc-Conjecture (Masser–Oesterlé)

Let $\varepsilon > 0$. For all non-zero coprime integers a, b, c such that $a + b = c$, we have

$$\max\left(|a|, |b|, |c|\right) \ll_\varepsilon \operatorname{rad}\left(abc\right)^{1+\varepsilon}.$$

Proposition

Assume the *abc*-Conjecture holds. Then, there are only finitely many triples (x, y, z) of coprime integers for which there exist integers p, q, $r \geq 2$ such that

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1 \quad \text{and} \quad Ax^p + By^q = Cz^r.$$

The special case $A = B = C = 1$

Fermat–Catalan Conjecture

The only primitive solutions in non-zero integers of the Generalized Fermat Equations

$$x^p + y^q = z^r, \quad \text{with } \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$$

correspond to the following identities :

$$1+2^3 = 3^2,\ 2^5+7^2 = 3^4,\ 7^3+13^2 = 2^9,\ 2^7+17^3 = 71^2,\ 3^5+11^4 = 122^2$$

and

$$17^7 + 76271^3 = 21063928^2,\quad 1414^3 + 2213459^2 = 65^7,$$

$$9262^3 + 15312283^2 = 113^7,\quad 43^8 + 96222^3 = 30042907^2,$$

$$33^8 + 1549034^2 = 15613^3.$$

Trivial solutions (I)

- While solving GFE for varying signatures, it is common to keep the notation p for a varying exponent and r for a fixed one.
- In these lectures, we'll be concerned with Generalized Fermat Equations of signatures (p, p, p), (p, p, r) and (r, r, p).
- As a consequence of *abc*-Conjecture, if (x, y, z) is a primitive solution of a GFE in non-zero integers, then for large enough p, we have

$$\begin{cases} |xyz| = 1 & \text{for signature } (p, p, p) \text{ ;} \\ |xy| = 1 & \text{for signature } (p, p, r) \text{ ;} \\ |z| = 1 & \text{for signature } (r, r, p). \end{cases}$$

Trivial solutions (II)

Definition

We call such triples the trivial solutions together with solutions (x, y, z) such that $xyz = 0$.

Remark

It is worth noting that these "trivial" solutions might be a highly non-trivial obstruction to solving the corresponding equation.

Table of contents

Statement and first reductions

Fermat's Last Theorem

For every $n \geq 3$, there is no non-trivial primitive solution to the equation

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

- The proof is by contradiction, assuming the existence of a non-trivial primitive solution (a, b, c) for some $n \geq 3$.
- Euler proved the case $n = 3$ and Fermat the case $n = 4$.
- Hence we may assume $n = p \geq 5$ is prime.
- Permuting a, b and c if necessary, we assume

$$a^P \equiv -1 \pmod 4 \quad \text{and} \quad b^P \equiv 0 \pmod{16}.$$

- We proceed in five steps. The whole argument is known as the modular method.

The Frey curve (I)

- Consider the elliptic curve $E_{a,b,c}$ given by the equation

$$Y^2 = X(X - a^p)(X + b^p). \tag{2}$$

- We compute the standard coefficients of this model

$$c_4 = 16\left(a^{2p} + (ab)^p + b^{2p}\right), \quad \Delta = 16(abc)^{2p} \quad \text{and} \quad j = \frac{c_4^3}{\Delta}.$$

- The equation (2) defines a minimal model for $E_{a,b,c}$ away from 2.
- The curve $E_{a,b,c}$ has bad reduction at an odd prime ℓ if and only if $\ell \mid abc$.
- Under our assumptions, the curve $E_{a,b,c}$ has bad multiplicative reduction at 2.

The Frey curve (II)

To summarize :

Proposition

The curve $E_{a,b,c}$ is semi-stable and has bad reduction precisely at the primes dividing abc. Moreover, if $\ell \mid abc$ is such a prime, then

$$v_\ell(j) = \begin{cases} -2pv_\ell(abc) & \equiv 0 \pmod{p} & \text{if } \ell \text{ odd;} \\ 8 - 2pv_2(abc) & \not\equiv 0 \pmod{p} & \text{if } \ell = 2. \end{cases}$$

Wiles' theorem

Theorem (Wiles, Taylor–Wiles)

Let $E/\mathbb{Q}$ be a semi-stable elliptic curve of conductor N and let

$$L(E,s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p(E)p^{-s} + \mathbf{1}_N(p)p^{1-2s}} = \sum_{n \geq 1} \frac{a_n(E)}{n^s}$$

be its L-function. Then, $f_E = \sum_{n \geq 1} a_n(E)q^n$ is a weight 2 newform of level N and trivial Nebentypus.

Remark

Note that the coefficients of f_E are all rational integers.

Elliptic Galois representations

- Let $E/\mathbb{Q}$ be an elliptic curve of conductor N.
- For every prime number p, denote by

$$\rho_{E,p}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

the Galois representation corresponding to the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion of E.

Definition

The representation $\rho_{E,p}$ is unramified at a prime ℓ if $\rho_{E,p}(I_\ell) = \{1\}$ where I_ℓ is an inertia group at ℓ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
It is ramified otherwise.

Remark

The representation $\rho_{E,p}$ is unramified outside Np.

Ramification at the bad primes

Let j be the j-invariant of E.

Proposition (Tate)

Let $\ell \neq p$ be a prime such that $\ell \parallel N$. Then, the representation $\rho_{E,p}$ is unramified at ℓ if and only if $v_\ell(j) \equiv 0 \pmod{p}$.

Using the arithmetic properties of the Frey curve, we obtain :

Corollary

The representation $\rho_{E_{a,b,c},p}$ is unramified away from 2 and p.

Irreducibility

Theorem (Mazur)

The only possible torsion subgroups of $E(\mathbb{Q})$ are

$$\begin{array}{ll} \mathbb{Z}/n\mathbb{Z} & \text{for } 1 \leq n \leq 10 \text{ and } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} & \text{for } 1 \leq n \leq 4. \end{array}$$

As a consequence of the local description of $\rho_{E_{a,b,c},p}$ and the previous result, we get :

Theorem

The representation $\rho_{E_{a,b,c},p}$ is (absolutely) irreducible.

Modular Galois representations (I)

- Let $f = \sum_{n \geq 1} a_n q^n$ be a weight 2 newform of level N and trivial Nebentypus.
- For every prime p, there is a Galois representation

$$\rho_{f,p} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

which is uniquely characterized (up to semi-simplification and isomorphism) by the following property : it is unramified outside Np and for every prime $\ell \nmid Np$, the characteristic polynomial of $\rho_{f,p}(\mathrm{Frob}_\ell)$ is the reduction of

$$X^2 - a_\ell X + \ell.$$

Modular Galois representations (II)

Definition

A Galois representation

$$\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

is modular of level $N \geq 1$ if there exists a weight 2 newform f of trivial Nebentypus and level N such that $\rho \simeq \rho_{f,p}$. In that case, we say that ρ arises from f.

Theorem

The Galois representation $\rho_{E_{a,b,c},p}$ is modular of level $N = \prod_{\substack{\ell \mid abc \\ \ell \text{ prime}}} \ell$.

Lowering the level

Theorem (Ribet)

Let $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be an irreducible Galois representation. Suppose that ρ is modular of level N and let $\ell \,\|\, N$ be a prime. If ρ is finite at ℓ, then ρ is modular of level N/ℓ.

Applying Ribet's theorem recursively to the representation $\rho_{E_{a,b,c},p}$ gives the following result.

Theorem

The representation $\rho_{E_{a,b,c},p}$ is modular of level 2.

End of the proof

- There is no non-zero weight 2 newform of level 2.
- Hence Fermat's Last Theorem is proved !

Table of contents

Fermat curves

We wish to apply the strategy of the previous section to the Fermat curves

$$Ax^p + By^p = Cz^p$$

for some fixed coprime non-zero integers A, B and C.

Good points (I)

Let (a, b, c) be a non-trivial primitive solution.

- The equation

$$Y^2 = X(X - Aa^p)(X + Bb^p)$$

still defines an elliptic curve $E_{a,b,c}^{A,B,C}/\mathbb{Q}$ with nice arithmetic properties.

- Thanks to the work of Breuil, Conrad, Diamond and Taylor, the curve $E = E_{a,b,c}^{A,B,C}$ is again modular.
- At least for large enough p, depending on A, B, C (but not on (a, b, c)) general results of Mazur apply to show that the representation

$$\rho_{E,p} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

is irreducible.

Good points (II)

- Combining arithmetic properties of E with modularity and irreducibility for $\rho_{E,p}$, Ribet's result applies to show that $\rho_{E,p}$ arises from a weight 2 newform $f = \sum_{n\geq 1} a_n(f)q^n$ of level M which is explicit and almost independant of the solution.
- The isomorphism $\rho_{E,p} \simeq \rho_{f,p}$ can be restated as follows. There exists a prime ideal $\mathfrak{p}$ over p in $\overline{\mathbb{Q}}$ such that for any prime ℓ, the following congruences hold :

$$\begin{cases} a_\ell(f) \equiv a_\ell(E) \pmod{\mathfrak{p}} & \text{if } \ell \nmid Np \\ a_\ell(f) \equiv \pm(\ell+1) \pmod{\mathfrak{p}} & \text{if } \ell \nmid Mp \text{ and } \ell \mid N \end{cases}$$

where N denotes the conductor of E.

Questions

Despite these good points, we are left with several questions :

1. How do we compute the forms f ?
2. How do we discard the previous congruences ?
3. How do we deal with the "small" primes ?

The equation $x^p + y^p = 2z^p$

Theorem (Ribet, Darmon–Merel)

For every $n \geq 3$, the Fermat equation $x^n + y^n = 2z^n$ has no non-trivial primitive solution.

Remark

Note the existence of the trivial solution $(1, 1, 1)$.

- The case $2 < n < 31$ of the above theorem is known thanks to the work of Dénes.
- Let (a, b, c) be a non-trivial primitive solution for $n = p \geq 7$ prime.

The Frey curve and its attached Galois representation

Proposition

- The elliptic curve $E = E_{a,b,c}^{A,B,C}$ has all of its points of order 2 defined over $\mathbb{Q}$ and conductor

$$N = \begin{cases} \mathrm{rad}(abc) & \text{if } abc \text{ is even} \\ 2^5\mathrm{rad}(abc) & \text{if } abc \text{ is odd.} \end{cases}$$

- There is at least one odd prime of bad multiplicative reduction.

Proposition

- The representation $\rho_{E,p}$ is absolutely irreducible.
- It has conductor $M = \begin{cases} 2 & \text{if } abc \text{ is even} \\ 32 & \text{if } abc \text{ is odd.} \end{cases}$

Congruences

- By modularity and level-lowering, the representation $\rho_{E,p}$ arises from a weight 2 newform of level M.
- For $M = 2$ (i.e. abc is even), we get a contradiction as in FLT.
- But for $M = 32$, the space $S_2^{\text{new}}(\Gamma_0(32))$ is 1-dimensional and spanned by a unique newform f corresponding to the (isogeny class of the) elliptic curve F with equation $Y^2 = X^3 - X$.

Remark

Note that this curve is precisely the Frey curve associated with the trivial solution $(1, 1, 1)$.

How do we contradict the isomorphism $\rho_{E,p} \simeq \rho_{F,p}$?

A conjectural answer

Conjecture (Frey–Mazur)

There exists a constant $C > 0$ such that for all elliptic curves E and F defined over $\mathbb{Q}$ and for all prime numbers $p > C$ we have

$$\rho_{E,p} \simeq \rho_{F,p} \Longrightarrow E \text{ and } F \text{ are isogenous over } \mathbb{Q}.$$

At least for large enough p, this conjecture would imply that $N = M = 32$ and hence a contradiction, for (a, b, c) is a non-trivial solution.

Complex Multiplication Theory

- The curve F has complex multiplication by $\mathbb{Q}(\sqrt{-1})$.
- Let G be the image of $\rho_{F,p}$ in $\mathrm{GL}_2(\mathbb{F}_p)$.

Proposition

The group G is the normalizer of a Cartan subgroup. This Cartan subgroup is split if $p \equiv 1 \pmod 4$ and non-split if $p \equiv -1 \pmod 4$.

The case $p \equiv 1 \pmod 4$

- Assume $\rho_{E,p} \simeq \rho_{F,p}$ and $p \equiv 1 \pmod 4$.
- The curve E gives rise to a rational point on the modular curve $X_{\mathrm{split}}(p)$.
- For $p \geq 17$, this implies that E has potentially good reduction at all primes $\ell \neq 2$ (Momose) and hence a contradiction.
- The conclusion now follows from more recent results by Bilu–Parent–Rebolledo (for $p \geq 17$) and Balakrishnan–Dogra–Müller–Tultman–Vonk (for $p = 13$).

The case $p \equiv -1 \pmod 4$

A more detailed study of the representation $\rho_{F,p}$ gives the following.

Proposition

We have $G = \rho_{F,p}(D_p)$ where D_p is a decomposition group at p. In particular, G is the normalizer of a non-split Cartan subgroup and the prime p does not divide abc.

Besides, Darmon and Merel proved the following integrality result which contradicts the proposition above and finishes the proof of their theorem in the case when abc is odd.

Theorem

The j-invariant of E belongs to $\mathbb{Z}[\frac{1}{p}]$.

Fermat curves with odd coefficients

Theorem (Halberstadt–Kraus)

Let A, B, C be three odd pairwise coprime integers. Then there exists a set of primes P of positive density such that for every prime $p \in P$, the Generalized Fermat equation $Ax^p + By^p = Cz^p$ has no non-trivial primitive solution.

- For large enough p, we have $\rho_{E,p} \simeq \rho_{F,p}$ where F is an ellitpic curve over $\mathbb{Q}$ of conductor $2\mathrm{rad}(ABC)$.
- Under some congruence conditions this isomorphism is both compatible and incompatible with the Weil pairing.

Remark

Note that this result does not require any modular forms computation.

Other known Frey curves over $\mathbb{Q}$

- Frey curves associated with the Generalized Fermat equations have been constructed by various authors for a few signatures including :

$$(p, p, 2), \quad (p, p, 3) \quad \text{and} \quad (r, r, p)$$

for $r = 3, 5, 7$.

- For a non-trivial primitive solution (a, b, c) of $x^3 + y^3 = z^p$ this Frey curve reads as follows

$$E\colon\ Y^2 = X^3 + 3abX + b^3 - a^3.$$

The case of $x^3 + y^3 = z^p$

The following result follows from works by Euler, Darmon–Granville, Kraus, Bruin, Chen–Siksek and Freitas.

Theorem

The generalized Fermat equation $x^3 + y^3 = z^p$ has no non-trivial primitive solution for $p \geq 3$ in a set of primes P of density ≈ 0.844. For instance, P contains primes p such that

$$p < 10^7, \quad \text{or } p \equiv 51, 103, 105 \pmod{106}, \quad \text{or } p \equiv 2 \pmod{3}.$$

Remark

The main obstacle here is to contradict the isomorphism $\rho_{E,p} \simeq \rho_{F,p}$ where F is the Frey curve associated with the pseudo-solution $2^3 + 1^3 = 3^2$.

The case of $x^7 + y^7 = Cz^p$

Associated with a non-trivial primitive solution (a, b, c) of $x^7 + y^7 = Cz^p$ are three different Frey objects :

- A Frey curve over $\mathbb{Q}$

$$Y^2 = X^3 + a_2X^2 + a_4X + a_6$$

where

$$\begin{aligned} a_2 &= -(a-b)^2, \\ a_4 &= -2a^4 + a^3b - 5a^2b^2 + ab^3 - 2b^4, \\ a_6 &= a^6 - 6a^5b + 8a^4b^2 - 13a^3b^3 + 8a^2b^4 - 6ab^5 + b^6. \end{aligned}$$

The case of $x^7 + y^7 = Cz^p$

- A Frey curve over a totally real cubic field :

$$Y^2 = X(X - A_{a,b})(X + B_{a,b}),$$

where $z = -(\zeta_7 + \zeta_7^{-1})$ and

$$\begin{aligned} A_{a,b} &= (-2 + z + z^2)(a + b)^2 \\ B_{a,b} &= (4 - z^2)(a^2 - zab + b^2). \end{aligned}$$

- A Frey hyperelliptic curve over $\mathbb{Q}$

$$y^2 = x^7 + 7abx^5 + 14a^2b^2x^3 + 7a^3b^3x + b^7 - a^7.$$

The case of $x^7 + y^7 = Cz^p$

- This is a very rich situation !
- How the modular method extends to such a situation is the topic of some of the next lectures and a great challenge for future research.

Thank you for your attention