Hecke characters and $\mathbb{Q}$-curves in the modular method

Seminari de Teoria de Nombres 2022, December 31.

Lucas Villagra Torcomian, Universidad Nacional de Córdoba.

Based on joint works with Ariel Pacetti.

Fermat-type equations

Given A, B, C integers, we are interested in equations of the form

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

Fermat-type equations

Given A, B, C integers, we are interested in equations of the form

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

Theorem (Darmon-Granville)
Fix A, B, C as above and fix a signature (p, q, r) such that $1/p + 1/q + 1/r < 1$. Then there exist only a finite number of solutions (a, b, c) satisfying $\gcd(a, b, c) = 1$.

Modular method

Modular method

(1) **Construction:** to a hypothetical primitive solution (a, b, c) of the equation, attach an elliptic curve and consider its Galois representation.

Modular method

(1) **Construction:** to a hypothetical primitive solution (a, b, c) of the equation, attach an elliptic curve and consider its Galois representation.

(2) **Modularity:** attach a newform to the Galois representation, with a specic level N and Nebentypus ε, not depending on the solution.

Modular method

(1) **Construction:** to a hypothetical primitive solution (a, b, c) of the equation, attach an elliptic curve and consider its Galois representation.

(2) **Modularity:** attach a newform to the Galois representation, with a specic level N and Nebentypus ε, not depending on the solution.

(3) **Contradiction:** Compute the space $S_2(\Gamma_0(N), \varepsilon)$ of the above step and prove that none of the newforms is related to a possible primitive solution.

The equation $x^4 + dy^2 = z^p$

The equation $x^4 + dy^2 = z^p$: the curve $E_{(a,b,c)}$

Definition

Let L be a number field and E/L an elliptic curve. The curve E is called a $\mathbb{Q}$-curve if for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, the curve $\sigma(E)$ is isogenous to E.The minimum field where the curve and all the isogenies are defined is usually called the field of total definition.

The equation $x^4 + dy^2 = z^p$: the curve $E_{(a,b,c)}$

Theorem (Ribet)
A twist of $\rho_{E_{(a,b,c)},p}$ extends to a two dimensional representation of $\mathrm{Gal}_{\mathbb{Q}}$.

The equation $x^4 + dy^2 = z^p$: the curve $E_{(a,b,c)}$

Theorem (Ribet)
A twist of $\rho_{E_{(a,b,c)},p}$ extends to a two dimensional representation of $\mathrm{Gal}_{\mathbb{Q}}$.

Goal:

$$\boxed{{}^{\tau}\chi = \chi \cdot \psi_{-2},}$$

where $\psi_{-2} : \mathrm{Gal}(K(\sqrt{-2})/K) \to \mathbb{C}^{\times}$.

Construction of the Hecke character

$$\boxed{{}^{\tau}\chi = \chi \cdot \psi_{-2}}$$

$$0 \longrightarrow K^\times \cdot \left(\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^\times \times (K \otimes \mathbb{R})^\times\right) \longrightarrow \mathbb{I}_K \xrightarrow{\mathrm{Id}} \mathrm{Cl}(K) \longrightarrow 0$$

Construction of the Hecke character

$$\boxed{{}^{\tau}\chi = \chi \cdot \psi_{-2}}$$

$$0 \longrightarrow K^{\times} \cdot \left(\prod_{\mathfrak{q}} \mathscr{O}_{\mathfrak{q}}^{\times} \times (K \otimes \mathbb{R})^{\times}\right) \longrightarrow \mathbb{I}_K \xrightarrow{\mathrm{Id}} \mathrm{Cl}(K) \longrightarrow 0$$

$$K^{\times} \cap \left(\mathscr{O}_{\mathfrak{q}}^{\times} \times (K \otimes \mathbb{R})^{\times}\right) = \mathscr{O}_K^{\times}.$$

Existence of the character

Theorem (Pacetti-V.)
There exists a Hecke character $\chi : \mathsf{Gal}_K \to \mathbb{C}^\times$ *such that:*

1. $\chi^2(\sigma) = \varepsilon(\sigma)$ *for all* $\sigma \in \mathsf{Gal}_K$,
2. χ *ramifies only at* 2 *and* 3,
3. ${}^\tau\chi = \chi \cdot \psi_{-2}$.

Existence of the character

Theorem (Pacetti-V.)
There exists a Hecke character $\chi : \mathrm{Gal}_K \to \mathbb{C}^\times$ *such that:*

1. $\chi^2(\sigma) = \varepsilon(\sigma)$ *for all* $\sigma \in \mathrm{Gal}_K$*,*
2. χ *ramifies only at* 2 *and* 3*,*
3. ${}^\tau\chi = \chi \cdot \psi_{-2}$*.*

Theorem (Pacetti-V.)
The twisted representation $\rho_{E_{(a,b,c)},p} \otimes \chi$ *extends to a* 2*-dimensional representation* $\tilde{\rho}_p$ *of* $\mathrm{Gal}_{\mathbb{Q}}$ *attached to a newform of weight* 2*, Nebentypus* ε *and level N given by*

$$N = 2^e \cdot 3 \cdot \prod_{\substack{q \mid c \\ q \neq 2,3}} q, \quad \text{where } e = 8, 9.$$

Back to the steps

(1) **Construction:** to a hypothetical primitive solution (a, b, c) of the equation, attach an elliptic curve and consider its Galois representation.

(2) **Modularity:** attach a newform to the Galois representation, with a specic level N and Nebentypus ε, not depending on the solution.

(3) **Contradiction:** Compute the space $S_2(\Gamma_0(N), \varepsilon)$ of the above step and prove that none of the newforms is related to a possible primitive solution.

Step 3: Contradiction

Proposition (Mazur's trick)
Let (a, b, c) be a non-trivial primitive solution, and $g \in S_2(\Gamma_0(n), \varepsilon)$ such that $\overline{\rho_{E_{(a,b,c)},p} \otimes \chi} \simeq \overline{\rho_{g,K,p}}$. Let q be a rational prime with $q \nmid pn$. Let $\mathfrak{q}$ be a prime of $\mathcal{O}_K$ dividing q and define

$$B(q, g; a, b) = \begin{cases} N(a_{\mathfrak{q}}(E_{(a,b,c)})\chi(\mathfrak{q}) - a_q(g)) & \text{if } q \nmid c \text{ and } q \text{ splits in } K, \\ N(a_q(g)^2 - a_q(E_{(a,b,c)})\chi(q) - 2q\varepsilon(q)) & \text{if } q \nmid c \text{ and } q \text{ is inert in } K, \\ N(\varepsilon^{-1}(q)(q+1)^2 - a_q(g)^2) & \text{if } q \mid c. \end{cases}$$

Then, $p \mid B(q, g; a, b)$.

An example of a Diophantine result

Theorem (Ellenberg)
Given d a positive integer, suppose that $E/\mathbb{Q}(\sqrt{-d})$ is a $\mathbb{Q}$-curve which has multiplicative reduction at an odd prime $\mathfrak{q}$ not dividing 3. Then, there exists an integer N_d such that the projective image of the residual representation of $\rho_{E,p}$ is surjective for all primes $p > N_d$.

An example of a Diophantine result

Theorem (Ellenberg)
Given d a positive integer, suppose that $E/\mathbb{Q}(\sqrt{-d})$ is a $\mathbb{Q}$-curve which has multiplicative reduction at an odd prime $\mathfrak{q}$ not dividing 3. Then, there exists an integer N_d such that the projective image of the residual representation of $\rho_{E,p}$ is surjective for all primes $p > N_d$.

Theorem (Pacetti - V.)
Let $p > 563$ be a prime number. Then there are no non-trivial primitive solutions of the equation

$$x^4 + 6y^2 = z^p.$$

The equation $x^2 + dy^6 = z^p$

Consider the equation $x^2 + dy^6 = z^p$.

The equation $x^2 + dy^6 = z^p$

Consider the equation $x^2 + dy^6 = z^p$.

(1) **Construction:** To a putative non-trivial primitive solution (a, b, c) we attach the elliptic curve

$$\widetilde{E}_{(a,b,c)} : y^2 + 6b\sqrt{-d}xy - 4d(a + b^3\sqrt{-d})y = x^3,$$

also defined over $\mathbb{Q}(\sqrt{-d})$.

The equation $x^2 + dy^6 = z^p$

Consider the equation $x^2 + dy^6 = z^p$.

(1) **Construction:** To a putative non-trivial primitive solution (a, b, c) we attach the elliptic curve

$$\widetilde{E}_{(a,b,c)} : y^2 + 6b\sqrt{-d}xy - 4d(a + b^3\sqrt{-d})y = x^3,$$

also defined over $\mathbb{Q}(\sqrt{-d})$.

(2) **Modularity:** Define a Hecke character such that ${}^{\tau}\chi = \chi \cdot \psi_{-3}$.

The equation $x^2 + dy^6 = z^p$

Consider the equation $x^2 + dy^6 = z^p$.

(1) **Construction:** To a putative non-trivial primitive solution (a, b, c) we attach the elliptic curve

$$\widetilde{E}_{(a,b,c)} : y^2 + 6b\sqrt{-d}xy - 4d(a + b^3\sqrt{-d})y = x^3,$$

also defined over $\mathbb{Q}(\sqrt{-d})$.

(2) **Modularity:** Define a Hecke character such that ${}^{\tau}\chi = \chi \cdot \psi_{-3}$.

(3) **Contradiction:** Using the following:

- Ellenberg's results.
- Mazur's trick.
- $\widetilde{E}_{(a,b,c)}$ has a three torsion point.
- Symplectic argument.

Thanks!