On solutions to $x^4 + dy^2 = z^p$.

Ariel Pacetti

Center for Research and Development in Mathematics and Applications (CIDMA),
University of Aveiro

19th of June 2023

Representation Theory XVIII

joint with Lucas Villagra Torcomian and Franco Golfieri

Let (a, b, c) be an integral solution to the equation $x^4 + dy^2 = z^p$ (an affine surface).

Definition

The solution is called:

- **trivial** *if one of its coordinates is zero.*
- **primitive** *if* $\gcd(a, b, c) = 1$.

Theorem (Darmon-Granville)

If $\frac{1}{4} + \frac{1}{2} + \frac{1}{p} < 1$ *then there are finitely many primitive solutions.*

Remark (Granville)

In general there are infinitely many non-primitive solutions.

A Frey curve attached to (a, b, c)

Consider the elliptic curve (over $K = \mathbb{Q}(\sqrt{-d})$) with equation

$$E_{(a,b,c)} : y^2 = x^3 + 4ax^2 + 2(a^2 + \sqrt{-d}b)x. \quad (1)$$

Proposition (P-Villagra)

The curve $E_{(a,b,c)}$ is a $\mathbb{Q}$-curve, i.e. $\overline{E_{(a,b,c)}}$ is 2-isogenous to the quadratic twist $E_{(a,b,c)} \otimes \psi_{-2}$.

- A result of Ribet implies that a twist of $\rho_{E_{(a,b,c)},p}$ extends to the whole Galois group $\mathrm{Gal}_{\mathbb{Q}}$.
- Serre's conjectures + results of Taylor-Wiles imply that the extension is modular (matching a newform in $S_2(\Gamma_0(N), \varepsilon)$).

Problem

Make N and ε explicit.

Properties of $\rho_{E_{(a,b,c)},p}$

- The discriminant of $E_{(a,b,c)}$ equals $2^9(a^2+b\sqrt{-d})c^p$.
- If $\mathfrak{q} \mid c$ is odd, $E_{(a,b,c)}$ has multiplicative reduction at $\mathfrak{q}$.
- In particular the residual representation has good reduction at odd primes dividing the discriminant.
- The conductor at primes dividing 2 can be explicitly computed.

Regarding the trivial solutions:

- The trivial solution $(0,0,0)$ gives a singular curve.
- The solutions $(\pm 1,0,1)$ are curves with CM by $\mathbb{Z}[\sqrt{-2}]$.
- When $d=1$, the solution $(0,\pm 1,1)$ gives a curve with CM by $\mathbb{Z}[\sqrt{-1}]$.

Let $\tau \in \mathrm{Gal}_{\mathbb{Q}}$ be non trivial on $K := \mathbb{Q}(\sqrt{-d})$. Then

$$^{\tau}\rho_{E_{(a,b,c)},p}(\sigma) := \rho_{E_{(a,b,c)},p}(\tau\sigma\tau^{-1}) = \rho_{E_{(a,b,c)},p} \otimes \psi_{-2}.$$

Our goal is to construct $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}}^{\times}$ such that

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

Then $^{\tau}(\rho_{E_{(a,b,c)},p} \otimes \chi) = \rho_{E_{(a,b,c)},p} \otimes \chi$, so it extends to $\mathrm{Gal}_{\mathbb{Q}}$.
By CFT, it is enough to construct $\chi : \mathbb{I}_K \to \overline{\mathbb{Q}}^{\times}$ with this property.
Using the short exact sequence

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

it is enough to define χ on elements of the first place and on idèles corresponding to representatives of $\mathrm{Cl}(K)$.

First construct the Nebentypus

We construct an extra character $\varepsilon : \mathbb{I}_{\mathbb{Q}} \to \overline{\mathbb{Q}}^{\times}$ that will be the "determinant" of the extension (the Nebentypus).
For $i = 1, 3, 5, 7$, let

$$Q_i = \{\, p \text{ prime } : p \mid d,\ p \equiv i \pmod 8\}.$$

and define the character ε_p to be:

- Unramified at primes p of $Q_1 \cup Q_7$.
- Quadratic at $\mathbb{Z}_p^{\times}$ for primes p of Q_3.
- Of order 4 at $\mathbb{Z}_p^{\times}$ for primes p of Q_5.
- At $\mathbb{Z}_2^{\times}$, $\varepsilon_2 = \psi_{-1}^{\#Q_3 + \#Q_5}$.
- The archimedean component is trivial.

From ε, construct the character χ

We impose on χ the following condition

$$\chi^2 = \varepsilon \circ \mathcal{N}\mathrm{m}.$$

Let $\mathfrak{p}$ be a prime of K and define $\chi_{\mathfrak{p}}$ at $\mathcal{O}_{\mathfrak{p}}$ by

- If $\mathfrak{p} \nmid 2$ and $\mathfrak{p}$ is unramified, $\chi_{\mathfrak{p}}$ is trivial.
- If $\mathfrak{p}$ is odd and ramified, $\chi_{\mathfrak{p}} = \varepsilon_p \cdot \delta_p$.
- An explicit description at primes dividing 2 (depending on d modulo 16 and on the sizes of the sets Q_i).
- If $d < 0$, trivial at one archimidean place and the sign function at the other.

⚠ A hard problem is to verify that on the intersection

$$K^\times \cap (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times (K \otimes \mathbb{R})^\times) = \mathcal{O}_K^\times$$

the character is trivial (specially when $d < 0$ as we need some understanding of the fundamental unit).

Theorem (P-Villagra)

There exists a Hecke character $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}}$ *such that:*

1. $\chi^2(\sigma) = \varepsilon(\sigma)$ *for all* $\sigma \in \mathrm{Gal}_K$,
2. χ *is unramified at primes not dividing* $2\prod_{p \in Q_1 \cup Q_5 \cup Q_7} p$,
3. *If* $\tau \in \mathrm{Gal}_{\mathbb{Q}}$ *is not the identity on* K, ${}^{\tau}\chi = \chi \cdot \psi_{-2}$ *as characters of* Gal_K.

Proof.

Define the character as before, and extend it to representatives of $\mathrm{Cl}(K)$ using the formula

$$\chi^2 = \varepsilon \circ \mathcal{N}\mathrm{m}.$$

Key ingredients: patience and quadratic reciprocity. □

- By construction the character χ is unramified at primes not dividing $2d$, and we have a precise formula for its conductor.
- The character χ satisfying ${}^{\tau}\chi = \chi \cdot \psi_{-2}$ is unique up to multiplication by characters of $\mathrm{Gal}_{\mathbb{Q}}$.

Theorem (P-Villagra)

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

$$N = 2^e \cdot \prod_{q \in S(E_{(a,b,c)})} q \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2.$$

The hard part is to prove the Nebentypus statement when $d < 0$.

Theorem

Suppose that $p \nmid 2d$ and suppose that the residual Galois representation $\overline{\rho_{E_{(a,b,c)},p}}$ is absolutely irreducible. Then there exists a newform $g \in S_2(\Gamma_0(n), \varepsilon)$ with

$$n = 2^e \cdot \prod_{q \in Q_3} q \cdot \prod_{q \in Q_1 \cup Q_5 \cup Q_7} q^2,$$

such that $\rho_{E_{(a,b,c)},p} \equiv \rho_{g,K,p} \otimes \chi^{-1} \pmod{\mathfrak{p}}$, where $\rho_{g,K,p}$ is the restriction of the representation $\rho_{g,p}$ to the Galois group Gal_K and $\mathfrak{p}$ is a prime ideal of $\overline{\mathbb{Q}}$ dividing p.

Results on large residual image

Theorem (Ellenberg)

Suppose that c is divisible by a prime larger than 3. Then there exists an integer N_d such that the projective image of the residual representation of $\rho_{E_{(a,b,c)},p}$ is surjective for all primes $p > N_d$.

Theorem (Jiménez-Dieulefait)

If c is only supported in $\{2,3\}$ then there exists a constant N_d such that if $p > N_d$ then the representation $\overline{\rho_{E_{(a,b,c)},p}}$ has absolutely irreducible image.

It is quite hard to discard solutions when c is only supported at 2 and 3 (for example when $d = 7$).

Proposition

Let q be a rational prime with $q \nmid pn$. Let $\mathfrak{q}$ be a prime of $\mathcal{O}_K$ dividing q and define $B(q,g;a,b)$ by

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

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

In particular, p must divide

$$C(q,g) = \prod_{(a,b)\in\mathbb{F}_q^2} B(q,g;a,b).$$

Example: $d = 7$

Theorem (P-Villagra)

Let $p > 349$ be a prime number. Then there are no non-trivial primitive solutions of the equation

$$x^4 + 7y^2 = z^p.$$

- If c is even, $g \in S_2(\Gamma_0(2 \cdot 7^2))$ otherwise $g \in S_2(\Gamma_0(2^8 \cdot 7^2))$.
- The large image bound equals: 349 (Ellenberg) and 127 (J-D).
- The space $S_2(2 \cdot 7^2)$ has two conjugacy classes. Mazur's trick for a few primes q gives that $p \in \{2, 7, 17\}$.
- The space $S_2(2^8 \cdot 7^2)$ has 98 conjugacy classes, 30 with CM. Since c is odd, Ellenberg's result applies and all CM forms can be discarded (the trivial solutions are here). Mazur's trick discards the non-CM forms if $p \not\in \{2, 3, 5, 7, 11, 17, 23, 31\}$.

When does the method fail?

Once we discard the CM forms, Mazur's trick fails for a newform g precisely when $C(q,g)=0$ for all primes q, i.e. when for any prime q there exists an elliptic curve $E(q)$ such that

$$\overline{\rho_{g,K,p} \otimes \chi^{-1}} \equiv \overline{\rho_{E(q),p}}.$$

Question: is it true in this case that there exists an elliptic curve $\tilde{E}$ defined over K such that $\rho_{g,K,p} \otimes \chi^{-1} = \rho_{\tilde{E}}$?

Theorem (Golfieri-P.-Villagra)

If $C(q,g)=0$ for all primes q, then there exists a constant B (depending on n) such that is $p>B$ then there exists an elliptic curve $\tilde{E}$ defined over K such that

$$\rho_{g,K,p} \otimes \chi^{-1} = \rho_{\tilde{E}}.$$

Theorem

Let d be a prime number congruent to 3 modulo 8 and such that the class number of $K = \mathbb{Q}(\sqrt{-d})$ is not divisible by 3. Then there are no non-trivial primitive solutions of the equation

$$x^4 + dy^2 = z^p,$$

for p large enough.

Theorem

With the same hypothesis, the only elliptic curves defined over K having a K-rational point of order 2 and conductor supported at 2 are those that are base change of $\mathbb{Q}$.

Thank you for your attention!