International Seminar on Automorphic Forms $\mathbb{Q}$-curves, Hecke characters and some Diophantine equations

Ariel Pacetti

Universidad Nacional de Córdoba - CIEM

December 9, 2020

joint work with Lucas Villagra Torcomian

The Fermat curve

Let $p \geq 5$ be a prime number and consider the Fermat curve

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

Let (a, b, c) be any primitive solution, and consider the Frey elliptic curve

$$E_{a,b} : y^2 = x(x - a^p)(x + b^p).$$

It has the following properties:

- $\Delta(E_{a,b}) = 2^4(abc)^{2p}$.
- $j(E_{a,b}) = 2^8(b^p c^p + a^p c^p + a^p b^p)^3/(abc)^{2p}$.
- If $\ell \mid abc$ then $E_{a,b}$ has multiplicative reduction at ℓ.

The Fermat curve continued

Let's look at the residual p-adic representation attached to $E_{a,b}$:

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

It satisfies the following properties:

- (Hellegouarch) It is unramified outside $2p$.
- It has absolutely irreducible image.
- It is *finite* at p hence Serre's weight equals 2.

By Wiles, Taylor-Wiles result $E_{a,b}$ is modular, and by Ribet's lowering the level result, the representation $\overline{\rho_{E,p}}$ matches that of a form in $S_2(\Gamma_0(2))$, but there are no such forms.

A different diophantine equation

Consider the equation studied by Darmon, Ellemberg, Dieulefait-Jimenez.

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

To a solution (a, b, c) one attaches the Frey curve

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

over $K = \mathbb{Q}(\sqrt{-d})$. It satisfies the following properties:

- Its Galois conjugate $\overline{E_{a,b}}$ is isogenous to a twist by $\sqrt{-2}$ of $E_{a,b}$ hence $E_{a,b}$ is a $\mathbb{Q}$-curve (completely defined over $\mathbb{Q}(\sqrt{-d}, \sqrt{-2})$).
- By a result of Ribet, if E does not have CM, a twist of $\rho_{E,p}$ extends to a representation $\widetilde{\rho_{E,p}}$ of $\mathrm{Gal}_{\mathbb{Q}}$.

Ribet's result

For each $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ let $\phi_\tau : E^\tau \to E$ an isogeny. Define

$$c(\tau, \tau') = \phi_\tau \circ {}^\tau\phi_{\tau'} \circ \phi_{\tau\tau'}^{-1} \in \mathrm{End}(E) \otimes \mathbb{Q}.$$

- The element $\mathrm{Inf}(c) \in H^2(\mathrm{Gal}_\mathbb{Q}, \mathbb{Q}^\times)$.
- (Tate) $H^2(\mathrm{Gal}_\mathbb{Q}, \overline{\mathbb{Q}}^\times) = 0$ hence there is $\beta : \mathrm{Gal}_\mathbb{Q} \to \overline{\mathbb{Q}}^\times$ trivializing $\mathrm{Inf}(c)$.
- There exists M/K such that β factors through $\mathrm{Gal}(M/\mathbb{Q})$.
- The variety $\mathrm{Res}_{M/\mathbb{Q}} E$ contains a subvariety of GL_2-type.
- Issues: how to compute M-explicitly? What is the conductor of $\widetilde{\rho_{E,p}}$?

A different approach

Let $\tau \in \mathrm{Gal}_{\mathbb{Q}}$ restricting to a non-trivial automorphism of K.

Definition

Let $\rho : \mathrm{Gal}_K \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ be a continuous irreducible representation. The conjugate representation ρ^τ equals $\rho^t(\sigma) = \rho(\tau\sigma\tau^{-1})$.

Lemma

The representation $\rho : \mathrm{Gal}_K \to \mathrm{GL}_2(\overline{\mathbb{Q}_p})$ extends to $\mathrm{Gal}_{\mathbb{Q}}$ if and only if $\rho \simeq \rho^\tau$.

A different approach

Our hypothesis E^τ being 2-isogenous to E twisted by ψ_{-2} implies that

$$\rho^\tau_{E,p} = \rho_{E,p} \otimes \psi_{-2}.$$

Suppose $\chi : \mathrm{Gal}_K \to \overline{\mathbb{Q}_p}^\times$ is a Hecke character such that

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

then by the above Lemma $\rho_{E,p} \otimes \chi$ extends to $\mathrm{Gal}_\mathbb{Q}$.

Problem: How can we construct such a χ?

Construction of χ

From the exact sequence

$$0 \longrightarrow K^\times \cdot (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times) \longrightarrow \mathbb{I}_K \longrightarrow \mathrm{Cl}(K) \longrightarrow 0,$$

To define the Hecke character χ we start by defining it at $\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times$, provided that

$$\prod_{\mathfrak{q}} \chi_{\mathfrak{q}}(\epsilon) \cdot \chi_\infty(\epsilon) = 1 \tag{1}$$

for all $\epsilon \in \mathcal{O}_K^\times$. Then we extend it by specifying its values at representatives for the class group (satisfying some compatibility).

Strategy of the construction

Our strategy is the following: K will be imaginary quadratic.

- Construct $\epsilon : \mathbb{I}_{\mathbb{Q}} \to \mathbb{C}^{\times}$ an even finite order character (the Nebentypus).

Then construct χ satisfying:

- $\chi^2 = \epsilon \circ \mathcal{N}$ ($\mathcal{N} : \mathbb{I}_K \to \mathbb{I}_{\mathbb{Q}}$).
- For each $\mathfrak{p}$, ${}^{\tau}\chi_{\mathfrak{p}} = \chi_{\mathfrak{p}} \cdot \psi_{-2} \circ \mathcal{N}$.
- For all odd ramified primes p, $\chi_{\mathfrak{p}} = \epsilon_p \delta_p$.
- Extra condition at 2 (for (1) to hold).

This implies our result in the first term of the exact sequence.

Example: $d = 6$

For $d = 6$ the construction is as follows:

- The character ϵ corresponds to $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$.
- The character $\chi_{\mathfrak{p}}$ is unramified at all odd primes.
- The character χ_2 has conductor 4, with values $\chi_2(1+\sqrt{-6}) = i$, $\chi_2(-1) = 1$.

Clearly:

- $\prod_{\mathfrak{p}} \chi_{\mathfrak{p}}(-1) = 1$,
- $\chi_{\mathfrak{p}}^{\tau} = \chi_{\mathfrak{p}} \cdot (\psi_{-2} \circ \mathcal{N})$.
- $\chi_3 = \delta_3 \epsilon_3$.

The class group $\mathrm{Cl}(\sqrt{-6}) = \{1, \mathfrak{q}_5\}$ where $\mathfrak{q}_5 = \langle 5, 2+\sqrt{-6} \rangle$. Let $\alpha \in \mathbb{I}_K$ be the idèle with entries

$$\alpha_v = \begin{cases} 5 & \text{if } v = \mathfrak{q}_5, \\ 1 & \text{otherwise.} \end{cases}$$

Example $d = 6$ continued

Define:

- $\chi(\alpha) = \sqrt{\epsilon(5)} = \sqrt{-1}$,
- Extend to $\mathbb{I}_K = \{1, \alpha\} \times K^\times \cdot (\prod_{\mathfrak{q}} \mathcal{O}_{\mathfrak{q}}^\times \times \mathbb{C}^\times)$ multiplicatively.

By construction, $\chi^2 = \varepsilon \circ \mathcal{N}$. Need to check χ is a morphism.

- In general, if α corresponds to an ideal of odd order t, $\alpha = u\beta^2$ hence

$$\chi(\alpha^t) = \chi(u)^t \chi(\beta^t)^2 = \chi(u)^t \epsilon(\mathcal{N}(\beta^t)) = \chi(u\beta^2)^t = \chi(\alpha)^t.$$

- If α corresponds to an ideal of order 2^t, let $\beta = \alpha^{2^{t-1}}$ (of order 2). If the result holds for such elements, then

$$\chi(\alpha^{2^t}) = \chi(\beta^2) = \chi(\beta)^2 = \epsilon(\mathcal{N}(\beta)) = \chi^2(\alpha)^{2^{t-1}} = \chi(\alpha)^{2^t}.$$

- Only need to check at elements of order 2.

Multiplicativity at order 2 elements

Ideals of order two correspond to genus characters. Namely,

- Ideals of the form $\langle p, \sqrt{-d} \rangle$ (for $p \mid d$ odd).
- Also the ideal $\langle 2, 1 + \sqrt{-d} \rangle$ if $d \equiv 1 \pmod 4$.

Let α be the idèle

$$\alpha_v = \begin{cases} \sqrt{-6} & \text{if } v = 3, \\ 1 & \text{otherwise} \end{cases}$$

Then:

$$\chi(\alpha^2) = \chi_3(-6) = \chi_2(1/3)\chi_3(-2),$$

and

$$\chi(\alpha)^2 = \epsilon_3(6) = \epsilon_2(1/3)\epsilon_3(2).$$

the quotient equals $\delta_3(2)\delta_{-1}(3) = 1$ (quadratic reciprocity)

Example $d = 6$ continued

To finish our statement, the equality ${}^{\tau}\chi = \chi \cdot \psi_{-2}$ on class group representatives follows from quadratic reciprocity again.

Theorem

The representation $\rho_{E,p}$ extends to a representation of $\mathrm{Gal}_{\mathbb{Q}}$ with Nebentypus ϵ and level $2^8 \cdot 3$ or $2^9 \cdot 3$.

Sketch of proof.

We need to perform the following computations:

- Compute the conductor of $E_{a,b}$ at primes of bad reduction.
- The odd primes ramifying in $K/\mathbb{Q}$ are of good reduction.
- The bad odd primes $\mathfrak{q}$ dividing $\Delta(E)$ have multiplicative reduction and $p \mid v_{\mathfrak{q}}(\Delta(E))$.
- Compute the reduction at primes dividing 2.

Misssing ingredients

We need a big image result! (for Ribet's lowering the level)

- If there exists a prime $q \mid abc$, $q \nmid 6$ then a reult of Ellenberg implies that the projective residual representation is surjective for all $p > 569$ (can be improved to 11).
- Since $d = 6$, any solution is in the previous situation unless $C = 1$ (the trivial solution $(1, 0, 1)$). In general, another argument is needed.

Then by Serre's conjectures and Ribet's lowering the level result the statement follows.

Issue: the spaces have many eigenforms! Also, the trivial solution corresponds to an elliptic curve (the trivial solutions are usually hard to discard).

Advantage: The trivial solution corresponds to a CM elliptic curve.

Discarding forms

All CM forms can be discarded via Ellenberg's result (the image is not large enough). For the other ones, we use the so called *Mazur's trick* (local-global compatibility).

Let $g \in S_2(\Gamma_0(N), \epsilon)$ be a form we want to discard.

- Let q be a prime not ramifying in $K/\mathbb{Q}$. To each solution (a, b) modulo q attach an elliptic curve $E_{a,b}$.
- If q split in K, compute $C(q, g) = \mathcal{N}(a_{\mathfrak{q}}(E_{a,b}) - \chi(\mathfrak{q}) - a_q(g))$.
- If q is inert in K, compute $C(q, g) = \mathcal{N}(a_q(g)^2 - a_q(E_{a,b})\chi(q) - 2q\epsilon(q))$.

Then $p \mid C(q, g)$. Computing this constant for many primes q and all forms g gives.

Theorem

Let $p > 19$ be a prime number. Then there are no non-trivial solutions of the equation

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

A similar strategy can be used to study the equation

$$x^2 + dy^6 = z^p.$$

Now the $\mathbb{Q}$-curve attached to a solution is isogenous to a quadratic twist by $\sqrt{-3}$ (requires a different Hecke character construction).

Theorem

Let $p > 23$ be a prime number. Then there are no non-trivial solutions of the equation

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

Thank you for coming