On p-isogenies for elliptic curves with multiplicative reduction

George Țurcaș (partially joint work with Filip Najman)

Modular curves and Galois representations
Zagreb September 19, 2023

Motivation

Theorem (Mazur, 1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

- It can be rephrased in terms of Galois representations;

Motivation

Theorem (Mazur, 1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

- It can be rephrased in terms of Galois representations;
- It can be rephrased in terms of modular curves;

Motivation

Theorem (Mazur, 1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

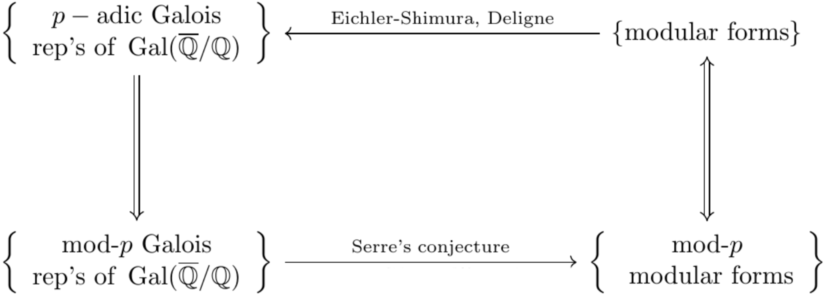
$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

- It can be rephrased in terms of Galois representations;
- It can be rephrased in terms of modular curves;
- It plays an important role in the modular method.

The modular method for Diophantine equations

$$a^p + b^p + c^p = 0 \to E_{p,a,b,c} : Y^2 = X(X - a^p)(X + b^p)$$

Figure: Source: M. H. Şengün's PhD Thesis



Arrows on the RHS go both ways because, in the classical case, for $p > 3$ mod p modular forms are just reductions of modular forms.

Some notation

- G_K - the absolute Galois group of K;
- p - a rational prime;
- E an elliptic curve defined over K;
- $\overline{\rho}_{E,p} : G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ is the representation arising from the action of G_K on the p-torsion points in $E(\overline{K})$;
- E has a p-isogeny defined over K if and only if $\overline{\rho}_{E,p}$ is **reducible**.

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix},$$

where $\lambda, \lambda' : G_K \to \mathbb{F}_p^\times$ are characters such that $\lambda\lambda' = \chi_p$ is the mod p cyclotomic character.

Theorem (Mazur, 1978)

For any elliptic curve E defined over $\mathbb{Q}$ and any prime $p > 163$, the representation $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is irreducible.

Question

For a general number field K, is there a constant B_K such that for any elliptic curve E/K and any prime $p > B_K$, the representation $\overline{\rho}_{E,p}$ is irreducible?

Theorem (Mazur, 1978)

For any elliptic curve E defined over $\mathbb{Q}$ and any prime $p > 163$, the representation $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is irreducible.

Question

For a general number field K, is there a constant B_K such that for any elliptic curve E/K and any prime $p > B_K$, the representation $\overline{\rho}_{E,p}$ is irreducible?

Short answer: No, due to the possible presence of elliptic curves with CM whose rings of endomorphisms are contained in K.

Theorem (Serre, 1972)

For general K, given E/K without CM, there exists a constant $B_{E,K}$ such that for any prime $p > B_{E,K}$, the representation $\overline{\rho}_{E,p}$ is **surjective**.

Question (aligned to Serre's uniformity question)

For a general number field K, is there a constant B_K such that for any elliptic curve E/K without CM and any prime $p > B_K$, the representation $\overline{\rho}_{E,p}$ is irreducible?

Theorem (Serre, 1972)

For general K, given E/K without CM, there exists a constant $B_{E,K}$ such that for any prime $p > B_{E,K}$, the representation $\overline{\rho}_{E,p}$ is **surjective**.

Question (aligned to Serre's uniformity question)

For a general number field K, is there a constant B_K such that for any elliptic curve E/K without CM and any prime $p > B_K$, the representation $\overline{\rho}_{E,p}$ is irreducible?

Fact: If E has CM, its $j(E)$ is an algebraic integer. In particular For any prime ideal $\mathfrak{q}$, we have $v_{\mathfrak{q}}(j(E)) \geq 0$.

Theorem (Serre, 1972)

For general K, given E/K without CM, there exists a constant $B_{E,K}$ such that for any prime $p > B_{E,K}$, the representation $\overline{\rho}_{E,p}$ is **surjective**.

Question (aligned to Serre's uniformity question)

For a general number field K, is there a constant B_K such that for any elliptic curve E/K without CM and any prime $p > B_K$, the representation $\overline{\rho}_{E,p}$ is irreducible?

Fact: If E has CM, its $j(E)$ is an algebraic integer. In particular For any prime ideal $\mathfrak{q}$, we have $v_{\mathfrak{q}}(j(E)) \geq 0$.

Idea (already appears in the work of Mazur for $K = \mathbb{Q}$)

If $\overline{\rho}_{E,p}$ is reducible for some large p, there should be a restricted set of primes that divide the denominator of $j(E)$.

$$a^p + b^p + c^p = 0 \rightarrow E : Y^2 = X(X - a^p)(X + b^p)$$

$$j(E) = \frac{2^4(b^{2p} - a^p c^p)}{(abc)^{2p}}$$

The elliptic curve has (potentially) multiplicative reduction at $\mathfrak{q}$ if and only if $\mathrm{ord}_{\mathfrak{q}}(j(E)) < 0$.

Theorem (Ţ., '20)

Let K be a quadratic imaginary number field of class number one. Assume Serre's modularity conjecture holds over K. Then, for any prime $p \geq 19$, the equation $a^p + b^p + c^p = 0$ does not have solutions in coprime $a, b, c \in \mathcal{O}_K \setminus \{0\}$ such that $2 \mid \mathrm{Norm}_{K/\mathbb{Q}}(abc)$.

Suppose K is a quadratic field

Theorem (Najman-Ţ. '21)

Let K be a quadratic field and let $q > 5$ be a rational prime that is unramified in K. Suppose an elliptic curve E/K has potentially multiplicative reduction at all primes $\mathfrak{q}$ of K above q and posses a p-isogeny defined over K. Then $p \leq 71$ if either:

1. *q is inert in K.*
2. *q splits in K as $\mathfrak{q}_1\mathfrak{q}_2$. Given $x \in X_0(p)(K)$ the quadratic point arrising from E and its Galois conjugate $x^\tau \in X_0(p)(K)$, both x and x^τ reduce to the same cusps when taken modulo $\mathfrak{q}_1$ and $\mathfrak{q}_2$, respectively.*

More general versions are presented in the work of Banwait and Derickx arXiv:2203.06009 and Michaud-Jacobs arXiv:2203.03533.

The proof makes use of the modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$. By adding the cusps $\infty, 0$ we make it into a compact Riemann surface $X_0(p)$.
- $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$ and has good reduction at primes $q \neq p$.

The proof makes use of the modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p) \backslash \mathbb{H}$. By adding the cusps $\infty, 0$ we make it into a compact Riemann surface $X_0(p)$.
- $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$ and has good reduction at primes $q \neq p$.
- The cusps are rational points: $\infty, 0 \in X_0(p)(\mathbb{Q})$.
- The j-map: $j : X_0(p) \to \mathbb{P}^1$. The poles of j are the two cusps.
- The Atkin-Lehner involution $w_p : X_0(p) \to X_0(p)$ swaps the cusps.
- $X_0(p)$ parametrises elliptic curves with p-isogenies: if E/K is an elliptic curve with a rational p-isogeny, φ, then

$$(E, \varphi) \to [(E, \varphi)] = x \in X_0(p)(K).$$

In this case, $j(x) = j(E)$.

- Let τ be the non-trivial element in $\mathrm{Gal}(K/\mathbb{Q})$.
- Let $x \in X_0(p)(K)$ be the point corresponding to (E, φ), and let $y = (x, x^\tau) \in X_0(p)^{(2)}(\mathbb{Q})$ be the point on the symmetric 2-th power of $X_0(p)$.

Fact

The point $y \in X_0(p)^{(2)}(\mathbb{Q})$ reduces to $(\infty, \infty)_{\mathbb{F}_q}$ after possibly applying an appropriate Atkin-Lehner involution.

Theorem (Mazur)

There is an optimal quotient $J_0^e(p)(\mathbb{Q})$ of the Jacobian whose rank is zero.

- Define $f_2 : X_0^{(2)}(p) \to J_0^e$ to be the composition of the natural map

$$X_0^{(2)}(p) \to J_0(p)$$

$$(\alpha_1, \alpha_2) \mapsto [\alpha_1 + \alpha_2 - 2\infty]$$

and the quotient map $J_0(p) \to J_0^e(p)$.

Key result

Theorem (Kamienny '92)

For $p > 71$, the map $f_2 : X_0(p)^{(2)} \to J_0^e(p)$ is a formal immersion at $(\infty, \infty)_{\mathbb{F}_q}$.

Consequence: If $f_2(y) - f_2((\infty, \infty)) = 0$, then $y = (\infty, \infty)$.

Key result

Theorem (Kamienny '92)

For $p > 71$, the map $f_2 : X_0(p)^{(2)} \to J_0^e(p)$ is a formal immersion at $(\infty, \infty)_{\mathbb{F}_q}$.

Consequence: If $f_2(y) - f_2((\infty, \infty)) = 0$, then $y = (\infty, \infty)$.

But we only know that $\mathrm{red}_q(f_2(y) - f_2((\infty, \infty))) = \tilde{0} \in J_0^e(p)(\mathbb{F}_q)$.

Here we use that $J_0^e(p)$ has rank 0 over $\mathbb{Q}$ and we use injectivity of torsion to deduce that $f_2(y) - f_2((\infty, \infty)) = 0$.

This implies that $y = (\infty, \infty)$ and contradicts the hypothesis that $x \in X_0(p)(K)$ is non-cuspidal.

Generalizations?

Fact

It was essential to assume that $y = (x, x^\tau) \in X_0(p)(\mathbb{Q})^{(2)}$ *reduces to* $(\infty, \infty)_{\mathbb{F}_q}$ *or to* $(\infty, 0)_{\mathbb{F}_q}$.

- However, this is not always the case. If $q = \mathfrak{q} \cdot \mathfrak{q}^\tau$ splits on K, it might well be the case that x reduces modulo $\mathfrak{q}$ to ∞ and x^τ reduces modulo $\mathfrak{q}^\tau$ to 0. There are plenty of such examples.

Some computational examples

```
Elliptic Curve defined by y^2 + x*y = x^3 +
1/1009789903698600299263047647787299646237216570869051443141875980097420140955 7\
1258244*(-828490183576148659183582102909802497293807934663115708174500955453731\
035860430000*d + 146965357503818434265352015127862261497978547427701367722853 45\
    2818124364682312 3453)*x + 1/363524365331496107734697153203427872645397965 51\
2858519531075352835071250744056529678 4*(-828490183576148659183582102909802497 29\
3807934663115708174500955453731035860430000*d +
    1469653575038184342653520151278622614979785474277013677228534528181243646 82\
    3123453) over K
[> K;
Number Field with defining polynomial x^2 + 1887405189403/262589629225 over the
Rational Field
```

- This elliptic curve has a $p = 79$-isogeny and also multiplicative reduction modulo both primes of K lying above 11.

Some computational examples

```
Elliptic Curve defined by y^2 + x*y = x^3 +
1/1009789903698600299263047647787299646237216570869051443141875980097420140955 7\
1258244*(-8284901835761486591835821029098024972938079346631157081745009554537 31\
035860430000*d + 14696535750381843426535201512786226149797854742770136772285345\
    2818124364682312345 3)*x + 1/3635243653314961077346971532034278726453979655 1\
2858519531075352835071250744056529678 4*(-828490183576148659183582102909802497 29\
380793466311570817450095545373103586043 0000*d +
    1469653575038184342653520151278622614979785474277013677228534528181243646 82\
    3123453) over K
> K;
Number Field with defining polynomial x^2 + 1887405189403/262589629225 over the
Rational Field
```

- This elliptic curve has a $p = 79$-isogeny and also multiplicative reduction modulo both primes of K lying above 11.
- Computation uses code accompanying "Computing points on bielliptic modular curves over fixed quadratic fields" by Philippe Michaud-Jacobs and "Computing quadratic points on modular curves $X_0(N)$" by Adzaga, Keller, Michaud-Jacobs, Najman and Ozman.

Similar examples can be found for $p = 37, 43, 53, 61, 83, 89, 101$ and 131, completing the list of primes p for which $X_0(p)$ is bielliptic (Bars '99).

$X_0(p)^{(2)}$

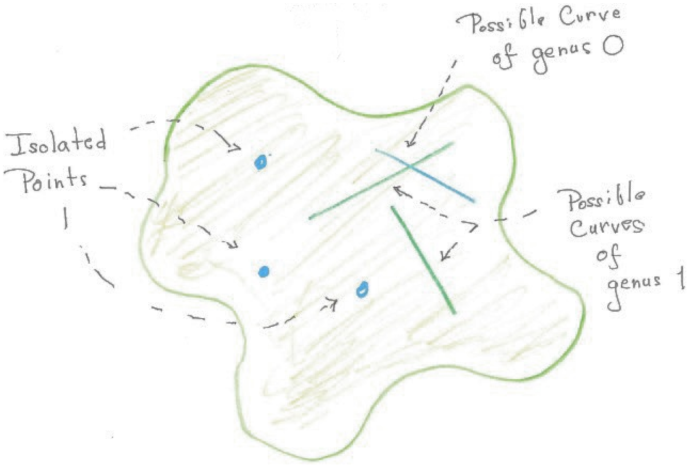


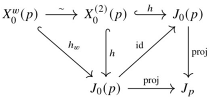
Figure: Diagram taken from "Ogg's Torsion conjecture: Fifty years later" by Balakrishnan and Mazur

Here come $\mathbb{Q}$-curves

Theorem (Michaud-Jacobs '22)

For $q \neq p$, if $(x, x^\tau) \in X_0^{(2)}(p)(\mathbb{Q})$ reduces to $(\infty, 0)_{\mathbb{F}_q}$ then $x^\tau = w_p(x)$.

We point out the existence of the following commutative diagram over Spec $\mathbb{Z}[1/p]$.



(4)

DOES NOT HELP !

The top left isomorphism above is given by $(y, z) \mapsto (w_p(z), y)$ and $h_w : X_0^w(p) \to J_0(p)$ is defined as

$$h_w(y, z) = [y + w_p(z) - 2\infty].$$

Note that the injectivity of h_w follows from that of h and the commutativity of the diagram.

Note that the isomorphism $X_0^w(p) \to X_0^{(2)}(p)$ sending $(y, z) \mapsto (w_p(z), y)$ maps $(\infty, 0) \in X_0^w(p)$ to $(\infty, \infty) \in X_0^{(2)}(p)$. Now, if we similarly denote by $f_w : X_0^w(p) \to J_p$ the composition between h_w and the natural projection proj on the diagram (4), the proof of the following result is a consequence of the fact that $f = h \circ \text{proj}$ is a formal immersion at $(\infty, \infty)_{\mathbb{F}_q}$ as discussed in the proof of Theorem 2.

Proposition 3 *For $q > 5$ and $p > 71$, the map*

$$f_w : X_0^w(p)_{/\mathrm{Spec}\,\mathbb{Z}[1/p]} \to J_{p/\mathrm{Spec}\,\mathbb{Z}[1/p]}$$

is a formal immersion at $(\infty, 0)_{\mathbb{F}_q}$.

Strategy for Diophantine equations

- If not a CM-point, x corresponds therefore to a quadratic $\mathbb{Q}$-curve, i.e. to a rational point on $X_0^+(p) = X_0(p)/\langle w_p \rangle$. A result of González '01 implies that $j(x) = \frac{\alpha}{M^p}$, where α is an algebraic integer which satisfies

$$\left(\mathrm{Tr}_{K/\mathbf{Q}}(\alpha), M\right) = 1, \quad \left(N_{K/\mathbf{Q}}(\alpha), M^p\right) = M^{p-1}.$$

- Controlling the primes of multiplicative reduction and Diophantine equations

$$E := E_{a,b,c,p} : Y^2 = X(X - a^p)(X + b^p).$$

- The j-invariant of this elliptic curve has the formula

$$j(E) = \frac{2^4(b^{2p} - a^p c^p)}{(abc)^{2p}}.$$

Continuation. K is fixed imaginary quadratic

- Suppose that $a, b, c \in \mathcal{O}_K$ are coprime and satisfy (a variant of the Asymptotic) Fermat equation $a^p + b^p + c^p = 0$, for some prime exponent p. One can construct the Frey elliptic curve
- With such results one can prove that if p is large and $\overline{\rho}_{E,p}$ is reducible, then $j(E)$ is integral outside a finite set S.
- The Fermat equation can be written as $(-a/c)^p + (-b/c)^p = 1$. Observe that $(-a/c)^p$ and $(-b/c)^p$ are solutions to the S-unit equation

$$x + y = 1, \text{ where } x, y \in \mathcal{O}_{K,S}^\times.$$

Thank you very much for your attention!