Cyclic Isogenies Under Isogenous Elliptic Curves

Tyler Genao

August 4, 2021

In this talk...

Following results of J. Cremona and F. Najman [1], we'll see that isogenous non-CM elliptic curves defined over F share the same primes $\ell \in \mathbb{Z}^+$ for which they have F-rational ℓ-isogenies.

Notations

- $F/\mathbb{Q}$ is an algebraic extension, and $\overline{F}$ is its algebraic closure.
- $G_F := \mathrm{Gal}(\overline{F}/F)$ is the **absolute Galois group** of F.
- $E_{/F}$ denotes an elliptic curve defined over F.
- $O \in E$ is "the point at infinity."

Galois representations of elliptic curves

- Given $E_{/F}$, the Galois group G_F naturally acts on E: $\forall \sigma \in G_F$,

$$\sigma \cdot (x, y) := (\sigma x, \sigma y).$$

"$G_F \circlearrowleft E$."

- For each $N \in \mathbb{Z}^+$, the **N-torsion subgroup**

$$E[N] := \{P \in E(\overline{F}) : NP = O\}.$$

- For each $N \in \mathbb{Z}^+$, this action induces $G_F \circlearrowleft E[N]$.
- Since $E[N]$ is a rank two $\mathbb{Z}/N\mathbb{Z}$-module, we have the **mod$-N$ Galois representation**

$$\rho_{E,N} : G_F \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Shapes of representations

- A representation $\rho_{E,N}(G_F)$ can be identified with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, up to conjugacy.
- For example, fixing a basis $\{P, Q\}$ of $E[N]$, for $\sigma \in G_F$, writing

$$\sigma(P) = aP + cQ$$

and

$$\sigma(Q) = bP + dQ$$

one has $\rho_{E,N}(\sigma) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \rho_{E,N}(G_F)$.

- First column describes action on P, second column describes action on Q.

Rational points

We'll always work with a basis $\{P, Q\}$ in mind.

- One has

$$\rho_{E,N}(G_F) \subseteq \left\{ \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}$$

  iff $\forall \sigma \in G_F$

$$\sigma(P) = P.$$

  So this shape implies P **is** F**-rational.**

Rational cyclic subgroups

- More generally, if

$$\rho_{E,N}(G_F) \subseteq \left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}$$

  then for all $\sigma \in G_F$

$$\sigma(P) = a_\sigma P$$

  for some $a_\sigma \in \mathbb{Z}/N\mathbb{Z}$.
- Thus, the subgroup $\langle P \rangle$ is *stable* under the action of G_F.
- Call $\langle P \rangle$ an F-**rational cyclic** N-**isogeny.**
- An F-rational cyclic N-subgroup $C \subseteq E(\overline{F})$ induces an F-rational N-isogeny

$$\phi : E \to E/C$$

  with cyclic kernel $\ker \phi = C$, and vice-versa.

F-rational isogenies

- How do cyclic isogenies transfer between isogenous elliptic curves?
- Say an isogeny $\phi : E \to E'$ is F-**rational** if E and E' are defined over F, and so is ϕ.

Main result

Theorem.
Let E and E' be non-CM elliptic curves defined over F which are isogenous. Then for all primes $\ell \in \mathbb{Z}^+$, one has that E has an F-rational ℓ-isogeny iff E' has an F-rational ℓ-isogeny.

So the existence of rational isogenies of prime degree ℓ is **invariant** under isogeny for non-CM elliptic curves.

Outline of the proof

Lemma 1.

For E and E' non-CM elliptic curves which are isogenous, then for each $d \in \mathbb{Z}^+$ there is at most one degree d isogeny $\phi : E \to E'$, up to sign.

Proof:

1. If $\phi, \varphi : E \to E'$ are both of degree d then $\varphi^\vee \circ \phi \in \mathrm{End}(E) = \mathbb{Z}$.
2. Writing $\varphi^\vee \circ \phi = [n]$, we get $[d] \circ \phi = [n] \circ \varphi$ by composing with φ.
3. Comparing degrees shows that $n = \pm d$.
4. Canceling $[d]$ gives $\phi = \pm\varphi$.

Lemma 2.

Any isogeny $\phi : E \to E'$ factors as $\phi = [n] \circ \phi_0$ where $\phi_0 : E \to E'$ is cyclic. Furthermore, any cyclic F-isogeny $\phi : E \to E'$ of degree ab factors as

$$E \xrightarrow{\phi_a} E'' \xrightarrow{\phi_b} E'$$

where ϕ_a, ϕ_b are F-rational and cyclic of degrees a and b, resp.

Proof:

1. Part 1: take $n \geq 1$ to be the largest integer for which $E[n] \subseteq \ker \phi$.
2. Part 2: writing $\ker \phi = \langle P \rangle$, we have

$$E \xrightarrow{a} E/\langle bP \rangle \xrightarrow{b} E' = E/\langle P \rangle.$$

Lemma 3.

For non-CM E and E' defined over F, if E and E' are isogenous, then there exists a quadratic twist E'_χ for which E and E'_χ are F-isogenous.

Proof:

1. Given an isogeny
$$\phi : E \to E'$$
applying $\sigma \in G_F$ to all sides gives another isogeny
$$\phi^\sigma : E \to E'.$$
2. Argue as in Lemma 1 and get that
$$\phi^\sigma = \chi(\sigma) \cdot \phi$$
where $\chi(\sigma) \in \{\pm 1\}$.
3. The map
$$\chi : G_F \to \{\pm 1\}$$
is a quadratic character, and the twist E'_χ has that the isogeny $E \to E'_\chi$ is F-rational.

Proof, I

Theorem.
If E and E' are non-CM elliptic curves defined over F which are isogenous, then for all prime $\ell \in \mathbb{Z}^+$, E has an F-rational ℓ-isogeny iff E' does.

Proof:

1. Twisting $E'_{/F}$ by a quadratic character gives the Gal. rep.

$$\rho_{E'_\chi,N} = \chi \cdot \rho_{E',N}.$$

$\chi(G_F) = \{\pm 1\}$, so $\rho_{E',N}(G_F)$ is contained in

$$B_0(N) := \left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}$$

iff $\rho_{E'_\chi,N}(G_F)$ is.
Thus, $E'[N]$ has an F-rational cyclic N-isogeny iff $E'_\chi[N]$ has an F-rational ℓ-isogeny.

2. So by Lemma 3, replace E' with a quadratic twist, and assume $\phi : E \to E'$ is F-rational.

Proof, II

So far: we have an F-rational isogeny $\phi : E \to E'$, say of degree $d \geq 1$.

1. We may assume ϕ is cyclic.
2. Factor $d = p_1 \cdots p_r$ as a product of (not necessarily distinct!) primes.
3. Lemma 2 implies a chain of F-isogenies

$$E \xrightarrow{p_1} E_1 \xrightarrow{p_2} \ldots \xrightarrow{p_{r-1}} E_r \xrightarrow{p_r} E'.$$

So if the result is true for F-isogenies of prime degree, then it's true for cyclic F-isogenies.

Proof, III

So far: we have an F-rational ℓ-isogeny $\phi : E \to E'$.

1. For all $p \neq \ell$ one has

$$\phi : E[p] \cong_{G_F} E'[p].$$

   Reason: $\ker \phi|_{E[p]} = \ker \phi \cap E[p] \subseteq E[\ell] \cap E[p] = \{O\}$.
2. When $p = \ell$: already $\ker \phi$ is an F-rational ℓ-isogeny of E. Similarly, $\ker \phi^\vee$ is an F-rational ℓ-isogeny of E'.

This proves the theorem.

Thank you!

[1] John Cremona and Filip Najman, $\mathbb{Q}$-*curves over odd degree number fields,* arXiv 2004.10054.