A local-global principle for rational isogenies of prime degree

Andrew V. Sutherland

Massachusetts Institute of Technology

July 13, 2010

http://arxiv.org/abs/1006.1782

Mazur's Theorem

Let $E/\mathbb{Q}$ be an elliptic curve and let ℓ be a prime.

E can have a rational point of order ℓ only when

$$\ell \in \{2, 3, 5, 7\}.$$

E can admit a rational isogeny of degree ℓ only when

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

All permitted cases occur.

The local-global question for ℓ-torsion

Suppose E has a rational point of order ℓ.
Then E has a point of order ℓ locally everywhere.

Suppose E has a point of order ℓ locally everywhere.
Must E have a rational point of order ℓ?

No, but E is isogenous to such a curve (Katz 1981).

The local-global question for ℓ-isogenies

Suppose E admits a rational ℓ-isogeny.
Then E admits an ℓ-isogeny locally everywhere.

Suppose E admits an ℓ-isogeny locally everywhere.
Must E admit a rational ℓ-isogeny?

No, the curve defined by

$$y^2 + xy = x^3 - x^2 - 107x - 379,$$

with $j(E) = 2268945/128$, is a counterexample for $\ell = 7$.

But up to isomorphism, this is the *only* counterexample.

Main result

Theorem

Let E be an elliptic curve over $\mathbb{Q}$, let ℓ be a prime, and assume that $(j(E), \ell) \neq (2268945/128, 7)$.

If E admits an ℓ-isogeny locally at a set of primes with density 1, then E admits an ℓ-isogeny over $\mathbb{Q}$.

Strategy of the proof

1. Reduce the problem to group theory.

The mod-ℓ Galois representation

Let S contain ℓ and the primes where E has bad reduction.
Let $\bar{\mathbb{Q}}_S$ be the maximal algebraic extension of $\mathbb{Q}$ unramified outside of S.

The action of $\mathrm{Gal}(\bar{\mathbb{Q}}_S/\mathbb{Q})$ on $E[\ell]$ yields a representation

$$\rho\colon\ \mathrm{Gal}(\bar{\mathbb{Q}}_S/\mathbb{Q}) \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell),$$

which maps φ_p to a conjugacy class $\varphi_{p,\ell}$ of $\mathrm{GL}_2(\mathbb{F}_\ell)$ with

$$\det(\varphi_{p,\ell}) \equiv p \bmod \ell, \qquad \mathrm{tr}(\varphi_{p,\ell}) \equiv p + 1 - |E(\mathbb{F}_p)| \bmod \ell.$$

Every $\varphi_{p,\ell}$ arises for a set of p with positive density.

Invariant subspaces of $E[\ell]$

Let G be the image of ρ in $\mathrm{GL}_2(\mathbb{F}_\ell)$.
Let Ω be the set of one dimensional subspaces of $\mathbb{F}_\ell^2$.
G acts on Ω via the Galois action on $E[\ell]$.

If E admits a rational ℓ-isogeny,
then G fixes some element of Ω.

If E admits an ℓ-isogeny locally everywhere,
then every element of G fixes an element of Ω.

A group-theoretic question

We are interested in subgroups $G \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ such that

(i) the determinant map from G to $\mathbb{F}_\ell^*$ is surjective;

(ii) every element of G fixes some element of Ω;

(iii) no element of Ω is fixed by every element of G.

Do any such G actually exist?

If $\ell < 7$ or if $\ell \equiv 1 \bmod 4$, the answer is no.

Otherwise, the answer is yes.

Subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$

A Cartan subgroup C is a semisimple maximal abelian subgroup, either split ($C \cong \mathbb{F}_\ell^* \times \mathbb{F}_\ell^*$) or nonsplit ($C \cong \mathbb{F}_{\ell^2}^*$).

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ with image H in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. If $|G|$ is prime to ℓ then exactly one of the following holds:

(a) H is cyclic and G is contained in a Cartan subgroup.

(b) H is dihedral and G is contained in the normalizer of a Cartan subgroup but not in a Cartan subgroup.

(c) H is isomorphic to A_4, S_4, or A_5.

(this is a standard result, see Serre or Lang)

The main lemma

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ satisfying (i), (ii) and (iii). Then the following also hold:

(iv) G is properly contained in the normalizer of a split Cartan subgroup, but not in the Cartan subgroup;

(v) $\ell \geq 7$ and $\ell \equiv 3 \bmod 4$;

(vi) Ω contains a G-orbit of size 2.

The proof is essentially combinatorial.

Strategy of the proof

1. Reduce the problem to group theory.
2. Apply a result of Parent (and some CM theory).

The modular curve $X_{\text{split}}(\ell)$

$X_{\text{split}}(\ell)$ parametrizes elliptic curves whose mod-ℓ Galois image lies in the normalizer of a split Cartan subgroup.

Theorem (Parent 2005)

Assume $\ell \geq 11$, $\ell \neq 13$ and $\ell \notin \mathcal{A}$. The only non-cuspidal rational points of $X_{\text{split}}(\ell)(\mathbb{Q})$ are CM points.

The excluded set of primes $\mathcal{A}$ is infinite, but happily it only contains primes congruent to 1 mod 4.

Ruling out complex multiplication (CM)

If $E/\mathbb{Q}$ has CM by $\mathcal{O}$ then $h(\mathcal{O}) = 1$.

If the mod-ℓ Galois image of E satisfies (i), (ii), and (iii), then the main lemma implies that E is ℓ-isogenous to two curves defined over a quadratic extension of $\mathbb{Q}$.

These curves must have CM by $\mathcal{O}'$ with $h(\mathcal{O}') = 2$.

CM theory requires $[\mathcal{O} : \mathcal{O}'] = \ell$.

Since $h(\mathcal{O}')/h(\mathcal{O}) = 2$, we must have $\ell \leq 7$.

Strategy of the proof

1. Reduce the problem to group theory.
2. Apply a result of Parent (and some CM theory).
3. Handle the case $\ell = 7$.

The case $\ell = 7$

We are interested in elliptic curves whose Galois image in $\mathrm{PGL}_2(\mathbb{F}_7)$ is dihedral of order 6.

The modular curves that parametrize elliptic curves with a given level 7 structure have been classified by Elkies.

The corresponding modular curve C is a quotient of $X(7)$ that corresponds to a twist of $X_0(49)$.

The curve C has exactly 2 rational points over $\mathbb{Q}$.
They both correspond to the j-invariant 2268945/128 of

$$y^2 + xy = x^3 - x^2 - 107x - 379.$$

A local-global principle for rational isogenies of prime degree

Andrew V. Sutherland

Massachusetts Institute of Technology

July 13, 2010

http://arxiv.org/abs/1006.1782