Constructing families of 3-Selmer companions

Harry Spencer

4 March 2025

Selmer companion curves

Definition (Mazur–Rubin)

Two elliptic curves E_1, E_2 over a number field K are n-*Selmer companions* if for all quadratic characters χ of K:

$$\mathrm{Sel}_n(E_1^{\chi}) \cong \mathrm{Sel}_n(E_2^{\chi}).$$

Selmer companion curves

Definition (Mazur–Rubin)

Two elliptic curves E_1, E_2 over a number field K are n-*Selmer companions* if for all quadratic characters χ of K:

$$\mathrm{Sel}_n(E_1^\chi) \cong \mathrm{Sel}_n(E_2^\chi).$$

Mazur and Rubin give a set of sufficient conditions for a pair of elliptic curves to be p-Selmer companions.

Tate parameterisation

Tate parameterisation

Let E be an elliptic curve over a local field of mixed characteristic with potentially multiplicative reduction.

Tate parameterisation

Let E be an elliptic curve over a local field of mixed characteristic with potentially multiplicative reduction.

There exists $q \in K^\times$ with positive valuation and an isomorphism

$$\tau_{E/K} : \bar{K}^\times / q^{\mathbb{Z}} \to E(\bar{K}).$$

Tate parameterisation

Let E be an elliptic curve over a local field of mixed characteristic with potentially multiplicative reduction.

There exists $q \in K^\times$ with positive valuation and an isomorphism

$$\tau_{E/K} : \bar{K}^\times / q^{\mathbb{Z}} \to E(\bar{K}).$$

Definition

The canonical p-torsion subgroup is $\mathcal{C}_{E/K}[p] = \tau_{E/K}(\mu_p)$.

Tate parameterisation

Let E be an elliptic curve over a local field of mixed characteristic with potentially multiplicative reduction.

There exists $q \in K^\times$ with positive valuation and an isomorphism

$$\tau_{E/K} : \bar{K}^\times / q^{\mathbb{Z}} \to E(\bar{K}).$$

Definition

The canonical p-torsion subgroup is $\mathcal{C}_{E/K}[p] = \tau_{E/K}(\mu_p)$.

These are the p-torsion points of good reduction.

Sufficient conditions

Theorem (Mazur–Rubin)

Let E_1 and E_2 be elliptic curves over a number field k, and write S_i for the set of primes of potentially multiplicative reduction of E_i. Suppose $p > 3$ and:

Sufficient conditions

Theorem (Mazur–Rubin)

Let E_1 and E_2 be elliptic curves over a number field k, and write S_i for the set of primes of potentially multiplicative reduction of E_i. Suppose $p > 3$ and:

- there is a G_k-isomorphism $\alpha : E_1[p] \xrightarrow{\sim} E_2[p]$;

Sufficient conditions

Theorem (Mazur–Rubin)

Let E_1 and E_2 be elliptic curves over a number field k, and write S_i for the set of primes of potentially multiplicative reduction of E_i. Suppose $p > 3$ and:

- there is a G_k-isomorphism $\alpha : E_1[p] \xrightarrow{\sim} E_2[p]$;
- $S_1 = S_2$;

Sufficient conditions

Theorem (Mazur–Rubin)

Let E_1 and E_2 be elliptic curves over a number field k, and write S_i for the set of primes of potentially multiplicative reduction of E_i. Suppose $p > 3$ and:

- there is a G_k-isomorphism $\alpha : E_1[p] \xrightarrow{\sim} E_2[p]$;
- $S_1 = S_2$;
- for every $\mathfrak{p}$ above p, $\mathfrak{p} \in S_1 = S_2$;

Sufficient conditions

Theorem (Mazur–Rubin)

Let E_1 and E_2 be elliptic curves over a number field k, and write S_i for the set of primes of potentially multiplicative reduction of E_i. Suppose $p > 3$ and:

- there is a G_k-isomorphism $\alpha : E_1[p] \xrightarrow{\sim} E_2[p]$;
- $S_1 = S_2$;
- for every $\mathfrak{p}$ above p, $\mathfrak{p} \in S_1 = S_2$;
- for every $\mathfrak{q} \in S_1 = S_2$, we have $\alpha(\mathcal{C}_{E_1/k_{\mathfrak{q}}}[p]) = \mathcal{C}_{E_2/k_{\mathfrak{q}}}[p]$.

Sufficient conditions

Theorem (Mazur–Rubin)

Let E_1 and E_2 be elliptic curves over a number field k, and write S_i for the set of primes of potentially multiplicative reduction of E_i. Suppose $p > 3$ and:

- there is a G_k-isomorphism $\alpha : E_1[p] \xrightarrow{\sim} E_2[p]$;
- $S_1 = S_2$;
- for every $\mathfrak{p}$ above p, $\mathfrak{p} \in S_1 = S_2$;
- for every $\mathfrak{q} \in S_1 = S_2$, we have $\alpha(\mathcal{C}_{E_1/k_\mathfrak{q}}[p]) = \mathcal{C}_{E_2/k_\mathfrak{q}}[p]$.

Then E_1 and E_2 are p-Selmer companions over every finite extension of k.

Sufficient conditions

Theorem (Mazur–Rubin)

Let E_1 and E_2 be elliptic curves over a number field k, and write S_i for the set of primes of potentially multiplicative reduction of E_i. Suppose $p > 3$ and:

- there is a G_k-isomorphism $\alpha : E_1[p] \xrightarrow{\sim} E_2[p]$;
- $S_1 = S_2$;
- for every $\mathfrak{p}$ above p, $\mathfrak{p} \in S_1 = S_2$;
- for every $\mathfrak{q} \in S_1 = S_2$, we have $\alpha(\mathcal{C}_{E_1/k_\mathfrak{q}}[p]) = \mathcal{C}_{E_2/k_\mathfrak{q}}[p]$.

Then E_1 and E_2 are p-Selmer companions over every finite extension of k.

Example

The curves

$$y^2 = x^3 + x^2 - 4x - 12$$

and

$$y^2 = x^3 - 28561x + 1856465$$

are 5-Selmer companions over every number field.

Sufficient conditions

Theorem (Mazur–Rubin)

Let E_1 and E_2 be elliptic curves over a number field k, and write S_i for the set of primes of potentially multiplicative reduction of E_i. Suppose the following:

- there is a G_k-isomorphism $\alpha : E_1[3] \xrightarrow{\sim} E_2[3]$;
- $S_1 = S_2$;
- for every $\mathfrak{p}$ above 3, $\mathfrak{p} \in S_1 = S_2$;
- for every $\mathfrak{q} \in S_1 = S_2$, we have $\alpha(\mathcal{C}_{E_1/k_{\mathfrak{q}}}[3]) = \mathcal{C}_{E_2/k_{\mathfrak{q}}}[3]$;
- neither E_1 nor E_2 has any prime of additive reduction with Kodaira type one of II, II*, IV, IV*.

Then E_1 and E_2 are 3-Selmer companions over every finite extension of k.

A family of companions

Theorem

For $t \in \mathbb{Z}$, $t \neq 0, 1$, the curves

$$\begin{aligned} E_t: \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t: \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

are non-isogenous 3-Selmer companions over every number field.

A family of companions

Theorem

For $t \in \mathbb{Z}$, $t \neq 0, 1$, the curves

$$\begin{aligned} E_t : \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t : \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

are non-isogenous 3-Selmer companions over every number field.

Proof.

A family of companions

Theorem

For $t \in \mathbb{Z}$, $t \neq 0, 1$, the curves

$$\begin{aligned} E_t : \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t : \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

are non-isogenous 3-Selmer companions over every number field.

Proof.

We check all the conditions of Mazur and Rubin's theorem, then we check for isogenies. □

Conditions:

$$
\begin{aligned}
E_t: \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\
D_t: \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x
\end{aligned}
$$

Conditions:

$$\begin{aligned} E_t : \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t : \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

1. (3-torsion isomorphism)

Conditions:

$$\begin{aligned} E_t: \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t: \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t;

Conditions:

$$\begin{aligned} E_t: \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t: \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t; they intersect precisely at inflection points and hence have isomorphic 3-torsion.

Conditions:

$$\begin{aligned} E_t: \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t: \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t; they intersect precisely at inflection points and hence have isomorphic 3-torsion.
2. $(S_1 = S_2)$

Conditions:

$$
\begin{aligned}
E_t: \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\
D_t: \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x
\end{aligned}
$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t; they intersect precisely at inflection points and hence have isomorphic 3-torsion.
2. $(S_1 = S_2)$

Lemma

1. If E_t has potentially multiplicative reduction at $p > 3$, then so does D_t.
2. If E_t has multiplicative reduction at $p > 3$, then so does D_t. Moreover, in this case, E_t has split multiplicative reduction if and only if D_t does also.

Conditions:

$$
\begin{aligned}
E_t : \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\
D_t : \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x
\end{aligned}
$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t; they intersect precisely at inflection points and hence have isomorphic 3-torsion.
2. $(S_1 = S_2)$

Lemma

1. If E_t has potentially multiplicative reduction at $p > 3$, then so does D_t.
2. If E_t has multiplicative reduction at $p > 3$, then so does D_t. Moreover, in this case, E_t has split multiplicative reduction if and only if D_t does also.

Proof.

Write everything out explicitly. □

Conditions:

$$\begin{aligned} E_t: \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t: \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t; they intersect precisely at inflection points and hence have isomorphic 3-torsion.
2. $(S_1 = S_2)$ From the lemma (mostly).
3. $(3 \in S_1 = S_2)$

Conditions:

$$\begin{aligned} E_t: \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t: \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t; they intersect precisely at inflection points and hence have isomorphic 3-torsion.
2. $(S_1 = S_2)$ From the lemma (mostly).
3. $(3 \in S_1 = S_2)$ We read off that they both have multiplicative reduction at 3.

Conditions:

$$\begin{aligned} E_t: \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t: \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t; they intersect precisely at inflection points and hence have isomorphic 3-torsion.
2. $(S_1 = S_2)$ From the lemma (mostly).
3. $(3 \in S_1 = S_2)$ We read off that they both have multiplicative reduction at 3.
4. (Canonical subgroups)

Conditions:

$$\begin{aligned} E_t: \ y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t: \ y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t; they intersect precisely at inflection points and hence have isomorphic 3-torsion.
2. $(S_1 = S_2)$ From the lemma (mostly).
3. $(3 \in S_1 = S_2)$ We read off that they both have multiplicative reduction at 3.
4. (Canonical subgroups) This also follows from one!

Conditions:

$$
\begin{aligned}
E_t : \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\
D_t : \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x
\end{aligned}
$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t; they intersect precisely at inflection points and hence have isomorphic 3-torsion.
2. ($S_1 = S_2$) From the lemma (mostly).
3. ($3 \in S_1 = S_2$) We read off that they both have multiplicative reduction at 3.
4. (Canonical subgroups) This also follows from one!
5. (Kodaira types)

Conditions:

$$\begin{aligned} E_t: \quad y^2 &= x^3 + x^2 + 3x + 3(8t+1), \\ D_t: \quad y^2 &= x^3 + (25 - 81(8t+1))x^2 - 512x \end{aligned}$$

1. (3-torsion isomorphism) D_t is the Hessian curve associated to E_t; they intersect precisely at inflection points and hence have isomorphic 3-torsion.
2. ($S_1 = S_2$) From the lemma (mostly).
3. ($3 \in S_1 = S_2$) We read off that they both have multiplicative reduction at 3.
4. (Canonical subgroups) This also follows from one!
5. (Kodaira types) It turns out we only have to check at $p = 2$, so apply Tate's algorithm.

Modular polynomials

It remains to check that E_t, D_t are non-isogenous.

Modular polynomials

It remains to check that E_t, D_t are non-isogenous.

Write $Y_0(N)$ for the (non-compact) modular curve defined by the N^{th} classical modular polynomial, Φ_N.

Modular polynomials

It remains to check that E_t, D_t are non-isogenous.

Write $Y_0(N)$ for the (non-compact) modular curve defined by the N^{th} classical modular polynomial, Φ_N.

Theorem (Kenku–Mazur)

$Y_0(N)(\mathbb{Q}) = \emptyset$, unless either $N \leq 19$ or $N \in \{21, 25, 27, 37, 43, 67, 163\}$.

Modular polynomials

It remains to check that E_t, D_t are non-isogenous.

Write $Y_0(N)$ for the (non-compact) modular curve defined by the N^{th} classical modular polynomial, Φ_N.

Theorem (Kenku–Mazur)

$Y_0(N)(\mathbb{Q}) = \emptyset$, unless either $N \leq 19$ or $N \in \{21, 25, 27, 37, 43, 67, 163\}$.

Recall that there is a degree N cyclic isogeny between two elliptic curves E and D over $\bar{\mathbb{Q}}$ if and only if $\Phi_N(j(E), j(D)) = 0$ or, equivalently, $(j(E), j(D)) \in Y_0(N)(\bar{\mathbb{Q}})$.

Proposition

E_t, D_t are non-isogenous for $t \neq 0, 1$.

Proposition

E_t, D_t are non-isogenous for $t \neq 0, 1$.

Proof.

Δ_{E_t} and Δ_{D_t} differ by a non-square independent of t.

Proposition

E_t, D_t are non-isogenous for $t \neq 0, 1$.

Proof.

Δ_{E_t} and Δ_{D_t} differ by a non-square independent of t. Therefore we only have to check for isogenies of even degrees appearing in the previous theorem.

Proposition

E_t, D_t are non-isogenous for $t \neq 0, 1$.

Proof.

Δ_{E_t} and Δ_{D_t} differ by a non-square independent of t. Therefore we only have to check for isogenies of even degrees appearing in the previous theorem.

The finitely many polynomials to check are stored in Magma, except Φ_{18}

Proposition

E_t, D_t are non-isogenous for $t \neq 0, 1$.

Proof.

Δ_{E_t} and Δ_{D_t} differ by a non-square independent of t. Therefore we only have to check for isogenies of even degrees appearing in the previous theorem.

The finitely many polynomials to check are stored in Magma, except Φ_{18} which is on Drew Sutherland's website.

Proposition

E_t, D_t are non-isogenous for $t \neq 0, 1$.

Proof.

Δ_{E_t} and Δ_{D_t} differ by a non-square independent of t. Therefore we only have to check for isogenies of even degrees appearing in the previous theorem.

The finitely many polynomials to check are stored in Magma, except Φ_{18} which is on Drew Sutherland's website.

For each N, we can solve for the rational zeroes of the numberator of $\Phi_N(j(E_t), j(D_t))$. □