Local points on twists of $X(p)$

joint with Nuno Freitas

Diana Mocanu

Max Planck Institute for Mathematics, Bonn

2 July 2026

Motivation

Motivation

Question (Mazur, 1978)

Does there exist non-isogenous elliptic curves $E, E'/\mathbb{Q}$ and $N \geq 7$ such that the Galois-modules $E[N]$ and $E'[N]$ are isomorphic?

- $E[N]$ and $E'[N]$ are both isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$ and have a natural bilinear alternating pairing into the N-th roots of unity μ_N (called the Weil pairing).
- Mazur's refinement: isomorphism $\phi : E[N] \to E'[N]$ respecting the Weil pairing (called a symplectic isomorphism).

Motivation

Question (Mazur, 1978)

Does there exist non-isogenous elliptic curves $E, E'/\mathbb{Q}$ and $N \geq 7$ such that the Galois-modules $E[N]$ and $E'[N]$ are isomorphic?

- $E[N]$ and $E'[N]$ are both isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$ and have a natural bilinear alternating pairing into the N-th roots of unity μ_N (called the Weil pairing).
- Mazur's refinement: isomorphism $\phi : E[N] \to E'[N]$ respecting the Weil pairing (called a symplectic isomorphism).
- Kraus–Oesterlé (1992) found non-isogenous

$$E : \quad y^2 = x^3 + 7x^2 + 28, \qquad E' : \quad y^2 = x^3 + x^2 - x + 3$$

with a symplectic isomorphism $\phi : E[7] \to E'[7]$.

Motivation

- For a fixed elliptic curve E, the pairs (E', ϕ) with $\phi : E[N] \to E'[N]$ a symplectic isomorphism are in bijection with (non-cuspidal) rational points of a modular curve denoted by $X_E(N)$.
- Halberstadt–Kraus (2003) showed that if $E : y^2 = x^3 + ax + b$, then a model of $X_E(7)$ is given by

$$ax^4 + 7bx^3 + 3(y^2 - a^2)x^2 - b(6y + 5a)x + (2y^3 + 3ay^2 + 2a^2y - 4b^2) = 0.$$

Motivation

- For a fixed elliptic curve E, the pairs (E', ϕ) with $\phi : E[N] \to E'[N]$ a symplectic isomorphism are in bijection with (non-cuspidal) rational points of a modular curve denoted by $X_E(N)$.
- Halberstadt–Kraus (2003) showed that if $E : y^2 = x^3 + ax + b$, then a model of $X_E(7)$ is given by

$$ax^4 + 7bx^3 + 3(y^2 - a^2)x^2 - b(6y + 5a)x + (2y^3 + 3ay^2 + 2a^2y - 4b^2) = 0.$$

- Moreover, they show that $X_{E_u}(7)$ has at least 6 non-cuspidal rational points for infinitely many $u \in \mathbb{Q}$ and

$$E_u : y^2 = x^3 - 3x + u$$

$\rightsquigarrow$ infinitely many u with symplectic isomorphisms $\phi_i : E_u[7] \to E_u^{(i)}[7]$, $i = 1, ..., 6$.

- Similarly, there is a curve denoted by $X_E^-(N)$ whose non-cuspidal points parametrize pairs (E', ϕ) such that there is a Galois isomorphism $\phi : E[N] \to E'[N]$ not respecting the Weil pairing (called an anti-symplectic isomorphism).

- Similarly, there is a curve denoted by $X_E^-(N)$ whose non-cuspidal points parametrize pairs (E', ϕ) such that there is a Galois isomorphism $\phi : E[N] \to E'[N]$ not respecting the Weil pairing (called an anti-symplectic isomorphism).
- The curves $X_E(p)$, $X_E^-(p)$ are twists of the arithmetic modular curve $X(p)$ $\rightsquigarrow$ they are smooth projective, geometrically irreducible curves defined over $\mathbb{Q}$ of genus $g = (p+2)(p-3)(p-5)/24$.

- Similarly, there is a curve denoted by $X_E^-(N)$ whose non-cuspidal points parametrize pairs (E', ϕ) such that there is a Galois isomorphism $\phi : E[N] \to E'[N]$ not respecting the Weil pairing (called an anti-symplectic isomorphism).
- The curves $X_E(p)$, $X_E^-(p)$ are twists of the arithmetic modular curve $X(p)$ $\rightsquigarrow$ they are smooth projective, geometrically irreducible curves defined over $\mathbb{Q}$ of genus $g = (p+2)(p-3)(p-5)/24$.
- Poonen–Schaefer–Stoll (2005), Freitas-Naskrecki–Stoll (2019) reduced the search of non-trivial, coprime solutions of the generalized Fermat equations $x^2 + y^3 = z^p$ (prime $p \geq 7$) to finding rational points on $X_E(p)$ and $X_E^-(p)$ for E in a finite list.

- Similarly, there is a curve denoted by $X_E^-(N)$ whose non-cuspidal points parametrize pairs (E', ϕ) such that there is a Galois isomorphism $\phi : E[N] \to E'[N]$ not respecting the Weil pairing (called an anti-symplectic isomorphism).
- The curves $X_E(p)$, $X_E^-(p)$ are twists of the arithmetic modular curve $X(p)$ $\rightsquigarrow$ they are smooth projective, geometrically irreducible curves defined over $\mathbb{Q}$ of genus $g = (p+2)(p-3)(p-5)/24$.
- Poonen–Schaefer–Stoll (2005), Freitas-Naskrecki–Stoll (2019) reduced the search of non-trivial, coprime solutions of the generalized Fermat equations $x^2 + y^3 = z^p$ (prime $p \geq 7$) to finding rational points on $X_E(p)$ and $X_E^-(p)$ for E in a finite list.
- For $p \geq 7$, the genus $\geq 2 \rightsquigarrow$ Faltings' Theorem: there are finitely many rational points. Effectively computing them is hard.

- Showing there are no local points (i.e. points with coordinates in some $\mathbb{Q}_\ell$ or $\mathbb{R}$) is enough to prove there are no rational points.
- $X_E(p)(\mathbb{Q})$ always contains the point $(E, \mathrm{id}_{E[p]})$, while $X_E^-(p)(\mathbb{Q})$ may be empty.

- Showing there are no local points (i.e. points with coordinates in some $\mathbb{Q}_\ell$ or $\mathbb{R}$) is enough to prove there are no rational points.
- $X_E(p)(\mathbb{Q})$ always contains the point $(E, \mathrm{id}_{E[p]})$, while $X_E^-(p)(\mathbb{Q})$ may be empty.

Question (1)

Given an elliptic curve $E/\mathbb{Q}$ and a prime $p \geq 7$, when does $X_E^-(p)$ have points over every completion of $\mathbb{Q}$?

Question (2)

If $X_E^-(p)$ has points over every completion of $\mathbb{Q}$, does it have a rational point? (i.e. does it satisfy Hasse's principle?)

Notation

Let $E/\mathbb{Q}_\ell$ be a curve with potentially good reduction.

- The semistability defect $e := e(E/\mathbb{Q}_\ell)$ is the degree of the minimal field extension $L/\mathbb{Q}_\ell^{\mathsf{un}}$ (inertial field) over which E acquires good reduction.
- It is well known that $e \in \{1, 2, 3, 4, 6, 8, 12, 24\}$ and work of Kraus (1990) explicitly determines it.

Notation

Let $E/\mathbb{Q}_\ell$ be a curve with potentially good reduction.

- The semistability defect $e := e(E/\mathbb{Q}_\ell)$ is the degree of the minimal field extension $L/\mathbb{Q}_\ell^{\mathrm{un}}$ (inertial field) over which E acquires good reduction.
- It is well known that $e \in \{1, 2, 3, 4, 6, 8, 12, 24\}$ and work of Kraus (1990) explicitly determines it.
- We define
$$c_4 = \ell^{v_\ell(c_4)}\tilde{c}_4, \qquad c_6 = \ell^{v_\ell(c_6)}\tilde{c}_6, \qquad \Delta_m = \ell^{v_\ell(\Delta_m)}\tilde{\Delta}.$$
- For ℓ of good reduction let $\bar{E}/\mathbb{F}_\ell$ be the reduced curve, $a_\ell := \ell + 1 - \#|\bar{E}(\mathbb{F}_\ell)|$ and $\Delta_\ell := a_\ell^2 - 4\ell$. Let $\pi \in \mathrm{End}(\bar{E})$ be the Frobenius endomorphism and set $b_{\bar{E}} := [\mathrm{End}(\bar{E}) : \mathbb{Z}[\pi]]$. Note that $b_{\bar{E}}$ is finite when $\bar{E}/\mathbb{F}_\ell$ is ordinary.
- We denote by (n/p) the Legendre symbol of n at p.

Main Theorem

Theorem (Freitas-M.)

*Let $E/\mathbb{Q}$ be an elliptic curve, $p \geq 7$ a prime and $K \neq \mathbb{Q}_p$ a completion of $\mathbb{Q}$. Then $X_E^-(p)(K) \neq \emptyset$ **unless** $K = \mathbb{Q}_\ell$, $E/\mathbb{Q}_\ell$ satisfies one of the exceptional cases:*

e	ℓ	*Additional conditions*
1	$\ell < p^2/16$	$p \equiv 3 \pmod 4$, $-p\Delta_\ell$ *is a square in* $\mathbb{Z}$ ($\Rightarrow \bar{E}/\mathbb{F}_\ell$ *ordinary*), $p \mid \Delta_\ell$ *and* $p \nmid b_{\bar{E}}$, *and* *if* $q \neq \ell$ *is prime and* $q \mid \Delta_\ell$ *then* $(q/p) \neq -1$
2	$\ell < p^2/16$	*Reduce to case* $e = 1$, *by replacing* E *with* $E^{\sqrt{\ell}}$
3, 6	$\ell \equiv 2 \pmod 3$	$(3/p) = 1$ *and* $(\ell/p) = 1$
	$\ell = 3$	$(3/p) = 1$ *and* $\tilde{\Delta} \equiv 2 \pmod 3$
4	$\ell \equiv 3 \pmod 4$	$(2/p) = 1$ *and* $(\ell/p) = 1$
	$\ell = 2$	$(2/p) = 1$ *and* $\tilde{c}_4 \equiv 5\tilde{\Delta} \pmod 8$
8, 24	$\ell = 2$	$(2/p) = 1$
12	$\ell = 3$	$(3/p) = 1$

Main Theorem

Remark: In particular $X_E^-(p)(\mathbb{R}) \neq \emptyset$ and $X_E^-(p)(\mathbb{Q}_\ell) \neq \emptyset$ for ℓ a prime of potentially multiplicative reduction.

Main Theorem

Remark: In particular $X_E^-(p)(\mathbb{R}) \neq \emptyset$ and $X_E^-(p)(\mathbb{Q}_\ell) \neq \emptyset$ for ℓ a prime of potentially multiplicative reduction.

Theorem (Freitas-M.)

Suppose that $E/\mathbb{Q}$ is an elliptic curve and p is a prime of

(i) *potentially multiplicative reduction; or*

(ii) *good reduction with $a_p(E) \neq 0$ if $p \equiv 7 \pmod 8$.*

Then $X_E^-(p)(\mathbb{Q}_p) \neq \emptyset$.

Main Theorem

Remark: In particular $X_E^-(p)(\mathbb{R}) \neq \emptyset$ and $X_E^-(p)(\mathbb{Q}_\ell) \neq \emptyset$ for ℓ a prime of potentially multiplicative reduction.

Theorem (Freitas-M.)

Suppose that $E/\mathbb{Q}$ is an elliptic curve and p is a prime of

(i) *potentially multiplicative reduction; or*

(ii) *good reduction with $a_p(E) \neq 0$ if $p \equiv 7 \pmod 8$.*

Then $X_E^-(p)(\mathbb{Q}_p) \neq \emptyset$.

Corollary (†)

Let $E/\mathbb{Q}$ be a semistable elliptic curve and $p \equiv 1 \pmod 4$ a prime. Then $X_E^-(p)$ has local points everywhere.

Hasse's principle

Hasse's principle

Definition (Hasse's principle over $\mathbb{Q}$)

Let $X/\mathbb{Q}$ be an algebraic variety. We say that *Hasse's principle* holds for X if

$$X(\mathbb{Q}) \neq \varnothing \quad \Longleftrightarrow \quad X(\mathbb{R}) \neq \varnothing \text{ and } X(\mathbb{Q}_\ell) \neq \varnothing \text{ for all primes } \ell.$$

Hasse's principle

Definition (Hasse's principle over $\mathbb{Q}$)

Let $X/\mathbb{Q}$ be an algebraic variety. We say that *Hasse's principle* holds for X if

$$X(\mathbb{Q}) \neq \varnothing \iff X(\mathbb{R}) \neq \varnothing \text{ and } X(\mathbb{Q}_\ell) \neq \varnothing \text{ for all primes } \ell.$$

Hasse–Minkovski: Hasse's Principle holds for X smooth plane conic.

Counterexamples to Hasse's principle:

- Selmer (1951):

$$3x^3 + 4y^3 + 5z^3 = 0.$$

Hasse's principle

Definition (Hasse's principle over $\mathbb{Q}$)

Let $X/\mathbb{Q}$ be an algebraic variety. We say that *Hasse's principle* holds for X if

$$X(\mathbb{Q}) \neq \varnothing \iff X(\mathbb{R}) \neq \varnothing \text{ and } X(\mathbb{Q}_\ell) \neq \varnothing \text{ for all primes } \ell.$$

Hasse–Minkovski: Hasse's Principle holds for X smooth plane conic.
Counterexamples to Hasse's principle:

- Selmer (1951):
$$3x^3 + 4y^3 + 5z^3 = 0.$$

- Özman (2009) $\rightsquigarrow$ certain quadratic twists of $X_0(N)$, denoted by $X^d(N)$.
- García-Vullers (2024) $\rightsquigarrow$ conjecturally infinitely many twists of $X(7)$.

Counterexamples to the Hasse Principle

Theorem

Let $K = \mathbb{Q}(\sqrt{D})$ where $D \in \{-11, -19, -43, -67, -163\}$. Let also $E/\mathbb{Q}$ be an elliptic curve with CM by K. If $p > 7$ is a prime such that $p \equiv 5 \pmod 8$ and $(D/p) = 1$, then $X_E^-(p)$ is a counterexample to the Hasse principle.

Counterexamples to Hasse's principle

Counterexamples to Hasse's principle

Conjecture (Frey–Mazur)

Any two elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ with $G_{\mathbb{Q}}$-isomorphic p-torsion modules for some $p > 17$ are $\mathbb{Q}$-isogenous.

Counterexamples to Hasse's principle

Conjecture (Frey–Mazur)

Any two elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ with $G_{\mathbb{Q}}$-isomorphic p-torsion modules for some $p > 17$ are $\mathbb{Q}$-isogenous.

Theorem (Freitas–M.)

Assume the Frey–Mazur Conjecture. Let $p \equiv 1 \pmod 4$ be a prime greater than 17. Then, for all semistable elliptic curves $E/\mathbb{Q}$ without $\mathbb{Q}$-isogenies, the curve $X_E^-(p)$ is a counterexample to Hasse's principle.

Sketch proof: Corollary † $\Rightarrow$ everywhere local points,
Frey-Mazur Conjecture + careful study of the Galois action on cusps $\Rightarrow$ no $\mathbb{Q}$-points.

Quantitative results

Recall that for an elliptic curve E given by a Weierstrass equation with integer coefficients $\mathbf{a} = (a_1, a_2, a_3, a_4, a_6) \in \mathbb{Z}^5$ one defines the naïve height of E by

$$\mathrm{ht}(E) := \mathrm{ht}(\mathbf{a}) = \max_i |a_i|^{1/i}.$$

When ordered by the naïve height:

- Cremona–Sadek (2023): just over 60% of elliptic curves are semistable.
- Duke (1997): 0% of all elliptic curves possess $\mathbb{Q}$-isogenies.

Quantitative results

Recall that for an elliptic curve E given by a Weierstrass equation with integer coefficients $\mathbf{a} = (a_1, a_2, a_3, a_4, a_6) \in \mathbb{Z}^5$ one defines the naïve height of E by

$$\mathrm{ht}(E) := \mathrm{ht}(\mathbf{a}) = \max_i |a_i|^{1/i}.$$

When ordered by the naïve height:

- Cremona–Sadek (2023): just over 60% of elliptic curves are semistable.
- Duke (1997): 0% of all elliptic curves possess $\mathbb{Q}$-isogenies.

Corollary

Assume the Frey–Mazur conjecture. When ordered by height, for at least 60% *of elliptic curves E, the modular curve $X_E^-(p)$ is a counterexample to Hasse's principle for at least* 50% *of primes p.*

Generalized Fermat equations

Generalized Fermat equations

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \text{ primes.}$$

A solution $(a, b, c) \in \mathbb{Z}^3$ is called **non-trivial** if $abc \neq 0$ and **primitive** if $\gcd(a, b, c) = 1$. The triple of exponents (p, q, r) is called the **signature** of the equation.

Generalized Fermat equations

Generalized Fermat Equation:

$$x^p + y^q = z^r, \quad p, q, r \text{ primes.}$$

A solution $(a, b, c) \in \mathbb{Z}^3$ is called **non-trivial** if $abc \neq 0$ and **primitive** if $\gcd(a, b, c) = 1$. The triple of exponents (p, q, r) is called the **signature** of the equation.

Conjecture (Tijdeman–Zagier, Darmon–Granville)

The above equation has finitely many integer solutions (a, b, c) which are non-trivial and primitive whenever $1/p + 1/q + 1/r < 1$. (Solutions $2^3 + 1^q = 3^2$ are counted only once.)

Some families of signatures that have been 'solved':

- $(p, p, p), p \geq 3$ Wiles, Taylor–Wiles.
- $(p, p, 2), p \geq 4$ and $(p, p, 3), p \geq 3$ Darmon–Merel, Poonen.
- $(2, 4, 6), (2, 6, 4), (4, 6, 2), (2, 8, 3)$, Bruin.
- $(2, 3, p)$ for $p = 7, 11^{\dagger}$ Poonen–Schaefer–Stoll, Freitas–Naskrecki–Stoll.
- $(3, 3, p)$ for 84.4% of primes p Bruin, Chen–Siksek, Dahmen, Freitas, Kraus.
- $(r, r, p)^{*}$, M. for $r \in \{5, 7, 11, 13, 19, 23, 37, 47, 53, 59, 61, 67, 71, 79, 83, 101, 103, 107, 131, 139, 149\}$.
- $x^3 + y^3 = qz^p$ has no solutions for "most" primes q and large p, Bennett–Bruni–Freitas.
- $x^r + y^r = dz^p$, for large p, Freitas–Najman*, Kara–M.–Özman†.

The superscript * indicates partial results that depend on local hypotheses, while † denotes results that rely on conjectures.

Generalized Fermat equation $x^3 + y^3 = 5^\alpha z^p$

Theorem (Freitas-M.)

Let $\alpha \in \mathbb{Z}_{>0}$. The Fermat-type equation

$$x^3 + y^3 = 5^\alpha z^p$$

has no non-trivial primitive integer solutions whenever $(\alpha/p) = -1$ and

$$p \in \{167, 383, 503, 599, 647, 719, 743, 839, 863, 887, 911, 983\}.$$

Modular method - first steps

Suppose that $(a, b, c) \in \mathbb{Z}^3$ is a non-trivial, primitive solution to

$$x^3 + y^3 = 5^\alpha z^p, \qquad (\alpha/p) = -1 \tag{1}$$

- We associate to such a solution a *Frey elliptic curve*

$$F := F_{a,b} \;\; : \;\; y^2 = x^3 + 3abx + b^3 - a^3, \quad \Delta_F = -2^4 3^3 5^{2\alpha} c^{2p}.$$

Modular method - first steps

Suppose that $(a, b, c) \in \mathbb{Z}^3$ is a non-trivial, primitive solution to

$$x^3 + y^3 = 5^\alpha z^p, \qquad (\alpha/p) = -1 \tag{1}$$

- We associate to such a solution a *Frey elliptic curve*

$$F := F_{a,b} \quad : \quad y^2 = x^3 + 3abx + b^3 - a^3, \quad \Delta_F = -2^4 3^3 5^{2\alpha} c^{2p}.$$

- Modularity and level lowering $\rightsquigarrow$ for $p \geq 17$, there exists a newform f of weight 2 and level $N_p \in \{90, 180, 360\}$ and a prime $\mathfrak{p} \mid p$ in $\mathbb{Q}_f$ such that

$$\overline{\rho}_{F,p} \simeq \overline{\rho}_{f,\mathfrak{p}}.$$

Modular method - first steps

- LMFDB shows that f is rational i.e ($\mathbb{Q}_f = \mathbb{Q}$) and thus modularity gives

$$\overline{\rho}_{f,\mathfrak{p}} \simeq \overline{\rho}_{E_f,p}$$

for some elliptic curve E_f in:

$$\{90a4, 90b2, 90c2, 180a2, 360a2, 360b2, 360c2, 360d2, 360e2\}.$$

Modular method - first steps

- LMFDB shows that f is rational i.e ($\mathbb{Q}_f = \mathbb{Q}$) and thus modularity gives

$$\overline{\rho}_{f,\mathfrak{p}} \simeq \overline{\rho}_{E_f,p}$$

for some elliptic curve E_f in:

$$\{90a4, 90b2, 90c2, 180a2, 360a2, 360b2, 360c2, 360d2, 360e2\}.$$

- Therefore $\overline{\rho}_{F,p} \simeq \overline{\rho}_{E_f,p}$ for some E_f in the list.

Elimination I

From $\overline{\rho}_{F,p} \simeq \overline{\rho}_{E_f,p}$, for all primes $\ell \nmid pN_p$ we have

$$a_\ell(E_f) \equiv a_\ell(F) \pmod{p} \quad \text{or} \quad a_\ell(E_f) \equiv \pm(\ell+1) \pmod{p}.$$

Elimination I

From $\overline{\rho}_{F,p} \simeq \overline{\rho}_{E_f,p}$, for all primes $\ell \nmid pN_p$ we have

$$a_\ell(E_f) \equiv a_\ell(F) \pmod{p} \quad \text{or} \quad a_\ell(E_f) \equiv \pm(\ell+1) \pmod{p}.$$

Let

$$S_\ell = \{a_\ell(F_{a,b}) : a, b \in \mathbb{F}_\ell,\ F_{a,b} \text{ is an elliptic curve}\}.$$

Then

$$p \mid B_\ell(E_f) := ((\ell+1)^2 - a_\ell(E_f)) \prod_{t \in S_\ell} (t - a_\ell(E_f)).$$

Elimination I

From $\overline{\rho}_{F,p} \simeq \overline{\rho}_{E_f,p}$, for all primes $\ell \nmid pN_p$ we have

$$a_\ell(E_f) \equiv a_\ell(F) \pmod{p} \quad \text{or} \quad a_\ell(E_f) \equiv \pm(\ell+1) \pmod{p}.$$

Let

$$S_\ell = \{a_\ell(F_{a,b}) : a, b \in \mathbb{F}_\ell,\ F_{a,b} \text{ is an elliptic curve}\}.$$

Then

$$p \mid B_\ell(E_f) := ((\ell+1)^2 - a_\ell(E_f)) \prod_{t \in S_\ell} (t - a_\ell(E_f)).$$

`Magma` $\Rightarrow B_7(E_f)$ eliminates $E_f \in \{180a2, 360b2, 360c2\}$ for $p > 7$.

Elimination II

Proposition

Let $(a, b, c) \in \mathbb{Z}^3$ *be a non-trivial, primitive solution to* $x^3 + y^3 = 5^\alpha z^p$ *with* $(\alpha/p) = -1$. *Suppose*

$$E_f \in \{90a4, 90b2, 90c2, 360a2, 360d2, 360e2\}.$$

Then $X_{E_f}^-(p)(\mathbb{Q}) \neq \emptyset$.

Elimination II

Proposition

Let $(a, b, c) \in \mathbb{Z}^3$ *be a non-trivial, primitive solution to* $x^3 + y^3 = 5^\alpha z^p$ *with* $(\alpha/p) = -1$. *Suppose*

$$E_f \in \{90a4, 90b2, 90c2, 360a2, 360d2, 360e2\}.$$

Then $X^-_{E_f}(p)(\mathbb{Q}) \neq \emptyset$.

Proof.

The isomorphism $\overline{\rho}_{F,p} \simeq \overline{\rho}_{E_f,p}$ gives $\phi : F[p] \to E_f[p]$ of $G_\mathbb{Q}$-modules. Work of Kraus–Oesterlé (1992) can be applied for the prime 5 of multiplicative reduction for both curves to deduce that ϕ is anti-symplectic (using the assumption $(\alpha/p) = -1$). □

Elimination II

For each pair (E_f, p) where

$$E_f \in \{90a4, 90b2, 90c2, 360a2, 360d2, 360e2\}.$$

and p in the list

$$p \in \{167, 383, 503, 599, 647, 719, 743, 839, 863, 887, 911, 983\}$$

we use our main theorem and `Magma` to find a prime of good reduction $\ell \neq p$ such that $X^-_{E_f}(p)(\mathbb{Q}_\ell) = \emptyset$, and therefore $X^-_{E_f}(p)(\mathbb{Q}) = \emptyset$, contradicting the previous proposition.

Thank you!