Primitive Points and Elliptic Curves

Arman Yagci
in collaboration with
Chi Nguyen *Yunchuan Zhou*

University of Oklahoma

May 21, 2026

Closed Points On The Modular Curve $X_1(n)$

For a positive integer n, the modular curve $X_1(n)$ is a smooth, projective algebraic curve whose non-cuspidal points parametrize isomorphism classes of elliptic curves E with a distinguished point P of exact order n.

A point $x = (E, P) \in X_1(n)$ is *closed* if $\{x\}$ is Zariski closed. In this case, $\mathbb{Q}(x)$ is a finite extension of $\mathbb{Q}$, and the degree of this extension is the *degree of the closed point* $x \in X_1(n)$. We write $[E, P]$ to specify that (E, P) is a closed point.

Closed points of $X_1(n)$ are in bijection with the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ orbits in $X_1(n)(\overline{\mathbb{Q}})$, with the degree of the closed point corresponding to the size of the Galois orbit.

Isolated Points

Definition

Fix some modular curve $X = X_1(n)$ and let $x \in X$ be a closed point of degree d. Let $\phi_d : \mathrm{Sym}^d(X) \to \mathrm{Pic}^d(X) \cong \mathrm{Pic}^0(X)$ be the degree d Abel-Jacobi morphism.

1. We say x is $\mathbb{P}^1$-**parameterized** if there exists a $\mathbb{Q}$-rational $x' \in \mathrm{Sym}^d(X)$ such that $x \neq x'$ and $\phi_d(x) = \phi_d(x')$.
2. We say x is **AV-parameterized** if there exists a positive rank abelian subvariety $A \subseteq \mathrm{Pic}^0(X)$ such that $\phi_d(x) + A \subseteq \mathrm{im}(\phi_d)$.
3. We say x is **isolated** if it is neither $\mathbb{P}^1$-parameterized nor AV-parameterized.

We call $j(E) \in X_1(1) \cong \mathbb{P}^1$ an *isolated j-invariant* if there exists an isolated point $x \in X_1(n)$ for some n such that $j(x) = j(E)$.

Connection to Serre's Uniformity Conjecture

Serre's Open Image Theorem implies that for a fixed non-CM elliptic curve $E/\mathbb{Q}$, the mod p Galois representations $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ are surjective for all sufficiently large primes p. Serre's Uniformity Conjecture asks for a single bound that works simultaneously for all non-CM $E/\mathbb{Q}$, often conjectured to be 37.

In 2021, Abbey Bourdon and Filip Najman showed that if there are only finitely many isolated j-invariants associated to non-CM $\mathbb{Q}$-curves, which are elliptic curves over number fields isogenous to their Galois conjugates, then Serre's Uniformity Conjecture holds.

This motivates the study of isolated points.

Primitive Points as a "Certificate Set"

In 2024, for each non-CM elliptic curve $E/\mathbb{Q}$, Bourdon et al. introduce a finite set $\mathcal{P}(E)$ that can detect if $j(E)$ is isolated.

Definition

Let $E/\mathbb{Q}$ be a non-CM elliptic curve. The set of **primitive points** $\mathcal{P}(E)$ associated to E is defined as the set of all closed points $x \in \sqcup_{n\in\mathbb{Z}^+} X_1(n)$ with $j(x) = j(E)$ such that $\deg(x) < \deg(f) \cdot \deg(f(x))$ for all natural maps $f : X_1(n) \to X_1(n')$ taking $x \in X_1(n)$ to $f(x) \in X_1(n')$ where $n' \mid n$ is some proper divisor.

Key Properties:

1. $\mathcal{P}(E) \neq \emptyset$ (the unique closed point in $X_1(1)$ above $j(E)$ is vacuously primitive due to the absence of a natural map to a lower level).
2. $|\mathcal{P}(E)|$ is finite (we give a bound for this).
3. $j(E)$ is isolated if and only if there exists an isolated point in $\mathcal{P}(E)$.

Galois Representations

Let $E/\mathbb{Q}$ be a non-CM elliptic curve and write $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The Galois action on the full torsion subgroup $E(\overline{\mathbb{Q}})_{\mathrm{tors}}$ is encoded by the **adelic Galois representation**

$$\rho_E : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(E(\overline{\mathbb{Q}})_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}) \cong \prod_{p \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_p).$$

For each integer $n \geq 1$, projecting to primes dividing n yields the n-**adic Galois representation**

$$\rho_{E,n^\infty} : \mathrm{Gal}_{\mathbb{Q}} \to \prod_{p|n} \mathrm{GL}_2(\mathbb{Z}_p),$$

which describes the action of $\mathrm{Gal}_{\mathbb{Q}}$ on points whose order is divisible only by primes dividing n, whereas reduction modulo n yields the **mod** n **Galois representation**, which records the Galois action on points of order dividing n,

$$\rho_{E,n} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

A Bound for $|\mathcal{P}(E)|$

Let $I(E)$ denote the adelic index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})]$, which is finite by Serre's Open Image Theorem. Let

$$S_E := \{2,3\} \cup \{\ell \text{ prime} : \rho_{E,\ell^\infty} \text{ is not surjective}\}, \qquad m := \prod_{\ell \in S_E} \ell,$$

and let $m_0 = m_0(E)$ denote the level of the m-adic image, which is the smallest positive integer such that $\mathrm{im}(\rho_{E,m^\infty}) = \pi^{-1}(\rho_{E,m_0}(\mathrm{Gal}_{\mathbb{Q}}))$ where $\pi : \prod_{p|m} \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}/m_0\mathbb{Z})$ is the natural reduction map. Then, Bourdon et al. show that every primitive point attached to E occurs on $X_1(n)$ for some divisor $n \mid m_0$.

A Bound for $|\mathcal{P}(E)|$

Thus, to bound $|\mathcal{P}(E)|$, it suffices to bound the number of closed points in $X_1(n)$ above $j(E)$ for each $n \mid m_0$, which corresponds to the $H(n) := \langle \rho_{E,n}(\mathrm{Gal}_{\mathbb{Q}}), -I \rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$-orbits in

$$\begin{aligned} V_n &:= \{v = (a,b) \in (\mathbb{Z}/n\mathbb{Z})^2 : \mathrm{ord}(v) = n\} \\ &\cong \{P \in E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 \ : \ \mathrm{ord}(P) = n\}. \end{aligned}$$

Bounding the number of $H(n)$-orbits in V_n for each $n \mid m_0$, we obtain the following:

Theorem (Nguyen, Y, Zhou)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Then,

$$|\mathcal{P}(E)| \leq \min\left\{ m_0^2,\ 1 + \frac{I(E)\,\sigma_0(m_0)}{2} \right\},$$

where $\sigma_0(m_0)$ denotes the number of positive divisors of m_0.

Uniqueness Criteria

If a non-CM elliptic curve $E/\mathbb{Q}$ satisfies $|\mathcal{P}(E)| = 1$, then we can conclude that $j(E)$ is not isolated. This is because the unique primitive point must necessarily be the unique closed point in $X_1(1)$, which is $\mathbb{P}^1$-parameterized and hence not isolated. Hence we ask when do we have $|\mathcal{P}(E)| = 1$.

Theorem (Nguyen, Y, Zhou)

Let E be a non-CM elliptic curve defined over $\mathbb{Q}$. The following are equivalent:

1. *E has a unique primitive point attached to it.*
2. *$H(n)$ acts transitively on V_n for all $n \mid m_0$.*
3. *$H(m_0)$ acts transitively on V_{m_0}.*
4. *There is a unique closed point $x \in X_1(m_0)$ with $j(x) = j(E)$.*

Sufficient Criteria for Uniqueness

The previous theorem reformulates the unique primitive point condition as $H(n)$ acting transitively on V_n for $n \mid m_0$. In particular, if $G(n) := \rho_{E,n}(\mathrm{Gal}(\mathbb{Q})) \subseteq H(n)$ acts transitively on V_n for each $n \mid m_0$, then we can conclude $|\mathcal{P}(E)| = 1$. For that, it turns out that it is sufficient to check the following two conditions:

(LT_G) : For every prime power $\ell^k \mid m_0$, $G(\ell^k) = \rho_{E,\ell^k}(\mathrm{Gal}(\mathbb{Q}))$ acts transitively on $V_{\ell^k} \subseteq (\mathbb{Z}/\ell^k\mathbb{Z})^2$.

(EF_{m_0}) : For $n \geq 1$, write $K_n := \mathbb{Q}(E[n])$, and for every coprime a, b with $ab \mid m_0$, let $Q_{a,b} := \mathrm{Gal}(K_a \cap K_b/\mathbb{Q})$. The natural surjections

$$\mathrm{res}_a : \mathrm{Gal}(K_a/\mathbb{Q}) \twoheadrightarrow Q_{a,b} \quad \mathrm{res}_b : \mathrm{Gal}(K_b/\mathbb{Q}) \twoheadrightarrow Q_{a,b}$$

remain surjective when restricted to stabilizers of exact-order points: for any $P_a \in E[a]$ and $P_b \in E[b]$ of exact order a, b (respectively),

$$\mathrm{res}_a(\mathrm{Stab}_{\mathrm{Gal}(K_a/\mathbb{Q})}(P_a)) = Q_{a,b} \qquad \mathrm{res}_b(\mathrm{Stab}_{\mathrm{Gal}(K_b/\mathbb{Q})}(P_b)) = Q_{a,b}.$$

Sufficient Criteria for Uniqueness

That is,

Theorem (Nguyen, Y, Zhou)

Assume (LT_G) and (EF_{m_0}) hold. Then, the set $\mathcal{P}(E)$ of primitive points associated to a non-CM elliptic curve $E/\mathbb{Q}$ has only one primitive point.

We implement an algorithm in SageMath that checks (LT_G) and (EF_{m_0}).

Uniqueness of Primitive Point for Serre Curves

An elliptic curve $E/\mathbb{Q}$ is called a *Serre curve* if $I(E) = 2$, i.e. if its adelic Galois representation has the largest possible image among non-CM elliptic curves.

Theorem (Nguyen, Y, Zhou)

Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Let m and m_0 be as previously defined. If $m_0 = 1$ (i.e. if the m-adic Galois representation is surjective), then E is a Serre curve.

Theorem (Nguyen, Y, Zhou)

Let $E/\mathbb{Q}$ be a Serre curve. Then $|\mathcal{P}(E)| = 1$.

In particular, this provides a new proof that no isolated points arise from Serre curves. Since almost all elliptic curves are Serre curves (Jones '09), this also shows that almost all elliptic curves have a unique primitive point (hence don't have isolated j-invariants).

Proof Outline

Put $G := \rho_E(\mathrm{Gal}(\mathbb{Q}))$ and $C := [\mathrm{GL}_2(\hat{\mathbb{Z}}), \mathrm{GL}_2(\hat{\mathbb{Z}})]$.

Since $I(E) = 2$, we have that $\mathrm{GL}_2(\hat{\mathbb{Z}})/G \cong \mathbb{Z}/2\mathbb{Z}$ is abelian so that $G \supseteq C$. For $n \mid m_0$, let $G(n)$ and $C(n)$ denote the respective mod n reductions. Then, we have

$$C(n) \subseteq G(n) \subseteq H(n) = \langle G(n), -I \rangle \ .$$

So it suffices to show $C(n)$ acts transitively on V_n by the uniqueness criterion.

Proof Outline (continued)

By CRT we have

$$\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_i \mathrm{GL}_2(\mathbb{Z}/p_i^{k_i}\mathbb{Z}), \qquad V_n \cong \prod_i V_{p_i^{k_i}},$$

with componentwise action.

Since the commutator operation commutes with direct products, $C(n) = [\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})]$ is transitive on V_n if and only if $C(p^k)$ is transitive on V_{p^k} for each $p^k \mid n$.

Case 1: $p = 2$. Induction on k.
Case 2: p *odd.* One can show $\mathrm{SL}_2(\mathbb{Z}/p^k\mathbb{Z}) \subseteq C(p^k)$, and $\mathrm{SL}_2(\mathbb{Z}/p^k\mathbb{Z})$ already is transitive on V_{p^k}.

Thank You!

References I

[BN21] Abbey Bourdon and Filip Najman. *Sporadic points of odd degree on $X_1(N)$ coming from $\mathbb{Q}$-curves*. 2021. arXiv: 2107.10909 [math.NT]. URL: https://arxiv.org/abs/2107.10909.

[Bou+24] Abbey Bourdon et al. "Towards a classification of isolated j-invariants". In: *Mathematics of Computation* 94.351 (Apr. 2024), pp. 447–473. ISSN: 1088-6842. DOI: 10.1090/mcom/3956. URL: http://dx.doi.org/10.1090/mcom/3956.

[Jon09] Nathan Jones. "Almost all elliptic curves are Serre curves". en. In: *Trans. Am. Math. Soc.* 362.3 (Sept. 2009), pp. 1547–1570.

[NYZ26] Chi Nguyen, Arman Yagci, and Yunchuan Zhou. *Local Transitivity and Entanglement Obstructions for Primitive Points*. 2026. arXiv: 2601.17559 [math.NT]. URL: https://arxiv.org/abs/2601.17559.

References II

[Ser72] Jean-Pierre Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques". In: *Invent. math* 15 (1972), pp. 259–331.