Serre Curves Relative to Obstructions Modulo 2

LuCaNT Conference
July 11, 2023

Jacob Mayle and Rakvi

University of Pennsylvania
Dept. of Mathematics

Galois Representations

Let $E/\mathbb{Q}$ be an elliptic curve. For $n \geq 2$, consider the n-torsion subgroup

$$E[n] = \{P \in E(\overline{\mathbb{Q}}) : nP = \mathcal{O}\} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Taking an inverse limit, we obtain the adelic Tate module of E,

$$T(E) = \varprojlim E[n] \cong \widehat{\mathbb{Z}} \oplus \widehat{\mathbb{Z}}$$

where $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ denotes the ring of profinite integers.

Then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $T(E)$, giving rise to the adelic Galois representation

$$\rho_E \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(T(E)) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

We write G_E for the image of ρ_E, which is defined up to conjugacy in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Serre's Open Image Theorem

Upon composing with the relevant projection maps, we obtain

$$\rho_{E,\ell^\infty}: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \qquad \ell\text{-adic}$$

$$\rho_{E,n}: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \qquad \text{mod } n$$

Theorem. If $E/\mathbb{Q}$ is non-CM (i.e., $\mathrm{End}(E_{\overline{\mathbb{Q}}}) = \mathbb{Z}$), then

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] < \infty.$$

Consequently, ρ_{E,ℓ^∞} is surjective for all sufficiently large prime numbers ℓ.

Example 1. The elliptic curve E with LMFDB label 11.a1 is non-CM. The ℓ-adic Galois representation ρ_{E,ℓ^∞} is nonsurjective for $\ell = 5$ and surjective for all $\ell \neq 5$.

Serre Curves

Example 2. The elliptic curve E with LMFDB label 37.a1 is non-CM. For this curve, the ℓ-adic Galois representation is surjective for all prime numbers ℓ.

Although the ℓ-adic Galois representation ρ_{E,ℓ^∞} may be surjective for all prime numbers ℓ, Serre noted that (over $\mathbb{Q}$) by the Weil pairing and Kronecker-Weber theorem, the adelic Galois representation ρ_E cannot be surjective. As such,

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] \geq 2. \tag{1}$$

An elliptic curve $E/\mathbb{Q}$ for which equality holds in (1) is a *Serre curve.*

In other words, Serre curves are elliptic curves where G_E is "as large as possible".

Relative Serre Curves

Building on work of Duke, in his 2005 Ph.D. thesis, Jones proved the following.

Theorem. When ordered by naive height, 100% of $E/\mathbb{Q}$ are Serre curves.

Empirically, 48.223% of elliptic curves of conductor $\leq 500\,000$ are Serre curves.

In a joint work with Mayle (to appear in LuCaNT), we consider elliptic curves whose adelic image G_E is "as large as possible" given a prescribed obstruction.

Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a subgroup and write $[\cdot,\cdot]$ for the commutator of a group.

An elliptic curve $E/\mathbb{Q}$ is a *G-Serre curve* if $G_E(n) \subseteq G$ and $[G_E, G_E] = [\widehat{G}, \widehat{G}]$.

In particular, we study G-Serre curves for the proper subgroups $G \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

These subgroups are of index 6, 3, and 2, and we denote them respectively by

$$\mathrm{2Cs} := \left\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}, \quad \mathrm{2B} := \left\langle\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\right\rangle, \quad \mathrm{2Cn} := \left\langle\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)\right\rangle.$$

Associated to these groups, we define the sets of subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$,

$$\begin{aligned}\mathcal{S}_{\mathrm{2Cs}} :=& \{2.6.0.1, 8.12.0.2, 4.12.0.2, 8.12.0.1, 4.12.0.1, 8.12.0.3, 8.24.0.5, 8.24.0.7, 8.24.0.2,\\ & 8.24.0.1, 8.12.0.4, 8.24.0.6, 8.24.0.8, 8.24.0.3, 8.24.0.4\},\\ \mathcal{S}_{\mathrm{2B}} :=& \{2.3.0.1, 8.6.0.2, 8.6.0.4, 8.6.0.1, 8.6.0.6, 8.6.0.3, 8.6.0.5\},\\ \mathcal{S}_{\mathrm{2Cn}} :=& \{2.2.0.1, 4.4.0.2, 8.4.0.1\}\end{aligned}$$

where `N.i.g.n` denotes the subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ with the given Rouse–Sutherland–Zureick-Brown label.

Characterization of Relative Serre Curves

Theorem (M.-Rakvi 2022). For a subgroup $G \in \{2\mathrm{Cs}, 2\mathrm{B}, 2\mathrm{Cn}\}$ and an elliptic curve $E/\mathbb{Q}$, we have that E is a G-Serre curve if and only if $\rho_{E,2^\infty}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \in \mathcal{S}_G$ and ρ_{E,ℓ^∞} is surjective for all odd prime numbers ℓ.

By work of Rouse–Sutherland–Zureick-Brown, our characterization can be used to computationally determine G-Serre curves. By running our code on all curves in Cremona's database, we now know that among curves of conductor $\leq 500\,000$:

$$\underset{\text{Serre curves}}{48.223\%} \rightarrow \underset{\substack{\text{Serre curves}\\ +\text{ Max relative to}\\ \text{obstruction mod 2}}}{78.075\%}.$$

Moreover, for all such curves we have a description of the adelic image G_E.

Summary of Proof

Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and write $\widehat{G}$ for the full preimage of G in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Let $E/\mathbb{Q}$ be such that $G_E(2) = G$.

Recall that E is a G-Serre curve if and only if $G_E \subseteq \widehat{G}$ and $[G_E, G_E] = [\widehat{G}, \widehat{G}]$.

Thus the problem of deciding whether E is a G-Serre curve is reduced to determining whether the commutator condition $[G_E, G_E] = [\widehat{G}, \widehat{G}]$ holds.

Jones showed that the commutator condition holds if and only if it holds modulo 216. We reduced the modulus m_0 to 36 if $G \in \{\mathrm{2B}, \mathrm{2Cn}\}$ and 72 if $G = \mathrm{2Cs}$.

In order for $[G_E, G_E] = [\widehat{G}, \widehat{G}] \pmod{m_0}$, it must be that

$$[G_E, G_E] = [\widehat{G}, \widehat{G}] \pmod{9} \quad \text{and} \quad [G_E, G_E] = [\widehat{G}, \widehat{G}] \pmod{2^k}. \tag{2}$$

The first condition $G_E(9) = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. The second condition puts a constraint on $G_E(2^k)$. Considering the possible images of $\rho_{E,2^k}$ and possible 2^k-9 interactions, we note (perhaps surprisingly) that (2) is also a sufficient condition for $[G_E, G_E] = [\widehat{G}, \widehat{G}]$. In this way, we prove the theorem.

Moreover, we know the adelic index of a G-Serre curve.

Proposition. If E is a G-Serre curve for a $G \in \{\texttt{2Cs}, \texttt{2B}, \texttt{2Cn}\}$, then

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}})\colon G_E] = \begin{cases} 12 & G \in \{\texttt{2B}, \texttt{2Cn}\} \\ 48 & G = \texttt{2Cs}. \end{cases}$$

Knowing the adelic index allows us to give a description of G_E.

2Cn-Serre Curves

- Let E be a 2Cn-Serre curve. Recall that $\mathcal{S}_{2\mathrm{Cn}} = \{2.2.0.1, 4.4.0.2, 8.4.0.1\}$. In particular, $G_E(2) = 2\mathrm{Cn}$.
- Thus, $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is cyclic of order 3. The conductor of $\mathbb{Q}(E[2])$ is given by $\sqrt{\Delta_{\mathbb{Q}(E[2])}}$. Further, it can be shown that $\sqrt{\Delta_{\mathbb{Q}(E[2])}}$ is odd.
- If $G_E(2^\infty) \neq 2.2.0.1$, then the adelic index of 12 is explained by $[\mathrm{GL}_2(\mathbb{Z}_2)\colon G_E(2^\infty)] = 4$ and the cubic entanglement arising from the containment $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(\zeta_{\sqrt{\Delta_{\mathbb{Q}(E[2])}}})$.
- If $G_E(2^\infty) = 2.2.0.1$, then there is an additional quadratic entanglement arising from inclusions $\mathbb{Q}(\sqrt[4]{\Delta_E}) \subseteq \mathbb{Q}(E[4])$ and $\mathbb{Q}(\sqrt[4]{\Delta_E}) \subseteq \mathbb{Q}(E[|\sqrt{\Delta_E}|])$.

An Example

- Consider the elliptic curve E with LMFDB label `392.a1` given by

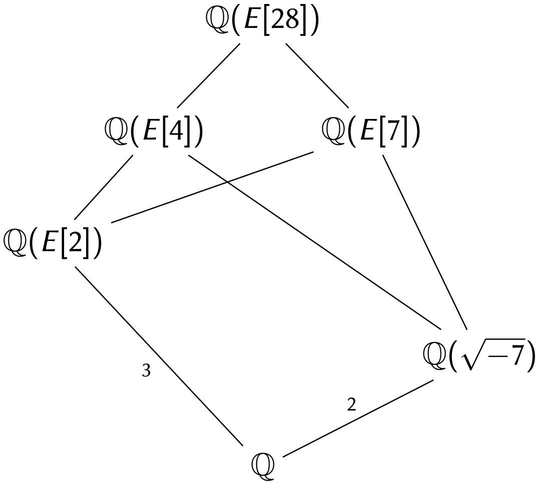
$$y^2 = x^3 - 7x + 7.$$

  We compute that $G_E(2^\infty) = \text{2.2.0.1}$ and that ρ_{E,ℓ^∞} is surjective for all primes $\ell > 2$. Thus, by our main theorem, E is a $2\mathrm{Cn}$-Serre curve.

- The conductor of $\mathbb{Q}(E[2])$ is 7, so there is a cubic entanglement between $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E[7])$.
- Further, since $\sqrt[4]{\Delta_E} = 2\sqrt{7} \in \mathbb{Q}(E[4])$, we know $\sqrt{-7} \in \mathbb{Q}(E[4]) \cap \mathbb{Q}(E[7])$. Thus there is a quadratic entanglement between $\mathbb{Q}(E[4])$ and $\mathbb{Q}(E[7])$.
- Using Sutherland's `galrep` code, we compute that

$$G_E(4) = \langle \left(\begin{smallmatrix} 2 & 3 \\ 3 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 3 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 3 & 1 \end{smallmatrix}\right) \rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}).$$

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = \underbrace{2}_{\text{2-adic index}} \cdot \underbrace{3}_{\text{2-7 entanglement}} \cdot \underbrace{2}_{\text{4-7 entanglement}} = 12.$$



An Example

Using Magma and our above work, we compute that

$$G_E(28) = \left\langle \begin{pmatrix} 26 & 23 \\ 1 & 19 \end{pmatrix}, \begin{pmatrix} 19 & 27 \\ 21 & 12 \end{pmatrix}, \begin{pmatrix} 8 & 5 \\ 27 & 21 \end{pmatrix} \right\rangle .$$

Further, the adelic image $G_E \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ is $\widehat{G_E(28)}$.

Our result agrees up to conjugacy with the output of Zywina's recent code.

Application

Knowing G_E for the entire family of G-Serre curves is valuable in applications.

1. Koblitz conjecture (and Zywina's refinement)
2. Lang-Trotter conjecture
3. Titchmarsh divisor problem for elliptic curves
4. Cyclicity conjecture

In particular, we give an application to the cyclicity conjecture.

Question. Given an elliptic curve $E/\mathbb{Q}$, what is the density C_E of primes p for which $E(\mathbb{F}_p)$ is cyclic?

Theorem (Serre). Assume GRH. If $E/\mathbb{Q}$ is an elliptic curve, then

$$C_E = \sum_{n=1}^{\infty} \frac{\mu(n)}{\#G_E(n)}.$$

The entanglement correction factor $\mathfrak{C}_E$ associated with E is defined by

$$C_E = \mathfrak{C}_E \prod_{\ell} \left(1 - \frac{1}{\#G_E(\ell)}\right).$$

In his thesis, Brau showed how to compute $\mathfrak{C}_E$ given G_E (under mild assumptions).

Example. Consider the elliptic curve E given by `392.a1` from before. We have

$$C_E \approx 1.000496 \cdot 0.651002 = 0.651324.$$

Table of Relative Serre Curves

G	$G_E(2^\infty)$	LMFDB	Weierstrass equation	m_E	$\mathfrak{C}_E$
2B	2.3.0.1	69.a1	$y^2 + xy + y = x^3 - 16x - 25$	276	1
2B	8.6.0.2	1152.d1	$y^2 = x^3 - 216x - 864$	24	1
2B	8.6.0.4	102.a1	$y^2 + xy = x^3 + x^2 - 2x$	136	$\frac{78337}{78336}$
2B	8.6.0.1	46.a2	$y^2 + xy = x^3 - x^2 - 10x - 12$	184	$\frac{267169}{267168}$
2B	8.6.0.6	46.a1	$y^2 + xy = x^3 - x^2 - 170x - 812$	184	1
2B	8.6.0.3	490.f1	$y^2 + xy = x^3 - 1191x + 15721$	56	1
2B	8.6.0.5	102.a2	$y^2 + xy = x^3 + x^2 + 8x + 10$	136	1
2Cn	2.2.0.1	392.a1	$y^2 = x^3 - 7x + 7$	28	$\frac{2017}{2016}$
2Cn	4.4.0.2	392.c1	$y^2 = x^3 - x^2 - 16x + 29$	28	$\frac{2017}{2016}$
2Cn	8.4.0.1	3136.b1	$y^2 = x^3 - 1372x - 19208$	56	$\frac{2017}{2016}$

Thank you!