Serre Curves Relative to Obstructions Modulo 2

LuCaNT Conference
July 11, 2023

Jacob Mayle and Rakvi
University of Pennsylvania
Dept. of Mathematics
Let $E/\mathbb{Q}$ be an elliptic curve. For $n \geq 2$, consider the $n$-torsion subgroup

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

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

$$\rho_E : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}(T(E)) \cong \text{GL}_2(\widehat{\mathbb{Z}}).$$

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

Rakvi (University of Pennsylvania)
Serre’s Open Image Theorem

Upon composing with the relevant projection maps, we obtain

\[ \rho_{E,\ell^{\infty}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}_{\ell^{\infty}}) \quad \ell\text{-adic} \]

\[ \rho_{E,n} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \quad \text{mod } n \]

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

\[ [\text{GL}_2(\hat{\mathbb{Z}}) : G_E] < \infty. \]

Consequently, \( \rho_{E,\ell^{\infty}} \) is surjective for all sufficiently large prime numbers \( \ell \).

**Example 1.** The elliptic curve \( E \) with LMFDB label 11.a1 is non-CM. The \( \ell \)-adic Galois representation \( \rho_{E,\ell^{\infty}} \) is nonsurjective for \( \ell = 5 \) and surjective for all \( \ell \neq 5 \).
**Example 2.** The elliptic curve $E$ with LMFDB label 37.a1 is non-CM. For this curve, the $\ell$-adic Galois representation is surjective for all prime numbers $\ell$.

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

$$[\text{GL}_2(\hat{\mathbb{Z}}) : G_E] \geq 2. \quad (1)$$

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”.

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 $G \subseteq \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ 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 $[G_E, G_E] = [\hat{G}, \hat{G}]$. 
In particular, we study $G$-Serre curves for the proper subgroups $G \subseteq \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$. These subgroups are of index 6, 3, and 2, and we denote them respectively by

$$2\text{Cs} := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}, \quad 2\text{B} := \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle, \quad 2\text{Cn} := \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle.$$

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

$$S_{2\text{Cs}} := \{2.6.0.1, 8.12.0.2, 4.12.0.2, 8.12.0.1, 4.12.0.1, 8.12.0.3, 8.24.0.5, 8.24.0.7, 8.24.0.2, 8.24.0.1, 8.12.0.4, 8.24.0.6, 8.24.0.8, 8.24.0.3, 8.24.0.4\},$$

$$S_{2\text{B}} := \{2.3.0.1, 8.6.0.2, 8.6.0.4, 8.6.0.1, 8.6.0.6, 8.6.0.3, 8.6.0.5\},$$

$$S_{2\text{Cn}} := \{2.2.0.1, 4.4.0.2, 8.4.0.1\}$$

where N. i. g. n denotes the subgroup of $\text{GL}_2(\hat{\mathbb{Z}})$ with the given Rouse–Sutherland–Zureick-Brown label.
Theorem (M.-Rakvi 2022). For a subgroup $G \in \{2Cs, 2B, 2Cn\}$ and an elliptic curve $E/\mathbb{Q}$, we have that $E$ is a $G$-Serre curve if and only if $\rho_{E,2\infty}(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \in S_G$ and $\rho_{E,\ell\infty}$ is surjective for all odd prime numbers $\ell$.

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 $\leq 500\,000$:

$$48.223\% \quad \rightarrow \quad 78.075\%.$$  
Serre curves  \quad Serre curves  
+ Max relative to obstruction mod 2

Moreover, for all such curves we have a description of the adelic image $G_E$. 
Let $G \subseteq GL_2(\mathbb{Z}/2\mathbb{Z})$ and write $\hat{G}$ for the full preimage of $G$ in $GL_2(\hat{\mathbb{Z}})$.

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

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

Thus the problem of deciding whether $E$ is a $G$-Serre curve is reduced to determining whether the commutator condition $[G_E, G_E] = [\hat{G}, \hat{G}]$ 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 $G \in \{2B, 2Cn\}$ and 72 if $G = 2Cs$.

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

$$[G_E, G_E] = [\hat{G}, \hat{G}] \pmod{9} \quad \text{and} \quad [G_E, G_E] = [\hat{G}, \hat{G}] \pmod{2^k}. \quad (2)$$
The first condition $G_E(9) = \text{GL}_2(\mathbb{Z}/9\mathbb{Z})$. 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 $[G_E, G_E] = [\hat{G}, \hat{G}]$. 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 $G \in \{2\text{Cs}, 2\text{B}, 2\text{Cn}\}$, then

$$[\text{GL}_2(\hat{\mathbb{Z}}) : G_E] = \begin{cases} 12 & G \in \{2\text{B}, 2\text{Cn}\} \\ 48 & G = 2\text{Cs} \end{cases}$$

Knowing the adelic index allows us to give a description of $G_E$. 
• Let $E$ be a 2Cn-Serre curve. Recall that $S_{2Cn} = \{2.2.0.1, 4.4.0.2, 8.4.0.1\}$. In particular, $G_E(2) = 2Cn$.

• Thus, $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ 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 $[\text{GL}_2(\mathbb{Z}_2) : G_E(2^\infty)] = 4$ 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 $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[4])$ and $\mathbb{Q}(\sqrt[4]{\Delta_E}) \subseteq \mathbb{Q}(E[\sqrt{\Delta_E}])$. 

Rakvi (University of Pennsylvania)
• Consider the elliptic curve $E$ with LMFDB label 392.a1 given by

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

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

$$G_E(4) = \langle \left( \begin{array}{cc} 2 & 3 \\ 3 & 3 \end{array} \right), \left( \begin{array}{cc} 1 & 3 \\ 1 & 0 \end{array} \right), \left( \begin{array}{cc} 2 & 1 \\ 3 & 1 \end{array} \right) \rangle \subseteq \text{GL}_2(\mathbb{Z}/4\mathbb{Z}).$$
$[\text{GL}_2(\hat{\mathbb{Z}}) : G_E] = 2 \cdot 3 \cdot 2 = 12$. 

\[
\begin{array}{c}
\mathbb{Q}(E[28]) \\
\downarrow \\
\mathbb{Q}(E[4]) \\
\downarrow \\
\mathbb{Q}(E[2]) \\
\downarrow \\
\mathbb{Q}(\sqrt{-7}) \\
\downarrow \\
\mathbb{Q}
\end{array}
\]
Using Magma and our above work, we compute that

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

Further, the adelic image \( G_E \subseteq \GL_2(\widehat{\mathbb{Z}}) \) is \( \widehat{G_E(28)} \).

Our result agrees up to conjugacy with the output of Zywina’s recent code.
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 $C_E$ associated with $E$ is defined by

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

In his thesis, Brau showed how to compute $c_E$ 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

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