# Serre curves relative to obstructions modulo 2

## Jacob Mayle and Rakvi

ABSTRACT. We consider elliptic curves $E/\mathbb{Q}$ for which the image of the adelic
Galois representation $\rho_E$ is as large as possible given a constraint on the image
modulo 2. For such curves, we give a characterization in terms of their $\ell$-adic
images, compute all examples of conductor at most 500,000, precisely describe
the image of $\rho_E$, and offer an application to the cyclicity problem. In this way,
we generalize some foundational results on Serre curves.

## 1. Introduction

Let $E/K$ be an elliptic curve defined over a number field $K$. Fix an alge-
braic closure $\overline{K}$ of $K$. Consider the adelic Galois representation of $E$, which is a
continuous homomorphism of profinite groups,

$$\rho_E \colon \operatorname{Gal}(\overline{K}/K) \longrightarrow \operatorname{Aut}(T(E))$$

that encodes the natural action of $\operatorname{Gal}(\overline{K}/K)$ on the adelic Tate module $T(E) \coloneqq$
$\varprojlim E[n]$ of $E$. We can identify $\operatorname{Aut}(T(E))$ with $\operatorname{GL}_2(\widehat{\mathbb{Z}})$ by choosing a $\widehat{\mathbb{Z}}$-basis for
$T(E)$. We will denote the image of $\rho_E$ in $\operatorname{GL}_2(\widehat{\mathbb{Z}})$ by $G_E$, which we understand
to be only defined up to conjugation in $\operatorname{GL}_2(\widehat{\mathbb{Z}})$. In a celebrated 1972 article [33],
Serre proved that if $E$ does not have complex multiplication, then $G_E$ is an open
subgroup of $\operatorname{GL}_2(\widehat{\mathbb{Z}})$, and hence is of finite index. In this sense, $G_E$ is a "large"
subgroup of $\operatorname{GL}_2(\widehat{\mathbb{Z}})$.

In fact, Greicius [14] constructed a cubic number field $K$ and an elliptic curve
$E/K$ such that $\rho_E$ is surjective. On the other hand, if $E$ is defined over $\mathbb{Q}$, then
Serre noted [33, Proposition 22] that by the Weil pairing and Kronecker–Weber
theorem,

$$(1.1) \qquad\qquad [\operatorname{GL}_2(\widehat{\mathbb{Z}}) : G_E] \geq 2.$$

Throughout the rest of this paper, we restrict our attention to elliptic curves defined
over $\mathbb{Q}$. A *Serre curve* is an elliptic curve $E/\mathbb{Q}$ for which $G_E$ is maximal, in the
sense that equality holds in (1.1). Such curves are abundant. Indeed, Jones [16]
proved that 100% of elliptic curves over $\mathbb{Q}$ are Serre curves in a suitable sense of
density. Serre curves have many applications (e.g., [1, 2, 3, 15, 17, 23, 37, 41])
largely because the adelic image $G_E$ of such a curve is readily known (it depends
only on the discriminant $\Delta_E$ of $E$).

---

Despite their abundance, until recently, only a few examples of Serre curves appeared in the literature. In 2015, Daniels [10] exhibited an infinite family, proving (for instance) that if $\ell$ is a prime number such that $\ell \notin \{2, 7\}$, then the elliptic curve given by

$$y^2 + xy = x^3 + \ell$$

is a Serre curve. In his Ph.D. thesis [25], the first author gave an algorithm that determines whether a given elliptic curve is a Serre curve. The algorithm is implemented in Sage. Running it on Cremona's database [9] (accessed via the LMFDB [39]) reveals that 1,477,879 of the 3,064,705 ($\approx 48.223\%$) curves of conductor at most 500,000 are Serre curves.

There is considerable interest in understanding the adelic image $G_E$ of an elliptic curve $E$. Mazur [26] articulated the overarching problem as follows: Given a subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, classify all elliptic curves $E/\mathbb{Q}$ such that the inclusion $G_E \subseteq G$ holds[1]. This problem is known as "Mazur's Program B" and Zywina [43] recently made a breakthrough on a computational variant of it. He gave an algorithm that, given a non-CM elliptic curve $E/\mathbb{Q}$ computes the adelic image $G_E$. Zywina's recent progress follows an earlier theoretical algorithm of Brau [5]. It also follows a vast body of work that aims to understand the images of $\ell$-adic and residual representations, which we now briefly discuss.

For a prime number $\ell$ and an integer $n \geq 2$, consider the $\ell$-adic and mod $n$ Galois representations of $E$,

$$\rho_{E,\ell^\infty} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \quad \text{and} \quad \rho_{E,n} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

These representations encode the natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\ell$-adic Tate module $T_\ell(E)$ and $n$-torsion subgroup $E[n]$ of $E$, respectively. Alternatively, they can be viewed as the composition of the adelic Galois representation $\rho_E$ with the natural projections $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, respectively. We write $G_E(\ell^\infty)$ and $G_E(n)$ for the images of $\rho_{E,\ell^\infty}$ and $\rho_{E,n}$, respectively. A second perspective on Serre's open image theorem [33] is that if $E$ does not have complex multiplication, then $\rho_{E,\ell^\infty}$ (and hence $\rho_{E,\ell}$) is surjective for all but finitely many prime numbers $\ell$.

Assume that $E$ does not have complex multiplication. In 2015, Zywina [44] gave an algorithm that computes a finite set of primes outside of which $\rho_{E,\ell}$ is surjective. In the same year, Zywina [42] and Sutherland [38] gave algorithms that compute the image of $\rho_{E,\ell}$ for any prime number $\ell$. Also that year, Rouse–Zureick-Brown [32] gave an algorithm that computes the image of $\rho_{E,2^\infty}$. In 2021, Rouse–Sutherland–Zureick-Brown [30] gave an algorithm that computes the image of $\rho_{E,\ell^\infty}$ for a given prime number $\ell$. There is also a growing body of research on entanglements [7, 12, 11, 13, 19, 27] that aims to understand images of mod $n$ representations for $n$ a product of at least two distinct primes.

In this paper, we study elliptic curves $E/\mathbb{Q}$ for which the adelic image $G_E$ is maximal relative to a prescribed obstruction. Roughly speaking, for an integer $n \geq 2$ and a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, an elliptic curve $E/\mathbb{Q}$ is a *G-Serre curve* if $G_E$ is "as large as possible" given the constraint that $G_E(n) \subseteq G$. This notion of a relative Serre curve was originally set forth by Jones in [16]. We give a proper definition and discuss the notion further in §2.

––––––––––

[1]In fact, Mazur posed this question for elliptic curves over number fields.

More specifically, in this paper we consider $G$-Serre curves for proper subgroups $G \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. The group $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is isomorphic to the symmetric group on 3 letters. Thus it has 3 proper subgroups up to conjugacy. These subgroups are of index 6, 3, and 2, and we denote them by $\mathtt{2Cs} \coloneqq \{(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})\}$, $\mathtt{2B} \coloneqq \langle (\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}) \rangle$, and $\mathtt{2Cn} \coloneqq \langle (\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}) \rangle$, respectively.

Our main theorem classifies $G$-Serre curves for subgroups $G \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. It relies crucially on the work of Rouse–Zureick-Brown on 2-adic images. This work was later subsumed by the work of Rouse–Sutherland–Zureick-Brown [**30**], which considers $\ell$-adic images more generally. Thus, in what follows, we write $\mathtt{A.B.C.D}$ for the subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ with the given RSZB label. Define the sets

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

With this notation in place, we now state our classification result.

THEOREM 1.1. *Let $G \in \{\mathtt{2Cs}, \mathtt{2B}, \mathtt{2Cn}\}$ and $E/\mathbb{Q}$ be an elliptic curve. We have that $E$ is a $G$-Serre curve if and only if $G_E(2^\infty) \in \mathcal{S}_G$ and $\rho_{E,\ell^\infty}$ is surjective for each odd prime $\ell$.*

We prove Theorem 1.1 in Section 2.3. Together with the work of Rouse–Sutherland–Zureick-Brown [**29, 30**], it yields an algorithm for determining whether a given elliptic curve is a $G$-Serre curve for a proper subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. We implemented this algorithm in Magma [**4**]. The code can be found in this paper's GitHub repository [**24**]:

https://github.com/maylejacobj/RelativeSerreCurves

There are 3,064,705 elliptic curves over $\mathbb{Q}$ of conductor at most 500,000 [**9**]. We find that of these, 83,637 ($\approx 2.729\%$) are $\mathtt{2Cs}$-Serre curves, 827,120 ($\approx 26.989\%$) are $\mathtt{2B}$-Serre curves, and 4,122 ($\approx 0.134\%$) are $\mathtt{2Cn}$-Serre curves. In total, 2,392,758 ($\approx 78.075\%$) curves of conductor at most 500,000 are either Serre curves or $G$-Serre curves for a proper subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. All of our computations were run on a machine with a 2.9 GHz 6-Core Intel Core i9 processor and 32 GB of memory.

In Section 3, we describe the adelic images of the considered $G$-Serre curves. In Section 4, we give an application of the above work to the cyclicity problem and briefly discuss other applications. In Section 5, we provide three detailed examples where we compute generators for the adelic Galois image using results of Section 3. Finally, in the appendix we give a table of minimal conductor $G$-Serre curves for each 2-adic image appearing in Theorem 1.1, including each curve's image conductor and cyclicity correction factor.

## 2. Characterization of relative Serre curves

In this section, we give a characterization of Serre curves relative to obstructions modulo 2. We begin by defining some notation and terminology, and giving some preliminaries.

Throughout this paper, $m$ and $n$ denote positive integers and $\ell$ denotes a prime number. We write $\mathbb{Z}_\ell$ to denote the ring of $\ell$-adic integers and $\widehat{\mathbb{Z}}$ for the ring of profinite integers. For a subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$, we write $G(\ell^\infty)$ and $G(n)$ for the images of $G$ under the natural projections $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, respectively. In the same way, if $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is a subgroup and $m$ divides $n$, then $G(m)$ denotes the image of $G$ under the natural projection $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. For a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we write $\widehat{G}$ for the preimage of $G$ under the natural projection $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Similarly if $G \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$, then $\widehat{G}$ denotes the preimage of $G$ under $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. For any profinite group $G$, we write $[G, G]$ to denote the closure of the commutator subgroup of $G$.

Let $E/\mathbb{Q}$ be an elliptic curve. Let $n \geq 2$ be an integer and $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a subgroup. We now define the notion of a $G$-Serre curve. Our definition is readily seen to be equivalent to the definition given by Jones [18], though our choice of notation is a bit better suited for our purposes. The definition (here and in [18]) is in terms of commutators, which offers a tractable condition to check in practice.

DEFINITION 2.1. We say that an elliptic curve $E/\mathbb{Q}$ is a $G$-*Serre curve* if $G_E(n) \subseteq G$ and $[G_E, G_E] = [\widehat{G}, \widehat{G}]$.

REMARK 2.2. It is possible that $E$ is a $G$-Serre curve yet $G_E(n)$ is a proper subgroup of $G$. For instance, consider the elliptic curve $E$ with LMFDB label 200.a1 given by the Weierstrass equation

$$y^2 = x^3 + 125x - 1250.$$

From the data provided in the "Galois representations" section of the curve's LMFDB page, we see that $E$ is a Serre curve. The property of an elliptic curve being a Serre curve is equivalent to it being a $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$-Serre curve for any $n$. In particular, $E$ is a $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$-Serre curve. However, the mod 8 Galois representation of $E$ is nonsurjective, i.e., $G_E(8)$ is a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$. While the phenomenon of $G_E(n) \subsetneq G$ is possible in general, we will see in Proposition 2.14 that if $E$ is a $G$-Serre curve for some $G \in \{\texttt{2Cs}, \texttt{2B}, \texttt{2Cn}\}$, then $G_E(2) = G$.

Next, we state a lemma that provides two useful properties of $G_E$ that follow from the Weil pairing and Kronecker–Weber theorem. In order to state it, we first recall some terminology. Let $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$ be a subgroup. We say that $H$ is *determinant-surjective* if $\det(H) = \widehat{\mathbb{Z}}^\times$. We say that $H$ is *commutator-thick* if $[H, H] = H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})$.

LEMMA 2.3. *If $E/\mathbb{Q}$ is an elliptic curve, then $G_E$ is determinant-surjective and commutator-thick.*

PROOF. See, for instance, [18, Remark 2.3] or [43, §1.2].                    □

The next lemma appears in [18, Remark 2.5] and is less well-known. It offers a second perspective on $G$-Serre curves in terms of the index of $G_E$. We relay its proof below.

LEMMA 2.4. *If $E$ is a $G$-Serre curve, then the index $[\widehat{G} : G_E]$ is minimal among the indices of determinant-surjective and commutator-thick subgroups of $\widehat{G}$.*

PROOF. Let $H$ be a determinant-surjective and commutator-thick subgroup of $\widehat{G}$. To prove the lemma, we need to show that $[\widehat{G} : G_E] \leq [\widehat{G} : H]$. Since $H$ is determinant-surjective we have the exact sequence for $H$,

$$1 \longrightarrow H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) \longrightarrow H \xrightarrow{\det} \widehat{\mathbb{Z}}^{\times} \longrightarrow 1.$$

As $H \subseteq \widehat{G}$, we have that $[H, H] \subseteq [\widehat{G}, \widehat{G}]$. Consequently,

$$[\widehat{G} : H] = [\widehat{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : H \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})] = [\widehat{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : [H, H]] \geq [\widehat{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\widehat{G}, \widehat{G}]].$$

As $G_E$ is determinant-surjective, commutator-thick, and satisfies $[G_E, G_E] = [\widehat{G}, \widehat{G}]$,

$$\begin{aligned} [\widehat{G} : G_E] &= [\widehat{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})] \\ &= [\widehat{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : [G_E, G_E]] \\ &= [\widehat{G} \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) : [\widehat{G}, \widehat{G}]]. \end{aligned}$$

Hence $[\widehat{G} : G_E] \leq [\widehat{G} : H]$, as needed.          □

The perspective on $G$-Serre curves conveyed by Lemma 2.4 more closely reflects the standard definition of a Serre curve in terms of the index of $G_E$. This point-of-view will be valuable when describing adelic images in Section 3.

**2.1. Reduction to a finite modulus.** Let $H$ be a subgroup of an open subgroup $G \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. In view of Definition 2.1, we turn to the problem of checking whether $[H, H] = [G, G]$ holds. Let $m$ be the *level* (sometimes called the *conductor*) of $G$, i.e., the least positive integer such that $G = \widehat{G(m)}$. As $G$ is open, such an $m$ must exist. The problem of checking whether $[H, H] = [G, G]$ can be simplified by the following theorem. When we state the result, we make an assumption on $m$ that by [**18**, Remark 2.8] allows us to use the value of $m_0$ as in the statement of the theorem rather than the larger value appearing in [**18**, Equation 10].

THEOREM 2.5. *Let $H \subseteq G$ be an open subgroup. There exists a constant $m_0$, depending on the group $G$, so that $[H, H] = [G, G]$ if and only if*

(1) *For each prime number $\ell \nmid m_0$, one has that $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq H(\ell)$ and*
(2) *One has that $[H(m_0), H(m_0)] = [G(m_0), G(m_0)]$.*

*If the level $m$ of $G$ is such that each prime $\ell$ dividing $m$ satisfies $\ell \not\equiv \pm 1 \pmod 5$, then $m_0$ may be taken to be the constant*

$$(2.1) \qquad\qquad m_0 := \mathrm{lcm}\left(2^3 \cdot 3^3, \prod_{\ell \mid m} \ell^{2\,\mathrm{ord}_\ell(m)+1}\right)$$

*where $\mathrm{ord}_\ell(m)$ denotes the exact power of $\ell$ dividing $m$.*

PROOF. See [**18**, Theorem 2.7 and Remark 2.8].          □

The above theorem is the starting point for our work. We are interested in the case of $m = 2$, where (2.1) gives a value of $m_0 = 216$ for the constant appearing in Theorem 2.5. We can reduce this constant as follows.

LEMMA 2.6. *In Theorem 2.5, we can take $m_0$ to be given by*

$$m_0 \coloneqq \begin{cases} 72 & G = \widehat{\mathtt{2Cs}} \\ 36 & G \in \left\{ \widehat{\mathtt{2B}}, \widehat{\mathtt{2Cn}} \right\} \end{cases}.$$

PROOF. For $G \in \{\widehat{\mathtt{2Cs}}, \widehat{\mathtt{2B}}, \widehat{\mathtt{2Cn}}\}$, let $m_1$ be the least positive integer dividing 216 such that for each maximal subgroup $K \subsetneq [G(216), G(216)]$, we have $K(m_1) \subsetneq [G(m_1), G(m_1)]$. Our `LevelLower1` script (available in the paper's GitHub repository [**24**]) computes $m_1$ directly by iterating over all maximal subgroups $K \subsetneq [G(216), G(216)]$. Running the script, we find that

$$m_1 = \begin{cases} 72 & G \in \left\{ \widehat{\mathtt{2Cs}}, \widehat{\mathtt{2B}} \right\} \\ 36 & G = \widehat{\mathtt{2Cn}}. \end{cases}$$

We can take $m_0$ to be $m_1$ in Theorem 2.5. This follows from the fact that $m_1$ is a multiple of 6 (which ensures that Theorem 2.5(1) is satisfied) and the definition of $m_1$ (which ensures that Theorem 2.5(2) is satisfied). In the case that $G = \widehat{\mathtt{2B}}$, we can lower $m_0$ further. Indeed, let $m_2$ be the least positive integer dividing 72 such that among all subgroups $K$ of $G = \widehat{\mathtt{2B}}$,

$$[K(m_2), K(m_2)] = [G(m_2), G(m_2)] \quad \implies \quad [K(72), K(72)] = [G(72), G(72)].$$

Our `LevelLower2` script [**24**] iterates over subgroups of $G(72)$ to compute that $m_2 = 36$ when $G = \widehat{\mathtt{2B}}$. Similarly as above, we can take $m_0$ to be $m_2$ in Theorem 2.5. $\qquad\square$

We break the proof of Lemma 2.6 down into two stages. In practice, this is worthwhile because `LevelLower1` is much more time efficient than `LevelLower2`.

**2.2. The group-theoretic characterization.** In this subsection, we consider possible group-theoretic entanglements to give a criterion on whether $[G, G] = [H, H]$ holds in the cases that we are considering. To this end, we begin by recalling the notion of a fiber product. Let $G_1$, $G_2$, and $Q$ be groups. Let $\psi_1 \colon G_1 \to Q$ and $\psi_2 \colon G_2 \to Q$ be surjective group homomorphisms. The *fiber product of $G_1$ and $G_2$ by* $\psi \coloneqq (\psi_1, \psi_2)$ is the subgroup

$$G_1 \times_\psi G_2 \coloneqq \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\} \subseteq G_1 \times G_2.$$

The group $G_1 \times_\psi G_2$ has the property that it surjects onto both $G_1$ and $G_2$ via the usual projection maps. Goursat's lemma gives that the only subgroups of $G_1 \times G_2$ that surject onto both factors are, in fact, fiber products (see, e.g., [**21**, p. 75] or [**5**, §1.2.2]).

We shall use the following lemma concerning commutators of fiber products.

LEMMA 2.7. *Let $G_1$, $G_2$, $Q$, and $\psi$ be as above. If $Q$ is cyclic, then*

$$[G_1 \times_\psi G_2, G_1 \times_\psi G_2] = [G_1, G_1] \times [G_2, G_2].$$

PROOF. See [**22**, p. 174] and [**7**, Lemma 2.3]. $\qquad\square$

To apply Lemma 2.7 in our context, we will need to understand the possible groups that can appear as $G_1, G_2$, and $Q$. Our next two lemmas help clarify this. We first set some notation. For a positive integer $n$ and a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, consider the set

$$\mathcal{M}(G) \coloneqq \{H \subseteq G : \det(H) = \det(G) \text{ and } [H, H] = [G, G]\}.$$

Now define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$,

$$K_1 := \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle,$$

$$K_2 := \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle,$$

$$K_3 := \left\langle \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \right\rangle.$$

Observe that $K_1(2) = \mathtt{2Cn}$ and $K_2(2) = K_3(2) = \mathtt{2Cs}$.

The next lemma specifies the sets $\mathcal{M}(G)$ for the groups $G$ that will be of relevance.

LEMMA 2.8. *Up to conjugacy, we have that*
- (1) $\mathcal{M}(\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})) = \{\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})\}$
- (2) $\mathcal{M}(\widehat{\mathtt{2Cn}}(4)) = \{\widehat{\mathtt{2Cn}}(4), K_1\}$
- (3) $\mathcal{M}(\widehat{\mathtt{2B}}(4)) = \{\widehat{\mathtt{2B}}(4))\}$
- (4) $\mathcal{M}(\widehat{\mathtt{2Cs}}(8)) = \{H \subseteq \widehat{\mathtt{2Cs}}(8) \,:\, H(4) \in \{\widehat{\mathtt{2Cs}}(4), K_2, K_3\} \text{ and } \det(H) = (\mathbb{Z}/8\mathbb{Z})^\times\}$.

PROOF. We have that (1) holds since if $H \in \mathcal{M}(\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}))$, then

$$\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) = [\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})] = [H, H] \subseteq H \quad \text{and} \quad \det(H) = (\mathbb{Z}/9\mathbb{Z})^\times.$$

Thus by considering the determinant map $H \xrightarrow{\det} (\mathbb{Z}/9\mathbb{Z})^\times$, we see that $H = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. For parts (2), (3), and (4), we compute the set $\mathcal{M}(G)$ using our $\mathtt{FullCommDet}$ script [**24**]. $\qquad\square$

In the previous lemma, our need to consider $\mathcal{M}(\widehat{\mathtt{2Cs}}(8))$ rather than just $\mathcal{M}(\widehat{\mathtt{2Cs}}(4))$ can be traced to the fact that $[\widehat{\mathtt{2Cs}}(4), \widehat{\mathtt{2Cs}}(4)]$ is trivial. The set $\mathcal{M}(\widehat{\mathtt{2Cs}}(8))$ is rather large compared to the other sets in Lemma 2.8; it contains 15 subgroups up to conjugacy.

Our next lemma describes the common quotients $Q$ that can appear for us in Lemma 2.7. For a group $G$, write $\mathrm{Quo}(G)$ to denote the set of *all* isomorphism classes of quotients $G/N$ for a normal subgroup $N \trianglelefteq G$. Note that this definition differs somewhat from elsewhere in the literature. We write $0$ for the trivial group and $\mathbb{Z}/n\mathbb{Z}$ for the cyclic group of order $n$.

LEMMA 2.9. *We have that*

$$\mathrm{Quo}(\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})) \cap \mathrm{Quo}(K)$$

$$= \begin{cases} \{0, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}\} & K \in \mathcal{M}(\widehat{\mathtt{2Cn}}(4)) \\ \{0, \mathbb{Z}/2\mathbb{Z}\} & K \in \mathcal{M}(\widehat{\mathtt{2B}}(4)) \cup \mathcal{M}(\widehat{\mathtt{2Cs}}(8)). \end{cases}$$

PROOF. We compute the intersections directly using our $\mathtt{QuoIntersection}$ script [**24**]. $\qquad\square$

We now state and prove our main group-theoretic proposition.

PROPOSITION 2.10. *Let $G \in \{\widehat{\mathtt{2Cs}}, \widehat{\mathtt{2B}}, \widehat{\mathtt{2Cn}}\}$ and let $m_0$ be as in Lemma 2.6. For a subgroup $H \subseteq G$ with $\det(H(m_0)) = (\mathbb{Z}/m_0\mathbb{Z})^\times$, we have that*

$$[H(m_0), H(m_0)] = [G(m_0), G(m_0)] \iff \begin{cases} H(9) = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) & and \\ H(2^k) \in \mathcal{M}(G(2^k)) \end{cases}$$

*where $k \in \{2, 3\}$ is such that $m_0 = 2^k \cdot 9$.*

PROOF. For the forward direction, note that by reducing modulo 9,

$$[H(9), H(9)] = [G(9), G(9)] \quad \text{and} \quad \det(H(9)) = (\mathbb{Z}/9\mathbb{Z})^\times.$$

Further, we have that $G(9) = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. Thus $H(9) \in \mathcal{M}(\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}))$, so by Lemma 2.8, $H(9) = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. Similarly, upon reducing modulo $2^k$, we find that $H(2^k) \in \mathcal{M}(G(2^k))$.

Now consider the reverse direction. By Goursat's lemma, $H(m_0)$ can be written as a fiber product

$$H(m_0) \cong \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \times_\psi H(2^k)$$

with $\psi = (\psi_1, \psi_2)$ where $\psi_1 \colon \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \to Q$ and $\psi_2 \colon H(2^k) \to Q$ are surjective homomorphisms onto a group $Q$. We have that $Q \in \mathrm{Quo}(\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})) \cap \mathrm{Quo}(H(2^k))$ is cyclic by Lemma 2.9. By Lemma 2.7, we conclude that $[H(m_0), H(m_0)] = [G(m_0), G(m_0)]$. □

**2.3. Relative Serre curves.** Proposition 2.10 shows (somewhat surprisingly) that only the $\ell$-adic Galois images of $E$ need to be considered when checking whether an elliptic curve $E/\mathbb{Q}$ is a Serre curve relative to an obstruction modulo 2. This is in contrast to the situation with usual Serre curves, where it is observed in [**7**] that whether $E$ is a Serre curve also depends on the mod 6 Galois image of $E$.

In this subsection, we prove Theorem 1.1, our characterization of Serre curves relative to obstructions modulo 2. We first give two lemmas that are used in the proof. The first is a lifting lemma for subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with surjective determinant.

LEMMA 2.11. *Let $\ell$ be an odd prime number and let $H \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup such that $\det(H) = \mathbb{Z}_\ell^\times$. If $\ell > 3$, then $H = \mathrm{GL}_2(\mathbb{Z}_\ell)$ if and only if $H(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. If $\ell = 3$, then $H = \mathrm{GL}_2(\mathbb{Z}_3)$ if and only if $H(9) = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$.*

PROOF. This follows from [**34**, Lemma 3, p. IV-23] and [**34**, Exercise 1b, p. IV-28]. See also [**14**, Corollary 2.13]. □

Recall that the sets $\mathcal{S}_{\mathtt{2Cs}}, \mathcal{S}_{\mathtt{2B}}$, and $\mathcal{S}_{\mathtt{2Cn}}$ of subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ were defined in §1. Our next lemma elucidates the connection between these sets and the problem at hand.

LEMMA 2.12. *For $G \in \{\mathtt{2Cs}, \mathtt{2B}, \mathtt{2Cn}\}$, we have that*

$$\mathcal{S}_G = \left\{ H \subseteq \mathrm{GL}_2(\mathbb{Z}_2) : H(2^k) \in \mathcal{M}(\widehat{G}(2^k)) \ \text{and} \ \exists E/\mathbb{Q} \ \text{with} \ G_E(2^\infty) = H \right\}$$

*where $k$ is as in the statement of Proposition 2.10.*

PROOF. Running our `ConstructSG` script [**24**] confirms that the claimed equality holds by iterating over all 1208 possible 2-adic images appearing in the database of Rouse–Zureick-Brown [**31**]. □

We now prove our main classification result.

PROOF OF THEOREM 1.1. Let $G \in \{\mathtt{2Cs}, \mathtt{2B}, \mathtt{2Cn}\}$. By Lemma 2.12, if $H \in \mathcal{S}_G$, then in particular, $H(2) \subseteq G$. Thus we assume that $E$ is such that $G_E(2) \subseteq G$. Hence $E$ is a $G$-Serre curve if and only if $[G_E, G_E] = [\widehat{G}, \widehat{G}]$. By Theorem 2.5 and Lemma 2.6, this commutator condition holds if and only if

(1) For each prime number $\ell \geq 5$, one has that $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq G_E(\ell)$ and

(2) One has that $[G_E(m_0), G_E(m_0)] = [G(m_0), G(m_0)]$.

By Lemma 2.11 and the fact that $G_E$ is determinant-surjective, we have that (1) is equivalent to $G_E(\ell^\infty) = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for each prime number $\ell \geq 5$. By Proposition 2.10, condition (2) is equivalent to $G_E(9) = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ and $G_E(2^k) \in \mathcal{M}(G_E(2^k))$ where $k$ is as in the statement of the proposition. The former of these is equivalent, by Lemma 2.11, to $G_E(3^\infty) = \mathrm{GL}_2(\mathbb{Z}_3)$. The latter is equivalent, by Lemma 2.12, to $G_E(2^\infty) \in \mathcal{S}_G$. □

The characterization that we just proved is well-suited for computations. For instance, if $E$ is in the LMFDB [**39**], then the data on $\ell$-adic images provided on the curve's page allows one to immediately decide, via Theorem 1.1, whether $E$ is a $G$-Serre curve for some $G \in \{2\mathtt{Cs}, 2\mathtt{B}, 2\mathtt{Cn}\}$. More generally, our `IsRelSerreCurve` script [**24**] uses Theorem 1.1 with [**29, 30**] to decide if $E$ is a $G$-Serre curve for such a $G$.

**2.4. The adelic index.** In this subsection, we determine the adelic index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E]$ for Serre curves $E/\mathbb{Q}$ relative to obstructions modulo 2. We start with a lemma.

LEMMA 2.13. *For $G \in \{2\mathtt{Cs}, 2\mathtt{B}, 2\mathtt{Cn}\}$, we have that*

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

PROOF. Let $G \in \{2\mathtt{Cs}, 2\mathtt{B}, 2\mathtt{Cn}\}$ and consider the subgroup $K := [\widehat{G}, \widehat{G}] \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}})$. By [**43**, Lemma 7.4], we have that $K$ is the preimage of $K(4)$ under the natural projection $\mathrm{SL}_2(\widehat{\mathbb{Z}}) \to \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$. It follows that

$$[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : K] = [\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) : K(4)].$$

The right-hand side is straightforward to compute in Magma because $K(4) = [\widehat{G}(4), \widehat{G}(4)]$. We do so using our `CommIndx` script [**24**], and obtain the claimed indices. □

Using Lemma 2.4 and Lemma 2.13, we now give a second characterization of the considered relative Serre curves in terms of the adelic index.

PROPOSITION 2.14. *For $G \in \{2\mathtt{Cs}, 2\mathtt{B}, 2\mathtt{Cn}\}$, an elliptic curve $E/\mathbb{Q}$ is a $G$-Serre curve if and only if*

$$(2.2) \qquad G_E(2) = G \quad and \quad [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = \begin{cases} 12 & G \in \{2\mathtt{B}, 2\mathtt{Cn}\} \\ 48 & G = 2\mathtt{Cs}. \end{cases}$$

PROOF. For any elliptic curve $E/\mathbb{Q}$, by Lemma 2.3 and the fact that

$$G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \ker(G_E \xrightarrow{\det} \widehat{\mathbb{Z}}^\times),$$

we observe that

$$(2.3) \qquad [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : G_E \cap \mathrm{SL}_2(\widehat{\mathbb{Z}})] = [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : [G_E, G_E]].$$

Suppose first that $E$ is a $G$-Serre curve. Then $[G_E, G_E] = [\widehat{G}, \widehat{G}]$, so the claim about the index of $G_E$ follows by (2.3) and Lemma 2.13. The claim that $G_E(2) = G$ follows by Theorem 1.1 and noting that $H(2) = G$ for each $H \in \mathcal{S}_G$. For the reverse direction, note that $G_E(2) = G$ implies that $G_E \subseteq \widehat{G}$. Hence $[G_E, G_E] \subseteq [\widehat{G}, \widehat{G}]$ and, in fact, equality holds by (2.3) and Lemma 2.13. □

### 3. Explicit descriptions of adelic images

In this section, we describe the adelic image $G_E$ of elliptic curves $E/\mathbb{Q}$ relative to obstructions modulo 2. We begin with some preliminaries on division fields. The *n-division field* of $E$ is the field $\mathbb{Q}(E[n])$ obtained by adjoining to $\mathbb{Q}$ all $x$- and $y$-coordinates of points in the $n$-torsion subgroup $E[n]$ of $E$. Recall that $\mathbb{Q}(E[n])/\mathbb{Q}$ is Galois and

$$G_E(n) \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}).$$

Define $\zeta_n := e^{\frac{2\pi i}{n}}$. Recall that by the Weil pairing on $E$,

$$(3.1) \qquad\qquad \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n]).$$

We begin by recalling a result that precisely describes the $2^k$-division field of an elliptic curve $E/\mathbb{Q}$ for $k \in \{1, 2, 3\}$. Fix an equation for $E$ of the form

$$(3.2) \qquad\qquad y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

for some $\alpha_1, \alpha_2, \alpha_3$ in the field $\overline{\mathbb{Q}}$ of algebraic numbers. Fix $A_1, A_2, A_3 \in \overline{\mathbb{Q}}$ so that

$$A_i^2 = \alpha_{i+1} - \alpha_{i+2}$$

where $i$ is considered modulo 3. Now set $B_1, B_2, B_3 \in \overline{\mathbb{Q}}$ so that

$$B_i^2 = A_i(A_{i+1} + \zeta_4 A_{i+2}).$$

With notation in place, we now state the result on 2-power division fields.

THEOREM 3.1. *We have the following.*

(1) $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$,
(2) $\mathbb{Q}(E[4]) = \mathbb{Q}(E[2], \zeta_4, A_1, A_2, A_3)$, *and*
(3) $\mathbb{Q}(E[8]) = \mathbb{Q}(E[4], \zeta_8, B_1, B_2, B_3)$.

PROOF. Part (1) is well-known. See [**40**, Theorem 1] for parts (2) and (3). $\square$

COROLLARY 3.2. *If $\sqrt{2} \in \mathbb{Q}(E[4])$, then $[\mathbb{Q}(E[8]) : \mathbb{Q}(E[4])] \leq 8$.*

PROOF. As $\zeta_4 \in \mathbb{Q}(E[4])$ and $\sqrt{2} \in \mathbb{Q}(E[4])$, we have $\zeta_8 \in \mathbb{Q}(E[4])$. Since, $B_i^2 \in \mathbb{Q}(E[4])$ for each $i \in \{1, 2, 3\}$, $[\mathbb{Q}(B_1, B_2, B_3) : \mathbb{Q}] \leq 8$, so the claim follows by Theorem 3.1. $\square$

We will make extensive use of Theorem 3.1 and Corollary 3.2 in this section. Let $\Delta_E$ denote the discriminant of any model of $E$. An immediate consequence of the theorem is that $\sqrt{\Delta_E} \in \mathbb{Q}(E[2])$ and $\sqrt[4]{\Delta_E} \in \mathbb{Q}(E[4])$ since, up to 12th powers, we compute from (3.2) that

$$(3.3) \qquad\qquad \Delta_E = 16(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

In view of (3.1), it is useful to review an aspect of cyclotomic fields. Namely, the Kronecker–Weber theorem gives that if $K/\mathbb{Q}$ is abelian, then there exists an integer $n$ such that $K \subseteq \mathbb{Q}(\zeta_n)$. The *conductor* of $K$, denoted $f(K)$, is the least positive integer $n$ with this property. Let $\Delta_K$ denote the discriminant of the ring of integers of $K$. If $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field, then it is well-known that

$$(3.4) \qquad\qquad f(K) = \Delta_K = \begin{cases} d & d \equiv 1 \pmod 4 \\ 4d & \text{otherwise.} \end{cases}$$

If $K/\mathbb{Q}$ is a cyclic cubic extension, then by the conductor-discriminant formula [**8**, 7.4.13, 7.4.14], we have that

$$(3.5) \qquad f(K) = \sqrt{\Delta_K}.$$

In Theorem 1.1 we learned that entanglements need not be considered when checking if an elliptic curve is Serre curve relative to an obstruction modulo 2. However in this section, entanglements will play an essential role in our descriptions of $G_E$. As such, we recall some preliminaries on entanglement fields. Let $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ be Galois extensions of $\mathbb{Q}$. The compositum $K_1K_2/\mathbb{Q}$ is Galois with

$$(3.6) \qquad \mathrm{Gal}(K_1K_2/\mathbb{Q}) \cong \mathrm{Gal}(K_1/\mathbb{Q}) \times_\psi \mathrm{Gal}(K_2/\mathbb{Q})$$

where $\psi := (\psi_1, \psi_2)$ with each map $\psi_i \colon \mathrm{Gal}(K_i/\mathbb{Q}) \to \mathrm{Gal}(K_1 \cap K_2/\mathbb{Q})$ given by restriction (see, e.g., [**5**, Lemma 1.2.8]). The field $K_1 \cap K_2$ is called the *entanglement field*. We refer to the degree $[K_1 \cap K_2 : \mathbb{Q}]$ as the degree of the entanglement between $K_1$ and $K_2$. By (3.6), we have that

$$(3.7) \qquad [K_1K_2 : \mathbb{Q}] = \frac{[K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]}{[K_1 \cap K_2 : \mathbb{Q}]}.$$

With these preliminaries in hand, we now turn to the problem of describing $G_E$.

**3.1. Serre curves relative to 2Cs.** Let $E$ be a 2Cs-Serre curve. Fix an equation

$$(3.8) \qquad E \colon y^2 = (x-a)(x-b)(x-c)$$

with $a, b, c \in \mathbb{Z}$. By Proposition 2.14, we know that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = 48.$$

Recall that by Theorem 1.1, we have $G_E(2^\infty) \in \mathcal{S}_{2\mathrm{Cs}}$ where

$$\mathcal{S}_{2\mathrm{Cs}} = \{\texttt{2.6.0.1}, \texttt{8.12.0.2}, \texttt{4.12.0.2}, \texttt{8.12.0.1}, \texttt{4.12.0.1}, \texttt{8.12.0.3},$$
$$\texttt{8.24.0.5}, \texttt{8.24.0.7}, \texttt{8.24.0.2}, \texttt{8.24.0.1}, \texttt{8.12.0.4}, \texttt{8.24.0.6},$$
$$\texttt{8.24.0.8}, \texttt{8.24.0.3}, \texttt{8.24.0.4}\}.$$

The above groups have index $6, 12$, or $24$ in $\mathrm{GL}_2(\mathbb{Z}_2)$, as indicated by the second number in the RSZB label. Hence to understand $G_E$, it remains to account for an index of 8 in the first case above, 4 in the second, and 2 in the third case. As we shall see, entanglements are the source of the greater adelic index in all cases.

For a squarefree integer $N$, define

$$(3.9) \qquad N' := \begin{cases} N & N \equiv 1 \pmod 4 \\ -N & N \equiv 3 \pmod 4 \\ \frac{1}{2}N & N \equiv 2 \pmod 8 \\ -\frac{1}{2}N & N \equiv 6 \pmod 8. \end{cases}$$

Note that $N' \in \mathbb{Z}$ and that since $N$ is squarefree, we must have that $N \not\equiv 0 \pmod 4$. Further the definition in (3.9) is such that $N' \equiv 1 \pmod 4$ for any squarefree integer $N$. Therefore, $\sqrt{N'} \in \mathbb{Q}(\zeta_{|N'|})$ which will be used later.

Let $A := a - b$, $B := a - c$, and $C := b - c$. Consider the following set

$$S := \{\pm A_{\mathrm{sf}}, \pm B_{\mathrm{sf}}, \pm C_{\mathrm{sf}}, \pm AB_{\mathrm{sf}}, \pm AC_{\mathrm{sf}}, \pm BC_{\mathrm{sf}}, \pm ABC_{\mathrm{sf}}\}$$

where $n_{\mathrm{sf}}$ denotes the squarefree part of an integer $n$ and, for instance, $AB_{\mathrm{sf}} := (AB)_{\mathrm{sf}}$. Observe that the set $S$ is partially ordered with respect to divisibility. If $[\mathrm{GL}_2(\mathbb{Z}_2) : G_E(2^\infty)] = 6$, then let $N_1, N_2, N_3 \in S$ be minimal with respect to divisibility in $S$ such that they are distinct (up to sign) and not $\pm 1$ or $\pm 2$. Similarly if $[\mathrm{GL}_2(\mathbb{Z}_2) : G_E(2^\infty)] = 12$ (resp. $[\mathrm{GL}_2(\mathbb{Z}_2) : G_E(2^\infty)] = 24$), let $N_1, N_2$ (resp. $N_1$) be chosen from $S$ in the same way as in the index 6 case. The proof of Lemma 3.3 justifies why the $N_i$ may be chosen in this way. In each of the three cases, for each $i$, set

$$(3.10) \qquad k_i = \begin{cases} 3 & N_i \equiv 0 \pmod 2 \\ 2 & N_i \equiv 1 \pmod 2. \end{cases}$$

We now give a lemma that describes the entanglements associated with $G_E$.

LEMMA 3.3. *If $G_E(2^\infty) = $ `2.6.0.1`, then for each $i \in \{1, 2, 3\}$, there is a quadratic entanglement between $\mathbb{Q}(E[2^{k_i}])$ and $\mathbb{Q}(E[|N_i'|])$. If*

$$G_E(2^\infty) \in \{\mathtt{8.12.0.2}, \mathtt{4.12.0.2}, \mathtt{8.12.0.1}, \mathtt{4.12.0.1}, \mathtt{8.12.0.3}, \mathtt{8.12.0.4}\},$$

*then for each $i \in \{1, 2\}$, there is a quadratic entanglement between $\mathbb{Q}(E[2^{k_i}])$ and $\mathbb{Q}(E[|N_i'|])$. For all the other cases, there is a quadratic entanglement between $\mathbb{Q}(E[2^{k_1}])$ and $\mathbb{Q}(E[|N_1'|])$.*

PROOF. By Theorem 3.1(2), we have that

$$\mathbb{Q}(E[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{A_{\mathrm{sf}}}, \sqrt{B_{\mathrm{sf}}}, \sqrt{C_{\mathrm{sf}}}).$$

Thus the quadratic subfields of $\mathbb{Q}(E[4])$ are the following:

$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{A_{\mathrm{sf}}}), \mathbb{Q}(\sqrt{B_{\mathrm{sf}}}), \mathbb{Q}(\sqrt{C_{\mathrm{sf}}}), \mathbb{Q}(\sqrt{AB_{\mathrm{sf}}}), \mathbb{Q}(\sqrt{AC_{\mathrm{sf}}}),$$
$$\mathbb{Q}(\sqrt{BC_{\mathrm{sf}}}), \mathbb{Q}(\sqrt{ABC_{\mathrm{sf}}}), \mathbb{Q}(\sqrt{-A_{\mathrm{sf}}}), \mathbb{Q}(\sqrt{-B_{\mathrm{sf}}}), \mathbb{Q}(\sqrt{-C_{\mathrm{sf}}}),$$
$$\mathbb{Q}(\sqrt{-AB_{\mathrm{sf}}}), \mathbb{Q}(\sqrt{-AC_{\mathrm{sf}}}), \mathbb{Q}(\sqrt{-BC_{\mathrm{sf}}}), \text{ and } \mathbb{Q}(\sqrt{-ABC_{\mathrm{sf}}}).$$

First assume that $G_E(2^\infty) = $ `2.6.0.1`. We verify in Magma that `2.6.0.1`(4) contains exactly 15 index 2 subgroups. Hence $\mathbb{Q}(E[4])$ has exactly $15 = 2^4 - 1$ quadratic subfields, so all of the above subfields are distinct. Moreover, since `2.6.0.1`(8) is the full preimage of `2.6.0.1`(4) under the reduction map $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ we know that $\sqrt{2} \notin \mathbb{Q}(E[4])$ by Corollary 3.2. Thus we may indeed choose $N_1, N_2, N_3 \in S$ as specified above the lemma. By (3.4) and Theorem 3.1, we observe that $\sqrt{N_i'} \in \mathbb{Q}(E[2^{k_i}]) \cap \mathbb{Q}(E[|N_i'|])$ provides a quadratic entanglement.

If $H \in \{\mathtt{8.12.0.2}, \mathtt{8.12.0.1}, \mathtt{8.12.0.3}, \mathtt{8.12.0.4}\}$, then $H(4)$ still contains exactly 15 index 2 subgroups. Hence $\mathbb{Q}(E[4])$ has exactly $15 = 2^4 - 1$ quadratic subfields. But in this case, $\sqrt{2} \in \mathbb{Q}(E[4])$ is possible, so we may only choose $N_1, N_2 \in S$ as specified above the lemma. In all of the remaining cases, we calculate in a similar way that $\mathbb{Q}(E[4])$ has $7 = 2^3 - 1$ quadratic subfields. If $H \in \{\mathtt{4.12.0.2}, \mathtt{4.12.0.1}\}$, then $H(8)$ is the full preimage of $H(4)$, so we know that $\sqrt{2} \notin \mathbb{Q}(E[4])$ by Corollary 3.2, and hence we may choose $N_1, N_2$ as specified. On the other hand, if $H \in \{\mathtt{8.24.0.5}, \mathtt{8.24.0.7}, \mathtt{8.24.0.2}, \mathtt{8.24.0.1}, \mathtt{8.24.0.6}, \mathtt{8.24.0.8}, \mathtt{8.24.0.3}, \mathtt{8.24.0.4}\}$, then it may be $\sqrt{2} \in \mathbb{Q}(E[4])$, but as $\mathbb{Q}(E[4])$ contains 7 quadratic subfields, we are still able to choose $N_1$ as specified. $\square$

3.1.1. *Description of image.* We now describe the adelic image $G_E$ of a $\mathtt{2Cs}$-Serre curve $E$. Let $N_i$ and $k_i$ be as in Lemma 3.3. For each $i$, let $G_i \subseteq G_E(2^{k_i})$ be such that $G_E(2^{k_i})/G_i \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{N_i'})/\mathbb{Q}) \cong \{\pm 1\}$. Let $\epsilon_i \colon G_E(2^{k_i}) \to G_E(2^{k_i})/G_i$ be the quadratic character and $\chi_{N_i'}$ be the Dirichlet character given by the unique surjective homomorphism $\widehat{\mathbb{Z}}^\times \to \mathrm{Gal}(\mathbb{Q}(\sqrt{N_i'})/\mathbb{Q}) \cong \{\pm 1\}$.

PROPOSITION 3.4. *With notation as above, if $E$ is a $\mathtt{2Cs}$-Serre curve, then*

$$G_E = \bigcap_i \{A \in \widehat{G_E(2^\infty)} | \epsilon_i(A) = \chi_{N_i'}(\det(A))\}.$$

*Here the intersection runs over $i$ such that $N_i$ is defined for $G_E(2^\infty)$.*

PROOF. Assume that $G_E(2^\infty) = \mathtt{2.6.0.1}$. The inclusion

$$(3.11) \qquad G_E \subseteq \bigcap_{i=1}^{3} \{A \in \widehat{G_E(2^\infty)} | \epsilon_i(A) = \chi_{N_i'}(\det(A))\}$$

follows from the containments $\mathbb{Q}(\sqrt{N_i'}) \subseteq \mathbb{Q}(E[2^{k_i}])$ and $\mathbb{Q}(\sqrt{N_i'}) \subseteq \mathbb{Q}(E[|N_i'|])$. By Proposition 2.14, to establish that (3.11) is actually an equality, it suffices to note that

$$(3.12) \qquad \left[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \bigcap_{i=1}^{3} \{A \in \widehat{G_E(2^\infty)} | \epsilon_i(A) = \chi_{N_i'}(\det(A))\}\right] = 48.$$

Observe that $\widehat{G_E(2^\infty)} = G_E(2^\infty) \times \prod_{\ell \text{ odd}} \mathrm{GL}_2(\mathbb{Z}_\ell)$. As each $N_i'$ is odd for $i \in \{1,2,3\}$, we can think of $\{A \in \widehat{G_E(2^\infty)} | \epsilon_i(A) = \chi_{N_i'}(\det(A))\}$ as the fiber product of $G_E(2^\infty)$ and $\prod_{\ell \text{ odd}} \mathrm{GL}_2(\mathbb{Z}_\ell)$ by $(\epsilon_i, \chi_{N_i'} \circ \det)$ which is index 2 in $\widehat{G_E(2^\infty)}$. Indeed, as $N_i'$ are distinct, we have that

$$\left[\widehat{G_E(2^\infty)} : \bigcap_{i=1}^{3} \{A \in \widehat{G_E(2^\infty)} | \epsilon_i(A) = \chi_{N_i'}(\det(A))\}\right] = 8.$$

Moreover,

$$\left[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \widehat{G_E(2^\infty)}\right] = [\mathrm{GL}_2(\mathbb{Z}_2) : G_E(2^\infty)] = 6.$$

Thus (3.12) holds as claimed. There are two remaining cases to consider, namely, when the index of $G_E(2^\infty)$ in $\mathrm{GL}_2(\mathbb{Z}_2)$ is 12 and 24. Both of these cases follow similarly to the case of $G_E(2^\infty) = \mathtt{2.6.0.1}$ just considered, and hence are omitted. $\square$

Let $m_E$ denote the *image conductor* of $E$, i.e., the level of the group $G_E \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$. From the above proposition, we obtain the following formula for $m_E$ in terms of the integers $N_i$ after noting that the level of each $H \in \mathcal{S}_{\mathtt{2Cs}}$ in $\mathrm{GL}_2(\mathbb{Z}_2)$ is always at most 8 (recall the 2-adic level is the first number in the RSZB label).

COROLLARY 3.5. *Let $E/\mathbb{Q}$ be a $\mathtt{2Cs}$-Serre curve with $G_E(2^\infty) = \mathtt{A.B.C.D}$.*
- *If $\mathtt{B} = 6$ (i.e., $G_E(2^\infty) = \mathtt{2.6.0.1}$), then*

$$m_E = \begin{cases} \mathrm{lcm}(4, |N_1'|, |N_2'|, |N_3'|) & 2 \nmid N_1 N_2 N_3 \\ \mathrm{lcm}(8, |N_1'|, |N_2'|, |N_3'|) & 2 \mid N_1 N_2 N_3. \end{cases}$$

- If $\mathtt{B} = 12$, then
$$m_E = \begin{cases} \operatorname{lcm}(4, |N_1'|, |N_2'|) & 2 \nmid N_1 N_2 \text{ and } \mathtt{A} = 4 \\ \operatorname{lcm}(8, |N_1'|, |N_2'|) & 2 \mid N_1 N_2 \text{ or } \mathtt{A} = 8. \end{cases}$$

- If $\mathtt{B} = 24$, then $m_E = \operatorname{lcm}(8, |N_1'|)$.

PROOF. Assume $G_E(2^\infty) = \mathtt{2.6.0.1}$. Since $m_E$ is the level of $G_E$, by Proposition 3.4 it is the smallest positive integer that is a multiple of $2^k, |N_1'|, |N_2'|, |N_3'|$. The proof is similar for the other cases. The corollary now follows. $\qquad\square$

**3.2. Serre curves relative to 2B.** Let $E$ be a $\mathtt{2B}$-Serre curve. Fix an equation

(3.13)                              $E\colon y^2 = (x^2 + ax + b)(x + c)$

with $a, b, c \in \mathbb{Z}$ and $x^2 + ax + b$ irreducible over $\mathbb{Q}$. By Proposition 2.14, we know that
$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = 12.$$
Recall that
$$\mathcal{S}_{\mathtt{2B}} = \{\mathtt{2.3.0.1}, \mathtt{8.6.0.2}, \mathtt{8.6.0.4}, \mathtt{8.6.0.1}, \mathtt{8.6.0.6}, \mathtt{8.6.0.3}, \mathtt{8.6.0.5}\}.$$
Consequently,

(3.14)                $[\mathrm{GL}_2(\mathbb{Z}_2) : G_E(2^\infty)] = \begin{cases} 3 & G_E(2^\infty) = \mathtt{2.3.0.1} \\ 6 & \text{otherwise.} \end{cases}$

Hence to understand $G_E$, it remains to account for an index of 4 if $G_E = \mathtt{2.3.0.1}$ and 2 otherwise. Considering each of the groups in $\mathcal{S}_{\mathtt{2B}}$ under reduction modulo 4, we verify in Magma the following useful observation: If $E$ is any $\mathtt{2B}$-Serre curve, then
(3.15)
$\quad [\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) : G_E(4)] = 3 \quad$ and $\quad G_E(4)$ contains exactly 7 index 2 subgroups.

The roots of $(x^2 + ax + b)(x + c)$ are
$$r_1 := \frac{1}{2}\left(\sqrt{a^2 - 4b} - a\right), \quad r_2 := \frac{1}{2}\left(-\sqrt{a^2 - 4b} - a\right), \text{ and } \quad r_3 := -c.$$
Let $A := r_1 - r_2$, $B := r_2 - r_3$, and $C := r_1 - r_3$. From Theorem 3.1, we now deduce an alternative expression for the 4-division field of $E$ in terms of the notation just introduced.

LEMMA 3.6. *With notation as above, if $E$ is a $\mathtt{2B}$-Serre curve, then*
$$\mathbb{Q}(E[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{a^2 - 4b}, \sqrt{ac - c^2 - b}, \sqrt{A}, \sqrt{B}).$$

PROOF. By Theorem 3.1(2), we have that
$$\mathbb{Q}(E[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{A}, \sqrt{B}, \sqrt{C}).$$
We have that $\sqrt{C} \in \mathbb{Q}(\sqrt{-1}, \sqrt{a^2 - 4b}, \sqrt{ac - c^2 - b}, \sqrt{A}, \sqrt{B})$ because

(3.16)                              $\sqrt{B}\sqrt{C} = \sqrt{-1}\sqrt{ac - b - c^2}.$

It follows that
$$\mathbb{Q}(E[4]) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{a^2 - 4b}, \sqrt{ac - c^2 - b}, \sqrt{A}, \sqrt{B}).$$
The reverse inclusion follows by (3.16) and the fact that $A = \sqrt{a^2 - 4b}$. $\qquad\square$

Recall that by (3.15), there are exactly seven distinct quadratic subfields of $\mathbb{Q}(E[4])$. Using Lemma 3.6, we now describe them explicitly.

LEMMA 3.7. *With notation as above, if $E$ is a* 2B*-Serre curve, then $\mathbb{Q}(E[4])$ has exactly 7 distinct quadratic subfields :* $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{\pm \Delta_E})$, $\mathbb{Q}(\sqrt{\pm(ac - c^2 - b)})$, *and* $\mathbb{Q}(\sqrt{\pm(ac - c^2 - b)\Delta_E})$.

PROOF. By (3.3), we note that $\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(\sqrt{a^2 - 4b})$. Thus it suffices to show that

$$[\mathbb{Q}(\sqrt{-1}, \sqrt{a^2 - 4b}, \sqrt{ac - c^2 - b}) : \mathbb{Q}] = 8.$$

We have that $A = \sqrt{a^2 - 4b}$ and $B = \frac{1}{2}\left(-\sqrt{a^2 - 4b} - a\right) + c$. Thus

$$\sqrt{a^2 - 4b} \in \mathbb{Q}(\sqrt{A}) \cap \mathbb{Q}(\sqrt{B}),$$

so in particular $[\mathbb{Q}(\sqrt{A}) \cap \mathbb{Q}(\sqrt{B}) : \mathbb{Q}] \geq 2$. Hence it follows by (3.7) that

$$[\mathbb{Q}(\sqrt{A}, \sqrt{B}) : \mathbb{Q}] = \frac{[\mathbb{Q}(\sqrt{A}) : \mathbb{Q}][\mathbb{Q}(\sqrt{B}) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt{A}) \cap \mathbb{Q}(\sqrt{B}) : \mathbb{Q}]} \leq \frac{4 \cdot 4}{2} = 8$$

Thus, by (3.7),(3.15), and Lemma 3.6 ,

$$32 = [\mathbb{Q}(E[4]) : \mathbb{Q}] \leq \frac{[\mathbb{Q}(\sqrt{-1}, \sqrt{a^2 - 4b}, \sqrt{ac - c^2 - b}) : \mathbb{Q}] \cdot 8}{2}$$

Hence

$$[\mathbb{Q}(\sqrt{-1}, \sqrt{a^2 - 4b}, \sqrt{ac - c^2 - b}) : \mathbb{Q}] \geq 8.$$

The reverse inequality is clear.                                                    □

We now consider entanglements. Define the set

$$S := \{\pm(a^2 - 4b)_{\mathrm{sf}}, \pm(ac - c^2 - b)_{\mathrm{sf}}, \pm((ac - c^2 - b)(a^2 - 4b))_{\mathrm{sf}}\}.$$

If $G_E(2^\infty) = $ 2.3.0.1, then let $N_1$ and $N_2$ be distinct (up to sign) and minimal with respect to divisibility in $S$. Using Corollary 3.2 we note that $\sqrt{2}, \sqrt{-2} \notin \mathbb{Q}(E[4])$, since $\#$2.3.0.1$(8) = 16 \cdot \#$2.3.0.1$(4)$, so $N_i' \neq 1$. We get two horizontal entanglements between $\mathbb{Q}(E[2^{k_i}])$ and $\mathbb{Q}(E[|N_i'|])$ for $i \in \{1, 2\}$. If $G_E(2^\infty) \neq $ 2.3.0.1, then let $N_1$ be minimal with respect to divisibility in $S$ such that $N_1' \neq 1$. In this case, we get one horizontal entanglement between $\mathbb{Q}(E[2^{k_1}])$ and $\mathbb{Q}(E[|N_1'|])$.

3.2.1. *Description of image.* We now describe the adelic image $G_E$ of a 2B-Serre curve $E$. Let $N_i$ be as above and let $k_i$ be as in (3.10). For each $i$, let $G_i \subseteq G_E(2^{k_i})$ be such that $G_E(2^{k_i})/G_i \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{N_i'})/\mathbb{Q}) \cong \{\pm 1\}$. Let $\epsilon_i : G_E(2^{k_i}) \to G_E(2^{k_i})/G_i$ be the quadratic character and $\chi_{N_i'}$ be the Dirichlet character given by the unique surjective homomorphism $\widehat{\mathbb{Z}}^\times \to \mathrm{Gal}(\mathbb{Q}(\sqrt{N_i'})/\mathbb{Q}) \cong \{\pm 1\}$.

PROPOSITION 3.8. *With notation as above, if $G_E(2^\infty) = $ 2.3.0.1, then*

$$G_E = \bigcap_{i=1}^{2} \{A \in \widehat{G_E(2^\infty)} | \epsilon_i(A) = \chi_{N_i'}(\det(A))\}$$

*for $i \in \{1, 2\}$. If $G_E(2^\infty) \neq $ 2.3.0.1, then*

$$G_E = \{A \in \widehat{G_E(2^\infty)} | \epsilon(A) = \chi_{N_1'}(\det(A))\}.$$

PROOF. Assume that $G_E(2^\infty) = \texttt{2.3.0.1}$. The inclusion

$$(3.17) \qquad G_E \subseteq \bigcap_{i=1}^{2} \{A \in \widehat{G_E(2^\infty)} | \epsilon_i(A) = \chi_{N_i'}(\det(A))\}$$

follows from the containments $\mathbb{Q}(\sqrt{N_i'}) \subseteq \mathbb{Q}(E[2^{k_i}])$ and $\mathbb{Q}(\sqrt{N_i'}) \subseteq \mathbb{Q}(E[|N_i'|])$. By Proposition 2.14, to establish that (3.17) is actually an equality, it suffices to note that

$$(3.18) \qquad \left[ \mathrm{GL}_2(\widehat{\mathbb{Z}}) : \bigcap_{i=1}^{2} \{A \in \widehat{G_E(2^\infty)} | \epsilon_i(A) = \chi_{N_i'}(\det(A))\} \right] = 12.$$

From (3.14), we have that

$$\left[ \mathrm{GL}_2(\widehat{\mathbb{Z}}) : \widehat{G_E(2^\infty)} \right] = [\mathrm{GL}_2(\mathbb{Z}_2) : G_E(2^\infty)] = 3.$$

Similar to the proof given in Proposition 3.4, we can show that

$$\left[ \widehat{G_E(2^\infty)} : \bigcap_{i=1}^{2} \{A \in \widehat{G_E(2^\infty)} | \epsilon_i(A) = \chi_{N_i'}(\det(A))\} \right] = 4.$$

. Thus (3.12) holds as claimed. When $G_E(2^\infty) \neq \texttt{2.3.0.1}$ the proof is similar. $\square$

From the above proposition, we obtain the following formula for $m_E$ upon noting that the level of $\texttt{2.3.0.1}$ is 2, and otherwise if $H \in \mathcal{S}_{\texttt{2B}}$, then the level of $H$ is 8.

COROLLARY 3.9. *Let $E/\mathbb{Q}$ be a $\texttt{2B}$-Serre curve.*

- *If $G_E(2^\infty) = \texttt{2.3.0.1}$, then*

$$m_E = \begin{cases} \mathrm{lcm}(4, |N_1'|, |N_2'|) & 2 \nmid N_1 N_2 \\ \mathrm{lcm}(8, |N_1'|, |N_2'|) & 2 \mid N_1 N_2. \end{cases}$$

- *If $G_E(2^\infty) \neq \texttt{2.3.0.1}$, then*

$$m_E = \mathrm{lcm}(8, |N_1'|).$$

PROOF. The proof is similar to the proof of Corollary 3.5. $\square$

**3.3. Serre curves relative to 2Cn.** Let $E$ be a $\texttt{2Cn}$-Serre curve. By Theorem 1.1, we know that $G_E(2^\infty) \in \mathcal{S}_{\texttt{2Cn}}$. In particular, $G_E(2) = \texttt{2Cn}$. Thus, the Galois extension $\mathbb{Q}(E[2])/\mathbb{Q}$ is cyclic of order 3. By (3.5), the conductor of $\mathbb{Q}(E[2])$ is given by

$$(3.19) \qquad f(\mathbb{Q}(E[2])) = \sqrt{\Delta_{\mathbb{Q}(E[2])}}.$$

Further, we claim that $f(\mathbb{Q}(E[2]))$ is odd. Indeed, a cubic extension of $\mathbb{Q}$ is given by $\mathbb{Q}(\alpha)$ where $\alpha$ satisfies the irreducible polynomial $T^3 - 3T + 1 - v(T^2 - T)$ for some $v \in \mathbb{Q}$ (see, e.g., [**35**, Section 1.1]). The square root of discriminant of $\mathbb{Q}(\alpha)$ is either $v^2 - 3v + 9$ or $(v^2 - 3v + 9)/3$. Since we know that it has to be an integer, $v \in \mathbb{Z}$, and the claim follows.

By Proposition 2.14, we have that

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_E] = 12.$$

Recall that $\mathcal{S}_{2\mathrm{Cn}} = \{\mathtt{2.2.0.1}, \mathtt{4.4.0.2}, \mathtt{8.4.0.1}\}$. Thus, considering the labels,

$$[\mathrm{GL}_2(\mathbb{Z}_2) : G_E(2^\infty)] = \begin{cases} 2 & G_E(2^\infty) = \mathtt{2.2.0.1} \\ 4 & \text{otherwise.} \end{cases}$$

If $G_E(2^\infty) \neq \mathtt{2.2.0.1}$, then the adelic index of 12 is explained by the fact that $[\mathrm{GL}_2(\mathbb{Z}_2) : G_E(2^\infty)] = 4$ and the cubic entanglement arising from the containment $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(\zeta_{\sqrt{\Delta_{\mathbb{Q}(E[2])}}})$. Consider the case that $G_E(2^\infty) = \mathtt{2.2.0.1}$. Here $[\mathrm{GL}_2(\mathbb{Z}_2) : G_E(2^\infty)] = 2$, so an additional quadratic entanglement must be described to account for the adelic index of 12. By (3.19), we know that $D_E \coloneqq (\sqrt{\Delta_E})_{sf} \in \mathbb{Z}$. We have that $\sqrt{D_E}$ lies in $\mathbb{Q}(E[4])$ and is not equal to $\sqrt{\pm 2}$ because if $\sqrt{2} \in \mathbb{Q}(E[4])$, then $[\mathbb{Q}(E[8]) : \mathbb{Q}(E[4])]$ is at most 8 by Corollary 3.2, which is a contradiction since we know that $\#\mathtt{2.2.0.1}(8) = 16 \cdot \#\mathtt{2.2.0.1}(4)$. Using the notation (3.9), there is a quadratic entanglement between $\mathbb{Q}(E[2^k])$ and $\mathbb{Q}(E[|D_E'|])$, where $k$ is as defined in (3.10).

3.3.1. *Description of image.* We now describe the adelic image $G_E$ of a $\mathtt{2Cn}$-Serre curve $E$. Let $G_1 \subseteq G_E(2^\infty)$ be the index 3 subgroup such that $G_E(2^\infty)/G_1 \cong \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$. Let $\omega \colon G_E(2^\infty) \to G_E(2^\infty)/G_1$ be the cubic character. Let $\xi \colon \widehat{\mathbb{Z}}^\times \to \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ be the restriction of cyclotomic character associated to $\mathbb{Q}(\zeta_{\sqrt{\Delta_{\mathbb{Q}(E[2])}}})$. If $G_E(2^\infty) = \mathtt{2.2.0.1}$, further let $G_2 \subseteq G_E(2^k)$ be the index 2 subgroup such that $G_E(2^k)/G_2 \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{D_E'})/\mathbb{Q}) \cong \{\pm 1\}$, where $k$ is 2 if $D_E$ is odd and $k$ is 3 otherwise. Let $\epsilon \colon G_E(2^k) \to G_E(2^k)/G_2$ be the associated quadratic character and let $\chi$ be the Dirichlet character given by the unique surjective homomorphism $\widehat{\mathbb{Z}}^\times \to \mathrm{Gal}(\mathbb{Q}(\sqrt{D_E'})/\mathbb{Q}) \cong \{\pm 1\}$.

PROPOSITION 3.10. *With notation as above, if $G_E(2^\infty) = \mathtt{2.2.0.1}$, then*

$$G_E = \{A \in \widehat{G_E(2^\infty)} | \omega(A) = \xi(\det(A))\} \cap \{A \in \widehat{G_E(2^\infty)} | \epsilon(A) = \chi(\det(A))\}.$$

*If $G_E(2^\infty) \in \{\mathtt{4.4.0.2}, \mathtt{8.4.0.1}\}$, then*

$$G_E = \{A \in \widehat{G_E(2^\infty)} | \omega(A) = \xi(\det(A))\}.$$

PROOF. Assume that $G_E(2^\infty) = \mathtt{2.2.0.1}$. The inclusion

$$(3.20) \quad G_E \subseteq \{A \in \widehat{G_E(2^\infty)} | \omega(A) = \xi(\det(A))\} \cap \{A \in \widehat{G_E(2^\infty)} | \epsilon(A) = \chi(\det(A))\}$$

follows from $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[8])$, $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(\zeta_{\sqrt{\Delta_{\mathbb{Q}(E[2])}}}) \subseteq \mathbb{Q}(E[\sqrt{\Delta_{\mathbb{Q}(E[2])}}])$ and $\mathbb{Q}(\sqrt{D_E'}) \subseteq \mathbb{Q}(E[4]) \cap \mathbb{Q}(E[|D_E'|])$. Similar to the proof given in Proposition 3.4 and by Proposition 2.14, we have that (3.20) is actually an equality. When $G_E(2^\infty) \neq \mathtt{2.2.0.1}$, the proof is similar. $\square$

From the above proposition, we obtain the following formula for $m_E$ upon noting that the level of $\mathtt{2.2.0.1}$ is 2, $\mathtt{4.4.0.2}$ is 4, and $\mathtt{8.4.0.1}$ is 8.

COROLLARY 3.11. *Let $E/\mathbb{Q}$ be a $\mathtt{2Cn}$-Serre curve.*
- *If $G_E(2^\infty) = \mathtt{4.4.0.2}$, then*

$$m_E = \mathrm{lcm}(4, \sqrt{\Delta_{\mathbb{Q}(E[2])}}).$$

- *If $G_E(2^\infty) = \mathtt{8.4.0.1}$, then*

$$m_E = \mathrm{lcm}(8, \sqrt{\Delta_{\mathbb{Q}(E[2])}}).$$

- If $G_E(2^\infty) = \texttt{2.2.0.1}$, *then*

$$m_E = \begin{cases} \operatorname{lcm}(4, \sqrt{\Delta_{\mathbb{Q}(E[2])}}, |D'_E|) & 2 \nmid D_E \\ \operatorname{lcm}(8, \sqrt{\Delta_{\mathbb{Q}(E[2])}}, |D'_E|) & 2 \mid D_E. \end{cases}$$

PROOF. The proof is similar to the proof of Corollary 3.5.  □

## 4. An application

In the previous section, we described the adelic Galois image of a Serre curve relative to an obstruction modulo 2. There are numerous applications of such an understanding, including to problems concerning the distribution of prime numbers with certain properties relating to the arithmetic of elliptic curves. The following problems are some well-known examples of this sort.

(1) Koblitz conjecture [20] (and Zywina's refinement [41])
(2) Lang-Trotter conjecture [22]
(3) Titchmarsh divisor problem for elliptic curves [28]
(4) Cyclicity conjecture [36]

In this section, we consider the cyclicity conjecture, which asks : For an elliptic curve $E/\mathbb{Q}$, what is the density of primes $p$ of good reduction for $E$ with the property that the group $E(\mathbb{F}_p)$ is cyclic? Serre first studied this problem. He proved the following conditional result.

THEOREM 4.1 (Serre [36]). *Assume GRH. If $E/\mathbb{Q}$ is an elliptic curve of conductor $N_E$, then*

$$\#\{p \le x : p \nmid N_E \text{ and } E(\mathbb{F}_p) \text{ is cyclic}\} \sim C_E \frac{x}{\log x}$$

*as $x \to \infty$, where $C_E := \sum_{n \ge 1} \frac{\mu(n)}{[\mathbb{Q}(E[n]):\mathbb{Q}]}$ in which $\mu(\cdot)$ denotes the Möbius function.*

The constant $C_E$, defined in Theorem 4.1, depends only on the adelic image $G_E$.

Assume that *E has abelian entanglements*, by which we mean that for every pair of relatively prime positive integers $(m_1, m_2)$, the extension $\mathbb{Q}(E[m_1]) \cap \mathbb{Q}(E[m_2])$ over $\mathbb{Q}$ is abelian. In his thesis, Brau [5, 6] gave a framework for explicitly computing $C_E$ (provided that $E$ has abelian entanglements). Let $m := (m_E)_{\mathrm{sf}}$ be the squarefree part of the image conductor $m_E$ and consider the quotient group

$$\Phi_E := \left( \prod_{\ell \mid m} G_E(\ell) \right) / G_E(m).$$

This group quantifies the prime-level entanglements of $E$.

With the above notation and terminology, Brau proved the following result.

THEOREM 4.2 (Brau [5, 6]). *Let $E/\mathbb{Q}$ be an elliptic curve with abelian entanglements. For a character $\chi$ of the group $\prod_{\ell \mid m} G_E(\ell)$ obtained by composing the natural quotient map $\prod_{\ell \mid m} G_E(\ell) \to \Phi_E$ with a character $\tilde{\chi}$ of the group $\Phi_E$, define the constant $E_{\chi,\ell}$ as follows:*

$$E_{\chi,\ell} = \begin{cases} 1 & \text{if } \chi \text{ is trivial on } G_E(\ell) \\ \frac{-1}{[\mathbb{Q}(E[\ell]):\mathbb{Q}]-1} & \text{otherwise.} \end{cases}$$

*Then the cyclicity constant of Theorem 4.1 is given by*

$$C_E = \mathfrak{C}_E \prod_\ell \left( 1 - \frac{1}{[\mathbb{Q}(E[\ell]) : \mathbb{Q}]} \right)$$

*where $\mathfrak{C}_E$ denotes the entanglement correction factor*

$$\mathfrak{C}_E := 1 + \sum_{\tilde{\chi} \in \widehat{\Phi}_E \setminus \{1\}} \prod_{\ell | m} E_{\chi,\ell}$$

*in which $\widehat{\Phi}_E$ denotes the character group of $\Phi_E$.*

If $E$ is a Serre curve or if $E$ is a $G$-Serre curve for $G \in \{\mathtt{2Cs}, \mathtt{2B}, \mathtt{2Cn}\}$, then $E$ has abelian entanglements. Applying Theorem 4.2 when $E$ is a Serre curve, Brau gave a formula for the cyclicity constant $C_E$ in terms of only the discriminant $\Delta_E$. In a similar way, we now apply Theorem 4.2 with our results of Section 3 to give an analogous formula for relative Serre curves. The case when $E$ is a $\mathtt{2Cs}$-Serre curve is trivial, since $G_E(2) = \mathtt{2Cs}$ implies that $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$ is contained in the rational torsion of $E$, so $C_E = 0$. Thus we only consider the cases of $\mathtt{2B}$- and $\mathtt{2Cn}$-Serre curves.

PROPOSITION 4.3. *Let $E$ be a $\mathtt{2B}$-Serre curve given by (3.13). Write $\Delta_{E,\mathsf{sf}}$ to denote the squarefree part of the discriminant of any model of $E$. Then the cyclicity constant is given by*

$$C_E = \mathfrak{C}_E \cdot \frac{1}{2} \prod_{\ell \text{ odd}} \left( 1 - \frac{1}{(\ell^2 - 1)(\ell^2 - \ell)} \right)$$

*where*

$$\mathfrak{C}_E = \begin{cases} 1 - \displaystyle\prod_{\ell | \Delta_{E,sf}} \frac{-1}{(\ell^2 - 1)(\ell^2 - \ell)} & \Delta_{E,sf} \equiv 1 \pmod 4 \\ 1 & \text{otherwise.} \end{cases}$$

PROOF. We have that $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{\Delta_{E,\mathrm{sf}}})$. Thus $\mathbb{Q}(E[2])$ entangles with $\mathbb{Q}(E[d])$ for some $d$ coprime to 2 if and only if $\Delta_{E,\mathrm{sf}} \equiv 1 \pmod 4$. By this fact, together with Proposition 3.8, we have that $\Phi_E$ is of order 2 if $\Delta_{E,\mathrm{sf}} \equiv 1 \pmod 4$ and $\Phi_E$ is trivial otherwise. Consider the former case. Here there are 2 characters of the group $\Phi_E$. Moreover, the non-identity character $\chi$ corresponds to the non-identity character of group $\Phi_E$ and is non-trivial on $G_E(\ell)$ for each $\ell | m$ because it factors through the quotient group $\Phi_E$. So, the entanglement correction factor must be given by

$$(4.1) \qquad \mathfrak{C}_E = 1 + (-1) \prod_{\ell | \Delta_{E,\mathrm{sf}}} \frac{-1}{(\ell^2 - 1)(\ell^2 - \ell)}$$

and cyclicity constant is given by

$$C_E = \mathfrak{C}_E \frac{1}{2} \prod_{\ell \text{ odd}} \left( 1 - \frac{1}{(\ell^2 - 1)(\ell^2 - \ell)} \right).$$

since $[\mathbb{Q}(E[\ell]) : \mathbb{Q}] = \#G_E(\ell) = 2$ if $\ell = 2$ and $[\mathbb{Q}(E[\ell]) : \mathbb{Q}] = \#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) = (\ell^2 - 1)(\ell^2 - \ell)$ otherwise. Note the $-1$ before the product in (4.1) comes from the prime $\ell = 2$. In the latter case, that $\Delta_{E,\mathrm{sf}} \not\equiv 1 \pmod 4$, we have that $\mathfrak{C}_E = 1$ as $\Phi_E$ is trivial. $\square$

PROPOSITION 4.4. *Let $E$ be a* 2Cn-*Serre curve. Then the cyclicity constant is given by*

$$C_E = \mathfrak{C}_E \cdot \frac{2}{3} \prod_{\ell \text{ odd}} \left( 1 - \frac{1}{(\ell^2 - 1)(\ell^2 - \ell)} \right)$$

*where*

$$\mathfrak{C}_E = \begin{cases} 1 - \prod\limits_{\ell \mid \sqrt{\Delta_{\mathbb{Q}(E[2])}}} \dfrac{-1}{(\ell^2 - 1)(\ell^2 - \ell)} & \text{if } \sqrt{\Delta_{\mathbb{Q}(E[2])}} \text{ is squarefree} \\ 1 & \text{otherwise.} \end{cases}$$

PROOF. We have that $\mathbb{Q}(E[2])$ is a cyclic cubic field of conductor $\sqrt{\Delta_{\mathbb{Q}(E[2])}}$. By this fact, together with Proposition 3.10, we have that $\Phi_E$ is of order 3 if $\sqrt{\Delta_{\mathbb{Q}(E[2])}}$ is squarefree, and $\Phi_E$ is trivial otherwise. Consider the former case. Here there are 3 characters of the group $\Phi_E$. Moreover, the non-identity characters $\chi$ correspond to non-identity characters of $\Phi_E$, and are non-trivial on $G_E(\ell)$ for each $\ell \mid m$ because they factor through $\Phi_E$. Thus, the entanglement correction factor of Theorem 4.2 is given by

$$\mathfrak{C}_E = 1 + 2(-1/2) \prod_{\ell \mid \sqrt{\Delta_{\mathbb{Q}(E[2])}}} \frac{-1}{(\ell^2 - 1)(\ell^2 - \ell)}$$

and cyclicity constant is given by

$$C_E = \mathfrak{C}_E \cdot \frac{2}{3} \prod_{\ell \text{ odd}} \left( 1 - \frac{1}{(\ell^2 - 1)(\ell^2 - \ell)} \right)$$

since $[\mathbb{Q}(E[\ell]) : \mathbb{Q}] = \#G_E(\ell)$ equals 3 if $\ell = 2$ and equals $\#\operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ otherwise. $\square$

## 5. Some examples

In this section, we build on Section 3 to explicitly compute the adelic Galois image of three relative Serre curves. In each case, our result agrees (up to conjugacy) with the output of Zywina's recent general algorithm [**43**]. The code that accompanies this section is available on this paper's GitHub repository [**24**].

EXAMPLE 5.1. Consider the elliptic curve $E$ with LMFDB label 315.a2 given by the Weierstrass equation

$$y^2 = x^3 - 1083x + 10582 = (x - 11)(x - 26)(x + 37).$$

Using our `IsRelSerreCurve` script, we find that $E$ is a 2Cs-Serre curve. With the notation of Section 3.1, we have that

$$S = \{\pm 3, \pm 5, \pm 7, \pm 15, \pm 21, \pm 35\}.$$

Thus $(N_1, k_1) = (3, 2), (N_2, k_2) = (5, 2)$, and $(N_3, k_3) = (7, 2)$. Hence $N_1' = -3, N_2' = 5$, and $N_3' = -7$. There is a quadratic entanglement between $\mathbb{Q}(E[4])$ and $\mathbb{Q}(E[|N_i'|])$ for each $i \in \{1, 2, 3\}$. Using Sutherland's `galrep` [**38**], we compute

$$G_E(4) = \left\langle \left( \begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & 2 \\ 0 & 3 \end{smallmatrix} \right), \left( \begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix} \right), \left( \begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix} \right) \right\rangle.$$

Let $G_i$ be the index 2 subgroup of $G_E(4)$ corresponding to $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}(\sqrt{N_i'}))$. By constructing the field $\mathbb{Q}(E[4])$ in Magma and considering its automorphisms that fix the subfield $\mathbb{Q}(\sqrt{N_i'})$, we determine that

$$G_1 = \langle \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 2 & 3 \end{smallmatrix}\right) \rangle,$$
$$G_2 = \langle \left(\begin{smallmatrix} 1 & 2 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 2 & 1 \end{smallmatrix}\right) \rangle,$$
$$G_3 = \langle \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 2 & 1 \end{smallmatrix}\right) \rangle.$$

Let $\epsilon_i : G_E(4) \to G_E(4)/G_i$ be the natural map and $\chi_i : \mathrm{GL}_2(\mathbb{Z}/|N_i'|\mathbb{Z}) \to \{\pm 1\}$ be the unique quadratic character (which is given by the determinant map composed with the Kronecker symbol). The image conductor of $E$ is $420 = \mathrm{lcm}(4, 3, 5, 7)$. In view of Proposition 3.4, we have that

$$G_E(420) = \{g \in \mathrm{GL}_2(\mathbb{Z}/420\mathbb{Z}) : \pi_4(g) \in G_E(4) \text{ and } \epsilon_i(g) = \chi_i(g) \text{ for each } i\}.$$

Using Magma, we compute this fiber product to be the group

$$G_E(420) = \langle \left(\begin{smallmatrix} 259 & 362 \\ 162 & 365 \end{smallmatrix}\right), \left(\begin{smallmatrix} 401 & 108 \\ 364 & 275 \end{smallmatrix}\right), \left(\begin{smallmatrix} 55 & 142 \\ 52 & 45 \end{smallmatrix}\right), \left(\begin{smallmatrix} 27 & 184 \\ 40 & 201 \end{smallmatrix}\right) \rangle.$$

Now the adelic image $G_E$ is the full preimage of $G_E(420)$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

EXAMPLE 5.2. Consider the elliptic curve $E$ with LMFDB label 69.a1 given by

$$y^2 = x^3 - 20115x - 1094418 = (x^2 - 78x - 14031)(x + 78).$$

This curve is a 2B-Serre curve. With the notation of Section 3.2, we have that

$$S = \{\pm 3, \pm 23, \pm 69\}.$$

Thus $(N_1, k_1) = (3, 2)$ and $(N_2, k_2) = (23, 2)$, so $N_1' = -3$ and $N_2' = -23$. Hence there is a quadratic entanglement between $\mathbb{Q}(E[4])$ and $\mathbb{Q}(E[|N_i'|])$ for each $i \in \{1, 2\}$. Using `galrep`, we compute that

$$G_E(4) = \langle \left(\begin{smallmatrix} 3 & 2 \\ 3 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 3 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 3 & 3 \end{smallmatrix}\right) \rangle.$$

Let $G_i$ be the index 2 subgroup of $G_E(4)$ corresponding to $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}(\sqrt{N_i'}))$. As in Example 5.1, we determine that

$$G_1 = \langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \rangle \quad \text{and} \quad G_2 = \langle \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 3 & 1 \end{smallmatrix}\right) \rangle.$$

Let $\epsilon_i : G_E(4) \to G_E(4)/G_i$ be the natural map and $\chi_i : \mathrm{GL}_2(\mathbb{Z}/|N_i'|\mathbb{Z}) \to \{\pm 1\}$ be the unique quadratic character. In view of Proposition 3.8, we have that

$$G_E(276) = \{g \in \mathrm{GL}_2(\mathbb{Z}/276\mathbb{Z}) : \pi_4(g) \in G_E(4) \text{ and } \epsilon_i(g) = \chi_i(g) \text{ for each } i\}.$$

Using Magma, we compute that

$$G_E(276) = \langle \left(\begin{smallmatrix} 43 & 128 \\ 65 & 53 \end{smallmatrix}\right), \left(\begin{smallmatrix} 13 & 140 \\ 63 & 269 \end{smallmatrix}\right), \left(\begin{smallmatrix} 167 & 26 \\ 23 & 45 \end{smallmatrix}\right), \left(\begin{smallmatrix} 129 & 176 \\ 155 & 145 \end{smallmatrix}\right), \left(\begin{smallmatrix} 175 & 188 \\ 182 & 189 \end{smallmatrix}\right) \rangle.$$

Now the adelic image $G_E$ is the full preimage of $G_E(276)$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

EXAMPLE 5.3. Consider the elliptic curve $E$ with LMFDB label 392.a1 given by

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

We have that $2\sqrt{7} = \sqrt[4]{\Delta_E} \in \mathbb{Q}(E[4])$. As $\sqrt{-1} \in \mathbb{Q}(E[4])$, this implies that $\sqrt{-7} \in \mathbb{Q}(E[4]) \cap \mathbb{Q}(E[7])$. Thus there is a quadratic entanglement between $\mathbb{Q}(E[4])$ and $\mathbb{Q}(E[7])$. Further $f(\mathbb{Q}(E[2])) = 7$, so there is a cubic entanglement between $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E[7])$ (and hence also between $\mathbb{Q}(E[4])$ and $\mathbb{Q}(E[7])$). Using `galrep`, we compute that

$$G_E(4) = \langle \left(\begin{smallmatrix} 2 & 3 \\ 3 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 3 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 3 & 1 \end{smallmatrix}\right) \rangle.$$

Let $G_1$ be the index 2 subgroup of $G_E(4)$ corresponding to $\mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q}(\sqrt{-7}))$. Let $G_2$ be the unique index 3 subgroup of $G_E(4)$. Using Magma, we find that

$$G_1 = \langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \rangle \quad \text{and} \quad G_2 = \langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right) \rangle.$$

Let $\epsilon : G_E(4) \to G_E(4)/G_1$ and $\omega : G_E(4) \to G_E(4)/G_2$ be the natural maps. There are two nontrivial cubic characters of $G_E(4)$ (both of which have kernel $G_2$). They are the maps $g \mapsto \omega(g)$ and $g \mapsto \omega(g)^2$. Thus by Proposition 3.10, there are two possible candidates for $G_E(28)$, namely,

$$H_1 = \langle \left(\begin{smallmatrix} 26 & 23 \\ 1 & 11 \end{smallmatrix}\right), \left(\begin{smallmatrix} 8 & 21 \\ 7 & 17 \end{smallmatrix}\right) \rangle \quad \text{and} \quad H_2 = \langle \left(\begin{smallmatrix} 26 & 23 \\ 1 & 19 \end{smallmatrix}\right), \left(\begin{smallmatrix} 19 & 27 \\ 21 & 12 \end{smallmatrix}\right), \left(\begin{smallmatrix} 8 & 5 \\ 27 & 21 \end{smallmatrix}\right) \rangle.$$

To determine the correct candidate, we consider the action of Frobenius. Let $\mathrm{Frob}_3 \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius automorphism associated with $p = 3$. Using Magma, we compute that the characteristic polynomial of $\rho_{E,28}(\mathrm{Frob}_3)$ is $x^2 + 3x + 3$. This polynomial does not appear as the characteristic polynomial of any matrix in $H_1$. As such, it must be that $G_E(28) = H_2$. We conclude that the adelic image $G_E$ is the full preimage of $G_E(28) = H_2$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

# References

1. Shabnam Akhtari, Chantal David, Heekyoung Hahn, and Lola Thompson, *Distribution of squarefree values of sequences associated with elliptic curves*, Women in numbers 2: research directions in number theory, Contemp. Math., vol. 606, Amer. Math. Soc., Providence, RI, 2013, pp. 171–188. MR 3204298

2. Nuno Arala, *On the density of a set of primes associated to an elliptic curve*, J. Number Theory **243** (2023), 241–255. MR 4499392

3. Renee Bell, Clifford Blakestad, Alina Carmen Cojocaru, Alexander Cowan, Nathan Jones, Vlad Matei, Geoffrey Smith, and Isabel Vogt, *Constants in Titchmarsh divisor problems for elliptic curves*, Res. Number Theory **6** (2020), no. 1, Paper No. 1, 24. MR 4041152

4. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478

5. Julio Brau, *Galois representations of elliptic curves and abelian entanglements*, Ph.D. thesis, Universiteit Leiden, 2015.

6. _____, *Character sums for elliptic curve densities*, 2017, arXiv:1703.04154.

7. Julio Brau and Nathan Jones, *Elliptic curves with 2-torsion contained in the 3-torsion field*, Proc. Amer. Math. Soc. **144** (2016), no. 3, 925–936. MR 3447646

8. Harvey Cohn, *Introduction to the construction of class fields*, Dover Publications, Inc., New York, 1994, Corrected reprint of the 1985 original. MR 1313719

9. John Cremona, *Elliptic curve data*, 2014, Available at `http://johncremona.github.io/ecdata/`.

10. Harris B. Daniels, *An infinite family of Serre curves*, J. Number Theory **155** (2015), 226–247. MR 3349445

11. Harris B. Daniels, Alvaro Lozano-Robledo, and Jackson S. Morrow, *Towards a classification of entanglements of Galois representations attached to elliptic curves*, Rev. Mat. Iberoam. **39** (2023), no. 3, 803–844. MR 4605883

12. Harris B. Daniels and Álvaro Lozano-Robledo, *Coincidences of division fields*, 2019, arXiv:1912.05618.

13. Harris B. Daniels and Jackson S. Morrow, *A group theoretic perspective on entanglements of division fields*, Trans. Amer. Math. Soc. Ser. B **9** (2022), 827–858. MR 4496973

14. Aaron Greicius, *Elliptic curves with surjective adelic Galois representations*, Experiment. Math. **19** (2010), no. 4, 495–507. MR 2778661

15. Nathan Jones, *Averages of elliptic curve constants*, Math. Ann. **345** (2009), no. 3, 685–710. MR 2534114

16. _____, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570. MR 2563740

17. _____ , *Elliptic aliquot cycles of fixed length*, Pacific J. Math. **263** (2013), no. 2, 353–371. MR 3068548

18. _____ , *GL₂-representations with maximal image*, Math. Res. Lett. **22** (2015), no. 3, 803–839. MR 3350106

19. Nathan Jones and Ken McMurdy, *Elliptic curves with non-abelian entanglements*, New York J. Math. **28** (2022), 182–229. MR 4374148

20. Neal Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–165. MR 917870

21. Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 1878556

22. Serge Lang and Hale Trotter, *Frobenius distributions in $GL_2$-extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin-New York, 1976, Distribution of Frobenius automorphisms in $GL_2$-extensions of the rational numbers. MR 0568299

23. Davide Lombardo and Sebastiano Tronto, *Some uniform bounds for elliptic curves over $\mathbb{Q}$*, Pacific J. Math. **320** (2022), no. 1, 133–175. MR 4496096

24. Jacob Mayle and Rakvi, *Github repository related to Serre curves relative to obstructions modulo 2*, https://github.com/maylejacobj/RelativeSerreCurves, 2022.

25. Jacob J. Mayle, *Galois Representations of Abelian Varieties*, ProQuest LLC, Ann Arbor, MI, 2022, Thesis (Ph.D.)–University of Illinois at Chicago. MR 4533238

26. Barry Mazur, *Rational points on modular curves*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), 1977, pp. 107–148. Lecture Notes in Math., Vol. 601. MR 0450283

27. Jackson S. Morrow, *Composite images of Galois for elliptic curves over **Q** and entanglement fields*, Math. Comp. **88** (2019), no. 319, 2389–2421. MR 3957898

28. Paul Pollack, *A Titchmarsh divisor problem for elliptic curves*, Math. Proc. Cambridge Philos. Soc. **160** (2016), no. 1, 167–189. MR 3432335

29. Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ell-adic-galois-images*, https://github.com/AndrewVSutherland/ell-adic-galois-images, 2022.

30. _____ , *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight)*, Forum Math. Sigma **10** (2022), Paper No. e62, 63, With an appendix with John Voight. MR 4468989

31. Jeremy Rouse and David Zureick-Brown, *Images of the 2-adic Galois representation attached to elliptic curves*, https://users.wfu.edu/rouseja/2adic/.

32. _____ , *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Res. Number Theory **1** (2015), Paper No. 12, 34. MR 3500996

33. Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR 387283

34. _____ , *Abelian l-adic representations and elliptic curves*, second ed., Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989, With the collaboration of Willem Kuyk and John Labute. MR 1043865

35. _____ , *Topics in Galois theory*, second ed., Research Notes in Mathematics, vol. 1, A K Peters, Ltd., Wellesley, MA, 2008, With notes by Henri Darmon. MR 2363329

36. _____ , *Résumé des cours de 1977–1978; Oeuvres/Collected papers. III. 1972–1984*, Springer Collected Works in Mathematics, Springer, Heidelberg, 2013, Reprint of the 2003 edition [of the 1986 original MR0926691]. MR 3223094

37. Hanson Smith, *Non-monogenic division fields of elliptic curves*, J. Number Theory **228** (2021), 174–187. MR 4271815

38. Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), Paper No. e4, 79. MR 3482279

39. The LMFDB Collaboration, *The L-functions and modular forms database*, 2021, Available at https://www.lmfdb.org/.

40. Jeffrey Yelton, *A note on 8-division fields of elliptic curves*, Eur. J. Math. **3** (2017), no. 3, 603–613. MR 3687433

41. David Zywina, *A refinement of Koblitz's conjecture*, Int. J. Number Theory **7** (2011), no. 3, 739–769. MR 2805578

42. _____ , *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, 2015, arXiv:1508.07660.

43. _____ , *Explicit open images for elliptic curves over $\mathbb{Q}$*, 2022, arXiv:2206.14959.

44.  _____ , *On the surjectivity of* mod $\ell$ *representations associated to elliptic curves*, Bull. Lond. Math. Soc. **54** (2022), no. 6, 2404–2417. MR 4549128

## Appendix A. Table of relative Serre curves

The table below gives, for each $G \in \{\texttt{2Cs}, \texttt{2B}, \texttt{2Cn}\}$ and $H \in \mathcal{S}_G$, an elliptic curve $E/\mathbb{Q}$ with minimal conductor among $G$-Serre curves for which $G_E(2^\infty) = H$. For each curve, the LMFDB label and minimal Weierstrass equation is listed, along with the image conductor $m_E$ and entanglement correction factor $\mathfrak{C}_E$. If $G_E(2) = \texttt{2Cs}$, then $C_E = 0$. Thus $\mathfrak{C}_E$ is not given for $\texttt{2Cs}$-Serre curves.

| $G$ | $G_E(2^\infty)$ | LMFDB | Weierstrass equation | $m_E$ | $\mathfrak{C}_E$ |
|---|---|---|---|---|---|
| 2Cs | 2.6.0.1 | 315.a2 | $y^2 + xy + y = x^3 - x^2 - 68x + 182$ | 420 | - |
| 2Cs | 8.12.0.2 | 1800.c3 | $y^2 = x^3 - 3675x + 35750$ | 120 | - |
| 2Cs | 4.12.0.2 | 1089.j2 | $y^2 + xy = x^3 - x^2 - 12546x + 173047$ | 132 | - |
| 2Cs | 8.12.0.1 | 120.a3 | $y^2 = x^3 + x^2 - 16x - 16$ | 120 | - |
| 2Cs | 4.12.0.1 | 33.a2 | $y^2 + xy = x^3 + x^2 - 11x$ | 132 | - |
| 2Cs | 8.12.0.3 | 350.b3 | $y^2 + xy = x^3 - x^2 - 442x - 2784$ | 280 | - |
| 2Cs | 8.24.0.5 | 392.d3 | $y^2 = x^3 - 931x - 10290$ | 56 | - |
| 2Cs | 8.24.0.7 | 3136.p3 | $y^2 = x^3 - 3724x + 82320$ | 56 | - |
| 2Cs | 8.24.0.2 | 112.b3 | $y^2 = x^3 - 19x - 30$ | 56 | - |
| 2Cs | 8.24.0.1 | 56.a3 | $y^2 = x^3 - 19x + 30$ | 56 | - |
| 2Cs | 8.12.0.4 | 198.a2 | $y^2 + xy = x^3 - x^2 - 198x + 1120$ | 264 | - |
| 2Cs | 8.24.0.6 | 288.b3 | $y^2 = x^3 - 21x - 20$ | 24 | - |
| 2Cs | 8.24.0.8 | 576.g2 | $y^2 = x^3 - 84x - 160$ | 24 | - |
| 2Cs | 8.24.0.3 | 96.b3 | $y^2 = x^3 + x^2 - 2x$ | 24 | - |
| 2Cs | 8.24.0.4 | 66.b2 | $y^2 + xy + y = x^3 + x^2 - 22x - 49$ | 264 | - |
| 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 | $\frac{2017}{2016}$ |

DEPARTMENT OF MATHEMATICS, WAKE FOREST UNIVERSITY, WINSTON-SALEM, NC 27109
*Email address*: maylej@wfu.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PA 19104
*Email address*: rakvi@sas.upenn.edu