MATHEMATICS OF COMPUTATION
Volume 88, Number 319, September 2019, Pages 2389–2421
https://doi.org/10.1090/mcom/3426
Article electronically published on April 9, 2019

COMPOSITE IMAGES OF GALOIS FOR ELLIPTIC CURVES OVER Q AND ENTANGLEMENT FIELDS

JACKSON S. MORROW

Abstract. Let E be an elliptic curve defined over $\mathbf{Q}$ without complex multiplication. For each prime ℓ, there is a representation $\rho_{E,\ell}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$ that describes the Galois action on the ℓ-torsion points of E. Building on recent work of Rouse–Zureick-Brown and Zywina, we find models for composite level modular curves whose rational points classify elliptic curves over $\mathbf{Q}$ with simultaneously non-surjective, composite images of Galois. We also provably determine the rational points on almost all of these curves. Finally, we give an application of our results to the study of entanglement fields.

1. Introduction

Let E be an elliptic curve over a number field K. For any positive integer n, we denote the n-torsion subgroup of $E(\overline{K})$, where $\overline{K}$ is a fixed algebraic closure of K, by $E[n]$. For a prime ℓ, let

$$E[\ell^\infty] \coloneqq \varprojlim_{n\geq 1} E[\ell^n]$$

and

$$E[\mathrm{tors}] \coloneqq \varprojlim_{n\geq 1} E[n].$$

By fixing a $\widehat{\mathbf{Z}}$-basis for $E[\mathrm{tors}]$, there is an induced $\mathbf{Z}/n\mathbf{Z}$-basis on $E[n]$ for any positive integer n. The absolute Galois group $G_K \coloneqq \mathrm{Gal}(\overline{K}/K)$ has a natural action on each torsion subgroup, which respects each group structure. In particular, we have the continuous representations

$$\begin{aligned}
\rho_{E,n}\colon G_K &\longrightarrow \mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \cong \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}) && (\mathrm{mod}\ n),\\
\rho_{E,\ell^\infty}\colon G_K &\longrightarrow \mathrm{Aut}(E[\ell^\infty]) \cong \mathrm{GL}_2(\mathbf{Z}_\ell) && (\ell\text{-adic}),\\
\rho_E\colon G_K &\longrightarrow \mathrm{Aut}(E[\mathrm{tors}]) \cong \mathrm{GL}_2(\widehat{\mathbf{Z}}) && (\text{adélic}),
\end{aligned}$$

where the image under ρ is uniquely determined up to conjugacy in its respective general linear group. The *n-division field* $K(E[n])$ is the fixed field of $\overline{K}$ by the kernel of the mod n representation; moreover, the Galois group of this number field is the image of the mod n representation.

A celebrated theorem of Serre [Ser72] says that for an elliptic curve over K without complex multiplication (non-CM), the adélic representation ρ_E has open image in $\mathrm{GL}_2(\widehat{\mathbf{Z}})$. Serre's theorem raised many questions concerning the possible images of the adélic representation. The group $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ is both a product group

Received by the editor September 4, 2017, and, in revised form, November 16, 2018.
2010 *Mathematics Subject Classification.* Primary 11F80, 11G05; Secondary 11D45, 11G18.

and a profinite group via the isomorphisms

$$\prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbf{Z}_\ell) \cong \mathrm{GL}_2(\widehat{\mathbf{Z}}) \cong \varprojlim_n \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z}).$$

Serge Lang [Lan87] referred to these two characterizations as the *horizontal* and *vertical* natures of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$, respectively, and this binal nature of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ provides two flavors of questions stemming from Serre's work.

Horizontally speaking, for any non-CM elliptic curve over K, there exists a smallest integer $r_{E/K} > 0$ such that for all $\ell \geq r_{E/K}$, the ℓ-adic representation is surjective. Serre asked if $r_{E/K}$ depends only on K, and whether $r_{E/\mathbf{Q}} = 37$. In [Zywb], Zywina gave a refined conjecture concerning the surjectivity of the mod ℓ image and provided a practical algorithm (implemented in Sage) to compute the finite set of primes ℓ for which $\rho_{E,\ell}$ is not surjective; a prime ℓ is called *exceptional* if it belongs to this finite set.

Vertically speaking, one interesting question is to determine when the adélic image is surjective. Serre showed that the adélic image is always contained in some index 2 subgroup of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ for E defined over $\mathbf{Q}$. Greicius [Gre10] found necessary and sufficient abstract conditions on a number field L for which ρ_E could be surjective. Building on previous work of Duke [Duk97] and Jones [Jon10], Zywina [Zyw10, Zywa] proved that for a number field $L \neq \mathbf{Q}$ such that $L \cap \mathbf{Q}^{\text{cyc.}} = \mathbf{Q}$, almost all elliptic curves over L (in the sense of density) have surjective, adélic image.

The vertical variant also leads us to ask for the possible values for the index of the adélic image for a given non-CM elliptic curve. This question is the focus of [Maz77, Program B]. In particular, given an open subgroup $H \subset \mathrm{GL}_2(\widehat{\mathbf{Z}})$, this program strives to classify all elliptic curves E/K such that the image of ρ_E is contained in H. The work of this program suggests that there exists a constant $B(K)$ such that for every elliptic curve E/K without complex multiplication, the index of $\rho_E(G_K)$ in $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ is bounded by $B(K)$.

To determine $\rho_E(G_K)$, one begins by computing the ℓ-adic image ρ_{E,ℓ^∞} for each prime ℓ, which leads to the inclusions

$$\rho_E(G_K) \hookrightarrow \prod_{\ell \text{ prime}} \rho_{E,\ell^\infty}(G_K) \subseteq \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbf{Z}_\ell).$$

The image of $\rho_E(G_K)$ under the above inclusion will project onto each ℓ-adic factor, and so a natural first step in Mazur's Program B is to classify the ℓ-adic image of Galois.

We briefly recall recent progress in Mazur's Program B. Zywina [Zywc] has described all known, and conjecturally all, pairs (E, ℓ) such that $\rho_{E,\ell}(G_{\mathbf{Q}})$ is nonsurjective. Rouse and Zureick-Brown [RZB15] provided a complete list of the 1208 possible 2-adic Galois representations associated to non-CM elliptic curves over $\mathbf{Q}$. Sutherland and Zywina [SZ] also determined all of the prime power level modular curves X_G for which $X_G(\mathbf{Q})$ is infinite. In all of these works, the authors give rational functions whose values correspond to j-invariants of non-CM elliptic curves over $\mathbf{Q}$ with image of Galois conjugate to a subgroup of G in the appropriate general linear group. The computations of these rational functions occupy the majority of these works.

In this paper, we investigate the *composite-*(m_1, m_2) *image* $(\rho_{E,m_1} \times \rho_{E,m_2})(G_K)$ for m_1, m_2 relatively prime. Let ℓ be a prime, let $G_{n,\ell} \subset \mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$ be a proper subgroup which arises as an image of $\rho_{E,\ell}(G_{\mathbf{Q}})$ and contains $-I$ (these subgroups

come from [Zywc], and we produce the list of these subgroups $G_{n,\ell}$ in Appendix A; here ℓ refers to the level of the group and n is simply an index), and let $H_i \subset \mathrm{GL}_2(\mathbf{Z}/2^m\mathbf{Z})$ be a proper subgroup which arises as an image of $\rho_{E,2^\infty}(G_{\mathbf{Q}})$ and contains $-I$ coming from [RZB, `gl2data.txt`]. Using the rational functions corresponding to the j-maps of the modular curves $X_{H_i}(2^m)$ and $X_{G_{n,\ell}}(\ell)$, construct the following fibered product:

$$\begin{array}{ccc} X' & \longrightarrow & X_{G_n}(\ell) \\ \downarrow & & \downarrow{\scriptstyle j(G_{n,\ell})} \\ X_{H_i}(2^m) & \xrightarrow[j(H_i)]{} & \mathbf{P}^1_{\mathbf{Q}} \end{array}$$

We define the *composite-*$(2^m,\ell)$ *level* modular curve $X_{H_i,G_{n,\ell}}(2^m\cdot\ell)$ to be the normalization of the fibered product X'. The aforementioned j-map equations allow us to readily find equations for X', but this curve is usually singular, which necessitates taking a normalization.

The $\mathbf{Q}$-points on $X_{H_i,G_{n,\ell}}(2^m\cdot\ell)$ correspond to elliptic curves E over $\mathbf{Q}$ with composite-$(2^m,\ell)$ image conjugate to some subgroup of $H_i\times G_{n,\ell}\subset \mathrm{GL}_2(\mathbf{Z}/2^m\mathbf{Z})\times \mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})\cong \mathrm{GL}_2(\mathbf{Z}/2^m\cdot\ell\mathbf{Z})$ via the chinese remainder theorem. Succinctly, these rational points classify elliptic curves over $\mathbf{Q}$ with simultaneously non-surjective, composite-$(2^m,\ell)$ image of Galois.

Notation. Before we state our main results, we set some notation for specific subgroups of $\mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$. Let $C_{\mathrm{sp}}(\ell)$ be the subgroup of diagonal matrices. Let $\epsilon=-1$ if $\ell\equiv 3 \pmod 4$ and otherwise let $\epsilon\geq 2$ be the smallest integer which is not a quadratic residue modulo ℓ. Let $C_{\mathrm{nsp}}(\ell)$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a & b\epsilon \\ b & a\end{smallmatrix}\right)$ with $(a,b)\in\mathbf{Z}/\ell\mathbf{Z}^2\backslash\{(0,0)\}$. Let $N_{\mathrm{sp}}(\ell)$ and $N_{\mathrm{nsp}}(\ell)$ be the normalizers of $C_{\mathrm{sp}}(\ell)$ and $C_{\mathrm{nsp}}(\ell)$, respectively, in $\mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$. We have $[N_{\mathrm{sp}}(\ell):C_{\mathrm{sp}}(\ell)]=2$ and the non-identity coset of $C_{\mathrm{sp}}(\ell)$ in $N_{\mathrm{sp}}(\ell)$ is represented by $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$. We have $[N_{\mathrm{nsp}}(\ell):C_{\mathrm{nsp}}(\ell)]=2$ and the non-identity coset of $C_{\mathrm{nsp}}(\ell)$ in $N_{\mathrm{nsp}}(\ell)$ is represented by $\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$. Let $B(\ell)$ be the subgroup of upper triangular matrices in $\mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$.

1.1. **Statement of results.** In this paper, we study the possible composite-$(2^m,3)$ for $m=1,2,3,4$ and composite-$(2,\ell)$ for $\ell=5,7,11,13$ images of Galois associated non-CM elliptic curves over $\mathbf{Q}$.

Theorem A. *Let $E/\mathbf{Q}$ be a non-CM elliptic curve.*

(1) *If the composite-$(2,3)$ image of E is simultaneously non-surjective, then the image is conjugate to a subgroup of one of the following subgroups of $\mathrm{GL}_2(\mathbf{Z}/6\mathbf{Z})$:*

$$\{G_{3,2}\times G_{3,3},\ G_{2,2}\times G_{2,3},\ G_{2,2}\times G_{1,3},\ G_{2,2}\times G_{3,3},\ G_{2,2}\times G_{4,3},\ G_{1,2}\times G_{3,3}\}.$$

(2) *If the composite-$(4,3)$ image of E is simultaneously non-surjective, then the image is conjugate to a subgroup of one of the following subgroups of $\mathrm{GL}_2(\mathbf{Z}/12\mathbf{Z})$:*

$$\{H_9\times G_{3,3},\ H_{10}\times G_{3,3},\ H_{11}\times G_{4,3},\ H_{12}\times G_{4,3},\ H_{13}\times G_{3,3}\}.$$

(3) *If the composite-*$(8,3)$ *image of* E *is simultaneously non-surjective, then the image is conjugate to a subgroup of one of the following subgroups of* $\mathrm{GL}_2(\mathbf{Z}/24\mathbf{Z})$*:*

$$\{H_{30} \times G_{4,3},\ H_{31} \times G_{4,3},\ H_{39} \times G_{4,3},\ H_{45} \times G_{4,3},\ H_{47} \times G_{4,3},\ H_{50} \times G_{4,3}\}.$$

(4) *If the composite-*$(16,3)$ *image of* E *is simultaneously non-surjective, then the image is conjugate to a subgroup of one of the following subgroups of* $\mathrm{GL}_2(\mathbf{Z}/48\mathbf{Z})$*:*

$$\left\{\begin{matrix} H_{103} \times G_{4,3},\ H_{104} \times G_{4,3},\ H_{105} \times G_{4,3},\ H_{107} \times G_{4,3},\ H_{110} \times G_{4,3},\ H_{112} \times G_{4,3}, \\ H_{113} \times G_{4,3},\ H_{114} \times G_{4,3},\ H_{150} \times G_{4,3},\ H_{153} \times G_{4,3},\ H_{165} \times G_{4,3},\ H_{166} \times G_{4,3} \end{matrix}\right\}.$$

Proposition B. *Let* $E/\mathbf{Q}$ *be a non-CM elliptic curve.*

(1) *It occurs infinitely often that the index of* $(\rho_{E,2} \times \rho_{E,3})(G_{\mathbf{Q}})$ *in* $\mathrm{GL}_2(\mathbf{Z}/6\mathbf{Z})$ *is either* $4, 8, 9, 12, 18,$ *or* 36.
(2) *It occurs infinitely often that the index of* $(\rho_{E,4} \times \rho_{E,3})(G_{\mathbf{Q}})$ *in* $\mathrm{GL}_2(\mathbf{Z}/12\mathbf{Z})$ *divides* 18 *or* 24.
(3) *It occurs infinitely often that the index of* $(\rho_{E,8} \times \rho_{E,3})(G_{\mathbf{Q}})$ *in* $\mathrm{GL}_2(\mathbf{Z}/24\mathbf{Z})$ *divides* 36.
(4) *It occurs infinitely often that the index of* $(\rho_{E,16} \times \rho_{E,3})(G_{\mathbf{Q}})$ *in* $\mathrm{GL}_2(\mathbf{Z}/48\mathbf{Z})$ *divides* 72.

By restricting our attention to non-CM elliptic curves E with a specified mod 2 image of Galois, we can prove additional results on the composite-$(2,\ell)$ image for $\ell = 5, 7, 11, 13$.

Theorem C. *Let* $E/\mathbf{Q}$ *be a non-CM elliptic curve. Suppose that* $\rho_{E,2}(G_{\mathbf{Q}})$ *conjugate to a subgroup of* $G_{3,2}$ *i.e., the discriminant of* E*, is a square.*

(1) *If the composite-*$(2,5)$ *image of* E *is simultaneously non-surjective, then the image is conjugate to a subgroup of* $G_{3,2} \times G_{9,5}$ *in* $\mathrm{GL}_2(\mathbf{Z}/10\mathbf{Z})$.
(2) *If the composite-*$(2,7)$ *image of* E *is simultaneously non-surjective, then the image is conjugate to a subgroup of* $G_{3,2} \times G_{7,7}$ *in* $\mathrm{GL}_2(\mathbf{Z}/14\mathbf{Z})$.
(3) *If the composite-*$(2,11)$ *image of* E *is simultaneously non-surjective, then the image is conjugate to a subgroup of* $G_{3,2} \times G_{3,11}$ *in* $\mathrm{GL}_2(\mathbf{Z}/22\mathbf{Z})$.
(4) *If the composite-*$(2,13)$ *image of* E *is simultaneously non-surjective, then the image is conjugate to a subgroup of* $G_{3,2} \times G_{7,13}$ *in* $\mathrm{GL}_2(\mathbf{Z}/26\mathbf{Z})$.

Proposition D. *Let* $E/\mathbf{Q}$ *be a non-CM elliptic curve. Suppose that* $\rho_{E,2}(G_{\mathbf{Q}})$ *conjugate to a subgroup of* $G_{3,2}$ *i.e., the discriminant of* E*, is a square.*

(1) *It occurs infinitely often that the index of* $(\rho_{E,2} \times \rho_{E,5})(G_{\mathbf{Q}})$ *in* $\mathrm{GL}_2(\mathbf{Z}/10\mathbf{Z})$ *divides* 10.
(2) *It occurs infinitely often that the index of* $(\rho_{E,2} \times \rho_{E,7})(G_{\mathbf{Q}})$ *in* $\mathrm{GL}_2(\mathbf{Z}/14\mathbf{Z})$ *divides* 16.
(3) *It occurs finitely often that* 110 *divides the index of* $(\rho_{E,2} \times \rho_{E,11})(G_{\mathbf{Q}})$ *in* $\mathrm{GL}_2(\mathbf{Z}/22\mathbf{Z})$.
(4) *It occurs finitely often that* 182 *divides the index of* $(\rho_{E,2} \times \rho_{E,13})(G_{\mathbf{Q}})$ *in* $\mathrm{GL}_2(\mathbf{Z}/26\mathbf{Z})$.

1.2. **Sketch of proof.** The first step in the proofs of Theorems A and C is to find models for the composite level modular curves corresponding to the subgroups coming from Rouse–Zureick-Brown [RZB15] and Zywina [Zywc]. Once we have the models for these modular curves, we determine their $\mathbf{Q}$-points. The analysis of rational points on this collection of modular curves involves a variety of techniques, which we discuss in Section 4 and execute in Sections 5, 6, and 7. The `Magma` code verifying claims made in these sections can be found at [Mor17] as well as diagrams summarizing the results of Theorem A.

1.3. **Organization of the paper.** In Section 2, we give a synopsis of the necessary background on modular curves of prime power level. In Section 3, we construct models for our composite level modular curves. In Section 4, we explain the techniques used to determine these rational points. The subsequent Sections 5, 6, and 7 provide further details of this analysis for curves of increasing genera. We conclude in Section 8 by applying our results to the study of entanglement fields. In Appendix A, we recall relevant background and introduce notation from [Zywc], which we use throughout.

2. Background

For a subgroup $G \subset \mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$ with $\det(G) = \mathbf{Z}/\ell\mathbf{Z}^\times$ and $-I \in G$, we can associate to it a modular curve X_G, which is a smooth, projective, and geometrically irreducible curve over $\mathbf{Q}$. It comes with a natural morphism

$$\pi_G \colon X_G \longrightarrow \operatorname{Spec} \mathbf{Q}[j] \cup \{\infty\} =: \mathbf{P}^1_{\mathbf{Q}},$$

such that for an elliptic curve $E/\mathbf{Q}$ with $j_E \notin \{0, 1728\}$, the group $\rho_{E,\ell}(G_{\mathbf{Q}})$ is conjugate to a subgroup of G if and only if $j_E = \pi_G(P)$ for some rational point $P \in X_G(\mathbf{Q})$. The modular curves X_G of genus 0 with $X_G(\mathbf{Q}) \neq \emptyset$ are isomorphic to the projective line, and for each such curve, the function field is of form $\mathbf{Q}(h)$ for some modular function h of level ℓ. Giving the morphism π_G is then equivalent to expressing the modular j-invariant in the form $J(h)$.

We now describe a set of necessary conditions on the possible non-surjective images of $\rho_{E,n}(G_{\mathbf{Q}})$, where $n \geq 2$.

Definition 2.1. A subgroup G of $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ is *applicable* if it satisfies the following conditions:

- $G \neq \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$,
- $-I \in G$ and $\det(G) = (\mathbf{Z}/n\mathbf{Z})^\times$,
- G contains an element with trace 0 and determinant -1 that fixes a point in $(\mathbf{Z}/n\mathbf{Z})^2$ of order n.

Proposition 2.2 ([Zywc, Proposition 2.2])**.** *Let E be an elliptic curve over $\mathbf{Q}$ for which $\rho_{E,n}(G_{\mathbf{Q}})$ is not surjective. Then $\pm\rho_{E,n}(G_{\mathbf{Q}})$ is an applicable subgroup of $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$.*

Proposition 2.2 gives necessary conditions for when a proper subgroup of $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$ can occur as the image of Galois, and hence reduces a part of the problem to a group-theoretic computation. From here, Zywina constructs the modular curves corresponding to these subgroups and classifies the rational points on them. This result gives a conjecturally complete description of the *horizontal* flavored question concerning the mod ℓ representations. We recall the applicable subgroups

$G_{n,\ell}$ of prime level ℓ as well as the j-map for their associated modular curve $X_{G_n}(\ell)$ in Appendix A. Unless otherwise stated, any subgroup $G_{n,\ell}$ of $\mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$ will be applicable and come from this list.

In [RZB15], Rouse and Zureick-Brown consider the *vertical* flavored question through their study of the 2-adic images. The authors determine the possible 2-adic images of Galois by finding all the rational points on the "tower" of 2-power level modular curves. For a subgroup H of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ and an integer n such that H contains the kernel of the reduction map $\mathrm{GL}_2(\widehat{\mathbf{Z}}) \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$, the authors define X_H to be the quotient of the modular curve $X(n)$ by the image $H(n)$ of H in $\mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$. This quotient roughly classifies elliptic curves whose adélic image of Galois is contained in H. Furthermore, the authors describe a necessary condition on the ℓ-adic image.

Definition 2.3. A subgroup $H \subset \mathrm{GL}_2(\mathbf{Z}_\ell)$ is *arithmetically maximal* if

- $\det\colon H \to \mathbf{Z}_\ell^\times$ is surjective,
- there is an $M \in H$ with determinant -1 and trace zero, and
- there is no subgroup K with $H \subseteq K$ so that X_K has genus ≥ 2.

Rouse and Zureick-Brown give an equivalent statement to that in Proposition 2.2. In particular if $E/\mathbf{Q}$ is an elliptic curve and $H = \rho_{E,2^\infty}(G_{\mathbf{Q}})$, then H is contained in an arithmetically maximal subgroup. The authors determine that there exist 727 arithmetically maximal subgroups of $\mathrm{GL}_2(\mathbf{Z}_2)$ and give a beautifully detailed diagram of these subgroups (see [RZB15, Figure 1]). As above, let H_i denote the ith subgroup in their list (as given in [RZB, `gl2data.txt`]) and $j(H_i)$ its respective j-map; the level of H_i will be clear from the context.

3. Composite level modular curves

In this section, we discuss models for our composite level modular curves. Recall that the composite-$(2^m, \ell)$ level modular curve is the normalization of the fibered product $X_{G_n}(\ell) \times_{\mathbf{P}^1_{\mathbf{Q}}} X_{H_i}(2^m)$, where the maps to $\mathbf{P}^1_{\mathbf{Q}}$ are the j-maps $j(G_{n,\ell})$ and $j(H_i)$ of $X_{G_n}(\ell)$ and $X_{H_i}(2^m)$, respectively.

3.1. **Models for Theorem A.** In the proof of Theorem A, we build the "tower" of $(2^n \cdot 3)$-power level modular curves. First, we compute the rational points on the level 6 modular curves, which acts as the foundation of our tower. If the subgroup $H \times G \subset \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \times \mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z}) \cong \mathrm{GL}_2(\mathbf{Z}/6\mathbf{Z})$ occurs as a composite image of Galois, then we find the subgroups of level 4 from [RZB, `gl2data.txt`] that cover H (e.g., that contain H in the kernel of reduction). We find such level 4 subgroups for all six possible composite-$(2, 3)$ images and proceed by computing the rational points on the composite-$(4, 3)$ level modular curves. We repeat this procedure for each tier of our tower ending with level 16.

For $n = 1$, we sometimes find hyperelliptic models. For $n = 2, 3, 4$, we often find models for the composite-$(2^n, 3)$ level modular curves as superelliptic curves defined by the affine equation $y^3 = f(x^2)$.

3.2. **Models for Theorem C.** The discriminant condition allows us to construct hyperelliptic models for the composite-$(2, \ell)$ level modular curves in Theorem C. Indeed, an elliptic curve $E/\mathbf{Q}$ with such a discriminant has 2-division field $\mathbf{Q}(E[2])$ isomorphic to $\mathbf{Q}(\alpha)$, where α is a root of the defining cubic equation $f(x)$ of E,

which is equivalent to j_E being of the form $s^2 + 1728$ for some $s \in \mathbf{Q}$. For applicable subgroups $G_{n,\ell} \subset \mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$, except for the level 11 subgroup $G_{3,11}$, the composite-$(2, \ell)$ level modular curve has the form

$$X_{G_{3,2},G_{n,\ell}}(2 \cdot \ell) \colon s^2 + 1728 = f(t)/g(t),$$

where $f, g \in \mathbf{Q}[t]$. Through some simple manipulation, we rewrite our modular curve as $g(t)^2 s^2 = f(t)g(t) - 1728g(t)^2 = h(t)^2 w(t)$ for some $h, w \in \mathbf{Q}[t]$. Then we consider the birational map

$$\begin{aligned} \varphi \colon X_{G_{3,2},G_{n,\ell}}(2 \cdot \ell) &\longrightarrow X \\ (s, t) &\longmapsto (g(t)s/h(t), t). \end{aligned}$$

Hence we have reduced our problem to finding the rational points on the hyperelliptic curve

$$X \colon y^2 = w(t).$$

Remark 3.1. In the proofs of Theorems A and C, we first consider maximal applicable subgroups. If $H, H' \subseteq \mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$ are both applicable such that H is maximal and $H' \subset H$, then we have a map between the composite level modular curves $X_{G,H'} \to X_{G,H}$. Hence, the points on $X_{G,H'}$ must map to points on $X_{G,H}$. In particular, if $X_{G,H}(\mathbf{Q})$ is finite, then so is $X_{G,H'}(\mathbf{Q})$.

4. Analysis of rational points—theory

The composite level curves whose models we computed have genera ranging from 0 to 7. See Table 1 for a list of the genera which appear in each composite level.

4.1. **Low genus curves.** For the genus 0 curves, we determine whether the curve has a rational point, and if so we compute an explicit isomorphism with $\mathbf{P}^1_{\mathbf{Q}}$. For the genus 1 curves, we determine whether the curves have a non-singular rational point, and if so we compute a model for the resulting elliptic curve and determine its rank and torsion subgroup. This is straightforward: most of the covering maps have degree 2, so we end up with a model of the form $y^2 = p(t)$, where $p(t)$ is a polynomial, and the desired technique is implemented in `Magma`. The remaining cases are handled via other techniques.

For the higher genera, our toolkit to analyze rational points consists of:

(1) local methods,
(2) the Chabauty–Coleman method,
(3) quotients,
(4) étale descent,
(5) the Mordell–Weil sieve,
(6) Prym varieties.

Below, we describe some of the theory behind these techniques and the subsequent sections provide a case by case analysis of the rational points on our composite level modular curves.

Remark 4.1 (Facts about rational points on $X_{G,H}$). Every rational point on a curve $X_{G,H}$ of genus one that has rank zero is a cusp or a CM point. Also, all the rational point curves of higher genera are either cusps or CM points, and hence there are no *sporadic* points.

TABLE 1. Data of isomorphism classes for composite level modular curves

Type	$(2,3)$	$(4,3)$	$(8,3)$	$(16,3)$	$(2,5)$	$(2,7)$	$(2,11)$
$\mathbf{P}^1$	6	5	4	4	1	1	
Elliptic curve with rank 0	2	14	12				
Elliptic curve with rank > 0			2				
Genus 2			8		1	3	
Genus 3 and hyperelliptic				8		2	
Genus 3 and non-hyperelliptic				5			
Genus 4 and non-hyperelliptic				6			
Genus 6 and hyperelliptic				2			
Genus 7 and non-hyperelliptic							1

4.2. **The Chabauty–Coleman method.** Let $X/\mathbf{Q}$ be a smooth, projective, and geometrically integral curve. In 1941, Chabauty [Cha41] proved the finiteness of $X(\mathbf{Q})$ under the condition that the Jacobian J of C has rank $r := \mathrm{rk}_{\mathbf{Z}}\, J(\mathbf{Q})$ less than the genus g of X. Chabauty's idea was to consider $X(\mathbf{Q})$ inside the more tractable space $X(\mathbf{Q}_p) \cap \overline{J(\mathbf{Q})}$, where $\overline{J(\mathbf{Q})}$ is the p-adic closure of $J(\mathbf{Q})$ inside of $J(\mathbf{Q}_p)$. To deduce finiteness of this intersection, Chabauty constructed locally analytic functions, which are p-adic integrals in modern parlance, vanishing on $X(\mathbf{Q})$ and deduced his result utilizing the fact that an analytic function cannot take a value infinitely often.

Using techniques from p-adic analysis, namely Newton polygons, Coleman [Col85] controlled the zeros of these p-adic integrals to give an explicit upper bound on the number of $\mathbf{Q}$-points of a curve over $\mathbf{Q}$ when the rank $r \leq g-1$ and p is a prime of good reduction. The practical output is that if $r \leq g-1$, then p-adic integration produces an explicit 1-variable power series $f \in \mathbf{Z}_p[\![t]\!]$ whose set of $\mathbf{Z}_p$-solutions contains all of the rational points. This is all implemented in `Magma` for genus 2 curves over $\mathbf{Q}$, and in Section 5.2, we discuss the documentation.

In Section 6.2.3, we perform an explicit Chabauty computation for a non-hyperelliptic genus 3 curves, so we briefly recall results from p-adic integration; we refer the reader to [MP12, KRZB18] for further details. Let $C_{\mathbf{Q}_p}$ denote the base change of C to $\mathbf{Q}_p$ for p a prime of good reduction. Given a point $P \in X_{\mathbf{F}_p}(\mathbf{F}_p)$, the inverse image of P under the surjective reduction map

$$\rho\colon C(\mathbf{Q}_p) \twoheadrightarrow C_{\mathbf{F}_p}(\mathbf{F}_p)$$

is isomorphic to a p-adic disk D_P; this isomorhpism is induced by the uniformizer t at any point $Q \in D_P$. Since the p-adic disk has trivial de Rham cohomology, any $\omega \in H^0(C_{\mathbf{Q}_p}, \Omega^1)$ can be expressed as a power series on D_P:

$$\omega|_{D_P} = \sum_{i=0}^{\infty} a_i t^i dt \in \mathbf{Z}_p[\![t]\!]dt.$$

Now for $Q_1, Q_2 \in D_P$, the p-adic integral is defined by formal antidifferentiation as

$$\int_{Q_1}^{Q_2} \omega := \int_{t(Q_1)}^{t(Q_2)} \sum_{i=0}^{\infty} a_i t^i dt = \left(\sum_{i=0}^{\infty} \frac{a_i}{i+1} t^{i+1} \right) \Bigg|_{t(Q_1)}^{t(Q_2)}.$$

To summarize, the Chabauty–Coleman method states that if $r \leq g-1$ and p is a prime of good reduction, then there exists a $(g-r)$-dimensional space of differentials $\Lambda_C \subset H^0(C_{\mathbf{Q}_p}, \Omega^1)$ such that the p-adic integrals $\int \omega$ vanish on $\mathbf{Q}$-points of C. Using results on Newton polygons, we can effectively bound these zeros inside each residue disk.

4.3. **Étale descent.** Étale descent is a "going up" style technique, first studied in [CG89, Wet97] and developed as a full theory in [Sko01]. It is now a standard technique for resolving the rational points on curves (cf. [FW01, Bru03]).

Let $\pi\colon X \to Y$ be a degree n étale cover defined over a number field K such that Y is the quotient of some free action of a group G on X. By Riemann–Hurwitz, the genus of X is $ng(Y) - (n-1)$. Then there exists a finite collection $\pi_1\colon X_1 \to Y, \ldots, \pi_n\colon X_n \to Y$ of twists of $X \to Y$ such that

$$\bigcup_{i=1}^{n} \pi_i(X_i(K)) = Y(K).$$

We shall use this procedure in the case of étale double covers. In this case, $G = \mathbf{Z}/2\mathbf{Z}$, and since the twists are consequently quadratic, we will instead denote the twist of a double cover $X \to Y$ by $X_d \to Y$, where $d \in K^\times/(K^\times)^2$. The above discussion gives that, for any point of $Y(K)$, there will exist $d \in \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^2$ such that P lifts to a point of $X_d(K)$, where S is the union of the sets of primes of bad reduction of X and Y and of the primes of $\mathcal{O}_K$ lying over 2.

4.4. **The Mordell–Weil sieve.** In many situations, we encounter a curve C with only one known, non-singular $\mathbf{Q}$-point ∞, and we wish to prove that $C(\mathbf{Q}) = \{\infty\}$. We can define an Abel–Jacobi map based at ∞, which allows us to consider the commuting diagram

$$\begin{array}{ccc} C(\mathbf{Q}) & \xhookrightarrow{\quad\iota\quad} & J(\mathbf{Q}) \\ \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\alpha} \\ \prod_{p\in S} C_{\mathbf{F}_p}(\mathbf{F}_p) & \xhookrightarrow{\quad\iota_S\quad} & \prod_{p\in S} J_{\mathbf{F}_p}(\mathbf{F}_p) \end{array}$$

where S is the set of primes of good reduction.

Suppose that there exist some other non-singular point $\infty \neq P \in C(\mathbf{Q})$. The idea of the Mordell–Weil sieve is to derive a contradiction from various bits of local information coming from ι_S, using the global constraint that a rational point on the curve maps into $J(\mathbf{Q})$. We explain the details in Section 6.1, and refer the reader to [BS10] for a further discussion.

4.5. **Prym varieties.** Let $\pi\colon D \to C$ be an unramified finite morphism of degree 2 between curves over K and let $\iota\colon D \to D$ be the non-trivial involution of D/C. The Riemann–Hurwitz theorem implies that $g(C) > 0$ and $g(D) = 2g(C) - 1$. The associated *Prym variety* $\mathrm{Prym}(D/C)$ is the connected component containing 0 of the kernel $\pi_*\colon J_D \to J_C$, which coincides with the image of $(\mathrm{id}_* - \iota_*)\colon J_D \to J_D$. Moreover, $\mathrm{Prym}(D/C)$ is an abelian subvariety of J_D of dimension $g(C) - 1$ with

principal polarization coming from the restriction of the principal polarization on J_D. Historically, Prym varieties provided examples of principally polarized abelian varieties, which are not Jacobian varieties.

In our situation, C is a genus 3 non-hyperelliptic curve. Bruin [Bru08] finds an explicit description of the associated Prym variety as J_F, where F is a genus 2 hyperelliptic curve. In addition to the description of the Prym variety, he gives an explicitly computable map $\varphi\colon D_\delta \to J_{F_\delta}$. Bruin's map does not require the existence of a rational point on D_δ, so we could apply this construction to prove that $D_\delta(\mathbf{Q})$ is empty even if D_δ does have local points everywhere. In good circumstances, the rank of $J_{F_\delta}(\mathbf{Q})$ is 0 for all relevant twists, and after finding the torsion subgroup of $J_{F_\delta}(\mathbf{Q})$ and pulling back to $D_\delta(\mathbf{Q})$, we can determine the $\mathbf{Q}$-points of C by computing the image of $D_\delta(\mathbf{Q})$ under π. If the rank is positive, then one must proceed in a different manner.

5. Analysis of rational points—genus 2

There are 12 isomorphism classes of composite level modular curves with genus 2. Among these, six have Jacobians with rank 0, four with rank 1, and two with rank 2. We will use étale descent on the rank 2 cases and Chabauty and quotients on the others. In each case, the rank of the Jacobian is computed with `Magma`'s `RankBound` instrinsic. In the subsections below, the curve X will denote a hyperelliptic curve of genus 2, and J_X its Jacobian.

5.1. **Rank 0.** If $\mathrm{rk}\, J_X(\mathbf{Q}) = 0$, then $J_X(\mathbf{Q})$ is torsion. To find all of the rational points on X, it suffices to compute the torsion subgroup of $J_X(\mathbf{Q})$ and compute the preimages under an Abel–Jacobi map $X \hookrightarrow J_X$. This is implemented in `Magma` as the `Chabauty0(J)` command, where `J` is J_X.

5.2. **Rank 1.** If $\mathrm{rk}\, J_X(\mathbf{Q}) = 1$, then one can attempt Chabauty's method. This is implemented in `Magma` as the `Chabauty(ptJ)` command, where `ptJ` is a $\mathbf{Q}$-point on J_X which generates $J_X / J_X[\mathrm{tors}]$. The intrinsic combines the Chabauty–Coleman method with the Mordell–Weil sieve to provably find the rational points on X.

5.3. **Rank 2.** If $\mathrm{rk}\, J_X(\mathbf{Q}) = 2$, then Chabauty's method does not apply; instead, we proceed with étale descent. In each case, the Jacobian of X has a rational 2-torsion point. Thus, given a model

$$X\colon y^2 = f(x)$$

of X, f factors as $f_1 f_2$ where both polynomials are of positive, even degree, and X admits étale double covers $C_d \to X$, where the curve C_d is given by

$$C_d\colon \begin{cases} dy_1^2 = f_1(x), \\ dy_2^2 = f_2(x). \end{cases}$$

Let S denote the set of bad places as in Section 4.3. By étale descent, every rational point on X lifts to a rational point on $C_d(\mathbf{Q})$ for d in the set divisors of primes in S, their multiples, and negations. The Jacobian of C_d is isogenous to $J_X \times E_d$, where E_d is the Jacobian of the (possibly pointless) genus 1 curve $dy_2^2 = f_2(x)$ (where we assume that $\deg f_2 \geq \deg f_1$, so that $\deg f_2 \geq 3$).

The two curves $X_{H_{40},G_{4,3}}(24)$ and $X_{H_{97},G_{4,3}}(24)$ are isomorphic to the rank 2 hyperelliptic curve

$$H\colon y^2 = 2x^6 + 2 = 2(x^2+1)(x^4 - x^2 + 1).$$

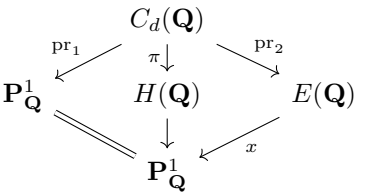
This curve admits étale covers by the genus 3 curves

$$C_d\colon \begin{cases} dy_1^2 = (x^2+1), \\ dy_2^2 = 2(x^4 - x^2 + 1) \end{cases}$$

for $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. We find that the genus 1 curves $dy_2^2 = 2(x^4 - x^2 + 1)$ only have local points everywhere when $d = 2$. We compute that the curve $2y_1^2 = (x^2+1)$ is isomorphic to $\mathbf{P}^1_{\mathbf{Q}}$ and the curve $2y_2^2 = 2(x^4 - x^2 + 1)$ is isomorphic to the rank 0 elliptic curve

$$E\colon y^2 + 2xy = x^3 - 8x^2 + 12x.$$

The diagram



tells us that the points on $C_d(\mathbf{Q})$ come from the preimages of the points on $E(\mathbf{Q})$. This allows us to determine the rational points on C_d and thus on H and on $X_{H_{40},G_{4,3}}(24)$ and $X_{H_{97},G_{4,3}}(24)$.

6. Analysis of rational points—genus 3

There are 15 isomorphism classes of genus 3 curves. Of these classes, 10 are hyperelliptic. The curves $X_{G_{3,2},G_{2,7}}(14)$ and $X_{G_{3,2},G_{6,7}}(14)$ are hyperelliptic and have rank equal to 0, and we handle these curves by using a Mordell–Weil sieve argument. The remaining hyperelliptic cases occur when considering composite-$(16,3)$ level modular curves, and we handle these cases using quotients or étale descent.

The other five isomorphism classes

$$X_{H_{105},G_{4,3}}(48),\ X_{H_{106},G_{4,3}}(48),\ X_{H_{107},G_{4,3}}(48),\ X_{H_{109},G_{4,3}}(48),\ \text{and}\ X_{H_{124},G_{4,3}}(48)$$

are non-hyperelliptic. The curve $X_{H_{109},G_{4,3}}(48)$ admits a rank 0 subquotient; by using Prym varieties, we determine the points on the rank 2 curve $X_{H_{124},G_{4,3}}(48)$; we also provably find the points on the rank 1 curve $X_{H_{106},G_{4,3}}(48)$ through a Chabauty argument. For the remaining two isomorphism classes, we are unable to compute all of the $\mathbf{Q}$-points, and we discuss our attempts in Section 6.2.4.

6.1. Analysis of genus 3 hyperelliptic curves.

As mentioned above, we find models for some composite level modular curves as genus 3 hyperelliptic curves.

6.1.1. *Analysis of* $X_{G_{3,2},G_{2,7}}(14)$. The modular curve $X_{G_{3,2},G_{2,7}}(14)$ has a model given by the genus 3 hyperelliptic curve

$$X_{G_{3,2},G_{2,7}}(14)\colon y^2 = (x^3 - 4x^2 + 3x + 1)(x^4 - 10x^3 + 27x^2 - 10x - 27).$$

For simplicity, we denote the smooth projective compactification of this modular curve by X. `Magma` computes that $\operatorname{rk} J_X(\mathbf{Q}) = 0$, so $J_X(\mathbf{Q})$ is torsion. We find that there exists a non-singular point $[1:0:0] \in X(\mathbf{Q})$, and we claim that this is in fact the only point on X. For ease of notation, we shall denote this point as P_0.

From [HS00, Exercise C.4], we have $\#J_{X_{\mathbf{F}_p}}(\mathbf{F}_p) = P_1(1)$, where $P_1(T)$ is the numerator of the Weil zeta function of $X_{\mathbf{F}_p}(\mathbf{F}_p)$ for some prime p. Moreover, by computing this value for a large number of primes and taking the greatest common divisor, we find that $\#J_X(\mathbf{Q})$ must divide 6. Since we have a non-singular point P_0 on X, we can embed X into J_X via an Abel–Jacobi map

$$\begin{array}{ccc} X(\mathbf{Q}) & \hookrightarrow & J_X(\mathbf{Q}) \\ P & \longmapsto & [P - P_0]. \end{array}$$

Our above computation tells us the possible torsion in $J_X(\mathbf{Q})$ is of order $1, 2, 3$, or 6. Recall that the prime to $p \neq 2$ torsion of $J_X(\mathbf{Q})$ injects into $J_{X,\mathbf{F}_p}(\mathbf{F}_p)$. Let $S = \{5, 11\}$ and consider the Mordell–Weil sieve from Section 4.4.

Suppose there exists another non-singular point $P \in X(\mathbf{Q})$. Since the divisor $[P - P_0]$ is a torsion point of $J_X(\mathbf{Q})$, then it must also be torsion over $\mathbf{F}_p$ for all p. Using `Magma`, we can enumerate $X_{\mathbf{F}_p}(\mathbf{F}_p)$ and check individually the orders of their respective images in $J_{X,\mathbf{F}_p}(\mathbf{F}_p)$. We compute that the points on $X_{\mathbf{F}_5}(\mathbf{F}_5)$ map to points of exact order in $\{1, 51\}$ in $J_{X,\mathbf{F}_5}(\mathbf{F}_5)$ and the points on $X_{\mathbf{F}_{11}}(\mathbf{F}_{11})$ map to points of exact order in $\{1, 8, 20, 40, 60, 120\}$ in $J_{X,\mathbf{F}_{11}}(\mathbf{F}_{11})$. Since none of these values, except for 1, coincide and the prime to p torsion injects, we have that the possible orders of the divisor $[P - P_0]$ in $J_X(\mathbf{Q})$ are either 5 or 11. However, our initial computation told us that the possible torsion in $J_X(\mathbf{Q})$ must divide 6, and so this absurdity proves that $\{P_0\} = X(\mathbf{Q})$.

6.1.2. *Analysis of* $X_{H_{156},G_{4,3}}(48)$. The modular curve $X_{H_{156},G_{4,3}}(48)$ has a model as a genus 3 hyperelliptic curve

$$X_{H_{156},G_{4,3}}(48)\colon y^2 = -x^7 - 8x.$$

For simplicity, we denote the smooth projective compactification of this modular curve by X. `Magma` computes that the rank of X is at most 3. The rational points on X lift to twists of the étale double cover by the genus 5 curves

$$C_d\colon \begin{cases} dy_1^2 = x, \\ dy_2^2 = -(x^2 + 2)(x^4 - 2x^2 + 4) \end{cases}$$

for $d \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Each of these curves maps to the genus 2 hyperelliptic curve

$$H_d\colon dy^2 = -(x^2 + 2)(x^4 - 2x^2 + 4).$$

For the above d, the Jacobian of H_d has rank 1. Using quotients and Chabauty, we determine that there are four CM points on $X_{H_{156},G_{4,3}}(48)$ corresponding to $j = -3375$ and $j = 16581375$.

6.2. **Analysis of genus 3 non-hyperelliptic curves.** In this subsection, we analyze the rational points on the composite-$(16, 3)$ level modular curves X which have affine equation $y^3 = f(x^2)$.

6.2.1. *Analysis of* $X_{H_{109},G_{4,3}}(48)$. The modular curve $X_{H_{109},G_{4,3}}(48)$ is a genus 3, non-hyperelliptic curve with affine equation

$$X_{H_{109},G_{4,3}}(48)\colon y^3 = 4(x^4 - 8x^2 + 8).$$

For simplicity, we denote the smooth projective compactification of this modular curve by X. The canonical image of $X \subset \mathbf{P}^2$ is the smooth plane quartic

$$C\colon\ -4v^4 + u^3w + 32v^2w^2 - 32w^4 = 0.$$

This curve has a two-to-one map to the elliptic curve

$$E\colon v^2 + 128v = u^3 - 2048,$$

which has rank 0 with trivial torsion subgroup. To wit, we conclude $X_{H_{109},G_{4,3}}(48)$ has no $\mathbf{Q}$-rational points.

6.2.2. *Analysis of* $X_{H_{124},G_{4,3}}(48)$. The modular curve $X_{H_{124},G_{4,3}}(48)$ is the genus 3 non-hyperelliptic curve with affine equation

$$X_{H_{124},G_{4,3}}(48)\colon y^3 = 2(x^4 + 4x^2 + 2)^2.$$

For simplicity, we denote the smooth projective compactification of this modular curve by X. We compute that X maps to an elliptic curve E with Mordell–Weil group $E(\mathbf{Q}) \cong \mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}$. The existence of two torsion in J_X implies that X admits an étale double cover. By [Bru08], a genus 3 non-hyperelliptic curve over $\mathbf{Q}$ admits an étale double cover if and only if it admits a model of the form

$$Q_1(u,v,w)Q_3(u,v,w) = Q_2(u,v,w)^2,$$

where $Q_1, Q_2, Q_3 \in \mathbf{Q}[u,v,w]$ are quadratic forms. The canonical image of $X \subset \mathbf{P}^2$ is the smooth plane quartic

$$C\colon u^4 + 4u^2v^2 + 2v^4 - 2vw^3 = 0$$

with determinantal decomposition

$$\begin{aligned} Q_1(u,v,w) &\coloneqq 2vw + 2v^2,\\ Q_2(u,v,w) &\coloneqq u^2 + 2v^2,\\ Q_3(u,v,w) &\coloneqq v^2 - vw + w^2. \end{aligned}$$

From these, we construct a genus 5, unramified double cover D_δ by

$$D_\delta\colon \begin{cases} Q_1(u,v,w) = \delta r^2,\\ Q_2(u,v,w) = \delta rs,\\ Q_3(u,v,w) = \delta s^2, \end{cases}$$

where $\delta \in \{\pm1, \pm2, \pm3, \pm6\}$. Let $\iota\colon [u:v:w:r:s] \mapsto [u:v:w:-r:-s]$ be an involution of D_δ. Every point on $C(\mathbf{Q})$ lifts to two points on $D_\delta(\mathbf{Q})$ via ι. Thus, in order to determine the rational points on C, it suffices to determine the rational points on D_δ for each δ.

Let $P_0 = [1:0:0:0:1] \in D_\delta(\mathbf{Q})$. We can embed D_δ in J_{D_δ} via an Abel–Jacobi map

$$\begin{array}{ccc} D_\delta & \hookrightarrow & J_{D_\delta}\\ P & \longmapsto & [P - P_0]. \end{array}$$

When we compose this map with the projection map $(\mathrm{id}_* - \iota_*)\colon J_{D_\delta} \to \mathrm{Prym}(D_\delta/C)$, we obtain the Abel–Prym map

$$\begin{array}{rcl} D_\delta & \longrightarrow & \mathrm{Prym}(D_\delta/C) \\ P & \longmapsto & [P - \iota(P)] - [P_0 - \iota(P_0)]. \end{array}$$

Using the `Magma` code from [Bru08], we have the diagram

$$\begin{array}{ccc} D_\delta & \xrightarrow{\varphi} & J_{F_\delta} \\ \downarrow & & \\ C & & \end{array}$$

where F_δ is a genus 2 hyperelliptic curve. We find that every twist but the trivial one either has no real points or is not locally soluble at 2 or 3. When $\delta = 1$, we find that $J_{F_1}(\mathbf{Q})$ has rank 0 and torsion subgroup of size four. We compute that the four known points on $D_\delta(\mathbf{Q})$ map to distinct points in $J_{F_1}(\mathbf{Q})$, and hence we deduce that the two known points on $C(\mathbf{Q})$ are in fact the only points. We conclude by checking that these points are cuspidal and CM corresponding to $j = 1728$.

6.2.3. *Analysis of* $X_{H_{106},G_{4,3}}(48)$. As above, the modular curve $X_{H_{106},G_{4,3}}(48)$ is a genus 3 non-hyperelliptic curve with affine equation

$$X_{H_{106},G_{4,3}}(48)\colon y^3 = x^4 + 8x^2 + 8.$$

For simplicity, we denote the smooth projective compactification of this modular curve by X. We first attempt the above methods of quotients and Prym varieties. We find a non-trivial map from our curve X to an elliptic curve E with positive rank and $\mathbf{Z}/2\mathbf{Z}$ torsion, and so quotients do not yield a desired result. As above, the existence of two torsion implies that our curve X admits an étale double cover, and we compute the determinantal decomposition of X as well as the double cover D_δ. There exists a twist δ such that the Prym variety $\mathrm{Prym}(D_\delta/C)$ has positive rank, and so the above technique does not apply.

Using the `Magma` instrinsic

```
RankBound(x^4 + 8x^2 + 8,3);
```

we compute that the rank of X is at most 1, which suggests that we proceed by a Chabauty argument. The canonical image of $X \subset \mathbf{P}^2$ is the smooth plane quartic

$$C\colon u^4 + 8u^2v^2 + 8v^4 + vw^3 = 0.$$

We compute that $C(\mathbf{Q})$ contains two non-singular points $Q_0 \coloneqq [2:0:1]$ and $Q_1 \coloneqq [1:0:0]$, and we claim that these are in fact the only points. By considering different reduction modulo p, we see that $J_C(\mathbf{Q})[\mathrm{tors}] \subset \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Recall that for a genus 3 non-hyperelliptic curve C, the differences of bitangents of $C_{\overline{\mathbf{Q}}}$ will generate $J_{C_{\overline{\mathbf{Q}}}}[2]$. Furthermore, by determining these differences, we see that there is only a single 2-torsion point coming from the elliptic curve E, and so $J_C(\mathbf{Q}) \cong \mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

Using the point Q_1, we can define an Abel–Jacobi map $C(\mathbf{Q}) \hookrightarrow J_C(\mathbf{Q})$ and form the degree zero divisor $D = [Q_0 - Q_1]$. Observe that 5 is a prime of good

reduction for C, and consider the Chabauty setup:

$$\begin{array}{ccc} C(\mathbf{Q}) & \hookrightarrow & C(\mathbf{Q}_5) \\ \downarrow & & \downarrow \\ J_C(\mathbf{Q}) & \hookrightarrow & J_C(\mathbf{Q}_5) \end{array}$$

By considering the reduction mod 5, we see that the class D is not divisible by two or three, and hence D generates a finite index subgroup of $J_C(\mathbf{Q})$ since prime to $p \neq 2$ torsion injects [Kat81, Appendix]. We wish to find a differential $\omega_J \in H^0(J_{\mathbf{Q}_5}, \Omega^1)$ such that

$$\int_0^D \omega_J = 0.$$

We see that $6D$ lies in the kernel of reduction modulo 5 and that there are six points in $C_{\mathbf{F}_5}(\mathbf{F}_5)$; two of these, $P_0 = \overline{Q_0}$ and $P_1 = \overline{Q_1}$, lie in the image of the Mordell–Weil group under the Abel–Jacobi induced by P_1. Since C is non-hyperelliptic, the linear system $|6D + 2[Q_1]|$ is either empty or zero-dimensional, and we verify that $|6D + 2[Q_1]| = D'$, where $D' = \mathrm{Tr}([34 : 2\sqrt{-86430} : 225])$. If we set $Q = [34 : 2\sqrt{-86430} : 225]$ and Q' to be the conjugate, then we see that Q and $Q_1 = [1 : 0 : 0]$ lie in the same residue disk D_{P_1} of $C(K)$ for the ramified extension $K = \mathbf{Q}_5(\sqrt{15})$. Moreover, we have

$$\begin{aligned} \int_0^D \omega_J = \ & \frac{1}{6}\int_0^{6D} \omega_J = \frac{1}{6}\left(\int_0^{[Q-Q_1]} \omega_J + \int_0^{[Q'-Q_1]} \omega_J\right) \\ = \ & \frac{1}{6}\left(\int_{Q_1}^{Q} \omega_C + \int_{Q_1}^{Q'} \omega_C\right), \end{aligned}$$

where we identify $H^0(C_{\mathbf{Q}_5}, \Omega^1)$ with $H^0(J_{\mathbf{Q}_5}, \Omega^1)$ via [Sik09, Proposition 2.1].

We compute a basis $\{\omega, \omega', \omega''\}$ for $H^0(C_{\mathbf{Q}_5}, \Omega^1)$ such that

$$\omega|_{D_{P_1}} \equiv 2t + 2t^3 + 2t^5 + \cdots \pmod 5,$$

in particular the expression is odd in the local coordinate $t = y$. Since $t(Q) = -t(Q')$ as Q and Q' are conjugate, we see that

$$\int_{Q_1}^{Q} \omega + \int_{Q_1}^{Q'} \omega = 0,$$

and so $\omega \in \Lambda_C$. Moreover, the number of zeros for $\int \omega$ inside D_{P_1} bounds the size of $\#(C(\mathbf{Q}) \cap D_{P_1})$. Standard Chabauty results (cf. [Sik09, Section 2]) assert that ω has one zero in the residue disk D_{P_1}, and since $5 > 2 + 1 + 1$, results of Stoll [Sto06, Lemma 6.1 & Proposition 6.3] imply that the number of zeros of $\int \omega$ within D_{P_1} is bounded by 2. Therefore, we deduce that the p-adic integral $\int \omega$ only vanishes on the conjugate tuple $\{Q, Q'\}$ and on the known rational point $Q_1 = [1 : 0 : 0]$ inside D_{P_1}, and so $C(\mathbf{Q}) \cap D_{P_1} = Q_1$. A similar argument for Q_0 shows that $C(\mathbf{Q}) \cap D_{P_0} = Q_0$. The residue disks around P_0 and P_1 are the only relevant ones since these are the only points which lie in the image of the Abel–Jacobi $C_{\mathbf{F}_5}(\mathbf{F}_5) \hookrightarrow J_{X,\mathbf{F}_5}(\mathbf{F}_5)$ determined by $P \mapsto [P - P_1]$. Furthermore, we conclude that $C(\mathbf{Q}) = \{Q_0, Q_1\}$.

6.2.4. *The impish ones.* There are two isomorphism classes

$$X_{H_{105},G_{4,3}}(48)\colon y^3 = x^4 - 8x^2 + 8,$$
$$X_{H_{107},G_{4,3}}(48)\colon y^3 = 8x^4 - 8x^2 + 1$$

of non-hyperelliptic genus 3 curves whose rational points we could not provably determine. We record our attempts here, discuss why the above methods do not work, and suggest further techniques for analysis. For the remainder of this section, let X denote the smooth projective compactification of one of these modular curves.

First, these two isomorphism classes have Jacobians of rank at most 3, which strongly suggests that Chabauty's method is not possible. We next attempt an argument using Prym varieties. For each isomorphism class, we find the determinantal decomposition and form the étale double cover D_δ. To our chagrin, each X has a twist F_δ with positive rank. The curve $X_{H_{107},G_{4,3}}(48)$ has a twist F_δ with rank 1, and while Chabauty on the Prym is possible, the implement is difficult; see [Bru08, Section 8] for a "by hand" example. The other curve $X_{H_{105},G_{4,3}}(48)$ has a twist with rank 2 meaning we cannot attempt Chabauty's method on the Prym. These curves could admit other étale double covers coming from non-trivial 2-torsion in $J_X(\mathbf{Q})$. However, we determine that $J_X(\mathbf{Q})[\text{tors}] \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ through local considerations, and so each curve X only admits one such double cover.

As above, we find that these curves map to a positive rank elliptic curve, and so $J_X \sim E \times A$, where A is some abelian surface over $\mathbf{Q}$. We first attempt to decompose A into subfactors and hope that we find a rank 0 piece. We determine that A is simple over $\mathbf{Q}$ using Honda–Tate theory and computing that the characteristic polynomial of Frobenius is irreducible for some prime p. Similar computations strongly suggest that A splits over a quadratic extension $K/\mathbf{Q}$ into the the two-fold product of an elliptic curve E_2 with good reduction outside of 2 and 3. In order to find this elliptic curve, we need to enumerate the non-isomorphic elliptic curves over K with such reduction.

Thankfully, a theorem of Shafarevich [Sil09, Theorem 6.1] states that there is a finite list of such elliptic curves over any number field $K/\mathbf{Q}$. Cremona and Lingham [CL07] give an explicit algorithm for finding such curves, which involves computing the integral points on a particular set of elliptic curves. This procedure has been implemented in `Magma` as the command

```
EllipticCurveWithGoodReductionSearch(2*3*0,500);
```

(see [BCP97] for the documentation). To our chagrin, we do not find our desired elliptic curves over any quadratic extension ramified at 2 and/or 3. If one did find a quadratic extension K and the elliptic curve E_2/K as above, then one could proceed with elliptic Chabauty, a technique pioneered by Bruin [Bru03]. However, this technique is not fully implemented in `Magma` since one needs to construct a map from the curve X_K to E_2, which may or may not come from a quotient mapping. To conclude, we check that the known points are CM and/or cuspidal and conjecture that there are no other $\mathbf{Q}$-points on these curves.

7. Analysis of rational points—higher genus

In our computations, we find models for our composite level modular curve of genus greater than 3. There are three genus 6 hyperellipitc curves (two isomorphism classes $X_{H_{171},G_{4,3}}(48)$ and $X_{H_{172},G_{4,3}}(48)$). These two curves have rank equal to 0,

and we handle them by finding explicit generators for the torsion subgroup of the Jacobian. We encounter one genus 7 curve coming from the anomalous genus 1 modular curve $X_{G_{3,2}}(11)$ with infinitely many points. We also come across eight genus 4 non-hyperelliptic curves whose construction resembles that of the genus 7 curve. In some cases, we can easily find the rational points on these curves using quotients. However, there are two isomorphism classes of such curves whose $\mathbf{Q}$-points we cannot provably determine. Finally, there are three curves with unknown, large genera that come from the three outstanding cases mentioned in List A.6.

7.1. **Analysis of genus 4 non-hyperelliptic curves.** There are eight non-hyperelliptic curves of genus 4 occurring as composite-$(16,3)$ level modular curves $X_{H_n,G_{4,3}}(48)$, where $n = 149, 150, 151, 153, 160, 161, 165, 166$. For $n = 149, 151, 160, 161$, the modular curve X_{H_n} is isomorphic to a rank 0 elliptic curve; hence by computing preimages, we easily find the points on our composite level modular curve. We cannot determine the $\mathbf{Q}$-points on the two isomorphism classes (represented via their canonical image in $\mathbf{P}^3$)

$$X_{H_{150},G_{4,3}}\colon \begin{cases} AC + 3BC - D^2, \\ A^2B - 2AB^2 - 7B^3 - C^3, \end{cases}$$

$$X_{H_{153},G_{4,3}}\colon \begin{cases} AC - BC - D^2, \\ A^2B + 2AB^2 - B^3 - 65536C^3, \end{cases}$$

but we discuss our attempts below.

Let $X \coloneqq X_{H_n,G_{4,3}}(48)$ be one of the two remaining isomorphism classes defined above. By construction, the curve X is a cover of the rank 1 elliptic curve $E_1 \coloneqq X_{H_n}$. We also find that X covers another non-isogenous elliptic curve E_2 of rank 1. Computations of local zeta functions at $p = 7$ assert that

$$J_X \sim E_1 \times E_2 \times A,$$

where A is a simple abelian surface. Similar computations of local zeta functions at p^2 suggest that A is not geometrically simple and splits over some quadratic extension of $\mathbf{Q}$.

We encounter similar issues with these curves as we did in Section 6.2.4. The best possible approach is elliptic Chabauty, but we were unsuccessful in finding elliptic curves E', E'' defined over a quadratic number field K such that $A_K \sim E' \times E''$. As before, the hardest part of the implementation is finding the morphism from X_K to E' or E'' defined over K. Another approach is to construct an étale double cover of these curves. To proceed, one first shows that part of the 2-torsion in $J_X(\mathbf{Q})$ comes from an elliptic factor E. Thus, one can form the normalization of the fibered diagram $X \times_{E_1} E_3$ with $\varphi^\vee\colon E_3 \to E_1$ the dual isogeny to $\varphi\colon E_1 \to E_3$ with kernel the known 2-torsion point of E_1. This construction produces our double cover $Z \to X$ with non-optimal equations. Furthermore, working on the double cover does not ameliorate the original issue. As above, we check that the known rational points correspond to CM and/or cuspidal points.

7.2. **Analysis of genus 6 hyperelliptic curves.** There are two isomorphism classes of genus 6 hyperelliptic curves. The hyperelliptic curves

$$X_{H_{171},G_{4,3}}(48)\colon y^2 = -x^{13} + 64x,$$
$$X_{H_{172},G_{4,3}}(48)\colon y^2 = -x^{13} - 64x$$

are representatives for these classes. `Magma` computes that the rank of each of these curves is 0, and so we proceed by computing the torsion subgroup of the Jacobian for each respective curve. By evaluating Weil zeta functions and comparing invariant factor decompositions of $J_{X,\mathbf{F}_p}$, we conclude that

$$J_X(\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^6.$$

Since the 2-torsion of a hyperelliptic Jacobian is determined by the roots of the defining equation for the curve, we can find generators for each part of $J_X(\mathbf{Q})$ and conclude that these curves only possess a point at infinity and another corresponding to $[0:0:1]$.

7.3. **Analysis of $X_{G_{3,2},G_{3,11}}(22)$.** There is only one modular curve from [Zywc] of genus 1 with rank 1, namely $X_{G_3}(11)$, which is isomorphic to the elliptic curve $\mathcal{E}\colon y^2 + y = x^3 - x^2 - 7x + 10$. In the appendix (cf. Section A.5), we recall the morphism $J(x,y)$ corresponding to the map from $\mathcal{E} \to \mathbf{A}^1_{\mathbf{Q}} \cup \{\infty\}$ and that $\mathcal{E}(\mathbf{Q}) \cong \langle (4,5) \rangle$. The composite-$(2,11)$ level modular curve

$$X_{G_{3,2},G_{3,11}}(22)\colon \begin{cases} y^2 + y = x^3 - x^2 - 7x + 10, \\ s^2 + 12^3 = J(x,y) \end{cases}$$

is a genus 7 non-hyperelliptic curve in $\mathbf{A}^3_{\mathbf{Q}}$. For simplicity, we denote the smooth compactification of this curve by X. By pulling back points from $\mathcal{E}(\mathbf{Q})$, we find a cuspidal point and the CM point $[x:y:s:z] = [2:0:0:1]$ on X. Unfortunately, we are unable to provably compute the rational points on the curve X. Below, we discuss the attempted techniques and facts about said curve.

We know that

$$J_X \hookrightarrow \mathcal{E} \times A,$$

where $\mathcal{E}$ is the elliptic curve defined above and A is some 6-dimensional abelian variety. Since $\operatorname{rk} \mathcal{E} = 1$, we want A to decompose in some way; ideally, we would want A to have rank 0 some elliptic factor. Empirical evidence suggests that A is not simple over $\mathbf{Q}$ and that A is isogenous to $A_1 \times A_2 \times A_3$, where A_i are abelian surfaces. However, we are not able to determine the genus 2 curves C_i whose Jacobians J_i are isomorphic to A_i.

Remark 7.1. Jeremy Rouse has written `Magma` code which "guesses" how the Jacobian of a modular curve X decomposes by comparing point counts of X with traces of $a_f(p)$, where f is a newform of level p, and he ran this code on the composite-$(2,11)$ level modular curve $X_{G_{3,2},G_{3,11}}(22)$. His results support that A decomposes as above, but also that each A_i has analytic rank 0! Unfortunately, the genus 2 curves whose Jacobians are isomorphic to A_i are not in the LMFDB of genus 2 curves [LMF13], but this does give evidence that there are no non-obvious points on $X_{G_{3,2},G_{3,11}}(22)$.

Following another suggestion of Jeremy Rouse, the geometry of the curve suggests that we search for subcurves of X. If there exists a curve C such that $X \to C$, then there *could* exist some applicable subgroup H such that $G_{3,2} \times G_{3,11} \subseteq H \subset \mathrm{GL}_2(\mathbf{Z}/22\mathbf{Z})$, which witnesses C as the modular curve associated to H. We compute the list of such subgroups and the genera of the associated modular curves to deduce that the only modular quotient that is a $\mathbf{P}^1_{\mathbf{Q}}$ comes from the unique maximal subgroup H' of $\mathrm{GL}_2(\mathbf{Z}/22\mathbf{Z})$ containing $G_{3,2} \times G_{3,11}$. The quotient of X by its automorphism group $\mathbf{Z}/2\mathbf{Z}$ produces the known elliptic subcurve E. Although

these techniques did not produce a subcurve, they do not entirely rule out the possibility of a map from X to a curve of lower genus. We conjecture the following.

Conjecture 7.2. *There does not exist a non-CM elliptic curve E over $\mathbf{Q}$ with square discriminant such that $(\rho_{E,2} \times \rho_{E,11})(G_{\mathbf{Q}})$ is simultaneously non-surjective.*

7.4. **The cursed ones.** Up to conjugacy, there are four maximal subgroups of $\mathrm{GL}_2(\mathbf{Z}/13\mathbf{Z})$ that have surjective determinant, namely $G_{6,13}, N_{\mathrm{sp}}(13), N_{\mathrm{nsp}}(13)$, and $G_{7,13}$. Zywina handles the cases concerning the subgroups of $G_{6,13}$, and the other three subgroups correspond to the outstanding cases.

Baran [Bar14] showed that the modular curves $X_{N_{\mathrm{sp}}}(13)$ and $X_{N_{\mathrm{nsp}}}(13)$ are both isomorphic to the genus 3 curve C defined in $\mathbf{P}^2_{\mathbf{Q}}$ with equation

$$(y-z)x^3 + (2y^2+zy)x^2 + (-y^3+zy^2-2z^2y+z^3)x + (2z^2y^2-3z^3y) = 0.$$

Baran also gives the morphism from the above model to the j-line. The seven known rational points on C all correspond to cusps and CM points on $X_{N_{\mathrm{sp}}}(13)$ and $X_{N_{\mathrm{nsp}}}(13)$. Recently, Balakrishnan, Dogra, Müller, Tuitman, and Vonk [BDM$^+$17] proved that C has no other rational points, using explicit Chabauty–Kim methods. Their result is equivalent to saying that there does not exist a non-CM elliptic curve over $\mathbf{Q}$ with $\rho_{E,13}(G_{\mathbf{Q}})$ conjugate to a subgroup of $N_{\mathrm{sp}}(13)$ and $N_{\mathrm{nsp}}(13)$.

Banwait and Cremona [BC14] have shown that $X_{G_{7,13}}(13)$ is isomorphic to the genus 3 curve C' defined in $\mathbf{P}^2_{\mathbf{Q}}$ with equation

$$4x^3y - 3x^2y^2 + 3xy^3 - x^3z + 16x^2yz - 11xy^2z + 5y^3z + 3x^2z^2 + 9xyz^2 + y^2z^2 + xz^3 + 2yz^3 = 0.$$

The authors also give the morphism from the modular curve to the j-line. The four known rational points on C' correspond to a CM point and three non-CM points. Conjecturally, C' has no other rational points, which is equivalent to saying that [Zywc, Theorem 1.8(iv)] gives a necessary and sufficient condition on $\rho_{E,13}(G_{\mathbf{Q}})$.

We check that: the points on C do not pull back to points $X_{G_{3,2},N_{\mathrm{sp}}}(26)$, the point $[0:0:1]$ on C pulls back to the CM point corresponding to $j=0$ on $X_{G_{3,2},N_{\mathrm{nsp}}}(26)$, and the known points on C' do not pull back to points on $X_{G_{3,2},G_{7,13}}(26)$. Following the above conjectures, we formulate our own concerning the composite-$(2,13)$ image of Galois.

Conjecture 7.3. *There does not exist a non-CM elliptic curve E over $\mathbf{Q}$ with square discriminant such that $(\rho_{E,2} \times \rho_{E,13})(G_{\mathbf{Q}})$ is simultaneously non-surjective.*

8. Applications—entanglement fields

In this final section, we discuss applications of our results to the study of entanglement fields. An elliptic curve E over K has (m_1, m_2)-*entanglement fields* if $K(E[m_1]) \cap K(E[m_2]) \neq K$ for some positive integers m_1, m_2.

In this scenario, "most" elliptic curves over $\mathbf{Q}$ have *quadratic* $(2,n)$-entanglement fields for some $n \in \mathbf{Z}_{>0}$. Indeed, elliptic curves with square discriminant form a thin set in the sense of Serre, so "most" elliptic curves have non-square discriminant. For these curves, the 2-division field $\mathbf{Q}(E[2])$ will contain $\mathbf{Q}(\sqrt{\Delta_E})$. By Kronecker–Weber, there exists some n such that $\mathbf{Q}(\sqrt{\Delta_E})$ is contained in $\mathbf{Q}(\zeta_n)$, and the Weil pairing implies that $\mathbf{Q}(\zeta_n) \subset \mathbf{Q}(E[n])$. Therefore, these curves satisfy $\mathbf{Q}(E[2]) \cap$

$\mathbf{Q}(E[n]) \supseteq \mathbf{Q}(\sqrt{\Delta_E})$, and so "most" elliptic curves have quadratic entanglement fields.

In light of this fact, we restrict our consideration to non-CM elliptic curves over $\mathbf{Q}$ with entanglement fields $\mathbf{Q}(E[\ell_1^{m_1}]) \cap \mathbf{Q}(E[\ell_2^{m_2}]) \neq \mathbf{Q}$ for distinct primes ℓ_1, ℓ_2 and positive integers m_1, m_2. Note that this condition corresponds to the phenomena of the $(\ell_1^{m_1}, \ell_2^{m_2})$-composite level image of Galois being contained in a proper subgroup of $\rho_{E,\ell_1^{m_1}}(G_{\mathbf{Q}}) \times \rho_{E,\ell_2^{m_2}}(G_{\mathbf{Q}})$.

8.1. **Statement of results.** Using Theorem C, we prove existence results for $(2,5)$ and $(2,7)$ entanglement fields of degree 3 when E has square discriminant. We also exhibit an infinite family of elliptic curves over $\mathbf{Q}$ with $(2,p^n)$-entanglement fields of degree 3 where $3 \mid p-1$. Finally, we complete the classification of non-abelian $(2,3)$-entanglement fields first studied by Brau and Jones [BJ16]. For the remainder of this section, we ignore elliptic curves with rational full 2-torsion since these curves cannot have $(2,n)$-entanglement fields by definition.

An important tool in our study of entanglements is Goursat's topological lemma (see [Rib76, Lemma 5.2.1] for a proof).

Lemma 8.1 (Goursat's lemma)**.** *Let G_0 and G_1 be groups and $G \subseteq G_0 \times G_1$ a subgroup satisfying*

$$\pi_i(G) = G_i \quad (i \in \{0,1\}),$$

where π_i denotes the canonical projection onto the ith factor. Then there exist a normal group Q and surjective homomorphisms $\psi_0 \colon G_0 \to Q$, $\psi_1 \colon G_1 \to Q$ for which

$$G = \{(g_0, g_1) \in G_0 \times G_1 : \psi_0(g_0) = \psi_1(g_1)\}.$$

The idea is to use our results concerning composite level modular curves to find possibilities for entanglement. Then we apply Goursat's lemma to sift out the cases where entanglement cannot occur from a group-theoretic viewpoint. From here, we compute division fields using `Magma` and check for entanglements. To demonstrate the technique, we first present a result proving the lack of entanglement fields for a family of elliptic curves over $\mathbf{Q}$.

Lemma 8.2. *Let E be a non-CM elliptic curve over $\mathbf{Q}$ with square discriminant. Then $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[5]) = \mathbf{Q}$.*

Proof. From Theorem C and Proposition 2.2, we know that there is only one possibility for non-surjective composite-$(2,5)$ image, namely the image is conjugate to $G_{3,2} \times G_{9,5}$. The subgroup $G_{9,5}$ does not contain an index 3 normal subgroup, hence Lemma 8.1 implies that there does not exist a subgroup $G \leq \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \times \mathrm{GL}_2(\mathbf{Z}/5\mathbf{Z})$ that projects onto the mod 2 and mod 5 image. Therefore, these curves cannot have entanglement fields via the Galois correspondence. □

8.2. $(2,7)$**-entanglement fields.** From Theorem C, the only possibility for simultaneous non-surjective composite-$(2,7)$ image of Galois is $G_{3,2} \times G_{7,7} \leq \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \times \mathrm{GL}_2(\mathbf{Z}/7\mathbf{Z})$. The subgroup G_7 does contain an index 3, normal subgroup, so the points on the modular curve $X_{G_{3,2},G_{7,7}}(14)$ correspond to j-invariants of elliptic curves with possible entanglement fields coming from $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[7])$. Since such an elliptic curve E has 7-division field of degree 252, it is computationally inefficient to study the subfields of $\mathbf{Q}(E[7])$ or even $\mathbf{Q}(x(E[7]))$, where the latter

number field contains the x-coordinates of the 7-torsion points. Hence, in order to perform computations, we need to find a subfield of $\mathbf{Q}(E[7])$ with manageable degree.

Since $Z(\mathrm{GL}_2(\mathbf{Z}/7\mathbf{Z})) \leq G_7$ and $\#Z(\mathrm{GL}_2(\mathbf{Z}/7\mathbf{Z})) = 6$, the fixed field $L := \mathbf{Q}(E[7])^{Z(\mathrm{GL}_2(\mathbf{Z}/7\mathbf{Z}))}$ is an index 6 subfield of $\mathbf{Q}(E[7])$. From [Ade01, Table 5.1], L is a degree 42 number field defined by the 7th-modular polynomial $\Phi_7(X, j_E)$. For non-CM E coming from $X_{G_{3,2},G_{7,7}}(14)$, we compute degree 3 subfields of L and check whether they are isomorphic to $\mathbf{Q}(E[2])$; below, we give two examples of non-CM elliptic curves with mod 2 and mod 7 entanglement fields.

Example 8.3. The non-CM elliptic curves

$$E_1 \colon y^2 + xy = x^3 - 4/129825457969x - 1/1168429121721,$$
$$E_2 \colon y^2 + xy = x^3 - 4/2209x - 1/19881$$

have $(2, 7)$-entanglement fields of degree three.

8.3. $(2, p)$**-entanglement fields.** In [RS01], Rubin and Silverberg give explicit equations for elliptic curves over a field of characteristic $\neq 2, 3$ with prescribed mod 2 image of Galois. By constructing an elliptic curve over $\mathbf{Q}$ with special 2-division field, we exhibit an infinite family of elliptic curves with $(2, p)$-entanglement of degree three.

Proposition 8.4. *Let p be a prime ≥ 7 such that $3 \mid p - 1$. Then there exist infinitely many elliptic curves over $E/\mathbf{Q}$ such that $\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[p]) \cong L$, where L is the degree 3 number field of $\mathbf{Q}(\zeta_p)$ by our assumption on p. Furthermore, we give an explicit parametrization of such elliptic curves.*

Proof. Since $\varphi(p) = (p - 1)$, where φ is the Euler-totient function, the cyclotomic field $\mathbf{Q}(\zeta_p)$ contains the degree 3 intermediate field L of $\mathbf{Q}(\zeta_p)$. Gauss [Gau66] (see [Gur82, Equation 4] for a modern reference) showed that the minimal polynomial of L is

$$g(X) = X^3 + X^2 + (p - 1)X/3 - ((p - 1)/3 + kp)/9,$$

where k is uniquely determined by the integral representation $4p = (3k-2)^2+27N^2$.

Let E be the elliptic curve with defining polynomial $g(X)$. Using the change of variables $(X, Y) \to (x - 1/3, y)$, we find a Weierstrass model of the form

$$E \colon y^2 = x^3 - \frac{p}{3}x + \frac{p(2 - 3k)}{27}.$$

The construction of E forces the 2-division field $\mathbf{Q}(E[2])$ to be isomoprhic to L. Using [RS01, Theorem 1.1], the elliptic curve

$$\begin{aligned}\mathbf{E}_t \colon y^2 = x^3 &+ \frac{(1727pt^2 + p + 9/4k^2t^2 - 9/4k^2 - 3kt^2 + 3k + t^2 - 1)}{(p - 9/4k^2 + 3k - 1)}x \\ &+ \frac{(-1727pt^3 - 5181pt^2 + 3pt + p - 9/4k^2t^3 - 27/4k^2t^2)}{(p - 9/4k^2 + 3k - 1)} \\ &+ \frac{(-27/4k^2t - 9/4k^2 + 3kt^3 + 9kt^2 + 9kt + 3k - t^3 - 3t^2 - 3t - 1)}{(p - 9/4k^2 + 3k - 1)}\end{aligned}$$

has 2-torsion subgroup isomorphic to that of E for $t \in \mathbf{Q}$. The existence of the Weil pairing implies that elliptic curves of the form $\mathbf{E}_t$ satisfy $\mathbf{Q}(\mathbf{E}_t[2]) \cap \mathbf{Q}(\mathbf{E}_t[p]) \cong L$. □

Remark 8.5. Above, we present the general equation for $\mathbf{E}_t$. For a specific prime p and unique k, the defining equation for $\mathbf{E}_t$ can be quickly computed using the `Magma` intrinsic `RubinSilverbergPolynomials(2,j)`, where j is the j-invariant of the elliptic curve E.

8.4. $(2,3)$**-entanglement fields.** In a recent work [BJ16], Brau and Jones exhibit a modular curve of level 6 over $\mathbf{Q}$ whose $\mathbf{Q}$-rational points correspond to j-invariants of elliptic curves E over $\mathbf{Q}$ with $\mathbf{Q}(E[2]) \subseteq \mathbf{Q}(\zeta_3, \Delta_E^{1/3}) \subseteq \mathbf{Q}(E[3])$ and hence $(2,3)$-entanglement fields. The construction of their modular curve begins with finding the unique index 6 normal subgroups $\mathcal{N} \leq \mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z})$ defined by

$$\mathcal{N} \coloneqq \left\{ \left(\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right) : x^2 + y^2 \equiv 1 \mod 3 \right\} \sqcup \left\{ \left(\begin{smallmatrix} x & y \\ y & -x \end{smallmatrix}\right) : x^2 + y^2 \equiv -1 \mod 3 \right\}.$$

The authors observe that $\mathcal{N}$ fits into the exact sequence

$$1 \longrightarrow \mathcal{N} \hookrightarrow \mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z}) \xrightarrow{\theta} \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \longrightarrow 1.$$

Their modular curve of level 6 corresponds to the subgroup $H' \leq \mathrm{GL}_2(\mathbf{Z}/6\mathbf{Z})$ coming from the graph of θ,

$$H' \coloneqq \{(g_2, g_3) \in \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \times \mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z}) : g_2 = \theta(g_3)\}.$$

The points lying in the image of $j(X_{H'})$ correspond to j-invariants of elliptic curves over $\mathbf{Q}$ satisfying the above division field condition. The surjectivity of θ tells us that such elliptic curves have surjective mod 2 image of Galois as well. We summarize and slightly clarify their results concerning these curves in the following theorem.

Theorem 8.6 ([BJ16, Theorem 1.4])**.** *Let E be a non-CM elliptic curve over $\mathbf{Q}$ with j-invariant of the form*

$$j_E = 2^{10}3^3t^3(1 - 4t^3),$$

where $t \in \mathbf{Q} \setminus \{0, 1/2\}$. This family of elliptic curves has surjective mod 2 image of Galois and non-abelian entanglement fields

$$\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \cong \mathbf{Q}(\zeta_3, \Delta_E^{1/3}).$$

Brau and Jones pose the question [BJ16, Question 1.1] of classifying the triples (E, m_1, m_2) with E an elliptic curve over a number field K and m_1, m_2 a pair of relatively prime integers for which the mod m_1 and mod m_2 entanglement field is non-abelian over K. We ask whether the elliptic curves defined in Theorem 8.6 are the only ones with non-abelian $(2,3)$-entanglement fields. By constructing covers of the modular curve $X_{H'}$, we find another family of elliptic curves with such entanglement fields and provide a complete answer to [BJ16, Question 1.1] in the case where $K = \mathbf{Q}$ and $(m_1, m_2) = (2,3)$.

Theorem 8.7. *There exist infinitely many non-CM elliptic curves E over $\mathbf{Q}$ with composite-$(2,3)$ image of Galois conjugate to $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \times G_{3,3}$ and non-abelian entanglement fields*

$$\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \cong \mathbf{Q}(\zeta_3, \Delta_E^{1/3}).$$

In particular, these curves satisfy either

$$\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \cong \mathbf{Q}(\zeta_3, \Delta_E^{1/3}) \cong \mathbf{Q}(x(E[3]))$$

or

$$\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \cong \mathbf{Q}(\zeta_3, \Delta_E^{1/3}) \cong \mathbf{Q}(E[3]).$$

Furthermore, we provide a parametrization of such elliptic curves.

Proof. Let $G_{3,3}$ be the level 3 applicable subgroup from List A.2, which we can identify as the Borel subgroup of $\mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z})$. There exists a unique index 6 normal subgroup of $G_{3,3}$, namely

$$G' \coloneqq \langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) \rangle .$$

Since $G' \leq \mathcal{N}$, we have the following exact sequences:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{N} & \hookrightarrow & \mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z}) & \xrightarrow{\theta_1} & \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 1 & \longrightarrow & G' & \hookrightarrow & G_3 & \xrightarrow{\theta_2} & \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) & \longrightarrow & 1 \end{array}$$

Let

$$H'' \coloneqq \{(g_2, g_3) \in \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \times G_{3,3} : g_2 = \theta_2(g_3)\}$$

denote the graph of θ_2. Since $H'' \leq H'$, there is a map between the modular curves $X_{H''} \to X_{H'}$. Using List A.2, we can construct the level 6 modular curve corresponding to H'', namely

$$X_{H''} \colon 2^{10}3^3 s^3(1 - 4s^3) = \frac{27(t+1)(t+9)^3}{t^3}.$$

This is a genus 0 curve endowed with a rational point, hence isomorphic to $\mathbf{P}^1_{\mathbf{Q}}$. The rational points on the curve $X_{H''}$ correspond to elliptic curves over $\mathbf{Q}$ with composite-$(2,3)$ image conjugate to a subgroup of $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \times G_{3,3}$ and $\mathbf{Q}(E[2]) \subseteq \mathbf{Q}(\zeta_3, \Delta_E^{1/3}) \subseteq \mathbf{Q}(E[3])$.

The surjectivity of θ_2 implies that the mod 2 image is surjective, and hence the conditions on $\rho_{E,3}(G_{\mathbf{Q}})$ imply that the 3-division field has degree at least 12 and contains $\mathbf{Q}(E[2]) \subset \mathbf{Q}(\zeta_3, \Delta_E^{1/3})$. Therefore, the rational points on $X_{H''}$ classify elliptic curves with non-abelian entanglement

$$\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \cong \mathbf{Q}(\zeta_3, \Delta_E^{1/3}).$$

When $\rho_{E,3}(G_{\mathbf{Q}})$ is conjugate to $G_{3,3}$ (equivalently when the composite-$(2,3)$ image surjects onto $G_{3,3}$), we have

$$\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \cong \mathbf{Q}(\zeta_3, \Delta_E^{1/3}) \cong \mathbf{Q}(x(E[3])),$$

and when $\rho_{E,3}(G_{\mathbf{Q}})$ is conjugate to $H_{\{3,1\},3}$ or $H_{\{3,2\},3}$, then

$$\mathbf{Q}(E[2]) \cap \mathbf{Q}(E[3]) \cong \mathbf{Q}(\zeta_3, \Delta_E^{1/3}) \cong \mathbf{Q}(E[3]).$$

The parametrization for these curves can be found at [Mor17]. □

Corollary 8.8. *There do not exist non-CM j-invariants outside of those from Theorems* 8.6 *and* 8.7 *corresponding to elliptic curves with non-abelian* $(2,3)$*-entanglement fields.*

Proof. The only applicable subgroups of level 3 that have an index 6, normal subgroup are $G_{3,3}$, $H_{\{3,1\},3}$, and $H_{\{3,2\},3}$, where the latter two subgroups are index two subgroups of the first. In particular, [Zyw10, Theorem 1.2] asserts that elliptic curves with such mod 3 images have the same j-invariant; curves with the latter two images of Galois contain rational 3-torsion whereas the first does not. Since the S_3 is the only non-abelian mod 2 image of Galois, our result follows from Lemma 8.1. □

Appendix A. Applicable prime level subgroups

In this appendix, we reproduce the list of applicable subgroups from [Zywc] and give the rational function expressing the modular j-invariant for certain exceptional primes ℓ in addition to presenting these subgroups as lattices in $\mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$ for easy navigation. We decorate the cases where we cannot provably analyze the rational points on the modular curve $X_{G_{3,2},G_{n,\ell}}(2\cdot\ell)$ with a tilde. Also the subgroups are hyperlinked to their definition.

A.1. **List**$(\ell = 2)$**.** Up to conjugacy there are three proper subgroups of $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$, all of which are arithmetically maximal (see Figure 1):

$$G_{1,2} = \{I\}, \qquad G_{2,2} = \{I, \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\}, \qquad G_{3,2} = \{I, \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right)\}.$$

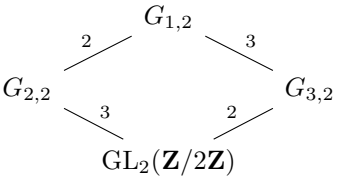


Figure 1. Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z})$

From [Zywc, Theorem 1.1], $\rho_{E,2}(G_{\mathbf{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbf{F}_2)$ to a subgroup of G_i if and only if j_E is of the form

$$J_1(t) = 256\frac{(t^2+t+1)^3}{t^2(t+1)}, \qquad J_2(t) = 256\frac{(t+1)^3}{t}, \qquad J_3(t) = t^2 + 1728$$

for some $t \in \mathbf{Q}$ and each respective i.

A.2. **List**$(\ell = 3)$**.** Define the following subgroups of $\mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z})$ (see Figure 2):

- let $G_{1,3}$ be the group $C_{\mathrm{sp}}(3)$,
- let $G_{2,3}$ be the group $N_{\mathrm{sp}}(3)$,
- let $G_{3,3}$ be the group $B(3)$,
- let $G_{4,3}$ be the group $N_{\mathrm{nsp}}(3)$,
- let $H_{\{1,1\},3}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}1&0\\0&*\end{smallmatrix}\right)$,
- let $H_{\{3,1\},3}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}1&*\\0&*\end{smallmatrix}\right)$,
- let $H_{\{3,2\},3}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix}*&*\\0&1\end{smallmatrix}\right)$.

Each of the groups G_i contains $-I$, and the groups $H_{\{i,j\},3}$ do not contain $-I$. Moreover, we have $G_{i,3} = \pm H_{\{i,j\},3}$.

From [Zywc, Theorem 1.2(ii)], $\rho_{E,3}(G_{\mathbf{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbf{F}_3)$ to a subgroup of $G_{i,3}$ if and only if j_E is of the form

$$J_1(t) = 27\frac{(t+1)^3(t+3)^3(t^2+3)^3}{t^3(t^2+3t+3)^3}, \qquad J_2(t) = 27\frac{(t+1)^3(t-3)^3}{t^3},$$

$$J_3(t) = 27\frac{(t+1)(t+9)^3}{t^3}, \qquad J_4(t) = t^3$$

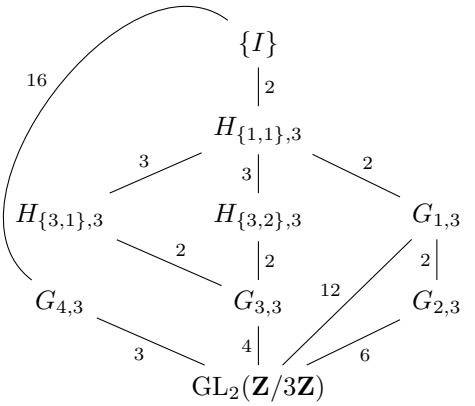


FIGURE 2. Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z})$

for some $t \in \mathbf{Q}$ and each respective i. Furthermore, [Zywc, Theorem 1.2(iii,iv)] provides explicit conditions (isomorphisms) when $\rho_{E,3}(G_{\mathbf{Q}})$ is conjugate to $H_{\{i,j\},3}$ for $i = 1, 3$ and $j = 1, 2$.

A.3. **List**$(\ell = 5)$**.** Define the following subgroups of $\mathrm{GL}_2(\mathbf{Z}/5\mathbf{Z})$ (see Figure A.3):

- let $G_{1,5}$ be the subgroup consisting of the matrices of the form $\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$,
- let $G_{2,5}$ be the group $C_{\mathrm{sp}}(5)$,
- let $G_{3,5}$ be the unique subgroup of $N_{\mathrm{nsp}}(5)$ of index 3; it is generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 0 & 1 \\ 3 & 0 \end{smallmatrix}\right)$,
- let $G_{4,5}$ be the group $N_{\mathrm{sp}}(5)$,
- let $G_{5,5}$ be the subgroup consisting of the matrices of the form $\pm\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$,
- let $G_{6,5}$ be the subgroup consisting of the matrices of the form $\pm\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$,
- let $G_{7,5}$ be the group $N_{\mathrm{nsp}}(5)$,
- let $G_{8,5}$ be the group $B(5)$,
- let $G_{9,5}$ be the unique maximal subgroup of $\mathrm{GL}_2(\mathbf{Z}/5\mathbf{Z})$ which contains $N_{\mathrm{sp}}(5)$; it is generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$,
- let $H_{\{1,1\},5}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$,
- let $H_{\{1,2\},5}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} a^2 & 0 \\ 0 & a \end{smallmatrix}\right)$,
- let $H_{\{5,1\},5}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$,
- let $H_{\{5,2\},5}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} a & * \\ 0 & a^2 \end{smallmatrix}\right)$,
- let $H_{\{6,1\},5}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$,
- let $H_{\{6,2\},5}$ be the subgroup consisting of the matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & a \end{smallmatrix}\right)$.

Each of the groups G_i contains $-I$, and the groups $H_{\{i,j\},5}$ do not contain $-I$. Moreover, we have $G_{i,5} = \pm H_{i,j}$.

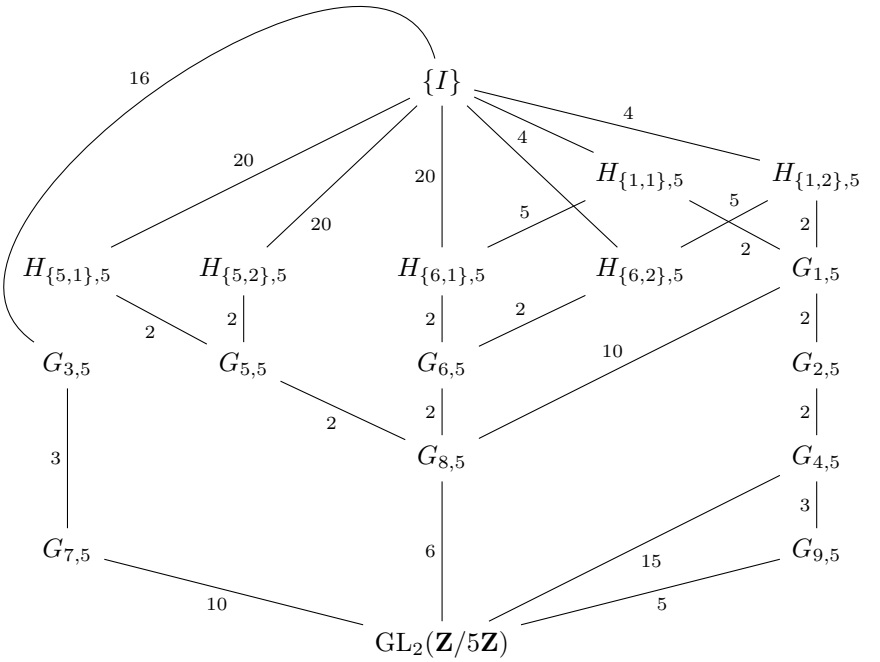


FIGURE 3. Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{Z}/5\mathbf{Z})$

From [Zywc, Theorem 1.4(ii)], $\rho_{E,5}(G_{\mathbf{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbf{F}_5)$ to a subgroup of $G_{i,5}$ if and only if j_E is of the form

$$J_1(t) = \frac{(t^{20} + 228t^{15} + 494t^{10} - 228t^5 + 1)^3}{t^5(t^{10} - 11t^5 - 1)^5},$$

$$J_2(t) = \frac{(t^2 + 5t + 5)^3(t^4 + 5t^2 + 25)^3(t^4 + 5t^3 + 20t^2 + 25t + 25)^3}{t^5(t^4 + 5t^3 + 15t^2 + 25t + 25)^5},$$

$$J_3(t) = \frac{5^4t^3(t^2 + 5t + 10)^3(2t^2 + 5t + 5)^3(4t^4 + 30t^3 + 95t^2 + 150t + 100)^3}{(t^2 + 5t + 5)^5(t^4 + 5t^3 + 15t^2 + 25t + 25)^5},$$

$$J_4(t) = \frac{(t + 5)^3(t^2 - 5)^3(t^2 + 5t + 10)^3}{(t^2 + 5t + 10)^3},$$

$$J_5(t) = \frac{(t^4 + 228t^3 + 494t^2 - 228t + 1)^3}{t(t^2 - 11t - 1)^5},$$

$$J_6(t) = \frac{(t^4 - 12t^3 + 14t^2 + 12t + 1)^3}{t^5(t^2 - 11t - 1)},$$

$$J_7(t) = \frac{5^3(t + 1)(2t + 1)^3(2t^3 - 3t + 3)^3}{(t^2 + t - 1)^5},$$

$$J_8(t) = \frac{5^2(t^2 + 10t + 5)^3}{t^5},$$

$$J_9(t) = t^3(t^2 + 5t + 40)$$

for some $t \in \mathbf{Q}$ and each respective i. Furthermore, [Zywc, Theorem 1.4(iii)] provides explicit conditions when $\rho_{E,5}(G_{\mathbf{Q}})$ is conjugate to $H_{\{i,j\},5}$ for $i = 1, 5, 6$ and $j = 1, 2$.

A.4. **List**$(\ell = 7)$**.** Define the following subgroups of $\mathrm{GL}_2(\mathbf{Z}/7\mathbf{Z})$ (see Figure 4):

- let $G_{1,7}$ be the subgroup of $N_{\mathrm{sp}}(7)$ consisting of elements of $C_{\mathrm{sp}}(7)$ with square determinant and elements of $N_{\mathrm{sp}}(7) \setminus C_{\mathrm{sp}}(7)$ with non-square determinant; it is generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 2 \\ 1 & 9 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$,
- let $G_{2,7}$ be the group $N_{\mathrm{sp}}(7)$,
- let $G_{3,7}$ be the subgroup consisting of matrices of the form $\pm\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$,
- let $G_{4,7}$ be the subgroup consisting of matrices of the form $\pm\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$,
- let $G_{5,7}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a & * \\ 0 & \pm a \end{smallmatrix}\right)$,
- let $G_{6,7}$ be the group $N_{\mathrm{nsp}}(7)$,
- let $G_{7,7}$ be the group $B(7)$,
- let $H_{\{1,1\},7}$ be the subgroup generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right)$,
- let $H_{\{3,1\},7}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$,
- let $H_{\{3,2\},7}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} \pm 1 & * \\ 0 & a^2 \end{smallmatrix}\right)$,
- let $H_{\{4,1\},7}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$,
- let $H_{\{4,2\},7}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & \pm 1 \end{smallmatrix}\right)$,
- let $H_{\{5,1\},7}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} \pm a^2 & * \\ 0 & a^2 \end{smallmatrix}\right)$,
- let $H_{\{5,2\},7}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & \pm a^2 \end{smallmatrix}\right)$,
- let $H_{\{7,1\},7}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & a^2 \end{smallmatrix}\right)$,
- let $H_{\{7,2\},7}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & * \end{smallmatrix}\right)$.

Each of the groups G_i contains $-I$, and the groups $H_{\{i,j\},7}$ do not contain $-I$. Moreover, we have $G_{i,7} = \pm H_{\{i,j\},7}$.

From [Zywc, Theorem 1.5(ii)], $\rho_{E,7}(G_{\mathbf{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbf{F}_7)$ to a subgroup of $G_{i,7}$ if and only if j_E is of the form

$$
\begin{aligned}
J_1(t) &= 3^3 \cdot 5 \cdot 7^5/2^7, \\
J_2(t) &= \frac{t(t+1)^3(t^2-5t-1)^3(t^2-5t+8)^3(t^4-5t^3+8t^2-7t+7)^3}{(t^3-4t^2+3t+1)^7}, \\
J_3(t) &= \frac{(t^2-t+1)^3(t^6-11t^5+30t^4-15t^3-10t^2+t+1)^3}{(t-1)^7t^7(t^3-8t^2+5t+1)}, \\
J_4(t) &= \frac{(t^2-t+1)^3(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)^3}{(t-1)t(t^3-8t^2+5t+1)^7}, \\
J_5(t) &= -\frac{(t^2-3t-3)^3(t^2-t+1)^3(3t^2-9t+5)^3(5t^2-t-1)^3}{(t^3-2t^2-t+1)(t^3-t^2-2t+1)^7}, \\
J_6(t) &= \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14y-7)^3}{(t^3-7t^2+7t+7)^7}, \\
J_7(t) &= \frac{(t^2+245t+2401)^3(t^2+13t+49)}{t^7}
\end{aligned}
$$

for some $t \in \mathbf{Q}$ and each respective i. Furthermore, [Zywc, Theorem 1.5(iii,iv)] provides us with explicit conditions when $\rho_{E,7}(G_{\mathbf{Q}})$ is conjugate to $H_{\{i,j\},7}$ for $i = 1, 3, 4, 5, 7$ and $j = 1, 2$.

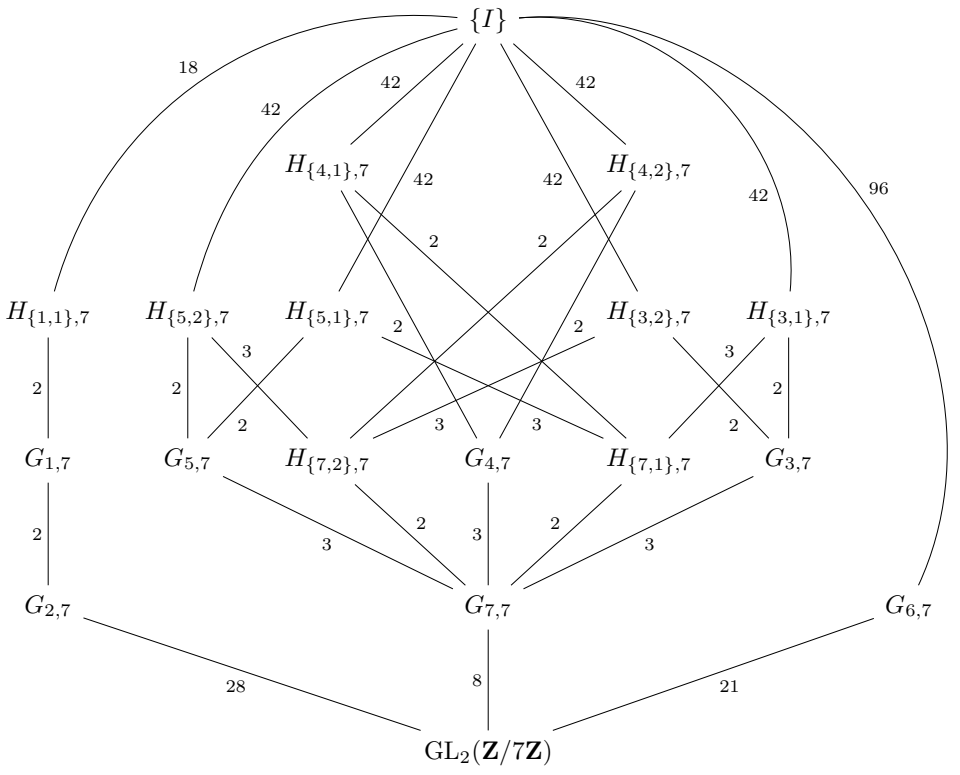


FIGURE 4. Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{Z}/7\mathbf{Z})$

A.5. **List**$(\ell = 11)$**.** Define the following subgroups of $\mathrm{GL}_2(\mathbf{Z}/11\mathbf{Z})$ (see Figure 5):

- let $G_{1,11}$ be the subgroup generated by $\pm\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}4&0\\0&6\end{smallmatrix}\right)$,
- let $G_{2,11}$ be the subgroup generated by $\pm\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}5&0\\0&7\end{smallmatrix}\right)$,
- let $G_{3,11}$ be the group $N_{\mathrm{nsp}}(11)$,
- let $H_{\{1,1\},11}$ be the subgroup generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}4&0\\0&6\end{smallmatrix}\right)$,
- let $H_{\{1,2\},11}$ be the subgroup generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}7&0\\0&5\end{smallmatrix}\right)$,
- let $H_{\{2,1\},11}$ be the subgroup generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}5&0\\0&7\end{smallmatrix}\right)$,
- let $H_{\{2,2\},11}$ be the subgroup generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}6&0\\0&4\end{smallmatrix}\right)$.

Each of the groups G_i contains $-I$, and the groups $H_{\{i,j\},11}$ do not contain $-I$. Moreover, we have $G_{i,11} = \pm H_{\{i,j\},11}$.

From [Zywc, Theorem 1.6(ii,iii)], there are unique values for j_E that correspond to $\pm\rho_{E,11}(G_{\mathbf{Q}})$ being conjugate in $\mathrm{GL}_2(\mathbf{Z}/11\mathbf{Z})$ to a subgroup of $G_{1,11}$ and $G_{2,11}$.

The modular curve $X_{G_3}(11) = X^+_{\mathrm{nsp}}(11)$ is the only one from Zywina's classification that has genus 1 with infinitely many rational points. To explicitly describe this modular curve, let $\mathcal{E}$ be the elliptic curve over $\mathbf{Q}$ defined by the Weierstrass equation $y^2 + y = x^3 - x^2 - 7x + 10$ and let $\mathcal{O}$ be the point at infinity. The Mordell–Weil group $\mathcal{E}(\mathbf{Q})$ is an infinite cyclic group generated by the point $(4, 5)$. Halberstadt [Hal98] showed that $X^+_{\mathrm{nsp}}(11)$ is isomorphic to $\mathcal{E}$ and that the morphism

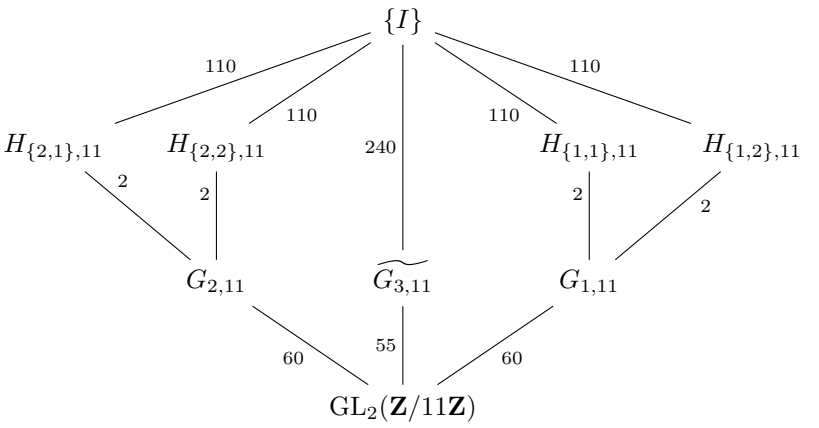


FIGURE 5. Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{Z}/11\mathbf{Z})$

to the j-line corresponds to

$$J(x,y) \coloneqq \frac{(f_1 f_2 f_3 f_4)^3}{f_5^2 f_6^{11}},$$

where

$f_1 = x^2 + 3x - 6$, $f_2 = 11(x^2 - 5y) + (2x^4 + 23x^3 - 72x^2 - 28x + 127)$,

$f_3 = 6_y + 11x - 19$, $f_4 = 22(x-2)y + (5x^3 + 17x^2 - 112x - 120)$,

$f_5 = 11y + (2x^2 + 17x - 34)$, $f_6 = (x-4)y - (5x - 9)$.

From [Zywc, Theorem 1.6(iv)], $\rho_{E,11}(G_{\mathbf{Q}})$ is conjugate to $G_{3,11}$ if and only if $j_E = J(P)$ for some point $P \in \mathcal{E}(\mathbf{Q}) \setminus \{\mathcal{O}\}$.

Remark A.1. In [Zywc, Section 4.5.5], Zywina gives explicit polynomials $A, B, C \in \mathbf{Q}[x]$ of degree 55 such that for a non-CM elliptic curve $E/\mathbf{Q}$, we have $j_E = J(P)$ for some $P \in \mathcal{E}(\mathbf{Q}) \setminus \{\mathcal{O}\}$ if and only if the polynomial $A(x)j_E^2 + B(x)j_E + C(x) \in \mathbf{Q}[x]$ has a rational root. Hence given a numerical j_E, this gives a straightforward way to check the criterion that $\rho_{E,11}(G_{\mathbf{Q}})$ is conjugate to a subgroup of $G_{3,11}$.

A.6. **List**($\ell = 13$)**.** Define the following subgroups of $\mathrm{GL}_2(\mathbf{Z}/13\mathbf{Z})$ (see Figure 6):

- let $G_{1,13}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & b^3 \end{smallmatrix}\right)$,
- let $G_{2,13}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^3 & * \\ 0 & * \end{smallmatrix}\right)$,
- let $G_{3,13}$ be the subgroup consisting of matrices $\left(\begin{smallmatrix} a & * \\ 0 & b \end{smallmatrix}\right)$ for which $(a/b)^4 = 1$,
- let $G_{4,13}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & b^2 \end{smallmatrix}\right)$,
- let $G_{5,13}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^2 & * \\ 0 & * \end{smallmatrix}\right)$,
- let $G_{6,13}$ be the group $B(13)$,
- let $G_{7,13}$ be the subgroup generated by the matrices $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)$; it contains the scalar matrices and its image in $\mathrm{PGL}_2(\mathbf{Z}/13\mathbf{Z})$ is isomorphic to $\mathfrak{S}_4$,
- let $H_{\{4,1\},13}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} * & * \\ 0 & a^4 \end{smallmatrix}\right)$,
- let $H_{\{4,2\},13}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} b^2 & * \\ 0 & a^4 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 4 \end{smallmatrix}\right)$,

- let $H_{\{5,1\},13}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^4 & * \\ 0 & * \end{smallmatrix}\right)$,
- let $H_{\{5,2\},13}$ be the subgroup consisting of matrices of the form $\left(\begin{smallmatrix} a^4 & * \\ 0 & b^2 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 4 & 0 \\ 0 & 2 \end{smallmatrix}\right)$.

Each of the groups $G_{\{i,13\}}$ contains $-I$, and the groups $H_{\{i,j\},13}$ do not contain $-I$. Moreover, we have $G_{i,13} = \pm H_{\{i,j\},13}$.

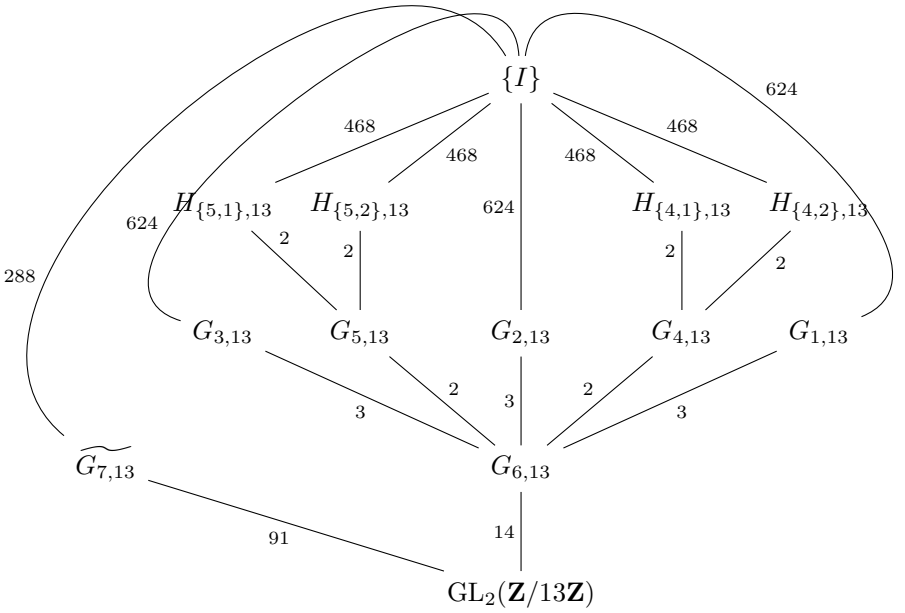


FIGURE 6. Applicable subgroup lattice for $\mathrm{GL}_2(\mathbf{Z}/13\mathbf{Z})$

Define the polynomials

$$P_1(t) = \begin{array}{c} t^{12} + 231t^{11} + 269t^{10} - 3160t^9 + 6022t^8 - 9616t^7 + 21880t^6 \\ -34102t^5 + 28297t^4 - 12455t^3 + 2876t^2 - 243t + 1 \end{array},$$

$$P_2(t) = \begin{array}{c} t^{12} - 9t^{11} + 29t^{10} - 40t^9 + 22t^8 - 16t^7 + 40t^6 \\ -22t^5 - 23t^4 + 25t^3 - 4t^2 - 3t + 1 \end{array},$$

$$P_3(t) = (t^4 - t^3 + 2t^2 - 9t + 3)(3t^4 - 3t^3 - 7t^2 + 12t - 4)(4t^4 - 4t^3 - 5t^2 + 3t - 1),$$

$$P_4(t) = t^8 + 235t^7 + 1207t^6 + 955t^5 + 3840t^4 - 955t^3 + 1207t^2 - 235t + 1,$$

$$P_5(t) = t^8 - 5t^7 + 7t^6 - 5t^5 + 5t^3 + 7t^2 + 5t + 1,$$

$$P_6(t) = t^4 + 7t^3 + 20t^2 + 19t + 1.$$

From [Zywc, Theorem 1.8(ii)], $\rho_{E,13}(G_{\mathbf{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbf{Z}/13\mathbf{Z})$ to $G_{i,13}$ if and only if j_E is of the form

$$J_1(t) = \frac{(t^2 - t + 1)^3 P_1(t)^3}{(t-1)t(t^3 - 4t^2 + t + 1)^{13}},$$

$$
\begin{aligned}
J_2(t) &= \frac{(t^2-t+1)^3 P_2(t)^3}{(t-1)^{13}t^{13}(t^3-4t^2+t+1)},\\
J_3(t) &= -\frac{13^4(t^2-t+1)^3 P_3(t)^3}{((t^3-4t^2+t+1)^{13}(5t^3-7t^2-8t+5))},\\
J_4(t) &= \frac{(t^4-t^3+5t^2+t+1)P_4(t)^3}{t(t^2-3t-1)^{13}},\\
J_5(t) &= \frac{(t^4-t^3+5t^2+t+1)P_5(t)^3}{t^{13}(t^2-3t-1)},\\
J_6(t) &= \frac{(t^2+5t+13)P_6(t)^3}{t}
\end{aligned}
$$

for some $t \in \mathbf{Q}$ and each respective i. Furthermore, [Zywc, Theorem 1.8(iii)] gives explicit conditions on when $\rho_{E,13}(G_{\mathbf{Q}})$ is conjugate to $H_{\{i,j\},13}$ for $i = 4, 5$ and $j = 1, 2$, and [Zywc, Theorem 1.8(iv)] gives necessary numerical conditions for when $\rho_{E,13}(G_{\mathbf{Q}})$ is conjugate to $G_{7,13}$. The case $\ell = 13$ is the first case for which Zywina does not give a complete description, which is due to three outstanding cases (see Section 7.4). Furthermore, the author gives equations for the modular curves $X_H(\ell)$ of level ℓ, where ℓ is a primes ≤ 37 and H is an applicable subgroup of $\mathrm{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$.

Acknowledgments

This work clearly owes a debt to Rouse–Zureick-Brown [RZB15] and Zywina [Zywc]. The author would like to graciously thank his advisor, David Zureick-Brown, for suggesting the problem and for the multitude of helpful conversations on the topic. The author extends his thanks to Jeremy Rouse for useful discussions, to Nils Bruin for supplying the proof in Section 6.2.3, and to Lea Beneish, Pete Clark, Maarten Derickx, and Filip Najman for constructive comments on an earlier draft. The computations in this paper were performed using the `Magma` computer algebra system [BCP97]. The author would also like to thank the referees for their thoughtful comments.

References

[Ade01] C. Adelmann, *The Decomposition of Primes in Torsion Point Fields*, Lecture Notes in Mathematics, vol. 1761, Springer-Verlag, Berlin, 2001. MR1836119

[BDM+17] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level* 13, Preprint (November 15, 2017). `https://arxiv.org/abs/1711.05846`.

[BC14] B. S. Banwait and J. E. Cremona, *Tetrahedral elliptic curves and the local-global principle for isogenies*, Algebra Number Theory **8** (2014), no. 5, 1201–1229, DOI 10.2140/ant.2014.8.1201. MR3263141

[Bar14] B. Baran, *An exceptional isomorphism between modular curves of level 13*, J. Number Theory **145** (2014), 273–300, DOI 10.1016/j.jnt.2014.05.017. MR3253304

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[BJ16] J. Brau and N. Jones, *Elliptic curves with* 2*-torsion contained in the* 3*-torsion field*, Proc. Amer. Math. Soc. **144** (2016), no. 3, 925–936, DOI 10.1090/proc/12786. MR3447646

[Bru03] N. Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49, DOI 10.1515/crll.2003.076. MR2011330

[Bru08] N. Bruin, *The arithmetic of Prym varieties in genus 3*, Compos. Math. **144** (2008), no. 2, 317–338, DOI 10.1112/S0010437X07003314. MR2406115

[BS10] N. Bruin and M. Stoll, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306, DOI 10.1112/S1461157009000187. MR2685127

[Cha41] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité* (French), C. R. Acad. Sci. Paris **212** (1941), 882–885. MR0004484

[Col85] R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770, DOI 10.1215/S0012-7094-85-05240-8. MR808103

[CG89] K. R. Coombes and D. R. Grant, *On heterogeneous spaces*, J. London Math. Soc. (2) **40** (1989), no. 3, 385–397, DOI 10.1112/jlms/s2-40.3.385. MR1053609

[CL07] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312. MR2367320

[Duk97] W. Duke, *Elliptic curves with no exceptional primes* (English, with English and French summaries), C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818, DOI 10.1016/S0764-4442(97)80118-8. MR1485897

[FW01] E. V. Flynn and J. L. Wetherell, *Covering collections and a challenge problem of Serre*, Acta Arith. **98** (2001), no. 2, 197–205, DOI 10.4064/aa98-2-9. MR1831612

[Gau66] C. F. Gauss, *Disquisitiones Arithmeticae*, Translated into English by Arthur A. Clarke, S. J, Yale University Press, New Haven, Conn.-London, 1966. MR0197380

[Gre10] A. Greicius, *Elliptic curves with surjective adelic Galois representations*, Experiment. Math. **19** (2010), no. 4, 495–507, DOI 10.1080/10586458.2010.10390639. MR2778661

[Gur82] S. Gurak, *Minimal polynomials for Gauss circulants and cyclotomic units*, Pacific J. Math. **102** (1982), no. 2, 347–353. MR686555

[Hal98] E. Halberstadt, *Sur la courbe modulaire $X_{ndép}(11)$* (French, with English and French summaries), Experiment. Math. **7** (1998), no. 2, 163–174. MR1677158

[HS00] M. Hindry and J. H. Silverman, *Diophantine Geometry: An introduction*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. MR1745599

[Jon10] N. Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570, DOI 10.1090/S0002-9947-09-04804-1. MR2563740

[KRZB18] E. Katz, J. Rabinoff, and D. Zureick-Brown, *Diophantine and tropical geometry, and uniformity of rational points on curves*, Algebraic Geometry: Salt Lake City 2015, Proc. Sympos. Pure Math., vol. 97, Amer. Math. Soc., Providence, RI, 2018, pp. 231–279. MR3821174

[Kat81] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502, DOI 10.1007/BF01394256. MR604840

[Lan87] S. Lang, *Elliptic Functions*, 2nd ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987. With an appendix by J. Tate. MR890960

[LMF13] The LMFDB Collaboration, *The l-functions and modular forms database*, `http://www.lmfdb.org`, 2013. [Online; accessed 16 September 2013].

[Maz77] B. Mazur, *Rational points on modular curves*, Modular Functions of One Variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Lecture Notes in Math., vol. 601, Springer, Berlin, 1977, pp. 107–148. MR0450283

[MP12] W. McCallum and B. Poonen, *The method of Chabauty and Coleman* (English, with English and French summaries), Explicit Methods in Number Theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, pp. 99–117. MR3098132

[Mor17] J. S. Morrow, *Electronic transcript of computations for the manuscript "Composite images of Galois for elliptic curves over* $\mathbf{Q}$ *& Entanglement fields"*, 2017. Available at `https://github.com/jmorrow4692/CompositeLevelandEntanglemets`.

[Rib76] K. A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804, DOI 10.2307/2373815. MR0457455

[RZB] J. Rouse and D. Zureick-Brown, *Electronic transcript of computations for the paper "Elliptic curves over* $\mathbf{Q}$ *and 2-adic images of Galois"*. Available at `http://users.wfu.edu/rouseja/2adic/`.

[RZB15] J. Rouse and D. Zureick-Brown, *Elliptic curves over* $\mathbb{Q}$ *and 2-adic images of Galois*, Res. Number Theory **1** (2015), Art. 12, 34, DOI 10.1007/s40993-015-0013-7. MR3500996

[RS01] K. Rubin and A. Silverberg, *Mod* 2 *representations of elliptic curves*, Proc. Amer. Math. Soc. **129** (2001), no. 1, 53–57, DOI 10.1090/S0002-9939-00-05539-8. MR1694877

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (French), Invent. Math. **15** (1972), no. 4, 259–331, DOI 10.1007/BF01405086. MR0387283

[Sik09] S. Siksek, *Chabauty for symmetric powers of curves*, Algebra Number Theory **3** (2009), no. 2, 209–236, DOI 10.2140/ant.2009.3.209. MR2491943

[Sil09] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094

[Sko01] A. Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001. MR1845760

[Sto06] M. Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214, DOI 10.1112/S0010437X06002168. MR2264661

[SZ] A. V. Sutherland and D. Zywina, *Modular curves of genus zero and prime-power level*, Algebra Number Theory, to appear.

[Wet97] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, ProQuest LLC, Ann Arbor, MI, 1997. Thesis (Ph.D.)–University of California, Berkeley. MR2696280

[Zyw10] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), no. 5, 811–826, DOI 10.1112/blms/bdq039. MR2721742

[Zywa] D. Zywina, *Hilbert's irreducibility theorem and the larger sieve*, arXiv preprint arXiv:1011.6465, 2010.

[Zywb] D. Zywina, *On the surjectivity of mod ℓ representations associated to elliptic curves*, preprint, 2011.

[Zywc] D. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over* **Q**, 2015. Available at `http://www.math.cornell.edu/~zywina/papers/PossibleImages/index.html`.

Department of Mathematics and Computer Science, Emory University, Atlanta, Georgia 30322

Email address: `jmorrow4692@gmail.com`