Vissuet_Kevin_PP1-144.PDF

By Kevin Vissuet

WORD COUNT	26642	TIME SUBMITTED	09-JAN-2021 09:12PM
		PAPER ID	67709094

Elliptic curves with missing Frobenius traces

by

Kevin Vissuet
B.A., Mathematics, 2013
M.S., Mathematics, 2016
M.S., Mathematics, 2018

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Chicago, 2021

Chicago, Illinois

Defense Committee:
Nathan Jones, Chair and Advisor
Alina Cojocaro
Ramin Takloo-Bighash
James Freitag
Alvaro Lozano-Robledo, University of Connecticut

To Alicia, Odin, and Freya.

ACKNOWLEDGMENT

First and foremost, I want to thank my advisor, Nathan Jones. Nathan, your unbounded and unwavering support and mentorship is what made this thesis possible. I am so grateful for your unabating patience, commitment, and encouragement throughout my mathematical career, and especially in the last few years, as the path to finishing this work became more winding than expected. I have immensely enjoyed our discussions regarding matters both mathematical and otherwise, and they are something I will always look back on with fond memories.

I would also like to thank the other members of the Number Theory group at UIC, especially Ramin Takloo-Bighash and Alina Cojocaro, for being formative influences throughout my graduate school career. Ramin, you have always been such a positive, humble, and inclusive leader and I hope to effectuate these traits as I continue my own career. Alina, your passion for Number Theory is unparalleled and inspirational, and I will never forget the kindness you have shown me. Thank you both for being members of this committee and supporting this work and my career.

I am very appreciative of the other members of my committee, James Frietag and Alvaro Lozano-Robledo, as well. Thank you for taking the time to read and provide feedback on this work, all during one of the strangest and craziest years we have witnessed.

As I move towards completing this chapter in my life, I can't help but reflect on other prominent, positive forces that helped shape who I am today. Thank you to the UIC Mathletes, particularly Sam Shideler and Jonathan Wolf, for all the miles and races that we shared. Thank

ACKNOWLEDGMENT (Continued)

you to Amit Shaw, one of the most hardworking mathematicians I know, for being a great study partner during my first two years at UIC.

Finally, I would like to thank Alicia Vissuet. I could not have asked for a better life partner. You, Odin and Freya are my greatest motivation and what pushes me to be better. I can't wait to see what is next for us.

KV

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF TABLES

SUMMARY

Let E be an elliptic curve defined over $\mathbb{Q}$. In 1976, Lang and Trotter conjectured an asymptotic formula for the number $\pi_{E,r}(X)$ of primes $p \leq X$ of good reduction for which the Frobenius trace at p associated to E is equal to a given fixed integer r. We investigate elliptic curves E over $\mathbb{Q}$ that have a missing Frobenius trace, i.e. for which the counting function $\pi_{E,r}(X)$ remains bounded as $X \to \infty$, for some $r \in \mathbb{Z}$. In particular, we classify all elliptic curves E over $\mathbb{Q}(t)$ that have a missing Frobenius trace.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Let E an elliptic curve over $\mathbb{Q}$ of conductor N_E. For a prime p not dividing N_E, we consider the Frobenius trace $a_p(E) \in \mathbb{Z}$ associated to p, which satisfies the equation

$$\#E(\mathbb{F}_p) = p + 1 - a_p(E).$$

The following conjecture, formulated by S. Lang and H. Trotter in 1976, articulates one distributional aspect of the infinite sequence $(a_p(E) : p \nmid N_E)$. Specifically, it states a precise asymptotic formula for the counting function

$$\pi_{E,r}(X) := \#\{p \leq X : p \nmid N_E,\ a_p(E) = r\}. \tag{1.1}$$

Conjecture 1.1.1. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication, let $r \in \mathbb{Z}$ and define the quantity $\pi_{E,r}(X)$ by* (Equation 1.1). *There exists a constant $C_{E,r} \geq 0$ so that, as $X \to \infty$, we have*

$$\pi_{E,r}(X) \sim C_{E,r} \frac{\sqrt{X}}{\log X}.$$

Remark 1.1.2. Conjecture 1.1.1 was developed using a probabilistic model based upon the Sato-Tate conjecture and the Chebotarev density theorem for division fields of E. In spite of the Sato-Tate conjecture having been proved (see (3) and (26)), Conjecture 1.1.1 remains open.

In case $C_{E,r} = 0$, we interpret the asymptotic of Conjecture 1.1.1 as

$$\pi_{E,r}(X) \sim 0 \text{ as } X \to \infty \iff^{\text{def}} \lim_{X\to\infty} \pi_{E,r}(X) < \infty. \tag{1.2}$$

We will presently state a precise formula for the constant $C_{E,r}$. As will be seen from that formula, in the case $C_{E,r} = 0$, we *provably* have $\lim_{X\to\infty} \pi_{E,r}(X) < \infty$. In fact, it follows from the Chebotarev density theorem that the stronger statement

$$C_{E,r} = 0 \implies \{p \text{ prime} : p \nmid N_E,\ a_p(E) = r\} = \emptyset$$

holds. When this is the case, we will call r a ***missing Frobenius trace for*** E.

In this paper, we consider elliptic curves E over $\mathbb{Q}$ that have a missing Frobenius trace, the broad goal being to classify all such elliptic curves. Here are a few examples.

Example 1.1.3. *Consider the elliptic curve* E_3 *over* $\mathbb{Q}$ *defined by the Weierstrass equation*

$$E_3 : y^2 + xy + y = x^3 - x^2 - 56x + 163.$$

The finite sequence $(a_p(E_3) \bmod 3 : p \leq 150$ *and* $p \nmid N_{E_3})$ *is equal to*

$$(0,2,0,2,0,2,0,0,2,2,0,2,0,0,0,2,2,0,2,2,0,0,2,0,2,0,2,0,2,0,0,2,0).$$

We see that the residue class $1 \bmod 3$ *is missing from this list. This is caused by the presence of a rational 3-torsion point* $P := (7,5) \in E_3[3]$. *Examining the effect of* P *on the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on* $E_3[3]$, *it follows that every* $r \in \mathbb{Z}$ *satisfying* $r \equiv 1 \bmod 3$ *is a missing Frobenius trace for* E_3.

Example 1.1.4. *Consider the elliptic curve* E_6 *over* $\mathbb{Q}$ *defined by the Weierstrass equation*

$$E_6 : \ y^2 = x^3 - 15876x - 777924.$$

The finite sequence $(a_p(E_6) \bmod 6 : p \leq 150$ *and* $p \nmid N_{E_6})$ *is equal to*

$$(4,4,5,2,5,4,0,5,0,0,5,0,2,2,5,1,2,5,5,4,0,1,0,1,0,1,0,5,4,0,0,4).$$

We see that the residue class $3 \bmod 6$ *is missing from this list. As we shall see, due to the nature of the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on the 6-torsion of* E_6, *every* $r \in \mathbb{Z}$ *satisfying* $r \equiv 3 \bmod 6$ *is a missing Frobenius trace for* E_6. *Furthermore,* $m = 6$ *is the smallest level for which* E_6 *has a missing trace modulo* m.

Example 1.1.5. *Consider the elliptic curve* E_{28} *over* $\mathbb{Q}$ *defined by the Weierstrass equation*

$$E_{28}: \ y^2 = x^3 - 7138223372x + 232131092574192.$$

The finite sequence $(a_p(E_{28}) \bmod 28 : p \leq 580$ *and* $p \nmid N_{E_{28}})$ *is equal to*

$(0, 1, 2, 26, 25, 22, 24, 19, 10, 9, 26, 22, 2, 24, 1, 10, 6, 10, 10, 16, 21, 21, 25, 22, 18, 23, 6, 20, 0, 19, 16,$
$11, 4, 17, 6, 16, 21, 16, 5, 24, 19, 15, 10, 26, 0, 14, 1, 3, 6, 14, 14, 21, 4, 18, 14, 3, 27, 14, 5, 14, 18, 21, 27,$
$20, 27, 16, 9, 25, 24, 0, 11, 22, 6, 3, 13, 10, 25, 2, 19, 18, 21, 20, 4, 6, 3, 2, 6, 20, 4, 12, 26, 18, 26, 21, 14,$
$8, 11, 26, 23, 4, 3, 16, 18).$

We see that the residue class $7 \bmod 28$ *is missing from this list. As we shall see, due to the nature of the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on the* 28*-torsion of* E_{28}*, every* $r \in \mathbb{Z}$ *satisfying* $r \equiv 7 \bmod 28$ *is a missing Frobenius trace for* E_{28}*. Furthermore, we see that* $m = 28$ *is the smallest level for which* E_{28} *has a missing trace modulo* m*.*

Towards the goal of describing explicitly the constant $C_{E,r}$, we now consider the continuous Galois representations

$$\rho_{E,m} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

$$\rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

where $\rho_{E,m}$ is defined by letting $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ act on $E[m]$ and fixing a $\mathbb{Z}/m\mathbb{Z}$-basis thereof, and ρ_E is likewise defined by letting $G_{\mathbb{Q}}$ act on the entire torsion subgroup $E_{\mathrm{tors}} := \bigcup_{m=1}^{\infty} E[m]$ of E and choosing a $\mathbb{Z}/m\mathbb{Z}$-basis of each $E[m]$ in a compatible manner. Here,

$$\hat{\mathbb{Z}} := \varprojlim \mathbb{Z}/m\mathbb{Z} \simeq \prod_{\ell \text{ prime}} \mathbb{Z}_\ell,$$

is the inverse limit of the projective system $\{\mathbb{Z}/m\mathbb{Z} : m \in \mathbb{N}\}$, ordered according to divisibility and with the canonical projection maps. We may likewise view ρ_E as being the inverse limit of the system of representations $\rho_{E,m}$, with $m \in \mathbb{N}$. A famous theorem due to Serre (23) states that, if E has no complex multiplication, then $\rho_E(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is an *open* subgroup, or, equivalently, that the index of $\rho_E(G_{\mathbb{Q}})$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is finite. Consequently, there is a positive integer m for which

$$\ker\left(\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})\right) \subseteq \rho_E(G_{\mathbb{Q}}).$$

We define $m_E \in \mathbb{N}$ to be the smallest positive integer m for which this holds.

As described in detail in (16), the constant $C_{E,r}$ appearing in Conjecture 1.1.1 is given by

$$C_{E,r} = \frac{m_E |\rho_{E,m_E}(G_{\mathbb{Q}})_r|}{|\rho_{E,m_E}(G_{\mathbb{Q}})|} \prod_{\substack{\ell \text{ prime} \\ \ell \nmid m_E}} \frac{\ell |\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})_r|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}, \tag{1.3}$$

where, for any subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, we are employing the notation

$$H_r := \{g \in H : \mathrm{tr}\, g \equiv r \bmod m\}.$$

Furthermore, it can be verified by direct computation that the infinite product over primes $\ell \nmid m_E$ in (Equation 1.3) is *convergent*, and a straightforward computation shows that each ℓ-th factor $\frac{\ell|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})r|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}$ is nonzero for any $r \in \mathbb{Z}$. It follows that, for any elliptic curve E over $\mathbb{Q}$ without complex multiplication, we have

$$C_{E,r} = 0 \iff \exists m \mid m_E \text{ for which } \rho_{E,m}(G_{\mathbb{Q}})_r = \emptyset.$$

To find elliptic curves E with missing Frobenius traces (i.e. which satisfy $C_{E,r} = 0$ for some $r \in \mathbb{Z}$), we are thus led to associate such elliptic curves E with points on a modular curve of level m. Specifically, fix a subgroup $G \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ satisfying

$$\exists r \in \mathbb{Z} \text{ for which } G_r = \emptyset. \tag{1.4}$$

For such a group G, let $\tilde{G} := \langle G, -I \rangle$, and consider the modular curve $X_{\tilde{G}}$, whose non-CM rational points correspond to j-invariants of elliptic curves E with $\rho_{E,m}(G_{\mathbb{Q}}) \subseteq \tilde{G}$, up to conjugation inside $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ (for more details, see (7)). Our main theorem focuses on the case where $X_{\tilde{G}}$ has genus zero. Since our goal is to classify all elliptic curves E such that $C_{E,r} = 0$ for some $r \in \mathbb{Z}$, we may as well consider only *maximal* subgroups $G \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ among those satisfying (Equation 1.4). Furthermore, because we will be varying the level m, we will phrase our definitions in terms of open subgroups $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$. For any open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$,

we denote by $\mathfrak{m}_G$ its *level*, i.e. the smallest $\mathfrak{m} \in \mathbb{N}$ for which $\ker\left(\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/\mathfrak{m}\mathbb{Z})\right) \subseteq G$, and for any $\mathfrak{m} \in \mathbb{N}$ we define

$$G(\mathfrak{m}) := G \bmod \mathfrak{m} \subseteq \mathrm{GL}_2(\mathbb{Z}/\mathfrak{m}\mathbb{Z}).$$

We extend our notation for the associated modular curve by setting $\tilde{G} := \langle G, -I \rangle$ and setting the notation

$$X_{\tilde{G}} := X_{\tilde{G}(\mathfrak{m}_{\tilde{G}})}.$$

Furthermore, we denote by $j_{\tilde{G}} : X_{\tilde{G}} \longrightarrow X(1)$ the map which associates to any point in $X_{\tilde{G}}$ the underlying elliptic curve E. Finally, since we are only interested in subgroups G up to conjugation inside $\mathrm{GL}_2(\hat{\mathbb{Z}})$, we define the following notation, for subgroups $G_1, G_2, G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ and any integer r:

$$\begin{aligned} G_1 \doteq G_2 &\overset{\text{def}}{\iff} \exists g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) \text{ with } G_1 = gG_2g^{-1}, \\ G_1 \dot{\subseteq} G_2 &\overset{\text{def}}{\iff} \exists g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) \text{ with } G_1 \subseteq gG_2g^{-1}, \\ G_r &:= \{g \in G : \operatorname{tr} g \equiv r \bmod \mathfrak{m}_G\}. \end{aligned} \tag{1.5}$$

We consider the following collections of open subgroups $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$:

$$\begin{aligned}
\mathfrak{G} &:= \{G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}}) : G \text{ is open and } \det G = \hat{\mathbb{Z}}^\times\},\\
\mathfrak{G}(g) &:= \{G \in \mathfrak{G} : X_{\tilde{G}} \text{ has genus } g\},\\
\mathfrak{G}_{\mathrm{MT}} &:= \{G \in \mathfrak{G} : \exists r \in \mathbb{Z} \text{ with } G_r = \emptyset\},\\
\mathfrak{G}_{\mathrm{MT}}^{\max} &:= \{G \in \mathfrak{G}_{\mathrm{MT}} : G \text{ is maximal with respect to } \dot{\subseteq}\},\\
\mathfrak{G}_{\mathrm{MT}}(g) &:= \mathfrak{G}_{\mathrm{MT}} \cap \mathfrak{G}(g), \qquad \mathfrak{G}_{\mathrm{MT}}^{\max}(g) := \mathfrak{G}_{\mathrm{MT}}^{\max} \cap \mathfrak{G}(g).
\end{aligned} \tag{1.6}$$

As a consequence of the Weil pairing, for any elliptic curve E over $\mathbb{Q}$, we have $\det \rho_E(G_{\mathbb{Q}}) = \hat{\mathbb{Z}}^\times$ (see Lemma 4.2.1); this is the reason for the condition $\det G = \hat{\mathbb{Z}}^\times$ in the definition of $\mathfrak{G}$ in (Equation 1.6). As we will see, for any elliptic curve E over $\mathbb{Q}$, Conjecture 1.1.1 implies that

$$\exists r \in \mathbb{Z} \text{ with } \lim_{X\to\infty} \pi_{E,r}(X) < \infty \iff \exists G \in \mathfrak{G}_{\mathrm{MT}}^{\max} \text{ with } \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G. \tag{1.7}$$

(The implication "$\Longleftarrow$" is unconditional, whereas "$\Longrightarrow$" depends on Conjecture 1.1.1.) Thus, the goal of classifying elliptic curves E over $\mathbb{Q}$ satisfying the left-hand condition in (Equation 1.7) leads to our consideration of the rational points of the modular curves $X_{\tilde{G}}$, for each $G \in \mathfrak{G}_{\mathrm{MT}}^{\max}(g)$, for each fixed $g \geq 0$. We remark that, in case $G = \tilde{G}$ (i.e. in case $-I \in G$) and assuming $j_E \notin \{0, 1728\}$, the property that $\rho_E(G_{\mathbb{Q}}) \subseteq G$ does not vary as we twist E, i.e. we have

$$-I \in G \implies \left(\forall \tau \in \mathrm{Aut}_{\overline{\mathbb{Q}}}(E),\ \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G \Leftrightarrow \rho_{E^\tau}(G_{\mathbb{Q}}) \dot{\subseteq} G\right).$$

In particular, when $-I \in G$ and assuming $j_E \notin \{0, 1728\}$, the property that $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$ only depends on the j-invariant of E. By contrast, in case $-I \notin G$, the property $\rho_{E^\tau}(G_{\mathbb{Q}}) \dot{\subseteq} G$ depends, in general, on the automorphism τ. Thus, classifying elliptic curves E with $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$, amounts to

1. describing explicitly the map $j_{\tilde{G}} : X_{\tilde{G}} \longrightarrow X(1)$,
2. in case $-I \notin G$, describing the particular twists $\{E^\tau\}_{\tau \in \mathrm{Aut}_{\overline{\mathbb{Q}}}(E)}$ that satisfy $\rho_{E^\tau}(G_{\mathbb{Q}}) \dot{\subseteq} G$.

Our main result classifies the set of elliptic curves E over $\mathbb{Q}$ for which $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$ for some $G \in \mathfrak{G}_{\mathrm{MT}}^{\max}(0)$, in cases according to whether or not $-I \in G$, as described above. In particular, it extends each of Examples 1.1.3, 1.1.4, and 1.1.5 to the following one-parameter families. We define the rational functions in $\mathbb{Q}(t, D)$:

$$j_{3,1}(t) := 27\frac{(t+1)(t+9)^3}{t^3} \qquad d_{3,1,1}(t, D) := \frac{6(t+1)(t+9)}{t^2 - 18t - 27},$$

$$j_{6,1}(t) := 2^{10}3^3t^3(1 - 4t^3) \qquad d_{6,1,1}(t, D) := D,$$

$$j_{28,1}(t) := -\frac{(49t^4 - 13t^2 + 1)(2401t^4 - 245t^2 + 1)^3}{t^2}$$

$$d_{28,1,1}(t, D) := \frac{-7t(49t^4 - 13t^2 + 1)(2401t^4 - 245t^2 + 1)}{823543t^8 - 235298t^6 + 21609t^4 - 490t^2 - 1}. \tag{1.8}$$

Furthermore, for $(m, i) \in \{(3,1),(6,1),(28,1)\}$, we set the Weierstrass coefficients $a_{4;m,i}(t)$, $a_{6;m,i}(t) \in \mathbb{Q}(t)$ by

$$a_{4;m,i}(t) := \frac{108 j_{m,i}(t)}{1728 - j_{m,i}(t)}, \qquad a_{6;m,i}(t) := \frac{432 j_{m,i}(t)}{1728 - j_{m,i}(t)}. \tag{1.9}$$

For $(m, i, k) \in \{(3,1,1),(8,1,1),(28,1,1)\}$ we have already declared the twist parameters $d_{m,i,k}(t, D) \in \mathbb{Q}(t, D)$ in (Equation 1.8), and we define the elliptic curves $\mathcal{E}_{m,i,k}$ over $\mathbb{Q}(t, D)$ by

$$\mathcal{E}_{m,i,k} : \; d_{m,i,k}(t, D) y^2 = x^3 + a_{4;m,i}(t) x + a_{6;m,i}(t). \tag{1.10}$$

For $t_0, D_0 \in \mathbb{Q}$, we denote by $\mathcal{E}_{m,i,k}(t_0, D_0)$ the elliptic curve over $\mathbb{Q}$ obtained by specializing $\mathcal{E}_{m,i,k}$ at $t = t_0$ and $D = D_0$. The elliptic curves E_3, E_6 and E_{28} of Examples 1.1.3 - 1.1.5 satisfy

$$E_3 = \mathcal{E}_{3,1,1}(1,1), \qquad E_6 = \mathcal{E}_{6,1,1}(1,1), \qquad E_{28} = \mathcal{E}_{28,1,1}(1,1).$$

In Tables II - VI, which appear in Section 6, we associate j-invariants $j_{m,i}(t) \in \mathbb{Q}(t)$ and twist parameters $d_{m,i,k}(t, D) \in \mathbb{Q}(t, D)$ to all of the 3-tuples[1]

$$(m, i, k) \in \left\{ \begin{array}{c} (2,1,1), (3,1,1), (3,1,2), (4,1,1), (5,1,1), (5,2,1), (5,2,1), \\ (5,2,1), (6,1,1), (6,2,1), (6,3,1), (6,3,2), (7,1,1), (7,1,2), \\ (7,2,1), (7,2,2), (7,3,1), (7,3,2), (8,1,1), (9,1,1), (9,2,1), \\ (9,3,1), (9,4,1), (10,1,1), (10,1,2), (10,2,1), (10,2,2), (10,3,1), \\ (12,1,1), (12,1,2), (12,2,1), (12,3,1), (12,4,1), (14,1,1), (14,2,1), \\ (14,2,2), (14,3,1), (14,3,2), (14,4,1), (14,4,2), (14,5,1), (14,6,1), \\ (14,6,2), (14,7,1), (14,7,2), (28,1,1), (28,2,1), (28,2,2), (28,3,1), \\ (28,3,2) \end{array} \right\}. \quad (1.11)$$

Each j-invariant $j_{m,i}(t)$ in our list will correspond to the natural map $X_{\tilde{G}} \longrightarrow X(1)$ associated to a group $G \in \mathfrak{G}_{MT}^{max}(0)$ and a choice of parameter $t \in \mathbb{Q}(X_{\tilde{G}})$, and we will have $d_{m,i,k}(t, D) = D$ just in case $-I \in G$. When $-I \notin G$, we will have $d_{m,i,k}(t, D) \in \mathbb{Q}(t) \subseteq \mathbb{Q}(t, D)$, and we may also denote it simply by $d_{m,i,k}(t)$ in this case. For each j-invariant $j_{m,i}(t)$ corresponding to such a tuple (m, i, k) in (Equation 1.11), we again define the Weierstrass coefficients $a_{4;m,i}(t), a_{6;m,i}(t) \in \mathbb{Q}(t)$ by (Equation 1.9) and consider the associated elliptic curve $\mathcal{E}_{m,i,k}$ over $\mathbb{Q}(t, D)$ defined by (Equation 1.10); for $t_0, D_0 \in \mathbb{Q}$ we denote by $\mathcal{E}_{m,i,k}(t_0, D_0)$ the special-

[1] In each 3-tuple (m, i, k), the first entry m names the GL_2-level of the corresponding group; for a fixed m, the index i changes exactly if the j-invariant changes, and the last index k changes as that twist class changes for a fixed j-invariant.

ization of $\mathcal{E}_{m,i,k}(t, D)$ to $t = t_0$ and $d = D_0$. For all pairs (t_0, D_0) in a Zariski open subset of $\mathbb{A}_2(\mathbb{Q})$, the specialized curve $\mathcal{E}_{m,i,k}(t_0, D_0)$ is an elliptic curve over $\mathbb{Q}$. In case $-I \notin G$, since the corresponding elliptic curve $\mathcal{E}_{m,i,k}$ as in (Equation 1.10) is defined over $\mathbb{Q}(t)$, we may also denote simply by $\mathcal{E}_{m,i.k}(t_0)$ its specialization to $t = t_0$, which is an elliptic curve over $\mathbb{Q}$ for all but finitely many $t_0 \in \mathbb{Q}$.

Theorem 1.1.6. *Let E be an elliptic curve over $\mathbb{Q}$ with j-invariant j_E satisfying $j_E \notin \{0, 1728\}$. We have that $\exists G \in \mathfrak{G}_{MT}^{max}(0)$ with $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$ if and only if there are $t_0, D_0 \in \mathbb{Q}$ and a 3-tuple (m, i, k) in the set* (Equation 1.11) *so that E is isomorphic over $\mathbb{Q}$ to the elliptic curve*

$$\mathcal{E}_{m,i,k}(t_0, D_0): \ d_{m,i,k}(t_0, D_0)y^2 = x^3 + a_{4;m,i}(t_0)x + a_{6;m,i}(t_0),$$

where the j-invariant and twist parameter $j_{m,i}(t, D), d_{m,i,k}(t, D) \in \mathbb{Q}(t, D)$ are as listed in Tables II - VI of Section 6 and the coefficients $a_{4;m,i}(t), a_{6,m,i}(t) \in \mathbb{Q}(t)$ are defined by (Equation 1.9).

The proof of Theorem 1.1.6 falls into two steps, the first one bounding the levels associated to each of the groups $G \in \mathfrak{G}_{MT}^{max}(0)$. In addition to (Equation 1.6), we make the definitions

$$\begin{aligned} \mathfrak{G}(g, m) &:= \{G \in \mathfrak{G}(g) : m_G = m\} \\ \mathfrak{G}_{MT}(g, m) &:= \mathfrak{G}_{MT} \cap \mathfrak{G}(g, m) \\ \mathfrak{G}_{MT}^{max}(g, m) &:= \mathfrak{G}_{MT}^{max} \cap \mathfrak{G}(g, m). \end{aligned} \tag{1.12}$$

We will establish the following theorem.

Theorem 1.1.7. *Let the set* $\mathfrak{G}_{\mathrm{MT}}^{\max}(\mathfrak{g})$ *of open subgroups of* $\mathrm{GL}_2(\hat{\mathbb{Z}})$ *be as defined in* (Equation 1.6). *We then have*

$$\mathfrak{G}_{\mathrm{MT}}^{\max}(0) = \bigcup_{\mathfrak{m} \in \left\{ \substack{2,3,4,5,6,7,8, \\ 9,10,12,14,28} \right\}} \mathfrak{G}_{\mathrm{MT}}^{\max}(0, \mathfrak{m}), \tag{1.13}$$

where the set $\mathfrak{G}_{\mathrm{MT}}^{\max}(\mathfrak{g}, \mathfrak{m})$ *is as in* (Equation 1.12).

Theorem 1.1.7 is proved as follows. An equivalent formulation of a conjecture of Rademacher states that

$$\{\text{open subgroups } S \subseteq \mathrm{SL}_2(\hat{\mathbb{Z}}) : -\mathrm{I} \in S \text{ and } X_S \text{ has genus } 0\}/\doteq$$

is a finite set. This conjecture was proven by Denin (see (8), (9) and (10)). More generally, in (27) and (29), the same is shown with 0 replaced by a general $\mathfrak{g} \in \mathbb{N} \cup \{0\}$. In addition, there are several papers on the *effective* resolution of Rademacher's conjecture. In particular, Cummins and Pauli (5) have produced the complete list of the elements of

$$\{\text{open subgroups } S \subseteq \mathrm{SL}_2(\hat{\mathbb{Z}}) : -\mathrm{I} \in S \text{ and } X_S \text{ has genus } \mathfrak{g}\}/\doteq$$

for $\mathfrak{g} \leq 24$, and our proof of Theorem 1.1.7 makes use of the tables therein. We extend the notion of GL_2-level of an open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ by defining

$$\begin{aligned} \mathrm{level}_{\mathrm{GL}_2}(G) &:= \min\left\{\mathfrak{m} \in \mathbb{N} : \ker\left(\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/\mathfrak{m}\mathbb{Z})\right) \subseteq G\right\} \\ \mathrm{level}_{\mathrm{SL}_2}(G) &:= \min\left\{\mathfrak{m} \in \mathbb{N} : \ker\left(\mathrm{SL}_2(\hat{\mathbb{Z}}) \to \mathrm{SL}_2(\mathbb{Z}/\mathfrak{m}\mathbb{Z})\right) \subseteq G \cap \mathrm{SL}_2(\hat{\mathbb{Z}})\right\}. \end{aligned} \tag{1.14}$$

It is straightforward to see that $\mathrm{level}_{\mathrm{SL}_2}(G)$ divides $\mathrm{level}_{\mathrm{GL}_2}(G)$, and in general they can be different. Using the main result of (5), we will first show that

$$G \in \mathfrak{G}(0) \implies \mathrm{level}_{\mathrm{SL}_2}(G) \in \left\{ \begin{array}{c} 1,2,3,4,5,6,7,8,9,10, \\ 11,12,13,14,15,16,18,20, \\ 21,22,24,25,26,27,28,30,32, \\ 36,40,42,48,50,52,54,56,60, \\ 64,72,96 \end{array} \right\}. \tag{1.15}$$

Next, for each $G \in \mathfrak{G}_{\mathrm{MT}}^{\max}(0)$, we exhibit a positive integer d_G for which $\mathrm{level}_{\mathrm{GL}_2}(G)$ divides $d_G \cdot \mathrm{level}_{\mathrm{SL}_2}(G)$, and this, together with a MAGMA computation, yields Theorem 1.1.7.

To establish Theorem 1.1.6, we will utilize results of (25) and (30), which describe explicitly all prime power level modular curves with infinitely many rational points. For the prime power levels (other than the $m = 8$) occurring on the right-hand side of (Equation 1.13) we use those results directly; for each group G of level m that is not a prime power, the associated missing trace is caused by an *entanglement*, i.e. a non-trivial intersection

$$\mathbb{Q}(E[m_1]) \cap \mathbb{Q}(E[m_2]) \neq \mathbb{Q} \qquad (m = m_1 m_2,\ \gcd(m_1, m_2) = 1)$$

implicit in the group G (for $m = 8$, the missing trace is caused by a "vertical entanglement" and also requires additional work). In the cases involving entanglement, we undertake a finer

analysis, identifying precisely the underlying subfields and determining the subfamily for which those subfields agree.

The paper is organized as follows. In Section 4.1 we prove Theorem 1.1.7. In Section 5.1 we prove Theorem 1.1.6 and in Section 6 we summarize the results in three tables. Finally, in Section 7 we discuss future directions.

CHAPTER 2

NOTATION AND GROUP-THEORETIC PRELIMINARIES

2.1 Notation and Group-theoretic preliminaries

In this section, we gather notation and preliminary lemmas. Here and henceforth in the paper, given an open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we put

$$\mathfrak{m}_G := \mathrm{level}_{\mathrm{GL}_2}(G)$$

$$\mathfrak{m}_S := \mathrm{level}_{\mathrm{SL}_2}(G),$$

defined as in (Equation 1.14). For any open subgroup $S \subseteq \mathrm{SL}_2(\hat{\mathbb{Z}})$, we will also denote by $\mathfrak{m}_S$ its SL_2-level. Also, for any such subgroups we maintain the notation from the introduction:

$$\begin{aligned} \tilde{G} &:= \langle -I, G \rangle, \\ \tilde{S} &:= \langle -I, S \rangle. \end{aligned} \tag{2.1}$$

Proposition 2.1.1. *Let $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be an open subgroup. We then have*

$$\frac{\mathrm{level}_{\mathrm{SL}_2}(G)}{\mathrm{level}_{\mathrm{SL}_2}(\tilde{G})} \in \{1, 2\}, \tag{2.2}$$

where $\tilde{G}$ is as in (Equation 2.1).

Proof. See (15, Lemma 3.1). □

In the next lemma, for an open subgroup $\mathsf{G} \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of GL_2-level $\mathfrak{m}_\mathsf{G}$ and SL_2-level $\mathfrak{m}_\mathsf{S}$, and for an arbitrary positive integer $\mathfrak{m}$ with $\mathfrak{m}_\mathsf{S} \mid \mathfrak{m} \mid \mathfrak{m}_\mathsf{G}$, we let π_{GL_2} and $\pi_{\mathbb{G}_\mathfrak{m}}$ denote the canonical projection maps

$$\begin{aligned} \pi_{\mathrm{GL}_2} &: \mathrm{GL}_2(\mathbb{Z}/\mathfrak{m}_\mathsf{G}\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\mathfrak{m}\mathbb{Z}), \\ \pi_{\mathbb{G}_\mathfrak{m}} &: (\mathbb{Z}/\mathfrak{m}_\mathsf{G}\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/\mathfrak{m}\mathbb{Z})^\times. \end{aligned} \tag{2.3}$$

Lemma 2.1.2. *Let $\mathsf{G} \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be an open subgroup satisfying $\mathfrak{m}_\mathsf{G} \mid \mathfrak{m}_\mathsf{S}^\infty$ and let $\mathfrak{m}$ be any positive integer satisfying $\mathfrak{m}_\mathsf{S} \mid \mathfrak{m}$ and $\mathfrak{m} \mid \mathfrak{m}_\mathsf{G}$. Then there exists a unique group homomorphism*

$$\delta : \mathsf{G}(\mathfrak{m}) \longrightarrow (\mathbb{Z}/\mathfrak{m}_\mathsf{G}\mathbb{Z})^\times$$

satisfying $\pi_{\mathbb{G}_\mathfrak{m}} \circ \delta = \det$ (where $\pi_{\mathbb{G}_\mathfrak{m}}$ is the canonical projection as in (Equation 2.3)*), and such that*

$$\mathsf{G}(\mathfrak{m}_\mathsf{G}) = \left\{ g \in \pi_{\mathrm{GL}_2}^{-1}(\mathsf{G}(\mathfrak{m})) : \delta(\pi_{\mathrm{GL}_2}(g)) = \det g \right\}.$$

If $\det \mathsf{G} = \hat{\mathbb{Z}}^\times$, then δ is surjective and $\delta(\mathsf{G}(\mathfrak{m}) \cap \mathrm{SL}_2(\mathbb{Z}/\mathfrak{m}\mathbb{Z})) = \ker \pi_{\mathbb{G}_\mathfrak{m}}$.

Proof. Let $\pi_\mathsf{G} : \mathsf{G}(\mathfrak{m}_\mathsf{G}) \longrightarrow \mathsf{G}(\mathfrak{m})$ denote the restriction to $\mathsf{G}(\mathfrak{m}_\mathsf{G})$ of π_{GL_2}. We will first establish that

$$\ker \pi_\mathsf{G} = \ker\left(\mathrm{SL}_2(\mathbb{Z}/\mathfrak{m}_\mathsf{G}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/\mathfrak{m}\mathbb{Z})\right). \tag{2.4}$$

First, by definition of m_S and since $m_S \mid m$, we have

$$\ker \pi_G \supseteq \ker \left(SL_2(\mathbb{Z}/m_G\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z}) \right),$$

and we will now argue by induction that these kernels have the same size. Let p be any prime dividing m_G/m and factor π_G as

$$G(m_G) \xrightarrow{\pi_p} G(m_G/p) \xrightarrow{\pi_{m/p}} G(m), \qquad \pi_G : G(m_G) \to G(m).$$

By induction, we have that

$$\left| \ker \pi_{m/p} \right| = \left| \ker \left(SL_2(\mathbb{Z}/(m_G/p)\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z}) \right) \right|.$$

Since m_G divides m_S^∞, we see that p divides m_G/p, and so

$$\ker \left(GL_2(\mathbb{Z}/m_G\mathbb{Z}) \to GL_2(\mathbb{Z}/(m_G/p)\mathbb{Z}) \right),$$

$$\ker \left(SL_2(\mathbb{Z}/m_G\mathbb{Z}) \to SL_2(\mathbb{Z}/(m_G/p)\mathbb{Z}) \right)$$

are abelian groups of orders p^4 and p^3, respectively. Since m_G/p is not the GL_2-level of G, we have

$$\ker \left(SL_2(\mathbb{Z}/m_G\mathbb{Z}) \to SL_2(\mathbb{Z}/(m_G/p)\mathbb{Z}) \right) \subseteq \ker \pi_p \subsetneq \ker \left(GL_2(\mathbb{Z}/m_G\mathbb{Z}) \to GL_2(\mathbb{Z}/(m_G/p)\mathbb{Z}) \right).$$

It follows that $\ker\left(\mathrm{SL}_2(\mathbb{Z}/m_G\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/(m_G/p)\mathbb{Z})\right) = \ker \pi_p$, so

$$|\ker \pi_G| = \left|\pi_p^{-1}\left(\ker \pi_{m/p}\right)\right| = \left|\ker\left(\mathrm{SL}_2(\mathbb{Z}/m_G\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})\right)\right|,$$

and (Equation 2.4) is thus verified.

We now define the map $\delta : G(m) \longrightarrow (\mathbb{Z}/m_G\mathbb{Z})^\times$ as follows. For $g \in G(m)$, fix any element $\tilde{g} \in G(m_G)$ satisfying $\pi_G(\tilde{g}) = g$ and set $\Delta(g) := \det \tilde{g}$. By virtue of (Equation 2.4), we see that $\Delta(g)$ is independent of the choice of lift $\tilde{g}$ and thus δ is a well-defined group homomorphism; the condition $\pi_{\mathbb{G}_m} \circ \delta = \det$ is immediately verified, as is

$$\Delta(G(m)) = \det G(m_G). \tag{2.5}$$

In particular, if $\det G(m_G) = (\mathbb{Z}/m_G\mathbb{Z})^\times$, then δ is surjective. Furthermore, it follows from $\pi_{\mathbb{G}_m} \circ \delta = \det$ that

$$\delta\left(G(m) \cap \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})\right) = \ker \pi_{\mathbb{G}_m} \cap \delta\left(G(m)\right).$$

Thus, if δ is surjective then $\delta\left(G(m) \cap \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})\right) = \ker \pi_{\mathbb{G}_m}$. Finally, we clearly have

$$G(m_G) \subseteq \left\{ g \in \pi_{\mathrm{GL}_2}^{-1}\left(G(m)\right) : \delta\left(\pi_{\mathrm{GL}_2}(g)\right) = \det g \right\},$$

and, from (Equation 2.4), the two groups are seen to have equal size, and are thus equal. □

CHAPTER 3

BOUNDING THE GL_2-LEVEL OF MISSING TRACE GROUPS OF GENUS ZERO

3.1 Bounding the GL_2-level of missing trace groups of genus zero

In this section we prove Theorem 1.1.7. To begin with, the main results in (5) immediately imply that

$$\left\{\mathrm{level}_{\mathrm{SL}_2}(\tilde{G}) : G \in \mathfrak{G}(0)\right\} = \left\{\begin{array}{c} 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 \\ 18,20,21,24,25,26,27,28,30,32,36,48 \end{array}\right\}. \tag{3.1}$$

By Proposition 2.1.1 we then have

$$G \in \mathfrak{G}(0) \implies \mathrm{level}_{\mathrm{SL}_2}(G) \in \left\{\begin{array}{c} 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,20,21,22,24, \\ 25,26,27,28,30,32,36,40,42,48,50,52,54,56,60,64,72,96 \end{array}\right\}, \tag{3.2}$$

we will now establish the following proposition, which bounds m_G for $G \in \mathfrak{G}_{\mathrm{MT}}^{\max}(0)$ in terms of $m_S := \mathrm{level}_{\mathrm{SL}_2}(G)$. For an open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we set

$$d_G := \gcd\left(m_S^{\infty}, \left|\frac{G(m_S) \cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S), G(m_S)]}\right|\right), \tag{3.3}$$

i.e. d_G is the largest factor of $\left|\frac{G(m_S)\cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S),G(m_S)]}\right|$ supported on primes dividing m_S.

Proposition 3.1.1. *Let* $G \in \mathfrak{G}_{MT}^{max}$ *be a maximal missing trace group of* GL_2*-level* $\mathfrak{m}_G$ *and* SL_2*-level* $\mathfrak{m}_S$ *satisfying* $\det G = \hat{\mathbb{Z}}^\times$*. Then* $\mathfrak{m}_G$ *divides* $d_G\mathfrak{m}_S$*, where* d_G *is defined by* (Equation 4.3).

.

Proof. Without loss of generality, we may assume that $\mathfrak{m}_G > \mathfrak{m}_S$; we let p be any prime for which $\nu_p(\mathfrak{m}_G) > \nu_p(\mathfrak{m}_S)$ and set $\mathfrak{m}'_G := \mathfrak{m}_G/p^{\nu_p(\mathfrak{m}_G)-\nu_p(\mathfrak{m}_S)}$. Note that, for any prime ℓ, we have

$$\nu_\ell(\mathfrak{m}'_G) = \begin{cases} \nu_\ell(\mathfrak{m}_G) & \text{if } \ell \neq p \\ \nu_\ell(\mathfrak{m}_S) & \text{if } \ell = p. \end{cases} \tag{3.4}$$

In particular, since $\mathfrak{m}_S$ divides $\mathfrak{m}'_G$, we then have

$$\ker\left(SL_2(\mathbb{Z}/\mathfrak{m}_G\mathbb{Z}) \to SL_2(\mathbb{Z}/\mathfrak{m}'_G\mathbb{Z})\right) \subseteq G(\mathfrak{m}_G). \tag{3.5}$$

Furthermore, since G is maximal among missing trace groups, it follows that

$$\mathrm{tr}\left(G(\mathfrak{m}'_G)\right) = \mathbb{Z}/\mathfrak{m}'_G\mathbb{Z}. \tag{3.6}$$

We first claim that

$$p \mid \mathfrak{m}'_G. \tag{3.7}$$

To see this, suppose for the sake of contradiction that $p \nmid m'_G$, and define $\alpha := \nu_p(m_G) - \nu_p(m_S)$. Then, since m_S divides m'_G, under the Chinese Remainder Isomorphism $\mathbb{Z}/m_G\mathbb{Z} \simeq \mathbb{Z}/m'_G\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z}$, condition (Equation 4.5) reads

$$\{1\} \times \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq G(m_G). \tag{3.8}$$

By surjectivity of $\det : G(p^\alpha) \twoheadrightarrow (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ and Goursat's lemma, we then have

$$G(m_G) \simeq G(m'_G) \times_\psi \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}), \tag{3.9}$$

where $\psi_{m'_G} : G(m'_G) \longrightarrow \Gamma$ and $\psi_p : \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \longrightarrow \Gamma$ denote the surjective group homomorphisms onto the common quotient group Γ implicit in the fibered product. It follows from (Equation 4.8) that $\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq \ker \psi_p$, and thus, for every $\gamma \in \Gamma$, there exists $d \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ for which

$$\{g \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) : \det g = d\} \subseteq \psi_p^{-1}(\gamma).$$

Since $\mathrm{tr}\,(\{g \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) : \det g = d\}) = \mathbb{Z}/p^\alpha\mathbb{Z}$, it is then easy to deduce from (Equation 4.9) and (Equation 4.6) that $\mathrm{tr}\,(G(m_G)) = \mathbb{Z}/m_G\mathbb{Z}$, a contradiction. Therefore we have established (Equation 4.7), and, by (Equation 4.4), $p \mid m_S$. Since the prime p was arbitrary, it follows that

$$m_G \mid m_S^\infty. \tag{3.10}$$

We now apply Lemma 2.1.2, which asserts that there is a surjective group homomorphism $\delta : G(m_S) \longrightarrow (\mathbb{Z}/m_G\mathbb{Z})^\times$ satisfying $\pi \circ \delta = \det : G(m_S) \longrightarrow (\mathbb{Z}/m_S\mathbb{Z})^\times$, and for which

$$G(m_G) = \left\{ g \in \pi_{GL_2}^{-1}\left(G(m_S)\right) : \delta\left(\pi(g)\right) = \det g \right\}.$$

By (Equation 4.10) and Lemma 2.1.2, we have that

$$m_G/m_S = \left|\ker\left((\mathbb{Z}/m_G\mathbb{Z})^\times \to (\mathbb{Z}/m_S\mathbb{Z})^\times\right)\right| = \left|\delta\left(G(m_S) \cap SL_2(\mathbb{Z}/m_S\mathbb{Z})\right)\right|,$$

which in turn divides

$$\left|\frac{G(m_S) \cap SL_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S), G(m_S)]}\right|.$$

By (Equation 4.10), m_G/m_S also divides m_S^∞, and Proposition 4.1.1 follows. □

Theorem 1.1.7 follows from (Equation 4.2) and Proposition 4.1.1, together with a computer computation. The latter was carried out using the computational package MAGMA (2).

CHAPTER 4

PRELIMINARIES ON DIVISION FIELDS

4.1 Bounding the GL_2-level of missing trace groups of genus zero

In this section we prove Theorem 1.1.7. To begin with, the main results in (5) immediately imply that

$$\left\{\mathrm{level}_{\mathrm{SL}_2}(\tilde{G}) : G \in \mathfrak{G}(0)\right\} = \left\{\begin{array}{c} 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 \\ 18,20,21,24,25,26,27,28,30,32,36,48 \end{array}\right\}. \tag{4.1}$$

By Proposition 2.1.1 we then have

$$G \in \mathfrak{G}(0) \implies \mathrm{level}_{\mathrm{SL}_2}(G) \in \left\{\begin{array}{c} 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,20,21,22,24, \\ 25,26,27,28,30,32,36,40,42,48,50,52,54,56,60,64,72,96 \end{array}\right\}, \tag{4.2}$$

we will now establish the following proposition, which bounds m_G for $G \in \mathfrak{G}_{\mathrm{MT}}^{\max}(0)$ in terms of $m_S := \mathrm{level}_{\mathrm{SL}_2}(G)$. For an open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we set

$$d_G := \gcd\left(m_S^{\infty}, \left|\frac{G(m_S) \cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S), G(m_S)]}\right|\right), \tag{4.3}$$

i.e. d_G is the largest factor of $\left|\frac{G(m_S)\cap \mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S),G(m_S)]}\right|$ supported on primes dividing m_S.

Proposition 4.1.1. *Let* $\mathsf{G} \in \mathfrak{G}_{\mathrm{MT}}^{\max}$ *be a maximal missing trace group of* GL_2*-level* $\mathfrak{m}_{\mathsf{G}}$ *and* SL_2*-level* $\mathfrak{m}_{\mathsf{S}}$ *satisfying* $\det \mathsf{G} = \widehat{\mathbb{Z}}^{\times}$*. Then* $\mathfrak{m}_{\mathsf{G}}$ *divides* $\mathfrak{d}_{\mathsf{G}}\mathfrak{m}_{\mathsf{S}}$*, where* $\mathfrak{d}_{\mathsf{G}}$ *is defined by* (Equation 4.3).

.

Proof. Without loss of generality, we may assume that $\mathfrak{m}_{\mathsf{G}} > \mathfrak{m}_{\mathsf{S}}$; we let $\mathfrak{p}$ be any prime for which $\nu_{\mathfrak{p}}(\mathfrak{m}_{\mathsf{G}}) > \nu_{\mathfrak{p}}(\mathfrak{m}_{\mathsf{S}})$ and set $\mathfrak{m}'_{\mathsf{G}} := \mathfrak{m}_{\mathsf{G}}/\mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{m}_{\mathsf{G}})-\nu_{\mathfrak{p}}(\mathfrak{m}_{\mathsf{S}})}$. Note that, for any prime ℓ, we have

$$\nu_{\ell}(\mathfrak{m}'_{\mathsf{G}}) = \begin{cases} \nu_{\ell}(\mathfrak{m}_{\mathsf{G}}) & \text{if } \ell \neq \mathfrak{p} \\ \nu_{\ell}(\mathfrak{m}_{\mathsf{S}}) & \text{if } \ell = \mathfrak{p}. \end{cases} \tag{4.4}$$

In particular, since $\mathfrak{m}_{\mathsf{S}}$ divides $\mathfrak{m}'_{\mathsf{G}}$, we then have

$$\ker\left(\mathrm{SL}_2(\mathbb{Z}/\mathfrak{m}_{\mathsf{G}}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/\mathfrak{m}'_{\mathsf{G}}\mathbb{Z})\right) \subseteq \mathsf{G}(\mathfrak{m}_{\mathsf{G}}). \tag{4.5}$$

Furthermore, since G is maximal among missing trace groups, it follows that

$$\mathrm{tr}\left(\mathsf{G}(\mathfrak{m}'_{\mathsf{G}})\right) = \mathbb{Z}/\mathfrak{m}'_{\mathsf{G}}\mathbb{Z}. \tag{4.6}$$

We first claim that

$$\mathfrak{p} \mid \mathfrak{m}'_{\mathsf{G}}. \tag{4.7}$$

To see this, suppose for the sake of contradiction that $p \nmid m'_G$, and define $\alpha := \nu_p(m_G) - \nu_p(m_S)$. Then, since m_S divides m'_G, under the Chinese Remainder Isomorphism $\mathbb{Z}/m_G\mathbb{Z} \simeq \mathbb{Z}/m'_G\mathbb{Z} \times \mathbb{Z}/p^\alpha\mathbb{Z}$, condition (Equation 4.5) reads

$$\{1\} \times \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq G(m_G). \tag{4.8}$$

By surjectivity of $\det : G(p^\alpha) \twoheadrightarrow (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ and Goursat's lemma, we then have

$$G(m_G) \simeq G(m'_G) \times_\psi \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}), \tag{4.9}$$

where $\psi_{m'_G} : G(m'_G) \longrightarrow \Gamma$ and $\psi_p : \mathrm{GL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \longrightarrow \Gamma$ denote the surjective group homomorphisms onto the common quotient group Γ implicit in the fibered product. It follows from (Equation 4.8) that $\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq \ker \psi_p$, and thus, for every $\gamma \in \Gamma$, there exists $d \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ for which

$$\{g \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) : \det g = d\} \subseteq \psi_p^{-1}(\gamma).$$

Since $\mathrm{tr}\,(\{g \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) : \det g = d\}) = \mathbb{Z}/p^\alpha\mathbb{Z}$, it is then easy to deduce from (Equation 4.9) and (Equation 4.6) that $\mathrm{tr}\,(G(m_G)) = \mathbb{Z}/m_G\mathbb{Z}$, a contradiction. Therefore we have established (Equation 4.7), and, by (Equation 4.4), $p \mid m_S$. Since the prime p was arbitrary, it follows that

$$m_G \mid m_S^\infty. \tag{4.10}$$

We now apply Lemma 2.1.2, which asserts that there is a surjective group homomorphism $\delta : G(m_S) \longrightarrow (\mathbb{Z}/m_G\mathbb{Z})^\times$ satisfying $\pi \circ \delta = \det : G(m_S) \longrightarrow (\mathbb{Z}/m_S\mathbb{Z})^\times$, and for which

$$G(m_G) = \left\{ g \in \pi_{GL_2}^{-1}\left(G(m_S)\right) : \delta\left(\pi(g)\right) = \det g \right\}.$$

By (Equation 4.10) and Lemma 2.1.2, we have that

$$m_G/m_S = \left|\ker\left((\mathbb{Z}/m_G\mathbb{Z})^\times \to (\mathbb{Z}/m_S\mathbb{Z})^\times\right)\right| = \left|\delta\left(G(m_S) \cap SL_2(\mathbb{Z}/m_S\mathbb{Z})\right)\right|,$$

which in turn divides

$$\left|\frac{G(m_S) \cap SL_2(\mathbb{Z}/m_S\mathbb{Z})}{[G(m_S), G(m_S)]}\right|.$$

By (Equation 4.10), m_G/m_S also divides m_S^∞, and Proposition 4.1.1 follows. □

Theorem 1.1.7 follows from (Equation 4.2) and Proposition 4.1.1, together with a computer computation. The latter was carried out using the computational package MAGMA (2).

4.2 Preliminaries on division fields of elliptic curves

In this section, we gather various preliminary results to be used in the following section to develop explicit models for the modular curves associated to the groups occurring in Theorem 1.1.7. We recall the general set-up: $G \subseteq GL_2(\hat{\mathbb{Z}})$ is an open subgroup, $\tilde{G} := \langle G, -I \rangle$ and $X_{\tilde{G}}$ is the

modular curve associated to $\tilde{G}$. Denoting by m the GL_2-level of $\tilde{G}$ and by $j_{\tilde{G}} : X_{\tilde{G}} \longrightarrow X(1) \simeq \mathbb{P}^1$ the forgetful map, we have that, for any $j \in \mathbb{Q} - \{0, 1728\}$,

$$j \in j_{\tilde{G}}\left(X_{\tilde{G}}(\mathbb{Q})\right) \iff \exists E/\mathbb{Q} \text{ with } \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G} \text{ and } j_E = j. \tag{4.11}$$

We will use repeatedly the following consequence of the Weil pairing on an elliptic curve. Let K be a field, let E an elliptic curve defined over K, let $m \in \mathbb{N}$ be a positive integer co-prime with $\operatorname{char} K$ and let

$$\rho_{E,m} : G_K \longrightarrow \operatorname{Aut}(E[m]) \simeq GL_2(\mathbb{Z}/m\mathbb{Z})$$

be the Galois representation defined by letting G_K act on the m-torsion of E. On the other hand, let

$$\chi_m : G_K \longrightarrow \operatorname{Aut}(\mu_m) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$$

be the mod m cyclotomic character, defined by letting G_K act on μ_m.

Lemma 4.2.1. *We have* $\det \circ \rho_{E,m} = \chi_m$.

Proof. This follows from properties of the Weil pairing; see (24, Ch III, §8). □

We remark that, whenever the level m of a maximal missing trace group may be written in the form $m = m_1 m_2$ with $m_1, m_2 > 1$ and $\gcd(m_1, m_2) = 1$, the group $G(m)$ decomposes via the Chinese Remainder Theorem as a fibered product

$$G(m) = G(m_1 m_2) \simeq G(m_1) \times_\psi G(m_2) := \{(g_1, g_2) \in G(m_1) \times G(m_2) : \psi_1(g_1) = \psi_2(g_2)\},$$

where $\psi_i : G(\mathfrak{m}_i) \longrightarrow H$ are each surjective homomorphisms onto a common non-trivial quotient group H (if H were trivial, then $G(\mathfrak{m})$ would decompose as a full cartesian product, implying that either $G(\mathfrak{m}_1)$ or $G(\mathfrak{m}_2)$ would have a missing trace, contradicting maximality of G). The following lemma will be useful for determining when $\rho_{E,\mathfrak{m}_1\mathfrak{m}_2}(G_{\mathbb{Q}}) \dot{\subseteq} G(\mathfrak{m}_1) \times_{\psi} G(\mathfrak{m}_2)$. In general, let $\mathcal{G}_1$ and $\mathcal{G}_2$ be finite groups and let

$$G_i, G_i' \subseteq \mathcal{G}_i \qquad (i \in \{1,2\})$$

be subgroups. Let

$$\psi_i : G_i \longrightarrow H, \quad \psi_i' : G_i' \longrightarrow H' \qquad (i \in \{1,2\})$$

be surjective homomorphisms onto the finite groups H and H', respectively, and denote by $G_1 \times_{\psi} G_2$ and $G_1' \times_{\psi'} G_2'$ the corresponding fibered products. In particular, these fibered products are *honest* in the sense that, for each $i \in \{1,2\}$, the canonical projections $G_1 \times_{\psi} G_2 \longrightarrow G_i$ and $G_1' \times_{\psi'} G_2' \longrightarrow G_i'$ are each surjective.

Lemma 4.2.2. *With the notation just outlined, we have*

$$G_1' \times_{\psi'} G_2' \subseteq G_1 \times_{\psi} G_2$$

if and only if

1. $\forall i \in \{1,2\}$, $G_i' \subseteq G_i$,
2. *there exists a group homomorphism* $\varpi : H' \longrightarrow H$ *such that* $\forall i \in \{1,2\}$, $\varpi \circ \psi_i' = \psi_i|_{G_i'}$.

Proof. For the direction "⇒", condition (1) is immediate. To verify condition (2), we first note that $\ker\psi_1' \times \ker\psi_2' \subseteq G_1 \times_\psi G_2$, which implies that

$$\ker\psi_i' \subseteq \ker\psi_i \qquad (i \in \{1,2\})\,.$$

We thus have a well-defined group homomorphism $\varpi : H' \longrightarrow H$, given by $\varpi\left(\psi_1'(g_1')\right) := \psi_1(g_1')$. We observe that $\varpi \circ \psi_i' = \psi_i|_{G_i'}$ by definition when $i = 1$ and by $G_1' \times_{\psi'} G_2' \subseteq G_1 \times_\psi G_2$ when $i = 2$. This establishes (2).

For the converse, assume that (1) and (2) hold and let $(g_1', g_2') \in G_1' \times_{\psi'} G_2'$. By (1), $g_1' \in G_1$ and $g_2' \in G_2$. Furthermore, $\psi_1'(g_1') = \psi_2'(g_2')$, and thus

$$\psi_1(g_1') = \varpi\left(\psi_1'(g_1')\right) = \varpi\left(\psi_2'(g_2')\right) = \psi_2(g_2').$$

Thus, $(g_1', g_2') \in G_1 \times_\psi G_2$, and we have proved the converse, establishing the lemma. □

By (Equation 4.11), we need only consider such groups up to conjugation inside $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, i.e. up to the relation $\doteq$. It is straightforward to see that, for any inner automorphisms $\eta_1, \eta_2 : H \longrightarrow H$, we have

$$G(m_1) \times_{(\eta_1\psi_1, \eta_2\psi_2)} G(m_2) \doteq G(m_1) \times_{(\psi_1,\psi_2)} G(m_2).$$

However, the same is not always true for outer automorphisms $\eta_1, \eta_2 \in \mathrm{Aut}(H)$; given such a pair $(\eta_1, \eta_2) \in \mathrm{Aut}(H)^2$, we clearly have

$$G(m_1) \times_{(\eta_1\psi_1, \eta_2\psi_2)} G(m_2) = G(m_1) \times_{(\psi_1, \eta_1^{-1}\eta_2\psi_2)} G(m_2).$$

Thus, it suffices to consider postcomposing the pair (ψ_1, ψ_2) with pairs of automorphsims of the form $(1, \eta_2)$, or of the form $(\eta_1, 1)$.

Definition 4.2.3. Given the notation above, we say that an automorphism $\eta_i \in \mathrm{Aut}(H)$ ***is*** $\mathrm{GL}_2(\mathbb{Z}/m_i\mathbb{Z})$***-induced*** if there exists $g_i \in \mathrm{GL}_2(\mathbb{Z}/m_i\mathbb{Z})$ satisfying $g_i G(m_i) g_i^{-1} = G(m_i)$ and for which the diagram

$$\begin{array}{ccc} G(m_i) & \xrightarrow{\mathrm{Conj}_{g_i}} & G(m_i) \\ \downarrow{\scriptstyle \psi_i} & & \downarrow{\scriptstyle \psi_i} \\ H & \xrightarrow{\eta_i} & H \end{array}$$

commutes.

The following useful lemma is straightforward to prove.

Lemma 4.2.4. *With notation as just outlined and with* $\eta_2 \in \mathrm{Aut}(H)$*, we have*

$$G(m_1) \times_{(\psi_1, \eta_2\psi_2)} G(m_2) \doteq G(m_1) \times_{(\psi_1, \psi_2)} G(m_2) \iff \eta_2 \in \mathrm{Aut}(H) \textit{ is } \mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z})\textit{-induced,}$$

$$G(m_1) \times_{(\eta_1\psi_1, \psi_2)} G(m_2) \doteq G(m_1) \times_{(\psi_1, \psi_2)} G(m_2) \iff \eta_1 \in \mathrm{Aut}(H) \textit{ is } \mathrm{GL}_2(\mathbb{Z}/m_1\mathbb{Z})\textit{-induced.}$$

We will now describe an interpretation of $\rho_{E,m_1m_2}(G_{\mathbb{Q}}) \dot{\subseteq} G(m_1) \times_\psi G(m_2)$ in terms of entanglements. It will be convenient to decompose the representation ρ_E as

$$G_{\mathbb{Q}} \xrightarrow{\tilde{\rho}_E} \mathrm{Aut}(E_{\mathrm{tors}}) \xrightarrow{\iota_{\mathcal{B}}} \mathrm{GL}_2(\hat{\mathbb{Z}}), \qquad \rho_E = \iota_{\mathcal{B}} \circ \tilde{\rho}_E$$

where $\mathcal{B} = \{\mathcal{B}(m) := (b_{1,m}, b_{2,m}) : m \in \mathbb{N}\}$ is a collection of ordered $\mathbb{Z}/m\mathbb{Z}$-bases of $E[m] \subseteq E_{\mathrm{tors}}$, one for each $m \in \mathbb{N}$, chosen compatibly. This decomposition has a corresponding a finite level analogue

$$\rho_{E,m} = \iota_{\mathcal{B}(m)} \circ \tilde{\rho}_{E,m} \tag{4.12}$$

for any $m \in \mathbb{N}$. We will denote simply by ι either of the the isomorphisms $\mathrm{Aut}(E[m]) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ or $\mathrm{Aut}(E_{\mathrm{tors}}) \to \mathrm{GL}_2(\hat{\mathbb{Z}})$ induced by such a collection $\mathcal{B}$, suppressing the dependence on $\mathcal{B}$. Thus, for any $m \in \mathbb{N}$, we have

$$\rho_{E,m}(G_{\mathbb{Q}}) \dot{\subseteq} G(m) \iff \exists \iota : \tilde{\rho}_{E,m}(G_{\mathbb{Q}}) \hookrightarrow G(m).$$

Unraveling (Equation 4.11), we find that

$$\exists \iota : \tilde{\rho}_{E,m_1m_2}(G_{\mathbb{Q}}) \hookrightarrow G(m_1) \times_\psi G(m_2) \implies \begin{array}{l} \exists \iota_1 : \tilde{\rho}_{E,m_1}(G_{\mathbb{Q}}) \hookrightarrow G(m_1),\ \exists \iota_2 : \tilde{\rho}_{E,m_2}(G_{\mathbb{Q}}) \hookrightarrow G(m_2), \\ \qquad \text{and}\ \ \mathbb{Q}(E[m_1])^{\iota_1^{-1}(\ker \psi_1)} = \mathbb{Q}(E[m_2])^{\iota_2^{-1}(\ker \psi_2)}, \end{array}$$

where we are understanding the subfield $\mathbb{Q}(E[m_i])^{\iota_i^{-1}(\ker\psi_i)} \subseteq \mathbb{Q}(E[m_i])$ via the natural isomorphism $\mathrm{Gal}\,(\mathbb{Q}(E[m_i])/\mathbb{Q}) \simeq \tilde{\rho}_{E,m_i}(G_{\mathbb{Q}})$. The following corollary states conditions under which the converse holds.

Corollary 4.2.5. *Let* $\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/m_i\mathbb{Z})}(H) \subseteq \mathrm{Aut}(H)$ *denote the subgroup of* $\mathrm{GL}_2(\mathbb{Z}/m_i\mathbb{Z})$*-induced automorphisms, and suppose that either* $\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/m_1\mathbb{Z})}(H) = \mathrm{Aut}(H)$ *or* $\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z})}(H) = \mathrm{Aut}(H)$. *We then have*

$$\rho_{E,m_1m_2}(G_{\mathbb{Q}}) \dot{\subsetneq} G(m_1) \times_\psi G(m_2) \iff \begin{array}{c} \exists \iota_1 : \tilde{\rho}_{E,m_1}(G_{\mathbb{Q}}) \hookrightarrow G(m_1),\ \exists \iota_2 : \tilde{\rho}_{E,m_2}(G_{\mathbb{Q}}) \hookrightarrow G(m_2), \\ \textit{and} \quad \mathbb{Q}(E[m_1])^{\iota_1^{-1}(\ker\psi_1)} = \mathbb{Q}(E[m_2])^{\iota_2^{-1}(\ker\psi_2)}. \end{array}$$

We would like to apply Corollary 4.2.5 to groups $G \in \mathfrak{G}_{\mathrm{MT}}^{\max}(0)$. Our computation shows that, for every such group G whose GL_2-level m is divisible by at least two primes, and for any $m_1, m_2 > 1$ with $m = m_1m_2$ and $\gcd(m_1, m_2) = 1$, writing $G(m) \simeq G(m_1) \times_\psi G(m_2)$ and denoting by $H := \psi_i(G(m_i))$ the common quotient group implicit in the fibered product, we have

$$H \in \{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, S_3\}. \tag{4.13}$$

When $H \in \{\mathbb{Z}/2\mathbb{Z}, S_3\}$, all automorphisms of H are inner, whence $\mathrm{GL}_2(\mathbb{Z}/m_i\mathbb{Z})$-inner (no matter what the level m_i is. For the case $H \in \{\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}\}$, we will now look in more detail at the particulars.

The common quotient $H = \mathbb{Z}/3\mathbb{Z}$ arises as an entanglement between the groups $G(2)$ and $G(7)$, and in all such cases, we have

$$G(2) = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), \qquad \psi_2 : \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \simeq \mathbb{Z}/3\mathbb{Z}. \tag{4.14}$$

Thus, the image $H = \mathbb{Z}/3\mathbb{Z}$ is isomorphic to $G(2)$, an index two (and hence normal) subgroup of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. Since

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

it follows that the conjugation action of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ on $G(2)$ gives rise to all automorphisms of H, i.e. that $\mathrm{Aut}(H) = \mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})}(H)$ in this case.

The common quotient $H \simeq \mathbb{Z}/6\mathbb{Z}$ arises as an entanglement between $G(4)$ and $G(7)$, and in all such cases, we have

$$G(4) = \pi_{\mathrm{GL}_2}^{-1}\left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), \qquad \ker \psi_4 = \ker \pi_{\mathrm{GL}_2} \cap \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}),$$

where $\pi_{\mathrm{GL}_2} : \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ denotes the canonical projection map. Therefore the map ψ_4 decomposes as

$$\pi_{\mathrm{GL}_2}^{-1}\left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle\right) \xrightarrow{\psi_2 \times \det} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/6\mathbb{Z}, \qquad \psi_4 : \pi_{\mathrm{GL}_2}^{-1}\left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle\right) \to \mathbb{Z}/6\mathbb{Z},$$

where ψ_2 denotes the function $g \mapsto \psi_2(g \bmod 2)$, with ψ_2 as in (Equation 4.14). Thus, it follows from the discussion in the previous paragraph that $\mathrm{Aut}_{\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})}(H) = \mathrm{Aut}(H)$ in this case as well. Taking these observations together with the computation that establishes (Equation 4.13), we thus have

Corollary 4.2.6. *For each group $G \in \mathfrak{G}_{\mathrm{MT}}^{\max}(0)$ with the property that $m := \mathrm{level}_{\mathrm{GL}_2}(G)$ is divisible by at least two primes, choose any $m_1, m_2 \in \mathbb{N}$ with $\gcd(m_1, m_2) = 1$ and $m_1, m_2 > 1$ and write $G(m) \simeq G(m_1) \times_\psi G(m_2)$. For any elliptic curve E over $\mathbb{Q}$, we have*

$$\rho_{E,m_1 m_2}(G_{\mathbb{Q}}) \dot{\subseteq} G(m_1) \times_\psi G(m_2) \iff \begin{array}{c} \exists \iota_1 : \tilde{\rho}_{E,m_1}(G_{\mathbb{Q}}) \hookrightarrow G(m_1),\ \exists \iota_2 : \tilde{\rho}_{E,m_2}(G_{\mathbb{Q}}) \hookrightarrow G(m_2), \\ \text{and} \quad \mathbb{Q}(E[m_1])^{\iota_1^{-1}(\ker \psi_1)} = \mathbb{Q}(E[m_2])^{\iota_2^{-1}(\ker \psi_2)}, \end{array}$$

where the basis-induced embeddings ι_1 and ι_2 and the representations $\tilde{\rho}_{E,m_i}$ are as in (Equation 4.12)*, and the subfield $\mathbb{Q}(E[m_i])^{\iota_i^{-1}(\ker \psi_i)} \subseteq \mathbb{Q}(E[m_i])$ is understood via the natural isomorphism $\tilde{\rho}_{E,m_i}(G_{\mathbb{Q}}) \simeq \mathrm{Gal}\left(\mathbb{Q}(E[m_i])/\mathbb{Q}\right)$.*

4.2.1 Cyclic cubic fields

Since we will be dealing with cyclic cubic extensions of $\mathbb{Q}(t, D)$, we now state two lemmas about such field extensions that will be used in what follows. Our first lemma allows us to exhibits explicit polynomials for generators of each of the cyclic cubic subfields of a given $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$-extension. In general, let K be any field, let

$$\begin{aligned} f_S(x) &= x^3 - S_1x^2 + S_2x - S_3, \\ f_T(x) &= x^3 - T_1x^2 + T_2x - T_3 \end{aligned} \tag{4.15}$$

be two monic irreducible polynomials with coefficients in K, and denote by K_{f_S} (resp. by K_{f_T}) the splitting polynomial of f_S (resp. of f_T), viewed as subfields of a fixed algebraic closure $\overline{K}$ of K. Assume that

$$K_{f_S} \neq K_{f_T} \tag{4.16}$$

and that the discriminants $\Delta_S := \mathrm{disc}(f_S)$ and $\Delta_T := \mathrm{disc}(f_T)$ are each in $(K^\times)^2$, or equivalently that $\mathrm{Gal}(K_{f_S}/K) \simeq \mathrm{Gal}(K_{f_T}/K)$ is a cyclic group of order 3. The assumption (Equation 4.16) then implies that the composite field $K_{f_S f_T} = K_{f_S}K_{f_T}$ satisfies

$$\mathrm{Gal}(K_{f_S f_T}/K) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \tag{4.17}$$

and this field contains 4 cyclic cubic subfields. Fix square roots $\sqrt{\Delta_S}, \sqrt{\Delta_T} \in K$ and define the coefficients $R_1, R_2, R_3, R_3' \in K$ by

$$\begin{aligned}
R_1 :=& S_1 T_1, \\
R_2 :=& S_1^2 T_2 + T_1^2 S_2 - 3 S_2 T_2, \\
R_3 :=& S_1^3 T_3 + T_1^3 S_3 - 3 S_1 S_2 T_3 - 3 T_1 T_2 S_3 + 9 S_3 T_3 \\
&+ \left(S_1 S_2 - 3 S_3 + \sqrt{\Delta_S}\right)\left(T_1 T_2 - 3 T_3 + \sqrt{\Delta_T}\right)/4 \\
&+ \left(S_1 S_2 - 3 S_3 - \sqrt{\Delta_S}\right)\left(T_1 T_2 - 3 T_3 - \sqrt{\Delta_T}\right)/4, \\
R_3' :=& S_1^3 T_3 + T_1^3 S_3 - 3 S_1 S_2 T_3 - 3 T_1 T_2 S_3 + 9 S_3 T_3 \\
&+ \left(S_1 S_2 - 3 S_3 + \sqrt{\Delta_S}\right)\left(T_1 T_2 - 3 T_3 - \sqrt{\Delta_T}\right)/4 \\
&+ \left(S_1 S_2 - 3 S_3 - \sqrt{\Delta_S}\right)\left(T_1 T_2 - 3 T_3 + \sqrt{\Delta_T}\right)/4.
\end{aligned} \tag{4.18}$$

Define the cubic polynomials $f_R(x), f_{R'}(x) \in K[x]$ by

$$\begin{aligned}
f_R(x) &:= x^3 - R_1 x^2 + R_2 x - R_3, \\
f_{R'}(x) &:= x^3 - R_1 x^2 + R_2 x - R_3'.
\end{aligned} \tag{4.19}$$

Lemma 4.2.7. *Let K be a field, let $f_S(x), f_T(x) \in K[x]$ be irreducible monic cubic polynomials as in* (Equation 4.15)*, and assume the setup and notation laid out above (in particular, assume that the splitting field $K_{f_S f_T}$ of $f_S(x) f_T(x)$ satisfies* (Equation 4.17)*). Then the four cyclic cubic subfields of $K_{f_S f_T}$ are the splitting fields of the polynomials $f_S(x)$, $f_T(x)$, $f_R(x)$ and $f_{R'}(x)$, where $f_R(x)$ and $f_{R'}(x)$ are defined by* (Equation 4.19) *and* (Equation 4.18)*.*

Proof. An exercise in symmetric polynomials. □

Given a field K and elements $S_1, S_2, S_3, T_1, T_2, T_3 \in K$, we may consider the following system of equations in the variables a, b and c.

$$\begin{aligned} T_1 &= a\left(S_1^2 - 2S_2\right) + bS_1 + 3c, \\ T_2 &= a^2S_2^2 - 2a^2S_1S_3 + abS_1S_2 - 3abS_3 + 2acS_1^2 - 4acS_2 + b^2S_2 + 2bcS_1 + 3c^2, \\ T_3 &= a^3S_3^2 + a^2bS_2S_3 - 2a^2cS_1S_3 + a^2cS_2^2 + ab^2S_1S_3 + abcS_1S_2 - 3abcS_3 \\ &\quad + ac^2S_1^2 - 2ac^2S_2 + b^3S_3 + b^2cS_2 + bc^2S_1 + c^3. \end{aligned} \tag{4.20}$$

Lemma 4.2.8. *Let K be a field, let $f_S(x)$, $f_T(x) \in K[x]$ be irreducible monic cubic polynomials as in* (Equation 4.15) *and denote by K_{f_S} (resp. by K_{f_T}) the splitting field of $f_S(x)$ (resp. of $f_T(x)$), viewed as subfields of a fixed algebraic closure $\overline{K}$ of K. Assume that the discriminant Δ_S of $f_S(x)$ satisfies $\Delta_S \in (K^\times)^2$, so that $\mathrm{Gal}(K_{f_S}/K)$ is a cyclic group of order 3. We then have that $K_{f_S} = K_{f_T}$ if and only if the system of equations* (Equation 4.20) *has a solution $(a, b, c) \in K^3$.*

Proof. Let $\alpha \in \overline{K}$ denote a root of $f_S(x)$. Then $K_{f_S} = K(\alpha)$, and so we may write an arbitrary element $\beta \in K_{f_S}$ in the form

$$\beta = a\alpha^2 + b\alpha + c \qquad (a, b, c \in K)\,. \tag{4.21}$$

The elementary symmetric polynomials $S_i(a\alpha^2+b\alpha+c)$ of such an element are then readily computed to be

$$\begin{aligned}
S_1(a\alpha^2+b\alpha+c) =& a\left(S_1^2-2S_2\right)+bS_1+3c,\\
S_2(a\alpha^2+b\alpha+c) =& a^2S_2^2-2a^2S_1S_3+abS_1S_2-3abS_3+2acS_1^2-4acS_2+b^2S_2+2bcS_1+3c^2,\\
S_3(a\alpha^2+b\alpha+c) =& a^3S_3^2+a^2bS_2S_3-2a^2cS_1S_3+a^2cS_2^2+ab^2S_1S_3+abcS_1S_2-3abcS_3\\
&+ac^2S_1^2-2ac^2S_2+b^3S_3+b^2cS_2+bc^2S_1+c^3.
\end{aligned} \tag{4.22}$$

Thus, if (Equation 4.20) have a solution $(a,b,c)\in K^3$, we see that $f_T(x)$ has a root in K_{f_S}, thus $f_T(x)$ splits completely over K_{f_S}, and so $K_{f_T}=K_{f_S}$. Conversely, if $K_{f_T}=K_{f_S}$, then let $\beta\in K_{f_T}$ be a root of $f_T(x)$. Writing β in the form (Equation 4.21), we see that $(a,b,c)\in K^3$ is then a solution to (Equation 4.20). □

4.2.2 Division fields of elliptic curves and their subfields

In this section, we exhibit explicitly various subfields of the mth division field $\mathbb{Q}(t,D)(\mathcal{E}[m])$ for various levels m and elliptic curves $\mathcal{E}$ over $\mathbb{Q}(t,D)$. The Borel subgroup

$$B(\ell) := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subseteq GL_2(\mathbb{Z}/\ell\mathbb{Z})$$

plays a key role, as do the two multiplicative homomorphisms $\psi_{\ell,1}, \psi_{\ell,2} : B(\ell) \longrightarrow (\mathbb{Z}/\ell\mathbb{Z})^\times$ defined by

$$\psi_{\ell,1}\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) := a, \qquad \psi_{\ell,2}\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) := d. \tag{4.23}$$

2 For any elliptic curve E over $\mathbb{Q}$, we have

$$\rho_{E,\ell}(G_{\mathbb{Q}}) \subseteq B(\ell) \iff \exists \text{ a } G_{\mathbb{Q}}\text{-stable cyclic subgroup } \langle P \rangle \subseteq E[\ell]. \tag{4.24}$$

When this is the case, we denote by $E'_{\langle P \rangle} := E/\langle P \rangle$ the quotient curve, which is isogenous over $\mathbb{Q}$ to E. We have $\rho_{E'_{\langle P \rangle},\ell}(G_{\mathbb{Q}}) \subseteq B(\ell)$, or in other words,

$$\exists \text{ a } G_{\mathbb{Q}}\text{-stable cyclic subgroup } \langle P' \rangle \subseteq E'_{\langle P \rangle}[\ell] \tag{4.25}$$

(this 46 is the kernel of the dual isogeny $E'_{\langle P \rangle} \to E$). In these terms, the Galois representations $\psi_{\ell,1}$ and $\psi_{\ell,2}$ above are simply defined by restricting the action of $G_{\mathbb{Q}}$ respectively to $\langle P \rangle$ and to $\langle P' \rangle$, i.3e. we have

$$\sigma : P \mapsto [\psi_{\ell,1}(\sigma)]\,P, \qquad \sigma : P' \mapsto [\psi_{\ell,2}(\sigma)]\,P' \qquad (\sigma \in G_{\mathbb{Q}})\,. \tag{4.26}$$

Finally, we note that $\psi_{\ell,i}^{(\ell-1)/2}(g) \in \{\pm 1\} \subseteq (\mathbb{Z}/\ell\mathbb{Z})^\times$, and that this value agrees with the Legendre symbol evaluated at $\psi_{\ell,i}(g)$, i.e. we have

$$\psi_{\ell,1}^{(\ell-1)/2}\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) \equiv \left(\frac{a}{\ell}\right) \bmod \ell, \qquad \psi_{\ell,2}^{(\ell-1)/2}\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) \equiv \left(\frac{d}{\ell}\right) \bmod \ell.$$

4.2.2.1 The level $m = 2$

The group $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is a non-abelian group of order 6, and since there is only one such group up to isomorphism, we see that it is isomorphic to the symmetric group of order 6:

$$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{S}_3. \tag{4.27}$$

As such, there is a unique proper non-trivial normal subgroup

$$\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$$

which has index two (corresponding under (Equation 4.27) to the alternating subgroup A_3). This index two subgroup happens to be the commutator subgroup $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})'$ of $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$; as we shall see, both this fact and the next classical, well-known lemma generalize to levels 3 and 4.

Lemma 4.2.9. *Let E be an elliptic curve over $\mathbb{Q}$ and let Δ_{E} denote the discriminant of any*[1] *Weierstrass model of E. We have that $\mathbb{Q}(\sqrt{\Delta_{\mathsf{E}}}) \subseteq \mathbb{Q}(\mathsf{E}[2])$. Furthermore, this subfield corresponds via Galois theory to the subgroup $\rho_{\mathsf{E},2}(\mathsf{G}_{\mathbb{Q}}) \cap \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})'$, i.e. we have*

$$\mathbb{Q}(\mathsf{E}[2])^{\rho_{\mathsf{E},2}(\mathsf{G}_{\mathbb{Q}})\cap \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})'} = \mathbb{Q}\left(\sqrt{\Delta_{\mathsf{E}}}\right).$$

Proof. See for instance (16, pp. 218). □

Throughout the paper, the role played by restriction map $\mathrm{Gal}\left(\mathbb{Q}(\mathsf{E}[2])/\mathbb{Q}\right) \to \mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{\Delta_{\mathsf{E}}}\right)/\mathbb{Q}\right)$ is significant enough to warrant our giving it an explicit name. We make the definition

$$\varepsilon : \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\simeq} \mathrm{S}_3 \xrightarrow{\mathrm{can}} \frac{\mathrm{S}_3}{\mathrm{A}_3} \xrightarrow{\simeq} \{\pm 1\}. \tag{4.28}$$

Thus, we have

$$\ker \varepsilon = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \qquad \text{and} \qquad \mathbb{Q}(\mathsf{E}[2])^{\ker \varepsilon} = \mathbb{Q}\left(\sqrt{\Delta_{\mathsf{E}}}\right).$$

---

[1] *Note that the field $\mathbb{Q}(\sqrt{\Delta_{\mathsf{E}}})$ (resp. the fields $\mathbb{Q}(\Delta_{\mathsf{E}}^{1/3})$ and $\mathbb{Q}(\Delta_{\mathsf{E}}^{1/4})$ appearing in Lemmas 4.2.11 and 4.2.12) does not depend on the choice of Weierstrass model for E, even though the discriminant Δ_{E} does.*

4.2.2.2 The level $m = 3$

Using the classical theory of modular functions (see (30)), it can be shown that there is a rational parameter t on the genus zero modular curve $X_0(3)$ such that the forgetful map $X_0(3) \longrightarrow X(1)$ takes the form

$$\mathbb{P}^1(t) \longrightarrow \mathbb{P}^1(j), \quad t \mapsto 27\frac{(t+1)(t+9)^3}{t^3}.$$

We define $j_3(t) := 27\frac{(t+1)(t+9)^3}{t^3} \in \mathbb{Q}(t)$ and the elliptic curve $\mathcal{E}_3$ over $\mathbb{Q}(t, D)$ by

$$\mathcal{E}_3 : \ y^2 = x^3 + \frac{108D^2 j_3(t)}{1728 - j_3(t)}x + \frac{432D^3 j_3(t)}{1728 - j_3(t)}. \tag{4.29}$$

By restricting the action of $\mathrm{Gal}\,(\mathbb{Q}(t, D)(\mathcal{E}_3[3])/\mathbb{Q}(t, D))$ to $\mathcal{E}_3[3]$ and fixing a $\mathbb{Z}/3\mathbb{Z}$-basis thereof, we obtain an isomorphism

$$\mathrm{Gal}\,(\mathbb{Q}(t, D)(\mathcal{E}_3[3])/\mathbb{Q}(t, D)) \simeq \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}). \tag{4.30}$$

The following lemma explicitly characterizes the subfields cut out by the characters $\psi_{3,1}$ and $\psi_{3,2}$.

Lemma 4.2.10. *Let $\mathcal{E}_3$ be the elliptic curve over $\mathbb{Q}(t, D)$ defined by* (Equation 4.29) *and define the characters*

$$\psi_{3,1}, \psi_{3,2} : \mathrm{Gal}\,(\mathbb{Q}(t, D)(\mathcal{E}_3[3])/\mathbb{Q}(t, D)) \to \{\pm 1\}$$

to be the restrictions under (Equation 4.30) *of the characters defined in* (Equation 4.23). *We then have*

$$\begin{aligned}\mathbb{Q}(t,D)(\mathcal{E}_3[3])^{\ker\psi_{3,1}} &= \mathbb{Q}(t,D)\left(\sqrt{\frac{6D(t+1)(t+9)}{(t^2-18t-27)}}\right),\\ \mathbb{Q}(t,D)(\mathcal{E}_3[3])^{\ker\psi_{3,2}} &= \mathbb{Q}(t,D)\left(\sqrt{-\frac{2D(t+1)(t+9)}{(t^2-18t-27)}}\right).\end{aligned} \tag{4.31}$$

Proof. We compute that the 3rd division polynomial associated to $\mathcal{E}_3$ has the $\mathbb{Q}(t,D)$-rational factor

$$x - \frac{18D(t+1)(t+9)}{t^2-18t-27},$$

and this leads us to the point

$$P := \left(\frac{18D(t+1)(t+9)}{t^2-18t-27}, \frac{24Dt(t+9)}{t^2-18t-27}\sqrt{\frac{6D(t+1)(t+9)}{(t^2-18t-27)}}\right) \in \mathcal{E}_3[3].$$

Since $\mathbb{Q}(t,D)(\mathcal{E}_3[3])^{\ker\psi_{3,1}} = \mathbb{Q}(t,D)(P)$, this establishes the first formula in (Equation 4.31); the expression for the fixed field of $\ker\psi_{3,2}$ then follows from the fact that $\psi_{3,1}(g)\psi_{3,2}(g) = \det g$, whose corresponding fixed field is $\mathbb{Q}(t,D)\left(\sqrt{-3}\right)$. □

We will also make use of the following classical fact about the third division field of an elliptic curve. Note that the commutator subgroup $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})' := [\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}), \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})]$ is a normal subgroup of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and the quotient group is dihedral of order 6:

$$\frac{\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})}{\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})'} \simeq D_3.$$

Thus, the associated fixed field $\mathbb{Q}(E[3])^{\rho_{E,3}(G_{\mathbb{Q}})\cap SL_2(\mathbb{Z}/3\mathbb{Z})'} \subseteq \mathbb{Q}(E[3])$ is generically a D_3-extension of $\mathbb{Q}$; the next lemma specifies generators for this subfield.

Lemma 4.2.11. *Let E be an elliptic curve over $\mathbb{Q}$ and let Δ_E denote the discriminant of any Weierstrass model of E. We have that $\mathbb{Q}\left(\mu_3, \Delta_E^{1/3}\right) \subseteq \mathbb{Q}(E[3])$. Furthermore, this subfield corresponds via Galois theory to the subgroup $\rho_{E,3}(G_{\mathbb{Q}}) \cap SL_2(\mathbb{Z}/3\mathbb{Z})'$, i.e. we have*

$$\mathbb{Q}(E[3])^{\rho_{E,3}(G_{\mathbb{Q}})\cap SL_2(\mathbb{Z}/3\mathbb{Z})'} = \mathbb{Q}\left(\mu_3, \Delta_E^{1/3}\right).$$

Proof. This is a classical result; see for instance (16, pp. 181–183) and the references therein. □

4.2.2.3 The level $m = 4$

The following lemma details the relevant classical facts surrounding the fourth division field of an elliptic curve. Note that the commutator subgroup $SL_2(\mathbb{Z}/4\mathbb{Z})' := [SL_2(\mathbb{Z}/4\mathbb{Z}), SL_2(\mathbb{Z}/4\mathbb{Z})]$ is a normal subgroup of $GL_2(\mathbb{Z}/4\mathbb{Z})$ and the quotient group is dihedral of order 8:

$$\frac{GL_2(\mathbb{Z}/4\mathbb{Z})}{SL_2(\mathbb{Z}/4\mathbb{Z})'} \simeq D_4.$$

Thus, the associated fixed field $\mathbb{Q}(E[4])^{\rho_{E,4}(G_{\mathbb{Q}})\cap SL_2(\mathbb{Z}/4\mathbb{Z})'} \subseteq \mathbb{Q}(E[4])$ is generically a D_4-extension of $\mathbb{Q}$; we now specify generators for this subfield.

Lemma 4.2.12. *Let E be an elliptic curve over $\mathbb{Q}$ and let Δ_E denote the discriminant of any Weierstrass model of E. We have that $\mathbb{Q}\left(\mu_4, \Delta_E^{1/4}\right) \subseteq \mathbb{Q}(E[4])$. Furthermore, this subfield corresponds via Galois theory to the subgroup $\rho_{E,4}(G_{\mathbb{Q}}) \cap \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})'$, i.e. we have*

$$\mathbb{Q}(E[4])^{\rho_{E,4}(G_{\mathbb{Q}})\cap \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})'} = \mathbb{Q}\left(\mu_4, \Delta_E^{1/4}\right).$$

Proof. See (16, pp. 172–173) and (16, pp. 218–220). □

We will sometimes need to deal with this subfield in the case that $\rho_{E,4}(G_{\mathbb{Q}})$ is contained in a specific proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. In particular, we will be interested in the subgroup

$$\begin{aligned}\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} :=& \{g \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) : \chi_4(\det g) = \varepsilon(g \bmod 2)\} \\ =& \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 1 & 0 \end{pmatrix} \right\rangle, \end{aligned} \tag{4.32}$$

where $\chi_4 : (\mathbb{Z}/4\mathbb{Z})^\times \to \{\pm 1\}$ is the unique nontrivial multiplicative character and $\varepsilon : \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \to \{\pm 1\}$ is as in (Equation 4.28). For any elliptic curve E over $\mathbb{Q}$, we have

$$\rho_{E,4}(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\varepsilon=\chi_4} \iff \mathbb{Q}\left(\sqrt{\Delta_E}\right) = \mathbb{Q}(i).$$

There is a rational parameter t on the genus zero modular curve $X_{\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon}}$ with the property that the forgetful map $X_{\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon}} \to X(1)$ takes the form $t \mapsto j_4(t)$, where

$$j_4(t) := -t^2 + 1728.$$

As detailed in (25), for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, we have

$$\rho_{E,4}(G_{\mathbb{Q}}) \subseteq GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \iff \exists t_0 \in \mathbb{Q} \text{ with } j_E = j_4(t_0). \tag{4.33}$$

In particular, defining the elliptic curve $\mathcal{E}_4$ over $\mathbb{Q}(t, D)$ by

$$\mathcal{E}_4 : y^2 = x^3 + \frac{108D^2 j_4(t)}{1728 - j_4(t)}x + \frac{432D^3 j_4(t)}{1728 - j_4(t)}, \tag{4.34}$$

we have that $\rho_{\mathcal{E}_4,4}(G_{\mathbb{Q}(t,D)}) \doteq GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon}$. The following lemma summarizes the situation and will be useful in what follows.

Lemma 4.2.13. *For any elliptic curve E over $\mathbb{Q}$, we have*

$$\rho_{E,4}(G_{\mathbb{Q}}) \dot{\subseteq} GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \iff \exists t_0, D_0 \in \mathbb{Q} \text{ with } E \simeq_{\mathbb{Q}} \mathcal{E}_4(t_0, D_0), \tag{4.35}$$

where $\mathcal{E}_4$ is the elliptic curve over $\mathbb{Q}(t, D)$ defined by (Equation 4.34)*. Furthermore, when this is the case, we have*

$$\mathbb{Q}(\mu_4, \Delta_E^{1/4}) = \mathbb{Q}\left(\mu_4, \Delta_{\mathcal{E}_4(t_0,D_0)}^{1/4}\right) = \mathbb{Q}\left(i, \sqrt{D_0 t_0 (t_0^2 - 1728)}\right). \tag{4.36}$$

In particular, when (Equation 4.35) *holds, the subfield $\mathbb{Q}\left(\mu_4, \Delta_E^{1/4}\right) \subseteq \mathbb{Q}(E[4])$ is either bi-quadratic or quadratic over $\mathbb{Q}$.*

Proof. The assertion (Equation 4.35) follows immediately from (Equation 4.33). The equality (Equation 4.36) follows from

$$\Delta_{\mathcal{E}_4} = -\left(\frac{2^9 3^6 D^3 (t^2 - 1728)}{t^3}\right)^2,$$

using the fact that $(-1)^{1/4} = \zeta_8 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, and from (Equation 4.36) one sees that $\mathbb{Q}\left(\mu_4, \Delta_E^{1/4}\right)$ is either biquadratic or quadratic over $\mathbb{Q}$. □

4.2.2.4 The level $m = 5$

The subgroups

$$G_{5,1} := \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\}, \; G_{5,2} := \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\} \subseteq \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subseteq GL_2(\mathbb{Z}/5\mathbb{Z}) \tag{4.37}$$

correspond to two genus zero modular curves $X_{G_{5,1}}$ and $X_{G_{5,2}}$, each of which is a 2-fold cover of $X_0(5)$. As discussed in (30), the maps $\mathbb{P}^1(t) \to \mathbb{P}^1(j)$ corresponding to the forgetful maps $X_{G_{5,i}} \longrightarrow X(1)$ are given respectively by the rational functions

$$j_{5,1}(t) := \frac{(t^4 - 12t^3 + 14t^2 + 12t + 1)^3}{t^5(t^2 - 11t - 1)}, \qquad j_{5,2}(t) := \frac{(t^4 + 228t^3 + 494t^2 - 228t + 1)^3}{t(t^2 - 11t - 1)^5}.$$

We define the elliptic curves $\mathcal{E}_{5,i}$ over $\mathbb{Q}(t, D)$ by

$$\mathcal{E}_{5,i} : \; y^2 = x^3 + \frac{108 D^2 j_{5,i}(t)}{1728 - j_{5,i}(t)} x + \frac{432 D^3 j_{5,i}(t)}{1728 - j_{5,i}(t)} \qquad (i \in \{1, 2\}); \tag{4.38}$$

we have

$$\rho_{\mathcal{E}_{5,i},5}(G_{\mathbb{Q}(t,D)}) \doteq G_{5,i} \subseteq \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}) \qquad (i \in \{1,2\})\,. \tag{4.39}$$

The next lemma explicitly characterizes the subfields cut out by the characters

$$\psi_{5,1},\ \psi_{5,2}^2\psi_{5,1} : \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\} \subseteq (\mathbb{Z}/5\mathbb{Z})^\times\,,$$
$$\psi_{5,2},\ \psi_{5,1}^2\psi_{5,2} : \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\} \longrightarrow \{\pm 1\} \subseteq (\mathbb{Z}/5\mathbb{Z})^\times\,.$$

Lemma 4.2.14. *For each* $i \in \{1,2\}$*, let* $\mathcal{E}_{5,i}$ *be the elliptic curve over* $\mathbb{Q}(t,D)$ *defined by* (Equation 4.38) *and let*

$$\chi_{5,1}^{(i)},\ \chi_{5,2}^{(i)} : \mathrm{Gal}\left(\mathbb{Q}(t,D)(\mathcal{E}_{5,i}[5])/\mathbb{Q}(t,D)\right) \longrightarrow \{\pm 1\} \subseteq (\mathbb{Z}/5\mathbb{Z})^\times$$

denote the restrictions under (Equation 4.39) *of the characters* $\chi_{5,1}^{(i)} := \psi_{5,i}$ *and* $\chi_{5,2}^{(i)} := \psi_{5,i}\psi_{5,3-i}^2$*, where* $\psi_{5,i}$ *are as in* (Equation 4.23)*. We then have*

$$\begin{aligned}
\mathbb{Q}(t,D)(\mathcal{E}_{5,1}[5])^{\ker\chi_{5,1}^{(1)}} &= \mathbb{Q}(t,D)\left(\sqrt{-\frac{2D(t^4-12t^3+14t^2+12t+1)}{((t^2+1)(t^4-18t^3+74t^2+18t+1)}}\right),\\
\mathbb{Q}(t,D)(\mathcal{E}_{5,1}[5])^{\ker\chi_{5,2}^{(1)}} &= \mathbb{Q}(t,D)\left(\sqrt{-\frac{10D(t^4-12t^3+14t^2+12t+1)}{((t^2+1)(t^4-18t^3+74t^2+18t+1)}}\right),\\
\mathbb{Q}(t,D)(\mathcal{E}_{5,2}[5])^{\ker\chi_{5,1}^{(2)}} &= \mathbb{Q}(t,D)\left(\sqrt{-\frac{2D(t^4+228t^3+494t^2-228t+1)}{(t^2+1)(t^4-522t-10006t^2+522t+1)}}\right),\\
\mathbb{Q}(t,D)(\mathcal{E}_{5,2}[5])^{\ker\chi_{5,2}^{(2)}} &= \mathbb{Q}(t,D)\left(\sqrt{-\frac{10D(t^4+228t^3+494t^2-228t+1)}{(t^2+1)(t^4-522t-10006t^2+522t+1)}}\right).
\end{aligned} \tag{4.40}$$

Proof. For any elliptic curve E over $\mathbb{Q}$ with $\rho_{E,5}(G_{\mathbb{Q}}) \subseteq B(5)$, define $\langle P \rangle \subseteq E[5]$ and $\langle P' \rangle \subseteq E'_{\langle P \rangle}[5]$ as in (Equation 4.24) and (Equation 4.25). By (Equation 4.26) and (Equation 4.37), we have

$$\begin{aligned}
\rho_{E,5}(G_{\mathbb{Q}}) \dot{\subseteq} G_{5,1} &\iff \exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P \rangle \subseteq E[5] && \text{with} \quad [\mathbb{Q}(P) : \mathbb{Q}] \leq 2, \\
\rho_{E,5}(G_{\mathbb{Q}}) \dot{\subseteq} G_{5,2} &\iff \begin{array}{l} \exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P \rangle \subseteq E[5] \text{ and} \\ \exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P' \rangle \subseteq E'_{\langle P \rangle}[5] \end{array} && \text{with} \quad [\mathbb{Q}(P') : \mathbb{Q}] \leq 2,
\end{aligned} \tag{4.41}$$

and the same statement holds when the base field $\mathbb{Q}$ is replaced by $\mathbb{Q}(t, D)$. Furthermore, we have

$$\mathbb{Q}(t, D)\left(\mathcal{E}_{5,1}[5]\right)^{\ker \chi_{5,1}^{(1)}} = \mathbb{Q}(t, D)\left(P\right), \qquad \mathbb{Q}(t, D)\left(\mathcal{E}_{5,2}[5]\right)^{\ker \chi_{5,1}^{(2)}} = \mathbb{Q}(t, D)\left(P'\right), \tag{4.42}$$

where $P \in \mathcal{E}_{5,1}[5]$ and $P' \in (\mathcal{E}_{5,2})'_{\langle P \rangle}[5]$ are as in (Equation 4.41).

Using the linear factor of the 5th division polynomial of $\mathcal{E}_{5,1}$, we find the point $P_1 = (x_1, y_1) \in \mathcal{E}_{5,1}[5]$, where

$$\begin{aligned}
x_1 &:= -\frac{6D(t^2 - 6t + 1)(t^4 - 12t^3 + 14t^2 + 12t + 1)}{(t^2 + 1)(t^4 - 18t^3 + 74t^2 + 18t + 1)}, \\
y_1 &:= \frac{216dt(t^4 - 12t^3 + 14t^2 + 12t + 1)}{(t^2 + 1)(t^4 - 18t^3 + 74t^2 + 18t + 1)} \sqrt{\frac{-2D(t^4 - 12t^3 + 14t^2 + 12t + 1)}{(t^2 + 1)(t^4 - 18t^3 + 74t^2 + 18t + 1)}}.
\end{aligned}$$

By (Equation 4.42), this proves the first equality in (Equation 4.40). We now consider the character $\psi_{5,2}^2 : G_{5,1} \to \{\pm 1\}$, whose value $\psi_{5,2}(g_1)^2$ agrees with $\left(\frac{5}{\det g_1}\right)$, and thus has corresponding fixed field $\mathbb{Q}(t, D)\left(\sqrt{5}\right)$. Since $\chi_{5,2}^{(1)} = \psi_{5,2}^2 \psi_{5,1}$, this observation establishes the second equality in (Equation 4.40).

For the second pair of equalities in (Equation 4.40), we reason as follows. The 5th division polynomial associated to $\mathcal{E}_{5,2}$ has a quadratic factor that is irreducible over $\mathbb{Q}(t, D)$, and this leads to a $G_{\mathbb{Q}(t,D)}$-stable cyclic subgroup $\langle P\rangle \subseteq \mathcal{E}_{5,2}[5]$. We find that the isogenous elliptic curve $(\mathcal{E}_{5,2})'_{\langle P\rangle} = \mathcal{E}_{5,2}/\langle P\rangle$ is given by

$$\begin{aligned}(\mathcal{E}_{5,2})'_{\langle P\rangle} : \ y^2 = x^3 &- \frac{67500D^2(t^4-12t^3+14t^2+12t+1)(t^4+228t^3+494t^2-228t+1)^2}{(t^2+1)^2(t^4-522t^3-10006t^2+522t+1)^2}x \\ &- \frac{6750000D^3(t^4-18t^3+74t^2+18t+1)(t^4+228t^3+494t^2-228t+1)^3}{(t^2+1)^2(t^4-522t^3-10006t^2+522t+1)^3}.\end{aligned}$$

The 5th division polynomial of $(\mathcal{E}_{5,2})'_{\langle P\rangle}$ is seen to have a linear factor, which leads to the point $P'_2 = (x'_2, y'_2) \in (\mathcal{E}_{5,2})'_{\langle P\rangle}[5]$, where

$$\begin{aligned}x'_2 &:= -150\frac{D(t^2-6t+1)(t^4+228t^3+494t^2-228t+1)}{(t^2+1)(t^4-522t^3-10006t^2+522t+1)}, \\ y'_2 &:= 27000\frac{Dt(t^4+228t^3+494t^2-228t+1)}{(t^2+1)(t^4-522t^3-10006t^2+522t+1)}\sqrt{\frac{-2D(t^4+228t^3+494t^2-228t+1)}{(t^2+1)(t^4-522t^3-10006t^2+522t+1)}}.\end{aligned}$$

As before, this, together with the fact that for $g_2 \in G_{5,2}$, the value $\psi_{5,1}(g_2)^2$ agrees with $\left(\frac{5}{\det g_2}\right)$ and that $\chi^{(2)}_{5,2} = \psi^2_{5,1}\psi_{5,2}$, establishes the second two equalities in (Equation 4.40), proving the lemma. □

4.2.2.5 The level $m = 7$

We begin by describing an explicit Weierstrass model $\mathcal{E}_7$ over $\mathbb{Q}(t, D)$ that is generic in the sense that its specializations $\mathcal{E}_7(t_0, D_0)$ give rise to all elliptic curves E over $\mathbb{Q}$ for which $\rho_{E,7}(G_{\mathbb{Q}}) \dot{\subseteq} B(7)$, where we recall that

$$B(7) = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subseteq GL_2(\mathbb{Z}/7\mathbb{Z})$$

denotes the Borel subgroup. We then describe explicitly certain subfields of $\mathbb{Q}(\mathcal{E}_7[7])$ that will be useful in the next section.

Define $j_7(t) \in \mathbb{Q}(t)$ by

$$j_7(t) := \frac{(t^2 + 245t + 2401)^3(t^2 + 13t + 49)}{t^7}, \tag{4.43}$$

and the elliptic curve $\mathcal{E}_7$ over $\mathbb{Q}(t, D)$ by

$$\begin{aligned} &\mathcal{E}_7 : \ y^2 = x^3 + D^2 a_{4;7}(t)x + D^3 a_{6;7}(t), \\ &a_{4;7}(t) := \frac{108 j_7(t)}{1728 - j_7(t)}, \qquad a_{6;7}(t) := \frac{432 j_7(t)}{1728 - j_7(t)}. \end{aligned} \tag{4.44}$$

As proved in (30), we have

$$\rho_{\mathcal{E}_7,7}(G_{\mathbb{Q}(t,D)}) \doteq B(7) \subseteq GL_2(\mathbb{Z}/7\mathbb{Z}). \tag{4.45}$$

The next lemma explicitly characterizes the subfields cut out by the quadratic characters $\psi_{7,1}^3$ and $\psi_{7,2}^3$.

Lemma 4.2.15. *Let $\mathcal{E}_7$ be the elliptic curve over $\mathbb{Q}(t, D)$ defined by* (Equation 4.44) *and let*

$$\psi_{7,1}^3,\ \psi_{7,2}^3 : \mathrm{Gal}\left(\mathbb{Q}(t, D)(\mathcal{E}_7[7])/\mathbb{Q}(t, D)\right) \to \{\pm 1\}$$

denote the restrictions under (Equation 4.45) *of the cubes of the characters defined in* (Equation 4.23).

We then have

$$\begin{aligned}
\mathbb{Q}(t, D)(\mathcal{E}_7[7])^{\ker \psi_{7,1}^3} &= \mathbb{Q}(t, D)\left(\sqrt{\frac{14D(t^2+13t+49)(t^2+245t+2401)}{(t^4-490t^3-21609t^2-235298t-823543)}}\right), \\
\mathbb{Q}(t, D)(\mathcal{E}_7[7])^{\ker \psi_{7,2}^3} &= \mathbb{Q}(t, D)\left(\sqrt{-\frac{2D(t^2+13t+49)(t^2+245t+2401)}{(t^4-490t^3-21609t^2-235298t-823543)}}\right).
\end{aligned} \tag{4.46}$$

Proof. A computation reveals that the 7th division polynomial of $\mathcal{E}_7$ has the cubic factor

$$\begin{aligned}
&x^3 - \frac{126D(t^2+13t+49)(t^2+245t+2401)}{(t^4-490t^3-21609t^2-235298t-823543)}x^2 \\
&\quad + \frac{108D^2(t^2+13t+49)(t^2+245t+2401)^2(33t^2+637t+2401)}{(t^4-490t^3-21609t^2-235298t-823543)^2}x \\
&\quad - \frac{216D^3(t^2+13t+49)(t^2+245t+2401)^3(881t^4+38122t^3+525819t^2+3058874t+5764801)}{7(t^4-490t^3-21609t^2-235298t-823543)^3},
\end{aligned} \tag{4.47}$$

which is irreducible over $\mathbb{Q}(t, D)$ and whose discriminant is in $(\mathbb{Q}(t, D)^{\times})^2$. Writing this polynomial in the form $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, we have that $\mathbb{Q}(t, D)(\alpha_1)$ is cyclic cubic over $\mathbb{Q}(t, D)$ and that the point

$$P := \left(\alpha_1, \sqrt{\alpha_1^3 + D^2 a_{4;7}(t)\alpha_1 + D^3 a_{6;7}(t)}\right) \tag{4.48}$$

generates a cyclic submodule $\langle P \rangle \subseteq \mathcal{E}_7[7]$ on which $G_{\mathbb{Q}(t,D)}$ acts through the eigenfunction $\psi_{7,1}$ via

$$\sigma : P \mapsto [\psi_{7,1}(\sigma)]\, P. \tag{4.49}$$

We have

$$\begin{aligned} \mathbb{Q}(t, D)(P) &= \mathbb{Q}(t, D)\left(\alpha_1, \sqrt{\alpha_1^3 + D^2 a_{4;7}(t)\alpha_1 + D^3 a_{6;7}(t)}\right) \\ &\supseteq \mathbb{Q}(t, D)\left(\alpha_1, \sqrt{\prod_{j=1}^{3}(\alpha_j^3 + D^2 a_{4;7}(t)\alpha_j + D^3 a_{6;7}(t))}\right); \end{aligned} \tag{4.50}$$

a computation using the third equation in (Equation 4.22) shows that

$$\begin{aligned} \mathbb{Q}(t, D)\left(\sqrt{\prod_{j=1}^{3}(\alpha_j^3 + D^2 a_{4;7}(t)\alpha_j + D^3 a_{6;7}(t))}\right) = \\ \mathbb{Q}(t, D)\left(\sqrt{\frac{14D(t^2 + 13t + 49)(t^2 + 245t + 2401)}{(t^4 - 490t^3 - 21609t^2 - 235298t - 823543)}}\right), \end{aligned}$$

establishing the first equality in (Equation 4.46) (and also showing that we have equality in (Equation 4.50)). The second equality follows from the fact that the product $\psi_{7,1}^3(g)\psi_{7,2}^3(g)$ agrees with $\left(\frac{-7}{\det g}\right)$, whose fixed field is $\mathbb{Q}(t, D)\left(\sqrt{-7}\right)$. □

Our next lemma explicitly characterizes the subfields cut out by the cubic characters $\psi_{7,1}^2, \psi_{7,2}^2$ and $\psi_{7,1}^2\psi_{7,2}^4$, where $\psi_{7,i}$ is defined as in (Equation 4.23).

We define the polynomials

$$\begin{aligned} f_{\mathrm{cyc},7}^+(X) &:= X^3 + X^2 - 2X - 1, \\ f_T(X) &:= X^3 - T_1(t)X^2 + T_2(t)X - T_3(t), \\ f_R(X) &:= X^3 - R_1(t)X^2 + R_2(t)X - R_3(t), \\ f_{R'}(X) &:= X^3 - R_1(t)X^2 + R_2(t)X - R_3'(t), \end{aligned} \tag{4.51}$$

where

$$\begin{aligned} T_1(t) &:= -21(t^2 + 13t + 49), \\ T_2(t) &:= 3(t^2 + 13t + 49)(33t^2 + 637t + 2401), \\ T_3(t) &:= -\frac{1}{7}(t^2 + 13t + 49)(881t^4 + 38122t^3 + 525819t^2 + 3058874t + 5764801), \\ R_1(t) &:= 21(t^2 + 13t + 49), \\ R_2(t) &:= -21(t^2 + 13t + 49)(9t^2 - 91t - 343), \\ R_3(t) &:= -7(t^2 + 13t + 49)(223t^4 + 3542t^3 + 3381t^2 - 62426t - 117649), \\ R_3'(t) &:= -(t^2 + 13t + 49)(3289t^4 + 24794t^3 + 23667t^2 - 436982t - 823543). \end{aligned} \tag{4.52}$$

Lemma 4.2.16. *Let $\mathcal{E}_7$ be the elliptic curve over $\mathbb{Q}(t, D)$ defined by* (Equation 4.44) *and let*

$$\psi_{7,1}^2, \psi_{7,2}^2 : \mathrm{Gal}\left(\mathbb{Q}(t, D)(\mathcal{E}_7[7])/\mathbb{Q}(t, D)\right) \longrightarrow \left((\mathbb{Z}/7\mathbb{Z})^\times\right)^2 \simeq \mu_3$$

denote the restrictions under (Equation 4.45) *of the squares of the characters $\psi_{7,i}$ defined in* (Equation 4.23). *Let us denote by $\mathbb{Q}(t, D)_{f^+_{\mathrm{cyc},7}}$, $\mathbb{Q}(t, D)_{f_T}$, $\mathbb{Q}(t, D)_{f_R}$ and $\mathbb{Q}(t, D)_{f_{R'}}$ the splitting fields over $\mathbb{Q}(t, D)$ of the polynomials $f^+_{\mathrm{cyc},7}(X)$, $f_T(X)$, $f_R(X)$ and $f_{R'}(X)$, respectively, where these polynomials are defined by* (Equation 4.51) *and* (Equation 4.52). *We then have*

$$\begin{aligned} &\mathbb{Q}(t, D)\left(\mathcal{E}_7[7]\right)^{\ker \psi_{7,1}^2} = \mathbb{Q}(t, D)_{f_T}, \quad \mathbb{Q}(t, D)\left(\mathcal{E}_7[7]\right)^{\ker \psi_{7,1}^2 \psi_{7,2}^2} = \mathbb{Q}(t, D)_{f^+_{\mathrm{cyc},7}}, \\ &\mathbb{Q}(t, D)\left(\mathcal{E}_7[7]\right)^{\ker \psi_{7,2}^2} = \mathbb{Q}(t, D)_{f_R}, \quad \mathbb{Q}(t, D)\left(\mathcal{E}_7[7]\right)^{\psi_{7,1}^2 \psi_{7,2}^4} = \mathbb{Q}(t, D)_{f_{R'}}. \end{aligned} \tag{4.53}$$

Proof. Since $\rho_{\mathcal{E}_7,7}\left(G_{\mathbb{Q}(t,D)}\right) = B(7)$, it is straightforward to see that $\mathbb{Q}(t, D)\left(\mathcal{E}_7[7]\right)$ has exactly 4 cyclic cubic subfields. Furthermore, we have

$$\mathbb{Q}(t, D)\left(\mathcal{E}_7[7]\right)^{\ker \psi_{7,1}^2 \psi_{7,2}^2} = \mathbb{Q}(t, D)\left(\mu_7\right)^+ \subseteq \mathbb{Q}(t, D)\left(\mu_7\right),$$

the first equality above following from the fact that $\psi_{7,1}(g)\psi_{7,2}(g) = \det g$, which implies that the fixed field of $\ker \psi_{7,1}^2 \psi_{7,2}^2$ is the maximal real subfield $\mathbb{Q}(t, D)\left(\mu_7\right)^+$, i.e. the unique subfield of $\mathbb{Q}(t, D)\left(\mu_7\right)$ that is cyclic cubic over $\mathbb{Q}(t, D)$. We have $\mathbb{Q}(t, D)\left(\mu_7\right)^+ = \mathbb{Q}(t, D)\left(\zeta_7 + \zeta_7^{-1}\right)$, so $\mathbb{Q}(t, D)\left(\mu_7\right)^+$ is the splitting field of

$$f^+_{\mathrm{cyc},7}(X) = X^3 + X^2 - 2X - 1,$$

the minimal polynomial over $\mathbb{Q}(t, D)$ of the generator $\zeta_7 + \zeta_7^{-1}$. This establishes the second equality in (Equation 4.53).

For the equality in (Equation 4.53) involving the fixed field of $\ker \psi_{7,1}^2$, we reason as follows. By (Equation 4.49) and (Equation 4.48), we see that $\mathbb{Q}(t, D)\left(\mathcal{E}_7[7]\right)^{\ker \psi_{7,1}} = \mathbb{Q}(t, D)(P)$, where $\langle P \rangle \subseteq \mathcal{E}_7[7]$ is a cyclic $G_{\mathbb{Q}(t,D)}$-stable subgroup, and since this extension is cyclic of degree 6 over $\mathbb{Q}(t, D)$, it follows that

$$\mathbb{Q}(t, D)\left(\mathcal{E}_7[7]\right)^{\ker \psi_{7,1}^2} = \mathbb{Q}(t, D)\left(\alpha_1\right). \tag{4.54}$$

where α_1 is the x-coordinate of P. Finally, the substitution $x = -\frac{6D(t^2+245t+2401)}{(t^4-490t^3-21609t^2-235298t-823543)}X$ transforms the cyclic cubic polynomial (Equation 4.47) into $\left(-\frac{6D(t^2+245t+2401)}{(t^4-490t^3-21609t^2-235298t-823543)}\right)^3 f_T(X)$, and the first equality in (Equation 4.53) follows.

The discriminants Δ_T and $\Delta_{cyc,7}^+$ associated to the polynomials $f_T(X)$ and $f_{cyc,7}^+(X)$ satisfy

$$\sqrt{\Delta_T} = \frac{2^6 3^3 t^4 (t^2 + 13t + 49)}{7}, \qquad \sqrt{\Delta_{cyc,7}^+} = 7.$$

Applying Lemma 4.2.7, we find that $\mathbb{Q}(t, D)_{f_R}$ and $\mathbb{Q}(t, D)_{f_{R'}}$ are the remaining two cyclic cubic subfields of $\mathbb{Q}(t, D)\left(\mathcal{E}_7[7]\right)$. To see which subfield is which, we first note that, just as in (Equation 4.54), we have

$$\mathbb{Q}(t, D)\left(\mathcal{E}_7[7]\right)^{\ker \psi_{7,2}^2} = \mathbb{Q}(t, D)\left(x(P')\right),$$

where $P' \in (\mathcal{E}_7)'_{\langle P \rangle}$ is any generator of a cyclic $G_{\mathbb{Q}(t,D)}$-stable subgroup $\langle P' \rangle \subseteq (\mathcal{E}_7)'_{\langle P \rangle}[7]$. A direct computation reveals that the isogenous curve $(\mathcal{E}_7)'_{\langle P \rangle}$ has Weierstrass equation

$$(\mathcal{E}_7)'_{\langle P \rangle} : y^2 = x^3 - \frac{2^2 3^3 7^4 D^2 (t^2+5t+1)(t^2+13t+49)(t^2+245t+2401)^2}{(t^4-490t^3-21609t^2-235298t-823543)^3} x - \frac{2^4 3^3 7^6 D^3 (t^2+13t+49)(t^2+245t+2401)^3 (t^4+14t^3+63t^2+70t-7)}{(t^4-490t^3-21609t^2-235298t-823543)^3},$$

and that its 7th division polynomial has the cubic factor

$$x^3 + \frac{2 \cdot 3^2 7^2 D (t^2+13t+49)(t^2+245t+2401)}{(t^4-490t^3-21609t^2-235298t-823543)} x^2 + \frac{2^2 3^3 7^4 D^2 (t^2+13t+33)(t^2+13t+49)(t^2+245t+2401)^2}{(t^4-490t^3-21609t^2-235298t-823543)^2} x + \frac{2^3 3^3 7^6 D^3 (t^2+13t+49)(t^2+245t+2401)^3 (t^4+26t^3+219t^2+778t+881)}{(t^4-490t^3-21609t^2-235298t-823543)^3}.$$

Finally, applying Lemma 4.2.8 (and some extensive, tedious calculations), we see that the splitting field of this polynomial agrees with the splitting field of $f_R(X)$, and this finishes the proof. □

CHAPTER 5

DEVELOPING EXPLICIT MODELS FOR MISSING TRACE GROUPS

5.1 Developing explicit models for missing trace groups

In this section, we complete the proof of Theorem 1.1.6. Specifically, for each $\mathfrak{m}$ appearing in the union on the right-hand side of (Equation 1.13), we will now

1. list the groups $G \in \mathfrak{G}_{MT}^{max}(0, \mathfrak{m})$, up to conjugation in $GL_2(\hat{\mathbb{Z}})$;
2. for each such group G, exhibit a rational function $j_{\tilde{G}}(t) \in \mathbb{Q}(t)$ which defines the forgetful map $j_{\tilde{G}} : X_{\tilde{G}} \longrightarrow X(1)$;
3. in case $G \subsetneq \tilde{G}$, identify each twist parameter $d_G(t) \in \mathbb{Q}(t)$ for which the elliptic curve $\mathcal{E}_G$ over $\mathbb{Q}(t)$ given by

$$\mathcal{E}_G : \ d_G(t)y^2 = x^3 + a_{4,\tilde{G}}(t)x + a_{6,\tilde{G}}(t)$$

satisfies $\rho_{\mathcal{E}_G,\mathfrak{m}}(G_{\mathbb{Q}(t)}) = G$. (Here the Weierstrass coefficients $a_{4,\tilde{G}}(t)$, $a_{6,\tilde{G}}(t) \in \mathbb{Q}(t)$ are chosen as usual according to (Equation 1.9), so that the j-invariant of $\mathcal{E}_G$ is $j_{\tilde{G}}(t)$.)

Throughout this section, we denote by π_{GL_2} the canonical projection map

$$\pi_{GL_2} : GL_2(\hat{\mathbb{Z}}) \longrightarrow GL_2(\mathbb{Z}/m\mathbb{Z}),$$

suppressing the dependence of π_{GL_2} on the level $\mathfrak{m}$.

5.1.1 The level $\mathfrak{m} = 2$.

We have $\mathfrak{G}_{MT}^{max}(0,2) = \{G_{2,1}\}$, where $G_{2,1}(2) \subseteq GL_2(\mathbb{Z}/2\mathbb{Z})$ is given by

$$G_{2,1}(2) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$

and $G_{2,1} = \pi_{GL_2}^{-1}(G_{2,1}(2))$. Note that $-I \in G_{2,1}$, so $G_{2,1} = \tilde{G}_{2,1}$. Define the function $j_{2,1}(t) \in \mathbb{Q}(t)$ by

$$j_{2,1}(t) := 256\frac{(t+1)^3}{t}.$$

As detailed in (30), for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, one has

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{2,1} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{2,1}(t_0). \tag{5.1}$$

We define the coefficients $a_{4;2,1}(t)$ and $a_{6;2,1}(t)$ by (Equation 1.9) and the elliptic curve $\mathcal{E}_{2,1,1}$ over $\mathbb{Q}(t, D)$ by

$$\mathcal{E}_{2,1,1}: \; Dy^2 = x^3 + a_{4;2,1}(t)x + a_{6;2,1}(t).$$

It follows from (Equation 5.1) that

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{2,1} \iff \exists t_0, D_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{2,1,1}(t_0, D_0).$$

5.1.2 The level $m = 3$.

We have $\mathfrak{G}_{MT}^{max}(0,3) = \{G_{3,1,1}, G_{3,1,2}\}$, where $G_{3,1,1}(3), G_{3,1,2}(3) \subseteq GL_2(\mathbb{Z}/3\mathbb{Z})$ are given by

$$G_{3,1,1}(3) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{3,1,2}(3) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \right\}$$

and $G_{3,1,k} = \pi_{GL_2}^{-1}(G_{3,1,k}(3))$ for $k \in \{1,2\}$. Note that $-I \notin G_{3,1,k}$. We have

$$\tilde{G}_{3,1,1}(3) = \tilde{G}_{3,1,2}(3) = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\};$$

let us denote this group by $\tilde{G}_{3,1}(3)$, omitting the last subscript. Define the function $j_{3,1}(t) \in \mathbb{Q}(t)$ by

$$j_{3,1}(t) := 27\frac{(t+1)(t+9)^3}{t^3}.$$

As detailed in (30), for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, one has

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{3,1} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{3,1}(t_0). \tag{5.2}$$

We define the coefficients $a_{4;3,1}(t)$ and $a_{6;3,1}(t)$ by (Equation 1.9), the twist parameters $d_{3,1,1}(t), d_{3,1,2}(t) \in \mathbb{Q}(t)$ by

$$d_{3,1,1}(t) := \frac{(t+1)(t^2-18t-27)}{6(t+9)}, \qquad d_{3,1,2}(t) := -3d_{3,1,1}(t),$$

and the elliptic curves $\mathcal{E}_{3,1,k}$ over $\mathbb{Q}(t)$ by

$$\mathcal{E}_{3,1,k}: \; d_{3,1,k}(t)y^2 = x^3 + a_{4;3,1}(t)x + a_{6;3,1}(t) \qquad (k \in \{1,2\}).$$

As may be found in (30), for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, one has

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{3,1,1} \iff \exists t_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{3,1,1}(t_0),$$

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{3,1,2} \iff \exists t_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{3,1,2}(t_0).$$

5.1.3 The level $m = 4$.

We have $\mathfrak{G}_{MT}^{\max}(0,4) = \{G_{4,1,1}\}$, where $G_{4,1,1}(4) \subseteq GL_2(\mathbb{Z}/4\mathbb{Z})$ is given by

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

and $G_{4,1,1} = \pi_{GL_2}^{-1}(G_{4,1,1}(4))$. Note that $-I \notin G_{4,1,1}$. We have

$$\tilde{G}_{4,1,1}(4) = GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon},$$

defined as in (Equation 4.32). Let us set $\tilde{G}_{4,1} := \tilde{G}_{4,1,1}$. We define the j-invariant $j_{4,1}(t) := -t^2 + 1728$ and the elliptic curve $\mathcal{E}_{4,1}$ over $\mathbb{Q}(t, D)$ by

$$\mathcal{E}_{4,1} : y^2 = x^3 + \frac{108D^2 j_{4.1}(t)}{1728 - j_{4,1}(t)}x + \frac{432D^3 j_{4,1}(t)}{1728 - j_{4,1}(t)};$$

see (Equation 4.34). By Lemma 4.2.13, for any elliptic curve E over $\mathbb{Q}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{4,1} \iff \exists t_0, D_0 \in \mathbb{Q} \text{ with } E \simeq_{\mathbb{Q}} \mathcal{E}_{4,1}(t_0, D_0)$$

and

$$\mathbb{Q}(t, D)\left(i, \Delta_{\mathcal{E}_{4,1}}^{1/4}\right) = \mathbb{Q}(t, D)\left(i, \sqrt{Dt(t^2 - 1728)}\right). \tag{5.3}$$

Regarding the index two subgroup $G_{4,1,1}(4) \subseteq \tilde{G}_{4,1}(4)$, a computation reveals that

$$G_{4,1,1}(4) \cap SL_2(\mathbb{Z}/4\mathbb{Z})' = G_{4,1,1}(4) \cap SL_2(\mathbb{Z}/4\mathbb{Z}),$$

and $G_{4,1,1}(4)$ is the unique maximal subgroup (relative to $\dot{\subseteq}$) of $\tilde{G}_{4,1}(4)$ with this property. By Lemmas 4.2.12 and 4.2.13, together with the Galois correspondence and (Equation 5.3), it follows that

$$\begin{aligned} \rho_{\mathcal{E}_{4,1}(t_0,D_0)}(G_{\mathbb{Q}}) \dot{\subseteq} G_{4,1,1} &\iff \mathbb{Q}\left(i, \Delta_{\mathcal{E}_{4,1}(t_0,D_0)}^{1/4}\right) = \mathbb{Q}(i) \\ &\iff D_0 = \pm t_0(t_0^2 - 1728). \end{aligned} \tag{5.4}$$

Noting that $t \mapsto t(t^2 - 1728)$ is an odd function of t and $j_{4,1}(t)$ is even, we are led to the single twist parameter

$$d_{4,1,1}(t) := t(t^2 - 1728),$$

and we define the elliptic curve $\mathcal{E}_{4,1,1}$ over $\mathbb{Q}(t)$ by

$$\mathcal{E}_{4,1,1} : \ d_{4,1,1}(t)y^2 = x^3 + a_{4;4,1}(t)x + a_{6;4,1}(t).$$

For each elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, we evidently have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{4,1,1} \iff \exists t_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{4,1,1}(t_0).$$

5.1.4 The level $m = 5$.

We have $\mathfrak{G}_{MT}^{max}(0,5) = \{G_{5,1,1}, G_{5,1,2}, G_{5,2,1}, G_{5,2,2}\}$, where the groups $G_{5,i,k}(5) \subseteq GL_2(\mathbb{Z}/5\mathbb{Z})$ are given by

$$G_{5,1,1}(5) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{5,1,2}(5) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} a^2 & * \\ 0 & a \end{pmatrix} : a \in (\mathbb{Z}/5\mathbb{Z})^\times \right\},$$

$$G_{5,2,1}(5) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \right\},$$

$$G_{5,2,2}(5) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} a & * \\ 0 & a^2 \end{pmatrix} : a \in (\mathbb{Z}/5\mathbb{Z})^\times \right\},$$

and $G_{5,i,k} = \pi_{GL_2}^{-1}(G_{5,i,k}(5))$ for $i, k \in \{1,2\}$. Note that $-I \notin G_{5,i,k}$, for each $i, k \in \{1,2\}$. We have

$$\tilde{G}_{5,1}(5) := \tilde{G}_{5,1,1}(5) = \tilde{G}_{5,1,2}(5) = \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\},$$

$$\tilde{G}_{5,2}(5) := \tilde{G}_{5,2,1}(5) = \tilde{G}_{5,2,2}(5) = \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\}.$$

Define the functions $j_{5,1}(t), j_{5,2}(t) \in \mathbb{Q}(t)$ by

$$j_{5,1}(t) := \frac{(t^4 - 12t^3 + 14t^2 + 12t + 1)^3}{t^5(t^2 - 11t - 1)},$$
$$j_{5,2}(t) := \frac{(t^4 + 228t^3 + 494t^2 - 228t + 1)^3}{t(t^2 - 11t - 1)^5}.$$

As detailed in (30), for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, one has

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{5,1} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{5,1}(t_0),$$
$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{5,2} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{5,2}(t_0).$$

We define the coefficients $a_{4;5,i}(t)$, and $a_{6;5,i}(t)$ for each $i \in \{1,2\}$ by (Equation 1.9), the twist parameters $d_{5,i,k}(t) \in \mathbb{Q}(t)$ for each $i, k \in \{1,2\}$ by

$$d_{5,1,1}(t) := -\frac{(t^2+1)(t^4 - 18t^3 + 74t^2 + 18t + 1)}{2(t^4 - 12t^3 + 14t^2 + 12t + 1)}, \qquad d_{5,1,2}(t) := 5d_{5,1,1}(t),$$
$$d_{5,2,1}(t) := -\frac{(t^2+1)(t^4 - 522t^3 - 10006t^2 + 522t + 1)}{2(t^4 + 228t^3 + 494t^2 - 228t + 1)}, \qquad d_{5,2,2}(t) := 5d_{5,2,1}(t),$$

and the elliptic curves $\mathcal{E}_{5,i,k}$ over $\mathbb{Q}(t)$ by

$$\mathcal{E}_{5,i,k} : \; d_{5,i,k}(t)y^2 = x^3 + a_{4;5,i}(t)x + a_{6;5,i}(t) \qquad (i,k \in \{1,2\}).$$

As detailed in (30), for any elliptic curve E over $\mathbb{Q}$ and for each $i, k \in \{1,2\}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{5,i,k} \iff \exists t_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{5,i,k}(t_0).$$

5.1.5 The level $\mathfrak{m} = 6$

We have $\mathfrak{G}_{\mathrm{MT}}^{\max}(0,6) = \{\mathsf{G}_{6,1,1}, \mathsf{G}_{6,2,1}, \mathsf{G}_{6,3,1}, \mathsf{G}_{6,3,2}\}$, where $\mathsf{G}_{6,i,k}(6) \subseteq \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ are given by

$$\begin{aligned}
\mathsf{G}_{6,1,1}(6) &= \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(1,1)}} \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}), \\
\mathsf{G}_{6,2,1}(6) &= \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(2,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\
\mathsf{G}_{6,3,1}(6) &= \left\langle \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 5 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 3 & 1 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(3,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\
\mathsf{G}_{6,3,2}(6) &= \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 5 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 3 & 1 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(3,2)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},
\end{aligned} \tag{5.5}$$

and $\mathsf{G}_{6,i,k} = \pi_{\mathrm{GL}_2}^{-1}(\mathsf{G}_{6,i,k}(6))$. In the fibered product involving $\psi^{(1,1)} = (\psi_2^{(1,1)}, \psi_3^{(1,1)})$ on the right-hand side of $\mathsf{G}_{6,1,1}(6)$ above, the common quotient Γ is D_3, the dihedral group of order 6, the map $\psi_2^{(1,1)}$ is any isomorphism $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{D}_3$, and the map $\psi_3^{(1,1)} : \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{D}_3$ is a surjective homomorphism, whose kernel is

$$\ker \psi_3^{(1,1)} = \left\langle \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})' \subseteq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}).$$

In the fibered products involving $\psi^{(2,1)}$, $\psi^{(3,1)}$ and $\psi^{(3,2)}$, the underlying homomorphisms are as follows: $\psi_2^{(2,1)} = \psi_2^{(3,1)} = \psi_2^{(3,2)} = \varepsilon$, where ε is defined by (Equation 4.28), and $\psi_3^{(2,1)}$, $\psi_3^{(3,1)}$, and $\psi_3^{(3,2)}$ are defined by

$$\psi_3^{(2,1)} : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_3^{(2,1)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{ad}{3} \right),$$

$$\psi_3^{(3,1)} : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_3^{(3,1)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{d}{3} \right),$$

$$\psi_3^{(3,2)} : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_3^{(3,2)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{a}{3} \right).$$

Note that $-I \in G_{6,1,1}$ and $-I \in G_{6,2,1}$, but $-I \notin G_{6,3,k}$ for each $k \in \{1,2\}$. We have

$$\tilde{G}_{6,3,k}(6) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \qquad (k \in \{1,2\}). \tag{5.6}$$

Let us set $\tilde{G}_{6,i} := \tilde{G}_{6,i,k}$ and note that $G_{6,i,1} = \tilde{G}_{6,i}$ for $i \in \{1,2\}$. Also note that $\mathrm{level}_{\mathrm{GL}_2}(\tilde{G}_{6,3}) = 3$. The group $G_{6,1,1}$ is studied in (1) (see also (15) and (20)); for any elliptic curve E over $\mathbb{Q}$ we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subsetneq} G_{6,1,1} \iff \begin{array}{l} [\mathbb{Q}(E[2]) : \mathbb{Q}] = 6 \text{ and } \mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3]), \text{ or} \\ \mathbb{Q}(E[2]) = \mathbb{Q}(\mu_3) \text{ and } \rho_{E,3}(G_{\mathbb{Q}}) \dot{\subsetneq} \mathcal{N}_{\mathrm{ns}}(3), \end{array}$$

where $\mathcal{N}_{ns}(3)$ denotes the normalizer in $GL_2(\mathbb{Z}/3\mathbb{Z})$ of a non-split Cartan subgroup. Define $j_{6,1}(t) \in \mathbb{Q}(t)$ and the elliptic curve $\mathcal{E}_{6,1,1}$ over $\mathbb{Q}(t, D)$ by

$$\begin{aligned} j_{6,1}(t) :=& 2^{10}3^3t^3(1-4t^3), \\ \mathcal{E}_{6,1,1} : \ Dy^2 =& x^3 + \frac{108j_{6,1}(t)}{1728 - j_{6,1}(t)}x + \frac{432j_{6,1}(t)}{1728 - j_{6,1}(t)}. \end{aligned}$$

As detailed in (1), for any elliptic curve E over $\mathbb{Q}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{6,1,1} \iff \exists t_0, D_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{6,1,1}(t_0, D_0).$$

Regarding the group $G_{6,2,1} = \tilde{G}_{6,2}$: by (Equation 5.5), Corollary 4.2.6 and Lemma 4.2.9, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{6,2,1} \iff \mathbb{Q}\left(\sqrt{\Delta_E}\right) = \mathbb{Q}(\mu_3) \text{ and } \rho_{E,3}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}. \tag{5.7}$$

Recall $j_{3,1}(t) \in \mathbb{Q}(t)$, defined by $j_{3,1}(t) := 27\frac{(t+1)(t+9)^3}{t^3}$ and the coefficients $a_{4;3,1}(t)$ and $a_{6;3,1}(t)$ defined by (Equation 1.9); consider the elliptic curve $\mathcal{E}_{3,1}$ over $\mathbb{Q}(t, D)$ defined by

$$\mathcal{E}_{3,1} : \ y^2 = x^3 + D^2a_{4;3,1}(t)x + D^3a_{6;3,1}(t).$$

The discriminant $\Delta_{\mathcal{E}_{3,1}}$ of $\mathcal{E}_{3,1}$ satisfies

$$\Delta_{\mathcal{E}_{3,1}} = 2^{18}3^9\frac{D^6t^3(t+1)^2(t+9)^6}{(t^2-18t-27)^6}. \tag{5.8}$$

In particular, $\mathbb{Q}\left(\sqrt{\Delta_{\mathcal{E}_{3,1}}}\right) = \mathbb{Q}(\sqrt{3t})$, so by (Equation 5.7), we see that $\rho_{\mathcal{E}_{3,1}(t_0,D_0)}(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{6,2} = G_{6,2,1}$ if and only if $t_0 \in -(\mathbb{Q}^\times)^2$. We therefore set

$$j_{6,2}(t) := j_{3,1}(-t^2), \qquad a_{4;6,2}(t) := a_{4;3,1}(-t^2), \quad a_{6;6,2}(t) := a_{4;3,1}(-t^2)$$

and define the elliptic curve $\mathcal{E}_{6,2,1}$ over $\mathbb{Q}(t, D)$ by

$$\mathcal{E}_{6,2,1} : \; Dy^2 = x^3 + a_{4;6,2}(t)x + a_{6;6,2}(t).$$

For any E over $\mathbb{Q}$, we then have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{6,2,1} \iff \exists t_0, D_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{6,2,1}(t_0, D_0).$$

Finally, we turn to the groups $G_{6,3,1}$ and $G_{6,3,2}$. By (Equation 5.6) and (Equation 5.2), for any E over $\mathbb{Q}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{6,3} \iff \exists t_0, D_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{3,1}(t_0, D_0).$$

On the other hand, (Equation 5.5), Corollary 4.2.6 and Lemma 4.2.9 imply that

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{6,3,k} \iff \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{6,3} \text{ and } \mathbb{Q}\left(\sqrt{\Delta_E}\right) = \mathbb{Q}(E[3])^{\ker \psi_3^{(1,k)}} \quad (k \in \{1, 2\}).$$

Thus, by Lemma 4.2.10 together with (Equation 5.8), we are led to the twist parameters

$$d_{6,3,1}(t) := \frac{2t(t+1)(t+9)}{t^2-18t-27}, \qquad d_{6,3,2}(t) := -\frac{6t(t+1)(t+9)}{t^2-18t-27}.$$

We furthermore set

$$a_{4;6,3}(t) := a_{4;3,1}(t), \quad a_{6;6,3}(t) := a_{6;3,1}(t)$$

and define the elliptic curves $\mathcal{E}_{6,3,k}$ over $\mathbb{Q}(t)$ by

$$\mathcal{E}_{6,3,k}: \; d_{6,3,k}(t)y^2 = x^3 + a_{4;6,3}(t)x + a_{6;6,3}(t).$$

Our discussion demonstrates that, for any elliptic curve E over $\mathbb{Q}$ and for each $k \in \{1,2\}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{6,3,k} \iff \exists t_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{6,3,k}(t_0).$$

5.1.6 The level $m = 7$.

We have $\mathfrak{G}_{\mathrm{MT}}^{\max}(0,7) = \{G_{7,1,1}, G_{7,1,2}, G_{7,2,1}, G_{7,2,2}, G_{7,3,1}, G_{7,3,2}\}$, where the groups $G_{7,i,k}(7) \subseteq \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ are given by

$$G_{7,1,1}(7) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{7,1,2}(7) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & a^2 \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\},$$

$$G_{7,2,1}(7) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \right\},$$

$$G_{7,2,2}(7) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} a^2 & * \\ 0 & \pm 1 \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\},$$

$$G_{7,3,1}(7) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} \pm a^2 & * \\ 0 & a^2 \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\},$$

$$G_{7,3,2}(7) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} a^2 & * \\ 0 & \pm a^2 \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\}$$

and $G_{7,i,k} = \pi_{GL_2}^{-1}(G_{7,i,k}(7))$ for each $i \in \{1,2,3\}$ and $k \in \{1,2\}$. Note that $-I \notin G_{7,i,k}$, for each i,k. We have

$$\begin{aligned}
\tilde{G}_{7,1}(7) &:= \tilde{G}_{7,1,1}(7) = \tilde{G}_{7,1,2}(7) = \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\}, \\
\tilde{G}_{7,2}(7) &:= \tilde{G}_{7,2,1}(7) = \tilde{G}_{7,2,2}(7) = \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\}, \\
\tilde{G}_{7,3}(7) &:= \tilde{G}_{7,3,1}(7) = \tilde{G}_{7,3,2}(7) = \left\{ \begin{pmatrix} a & * \\ 0 & \pm a \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\}.
\end{aligned} \tag{5.9}$$

Define the functions $j_{7,1}(t), j_{7,2}(t), j_{7,3}(t) \in \mathbb{Q}(t)$ by

$$\begin{aligned}
j_{7,1}(t) &:= \frac{(t^2-t+1)^3(t^6-11t^5+30t^4-15t^3-10t^2+5t+1)^3}{t^7(t-1)^7(t^3-8t^2+5t+1)}, \\
j_{7,2}(t) &:= \frac{(t^2-t+1)^3(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)^3}{t(t-1)(t^3-8t^2+5t+1)^7}, \\
j_{7,3}(t) &:= -\frac{(t^2-3t-3)^3(t^2-t+1)^3(3t^2-9t+5)^3(5t^2-t-1)^3}{(t^3-2t^2-t+1)(t^3-t^2-2t+1)^7}.
\end{aligned} \tag{5.10}$$

As detailed in (30), for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, one has

$$\begin{aligned}
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{7,1} &\iff \exists t \in \mathbb{Q} \text{ for which } j_E = j_{7,1}(t), \\
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{7,2} &\iff \exists t \in \mathbb{Q} \text{ for which } j_E = j_{7,2}(t), \\
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{7,3} &\iff \exists t \in \mathbb{Q} \text{ for which } j_E = j_{7,3}(t).
\end{aligned} \tag{5.11}$$

We define the coefficients $a_{4;7,i}(t)$, and $a_{6;7,i}(t)$ for each $i \in \{1,2,3\}$ by (Equation 1.9), the twist parameters $d_{7,i,k}(t) \in \mathbb{Q}(t)$ for each $i \in \{1,2,3\}$ and $k \in \{1,2\}$ by

$$d_{7,1,1} := -\frac{t^{12} - 18t^{11} + 117t^{10} - 354t^9 + 570t^8 - 486t^7 + 273t^6}{2(t^2-t+1)(t^6-11t^5+30t^4-15t^3-10t^2+5t+1)} +$$

$$\frac{-222t^5 + 174t^4 - 46t^3 - 15t^2 + 6t + 1}{2(t^2-t+1)(t^6-11t^5+30t^4-15t^3-10t^2+5t+1)}$$

$$d_{7,2,1} := -\frac{\left(\begin{array}{c} t^{12} - 522t^{11} - 8955t^{10} + 37950t^9 - 70998t^8 + 131562t^7 - 253239t^6 + \\ 316290t^5 - 218058t^4 + 80090t^3 - 14631t^2 + 510t + 1 \end{array}\right)}{2(t^2-t+1)(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)}$$

$$d_{7,3,1} := \frac{7(t^4-6t^3+17t^2-24t+9)(3t^4-4t^3-5t^2-2t-1)(9t^4-12t^3-t^2+8t-3)}{2(t^2-3t-3)(t^2-t+1)(3t^2-9t+5)(5t^2-t-1)}$$

and $d_{7,i,2} := -7d_{7,i,1}$ for $i \in \{1,2,3\}$; define the elliptic curves $\mathcal{E}_{7,i,k}$ over $\mathbb{Q}(t)$ by

$$\mathcal{E}_{7,i,k} : \; d_{7,i,k}(t)y^2 = x^3 + a_{4;7,i}(t)x + a_{6;7,i}(t) \qquad (i \in \{1,2,3\},\, k \in \{1,2\})\,.$$

As may be found in (30), for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, and for each $i \in \{1,2,3\}$ and $k \in \{1,2\}$, one has

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{7,i,k} \iff \exists t_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{7,i,k}(t_0)\,.$$

5.1.7 The level $m = 8$.

We have $\mathfrak{G}_{\mathrm{MT}}^{\max}(0,8) = \{G_{8,1,1}, G_{8,2,1}\}$, where $G_{8,1,1}(8), G_{8,2,1}(8) \subseteq \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ are given by

$$G_{8,1,1}(8) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 5 & 5 \\ 5 & 2 \end{pmatrix} \right\rangle,$$

$$G_{8,2,1}(8) = \left\langle \begin{pmatrix} 5 & 6 \\ 6 & 7 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 5 & 5 \\ 5 & 2 \end{pmatrix} \right\rangle,$$

and $G_{8,i,1} = \pi_{\mathrm{GL}_2}^{-1}(G_{8,i,1}(8))$ for each $i \in \{1,2\}$. Note that $-I \notin G_{8,i,1}$, and we define groups $\tilde{G}_{8,1} := \tilde{G}_{8,1,1}$ and $\tilde{G}_{8,2} := \tilde{G}_{8,2,1}$.

As a consequence of (25, Lemma 28) and (25, Proposition 3.1), for any group $G \in \mathfrak{G}(0,8)$, we have

$$X_{\tilde{G}}(\mathbb{Q}) \neq \emptyset \iff \exists g \in \tilde{G} \text{ that is } \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})\text{-conjugate to } \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}. \quad (5.12)$$

A computation shows that $\tilde{G}_{8,2}(8)$ fails the condition on the right-hand side of (Equation 5.12), whereas $\tilde{G}_{8,1}(8)$ satisfies it. Thus, $\left|X_{\tilde{G}_{8,2}}(\mathbb{Q})\right| = 0$ and $\left|X_{\tilde{G}_{8,1}}(\mathbb{Q})\right| = \infty$, and we will therefore restrict our consideration to the groups $\tilde{G}_{8,1}$ and $G_{8,1,1}$. The group $\tilde{G}_{8,1}$ has GL_2-level 4, and one may verify by direct computation that

$$\tilde{G}_{8,1}(4) \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon}, \quad \tilde{G}_{8,1}(2) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \quad \text{and}$$

$$\ker\left(\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})\right) \cap \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})' \cap \tilde{G}_{8,1}(4) = \{I\},$$

where the group $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon}$ is as in (Equation 4.32). Furthermore, $\tilde{G}_{8,1}(4)$ is the unique subgroup (up to $\doteq$) of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ satisfying these three conditions. By the Galois correspondence and Lemma 4.2.12, it follows that, for any elliptic curve E over $\mathbb{Q}$, we have

$$\begin{aligned} \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{8,1} \quad &\iff \quad \rho_{E,4}(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{8,1}(4) \\ &\iff \quad \begin{aligned} &\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(i),\ [\mathbb{Q}(E[2]) : \mathbb{Q}] = 6, \\ &\text{and } \mathbb{Q}(E[4]) = \mathbb{Q}(E[2], \Delta_E^{1/4}). \end{aligned} \end{aligned} \tag{5.13}$$

Define the rational functions $g_{8,1}(t), f_{8,1}(t)$ and $j_{8,1}(t) \in \mathbb{Q}(t)$ by

$$g_{8,1}(t) := -\frac{t^2+2t-2}{t}, \qquad f_{8,1}(t) := 4t^3(8-t), \qquad j_{8,1}(t) := f_{8,1}(g_{8,1}(t)).$$

The group $\tilde{G}_{8,1}$ appears under the label $4D^0$-4a in (25), wherein it is shown that, for any elliptic curve E over $\mathbb{Q}$ of j-invariant j_E, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{8,1} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{8,1}(t_0).$$

The group $G_{8,1,1}$ entails an additional vertical entanglement. Specifically, we have

$$G_{8,1,1} \cap \pi_{\mathrm{GL}_2}\left(\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})'\right) = G_{8,1,1} \cap \pi_{\mathrm{GL}_2}\left(\mathrm{SL}_2(\mathbb{Z}/8\mathbb{Z})\right),$$

and $G_{8,1,1}$ is the unique maximal subgroup of $\tilde{G}_{8,1}$ (with respect to $\dot{\subseteq}$) that satisfies this. It follows that, for any elliptic curve E over $\mathbb{Q}$,

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{8,1,1} \iff \begin{array}{l} \mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(i),\ \mathbb{Q}(E[4]) = \mathbb{Q}(E[2], \Delta_E^{1/4}), \\ [\mathbb{Q}(E[2]) : \mathbb{Q}] = 6 \text{ and } \mathbb{Q}(i, \Delta_E^{1/4}) = \mathbb{Q}(\mu_8). \end{array} \tag{5.14}$$

We define the coefficients $a_{4;8,1}(t)$ and $a_{6;8,1}(t)$ by (Equation 1.9) and consider the elliptic curve $\mathcal{E}_{8,1}$ over $\mathbb{Q}(t, D)$ defined by

$$\mathcal{E}_{8,1} : y^2 = x^3 + D^2 a_{4;8,1}(t)x + D^3 a_{6;8,1}(t).$$

By (Equation 5.13), for any $t_0, D_0 \in \mathbb{Q}$ for which $\mathcal{E}_{8,1}(t_0, D_0)$ is an elliptic curve, we have $\mathbb{Q}\left(\sqrt{\Delta_{\mathcal{E}_{8,1}(t_0,D_0)}}\right) = \mathbb{Q}(i)$ and $\mathbb{Q}(\mathcal{E}_{8,1}(t_0, D_0)[4]) = \mathbb{Q}\left(\mathcal{E}_{8,1}(t_0, D_0)[2], \Delta^{1/4}_{\mathcal{E}_{8,1}(t_0,D_0)}\right)$. The discriminant $\Delta_{\mathcal{E}_{8,1}}$ satisfies

$$\Delta_{\mathcal{E}_{8,1}} = -2^{16}3^{12}\frac{D^6t^4(t^2+2t-2)^6(t^2+10t-2)^2}{(t^2+2)^6(t^2+8t-2)^6},$$

and thus, using $\zeta_8 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$, we find that

$$\mathbb{Q}\left(i, \Delta^{1/4}_{\mathcal{E}_{8,1}(t_0,D_0)}\right) = \mathbb{Q}\left(i, \sqrt{\frac{2D(t^2+2t-2)(t^2+10t-2)}{(t^2+2)(t^2+8t-2)}}\right).$$

Thus, it follows from (Equation 5.13) and (Equation 5.14) that

$$\rho_{\mathcal{E}_{8,1}(t_0,D_0)}(G_{\mathbb{Q}}) \dot{\subseteq} G_{8,1,1} \iff D = \pm\frac{(t^2+2t-2)(t^2+10t-2)}{(t^2+2)(t^2+8t-2)}.$$

Thus, we are led to the pair of twist parameters $d^{\pm}_{8,1,1}(t) := \pm\frac{(t^2+2t-2)(t^2+10t-2)}{(t^2+2)(t^2+8t-2)}$. Finally, noting that $j_{8,1}(-2/t) = j_{8,1}(t)$ and $d^{\pm}_{8,1,1}(-2/t) = d^{\mp}_{8,1,1}(t)$, we are led to the single twist parameter

$$d_{8,1,1}(t) := \frac{(t^2+2t-2)(t^2+10t-2)}{(t^2+2)(t^2+8t-2)},$$

and, defining the elliptic curve $\mathcal{E}_{8,1,1}$ over $\mathbb{Q}(t)$ by

$$\mathcal{E}_{8,1,1} : \ d_{8,1,1}(t)y^2 = x^3 + a_{4;8,1}(t)x + a_{6;8,1}(t),$$

we have that, for each elliptic curve E over $\mathbb{Q}$ with j-invariant j_E,

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{8,1,1} \iff \exists t_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{8,1,1}(t_0).$$

5.1.8 The level $\mathfrak{m} = 9$.

We have $\mathfrak{G}_{MT}^{max}(0,9) = \{G_{9,1,1}, G_{9,2,1}, G_{9,3,1}, G_{9,4,1}, G_{9,5,1}\}$, where $G_{9,i,1}(9) \subseteq GL_2(\mathbb{Z}/9\mathbb{Z})$ are given by

$$G_{9,1,1}(9) = \left\langle \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 0 & 5 \end{pmatrix} \right\rangle,$$

$$G_{9,2,1}(9) = \left\langle \begin{pmatrix} 2 & 1 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 3 & 5 \end{pmatrix} \right\rangle,$$

$$G_{9,3,1}(9) = \left\langle \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 2 \\ 3 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 5 \end{pmatrix} \right\rangle,$$

$$G_{9,4,1}(9) = \left\langle \begin{pmatrix} 0 & 2 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 5 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 5 \\ 0 & 5 \end{pmatrix} \right\rangle,$$

$$G_{9,5,1}(9) = \left\langle \begin{pmatrix} 5 & 7 \\ 2 & 8 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \right\rangle$$

and $G_{9,i,1} = \pi_{GL_2}^{-1}(G_{9,i,1}(9))$ for each $i \in \{1,2,3,4,5\}$. We have that $-I \in G_{9,i,1}$ for each $i \in \{1,2,3,4,5\}$; as usual we define $\tilde{G}_{9,i} := \tilde{G}_{9,i,1}$, which equals $G_{9,i,1}$ in this case. The group $\tilde{G}_{9,5}(9)$ fails the right-hand condition in (Equation 5.12), whereas, for $i \in \{1,2,3,4\}$, the groups $\tilde{G}_{9,i}(9)$ satisfy it. Since $X_{\tilde{G}_{9,5}}$ is a thus conic with no rational points, we will restrict our

consideration to the first four groups in our list, which appear in (25) under the labels $9H^0$-9c, $9I^0$-9b, $9J^0$-9c, and $9F^0$-9a, respectively. We define the functions

$$\begin{array}{lllllll} f_{9,1}(t) & := & \frac{(t+3)^3(t+27)}{t} & g_{9,1}(t) & := & \frac{729}{t^3-27} & h_{9,1}(t) := \frac{-6(t^3-9t)}{t^3+9t^2-9t-9} \\ & & & g_{9,2}(t) & := & t(t^2+9t+27) & h_{9,2}(t) := \frac{-3(t^3+9t^2-9t-9)}{t^3+3t^2-9t-3} \\ & & & g_{9,3}(t) & := & t^3 & h_{9,3}(t) := \frac{3(t^3+3t^2-9t-3)}{t^3-3t^2-9t+3} \end{array}$$

and the j-invariants

$$j_{9,1}(t) := f_{9,1}(g_{9,1}(h_{9,1}(t))), \quad j_{9,2}(t) := f_{9,1}(g_{9,2}(h_{9,2}(t))), \quad j_{9,3}(t) := f_{9,1}(g_{9,3}(h_{9,3}(t))),$$

$$j_{9,4}(t) := \frac{3^7(t^2-1)^3(t^6+3t^5+6t^4+t^3-3t^2+12t+16)^3(2t^3+3t^2-3t-5)}{(t^3-3t-1)^9}.$$

As demonstrated in (25), for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E and for each $i \in \{1,2,3,4\}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{9,i} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{9,i}(t_0).$$

We define the coefficients $a_{4;9,i}(t)$ and $a_{6;9,i}(t)$ by (Equation 1.9) and consider the elliptic curve $\mathcal{E}_{9,i}$ over $\mathbb{Q}(t, D)$ defined by

$$\mathcal{E}_{9,i} : Dy^2 = x^3 + a_{4;9,i}(t)x + a_{6;9,i}(t).$$

Since $G_{9,i,1} = \tilde{G}_{9,1}$ for each i, it follows immediately that, for each elliptic curve E over $\mathbb{Q}$ with j-invariant j_E and for each $i \in \{1,2,3,4\}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{9,i,1} \iff \exists t_0, D_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{9,i}(t_0, D_0).$$

5.1.9 The level $m = 10$.

We have $\mathfrak{G}_{MT}^{\max}(0,10) = \{G_{10,1,1}, G_{10,1,2}, G_{10,2,1}, G_{10,2,2}, G_{10,3,1}\}$, where $G_{10,i,k}(10) \subseteq GL_2(\mathbb{Z}/10\mathbb{Z})$ are given by

$$\begin{aligned}
G_{10,1,1}(10) &= \left\langle \begin{pmatrix} 9 & 9 \\ 0 & 9 \end{pmatrix}, \begin{pmatrix} 6 & 5 \\ 5 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} \right\rangle \simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(1,1)}} \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\}, \\
G_{10,1,2}(10) &= \left\langle \begin{pmatrix} 9 & 9 \\ 0 & 9 \end{pmatrix}, \begin{pmatrix} 6 & 5 \\ 5 & 1 \end{pmatrix}, \begin{pmatrix} 9 & 0 \\ 0 & 3 \end{pmatrix} \right\rangle \simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(1,2)}} \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\}, \\
G_{10,2,1}(10) &= \left\langle \begin{pmatrix} 9 & 9 \\ 0 & 9 \end{pmatrix}, \begin{pmatrix} 6 & 5 \\ 5 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix} \right\rangle \simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(2,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\}, \qquad (5.15) \\
G_{10,2,2}(10) &= \left\langle \begin{pmatrix} 9 & 9 \\ 0 & 9 \end{pmatrix}, \begin{pmatrix} 6 & 5 \\ 5 & 1 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(2,2)}} \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\}, \\
G_{10,3,1}(10) &= \left\langle \begin{pmatrix} 4 & 9 \\ 9 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 9 & 8 \end{pmatrix}, \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(3,1)}} G_{S_4}(5)
\end{aligned}$$

and $G_{10,i,k} = \pi_{GL_2}^{-1}(G_{10,i,k}(10))$. In the fibered product on the right-hand side of $G_{10,3,1}(10)$, the group $G_{S_4}(5)$ denotes the unique (up to conjugation in $GL_2(\mathbb{Z}/5\mathbb{Z})$) subgroup of $GL_2(\mathbb{Z}/5\mathbb{Z})$ of

index 5 (its image in $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ is isomorphic to S_4, the symmetric group on 4 symbols), and in that fibered product, the underlying maps $\psi_5^{(3,1)} = (\psi_2^{(3,1)}, \psi_5^{(3,1)})$, surject onto a common quotient isomorphic to D_3, the dihedral group of order 6. The map $\psi_2^{(3,1)}$ is any isomorphism $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq D_3$, and the map $\psi_5^{(3,1)} : G_{S_4}(5) \longrightarrow D_3$ is the restriction of the projection map $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}) \longrightarrow \mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$, followed by any surjection $S_4 \longrightarrow D_3$; its kernel is $\mathcal{N}_s(5)$, the normalizer in $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ of a split Cartan subgroup. In the fibered products involving $\psi^{(1,1)}$, $\psi^{(1,2)}$, $\psi^{(2,1)}$ and $\psi^{(2,2)}$, the underlying homomorphisms are as follows: $\psi_2^{(1,1)} = \psi_2^{(1,2)} = \psi_2^{(2,1)} = \psi_2^{(2,2)} = \varepsilon$ as in (Equation 4.28), whereas $\psi_5^{(1,1)}$, $\psi_5^{(1,2)}$, $\psi_5^{(2,1)}$ and $\psi_5^{(2,2)}$ are defined by

$$\psi_5^{(1,1)} : \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_5^{(1,1)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := a \in \{\pm 1\},$$

$$\psi_5^{(1,2)} : \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_5^{(1,2)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{d}{5}\right) a \in \{\pm 1\},$$

$$\psi_5^{(2,1)} : \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_5^{(2,1)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{a}{5}\right) d \in \{\pm 1\},$$

$$\psi_5^{(2,2)} : \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_5^{(2,2)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := d \in \{\pm 1\}.$$

We note that $-I \in G_{10,3,1}$ and $-I \notin G_{10,i,k}$, for each $i,k \in \{1,2\}$; we have

$$\begin{aligned} \tilde{G}_{10,1,k}(10) &\simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\}, \\ \tilde{G}_{10,2,k}(10) &\simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\} \qquad (k \in \{1,2\}). \end{aligned} \tag{5.16}$$

Let us set $\tilde{G}_{10,i} := \tilde{G}_{10,i,k}$ and note that $G_{10,3,1} = \tilde{G}_{10,3}$. Also note that $\mathrm{level}_{\mathrm{GL}_2}(\tilde{G}_{10,i}) = 5$ for $i \in \{1,2\}$. The group $\tilde{G}_{10,3}$ is studied in (15); for any elliptic curve E over $\mathbb{Q}$ we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{10,3} \iff \begin{array}{c} \mathbb{Q}(\sqrt{5}) \subsetneq \mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[5]) \text{ and } \rho_{E,5}(G_{\mathbb{Q}}) = G_{S_4}(5), \text{ or} \\ \mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{5}) \text{ and } \rho_{E,5}(G_{\mathbb{Q}}) \subsetneq G_{S_4}(5). \end{array}$$

Define $f_{10,3}(t), g_{10,3}(t) \in \mathbb{Q}(t)$ by

$$f_{10,3}(t) := t^3(t^2+5t+40), \qquad g_{10,3}(t) := \frac{3t^6+12t^5+80t^4+50t^3-20t^2-8t+8}{(t-1)^2(t^2+3t+1)^2}$$

and the j-invariant $j_{10,3}(t) \in \mathbb{Q}(t)$ and elliptic curve $\mathcal{E}_{10,3,1}$ over $\mathbb{Q}(t,D)$ by

$$\begin{aligned} j_{10,3}(t) :=& f_{10,3}\left(g_{10,3}(t)\right), \\ \mathcal{E}_{10,3,1}: Dy^2 =& x^3 + \frac{108 j_{10,3}(t)}{1728 - j_{10,3}(t)} x + \frac{432 j_{10,3}(t)}{1728 - j_{10,3}(t)}. \end{aligned}$$

As proved in (15), for any elliptic curve E over $\mathbb{Q}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{10,3,1} \iff \exists t_0, D_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{10,3,1}(t_0, D_0).$$

Regarding the groups $G_{10,i,k}$ for $i, k \in \{1, 2\}$, we first consider the groups $\tilde{G}_{10,i}$. Given (Equation 5.16), we may apply results in (30), which exhibits the j-invariants

$$j_{5,1}(t) := \frac{(t^4 - 12t^3 + 14t^2 + 12t + 1)^3}{t^5(t^2 - 11t - 1)}, \qquad j_{5,2}(t) := \frac{(t^4 + 228t^3 + 494t^2 - 228t + 1)^3}{t(t^2 - 11t - 1)^5}$$

and shows that, for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{10,1} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{5,1}(t_0),$$

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{10,2} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{5,2}(t_0).$$

If E is an elliptic curve satisfying

$$\rho_{E,5}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$$

then there is a $G_{\mathbb{Q}}$-stable cyclic subgroup $\langle P\rangle \subseteq E[5]$; given any such Galois-stable cyclic subgroup $\langle P\rangle$, we let $E'_{\langle P\rangle} := E/\langle P\rangle$ denote the associated isogenous curve (which is necessarily defined over $\mathbb{Q}$). By (Equation 5.16), we have that

$$\begin{aligned}
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{10,1} &\iff \exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P\rangle \subseteq E[5] && \text{with} \quad [\mathbb{Q}(P):\mathbb{Q}] \leq 2, \\
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{10,2} &\iff \begin{array}{l}\exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P\rangle \subseteq E[5] \text{ and} \\ \exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P'\rangle \subseteq E'_{\langle P\rangle}[5]\end{array} && \text{with} \quad [\mathbb{Q}(P'):\mathbb{Q}] \leq 2.
\end{aligned} \tag{5.17}$$

Furthermore, by (Equation 5.15), Corollary 4.2.6 and Lemma 4.2.9, we have

$$\begin{aligned}
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{10,1,1} &\iff \exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P\rangle \subseteq E[5] && \text{with} \quad \mathbb{Q}(P) = \mathbb{Q}(\sqrt{\Delta_E}), \\
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{10,1,2} &\iff \exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P\rangle \subseteq E[5] && \text{with} \quad \mathbb{Q}(P) = \mathbb{Q}(\sqrt{5\Delta_E}), \\
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{10,2,1} &\iff \begin{array}{l}\exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P\rangle \subseteq E[5] \text{ and} \\ \exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P'\rangle \subseteq E'_{\langle P\rangle}[5]\end{array} && \text{with} \quad \mathbb{Q}(P') = \mathbb{Q}(\sqrt{5\Delta_E}), \\
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{10,2,2} &\iff \begin{array}{l}\exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P\rangle \subseteq E[5] \text{ and} \\ \exists \text{ a } G_{\mathbb{Q}}\text{-stable } \langle P'\rangle \subseteq E'_{\langle P\rangle}[5]\end{array} && \text{with} \quad \mathbb{Q}(P') = \mathbb{Q}(\sqrt{\Delta_E}).
\end{aligned} \tag{5.18}$$

We define the coefficients $a_{4;10,i}(t)$ $a_{6;10,i}(t)$ defined by (Equation 1.9); consider the elliptic curves $\mathcal{E}_{10,i}$ over $\mathbb{Q}(t, D)$ defined by

$$\begin{aligned}
\mathcal{E}_{10,1} &: y^2 = x^3 + D^2 a_{4;10,1}(t)x + D^3 a_{6;10,1}(t), \\
\mathcal{E}_{10,2} &: y^2 = x^3 + D^2 a_{4;10,2}(t)x + D^3 a_{6;10,2}(t).
\end{aligned}$$

We have

$$\Delta_{\mathcal{E}_{10,1}} = \frac{2^{18}3^{12}D^6t^5(t^2-11t-1)(t^4-12t^3+14t^2+12t+1)^6}{(t^2+1)^6(t^4-18t^3+74t^2+18t+1)^6},$$
$$\Delta_{\mathcal{E}_{10,2}} = \frac{2^{18}3^{12}D^6t(t^2-11t-1)^5(t^4+228t^3+494t^2-228t+1)^6}{(t^2+1)^6(t^4-522t^3-10006t^2+522t+1)^6},$$

and thus

$$\mathbb{Q}\left(\sqrt{\Delta_{\mathcal{E}_{10,1}}}\right) = \mathbb{Q}\left(\sqrt{\Delta_{\mathcal{E}_{10,2}}}\right) = \mathbb{Q}\left(\sqrt{t(t^2-11t-1)}\right).$$

By Lemma 4.2.14, we are led to the twist parameters

$$d_{10,1,1}(t) := \frac{-2t(t^2-11t-1)(t^4-12t^3+14t^2+12t+1)}{(t^2+1)(t^4-18t^3+74t^2+18t+1)}, \qquad d_{10,1,2}(t) := 5d_{10,1,1}(t),$$
$$d_{10,2,1}(t) := \frac{-10t(t^2-11t-1)(t^4+228t^3+494t^2-228t+1)}{(t^2+1)(t^4-522t^3-10006t^2+522t+1)}, \qquad d_{10,2,2}(t) := 5d_{10,2,1}(t),$$

and to the elliptic curves $\mathcal{E}_{10,i,k}$ over $\mathbb{Q}(t)$, defined by

$$\mathcal{E}_{10,i,k}: \; d_{10,i,k}(t)y^2 = x^3 + a_{4;10,i}(t)x + a_{6;10,i}(t) \qquad (i,k \in \{1,2\}).$$

By (Equation 5.18) and Lemma 4.2.14, for each elliptic curve E over $\mathbb{Q}$ and for each $i,k \in \{1,2\}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{10,i,k} \iff \exists t_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{10,i,k}(t_0).$$

5.1.10 The level $\mathfrak{m} = 12$.

We have $\mathfrak{G}_{\mathrm{MT}}^{\max}(0,12) = \{\mathsf{G}_{12,1,1}, \mathsf{G}_{12,2,1}, \mathsf{G}_{12,3,1}, \mathsf{G}_{12,4,1}, \mathsf{G}_{12,4,2}\}$, where $\mathsf{G}_{12,i,k}(12) \subseteq \mathrm{GL}_2(\mathbb{Z}/12\mathbb{Z})$ are given by

$$
\begin{aligned}
\mathsf{G}_{12,1,1}(12) &= \left\langle \begin{pmatrix} 7 & 7 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 7 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 9 \\ 9 & 8 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times_{\psi^{(1,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\
\mathsf{G}_{12,2,1}(12) &= \left\langle \begin{pmatrix} 5 & 8 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 11 \\ 0 & 11 \end{pmatrix}, \begin{pmatrix} 7 & 6 \\ 3 & 7 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times_{\psi^{(2,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\
\mathsf{G}_{12,3,1}(12) &= \left\langle \begin{pmatrix} 5 & 11 \\ 0 & 11 \end{pmatrix}, \begin{pmatrix} 5 & 11 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 9 & 11 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times_{\psi^{(3,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\
\mathsf{G}_{12,4,1}(12) &= \left\langle \begin{pmatrix} 5 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 7 & 6 \\ 0 & 11 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \right\rangle \simeq \pi_{\mathrm{GL}_2}^{-1} \left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \times_{\psi^{(4,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\
\mathsf{G}_{12,4,2}(12) &= \left\langle \begin{pmatrix} 5 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 11 & 6 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \right\rangle \simeq \pi_{\mathrm{GL}_2}^{-1} \left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \times_{\psi^{(4,2)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}
\end{aligned}
\tag{5.19}
$$

and $G_{12,i,k} = \pi_{GL_2}^{-1}(G_{12,i,k}(12))$; as usual, the representations of the groups on the right-hand are to be understood via the Chinese Remainder Theorem. In the fibered products $\psi^{(i,k)}$, the underlying homomorphisms are as follows: the maps $\psi_4^{(i,k)}$, are defined by

$$\psi_4^{(i,1)} : GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \longrightarrow \{\pm 1\}, \qquad \ker \psi_4^{(i,1)} = \left\langle \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \right\rangle \quad (i \in \{1,2,3\}),$$

$$\psi_4^{(4,k)} : \pi_{GL_2}^{-1}\left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \to \{\pm 1\}, \quad \psi_4^{(4,k)}(g) = \det g \qquad (k \in \{1,2\}), \tag{5.20}$$

and the maps $\psi_3^{(i,k)}$ are defined by

$$\psi_3^{(1,1)} : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_3^{(1,1)}\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{ad}{3} \right),$$

$$\psi_3^{(2,1)} = \psi_3^{(4,2)} : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_3^{(2,1)}\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) = \psi_3^{(4,2)}\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{d}{3} \right),$$

$$\psi_3^{(3,1)} = \psi_3^{(4,1)} : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_3^{(3,1)}\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) = \psi_3^{(4,1)}\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{a}{3} \right).$$

We note that $-I \in G_{12,2,1}, G_{12,3,1}$ and $-I \notin G_{12,1,1}, G_{12,4,k}$, for each $k \in \{1,2\}$. We have

$$\begin{aligned}
\tilde{G}_{12,1}(12) &:= \tilde{G}_{12,1,1}(12) \simeq GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\
\tilde{G}_{12,4}(12) &:= \tilde{G}_{12,4,k}(12) \simeq \pi_{GL_2}^{-1} \left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \quad (k \in \{1,2\}).
\end{aligned} \tag{5.21}$$

As detailed in (25), for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, we have

$$\begin{aligned}
\rho_{E,4}(G_{\mathbb{Q}}) \dot{\subseteq} GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} &\iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = -t_0^2 + 1728, \\
\rho_{E,4}(G_{\mathbb{Q}}) \dot{\subseteq} \pi_{GL_2}^{-1} \left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) &\iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = t_0^2 + 1728, \\
\rho_{E,3}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} &\iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = 27\frac{(t_0+1)(t_0+9)^3}{t_0^3}.
\end{aligned}$$

To obtain models for the modular curves corresponding to the groups in (Equation 5.21), we are led to the equations

$$-t^2 + 1728 = 27\frac{(s+1)(s+9)^3}{s^3}, \qquad t^2 + 1728 = 27\frac{(s+1)(s+9)^3}{s^3},$$

each of which is a singular model of a conic. Resolving the singularities in MAGMA, we are led to the substitutions $s = -\frac{27}{u^2}$, $t = \frac{u^4-18u^2-27}{u}$ for the first equation and $s = \frac{1}{27u^2}$, $t = \frac{1-486u^2-19683u^4}{u}$ for the second, and these lead to the j-invariants

$$j_{12,i}(u) := -\frac{(u^2-27)(u^2-3)^3}{u^2} \quad (i \in \{1,2,3\}), \qquad j_{12,4}(u) := \frac{(27u^2+1)(243u^2+1)^3}{u^2}.$$

(Note that $G_{12,i,1} \subseteq \tilde{G}_{12,1}$ for any $i \in \{1,2,3\}$.). We thus have

$$\rho_{E,12}(G_{\mathbb{Q}}) \dot{\subseteq} \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \iff \exists u_0 \in \mathbb{Q} \text{ with } j_E = j_{12,1}(u_0),$$

$$\rho_{E,12}(G_{\mathbb{Q}}) \dot{\subseteq} \pi_{\mathrm{GL}_2}^{-1}\left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \iff \exists u_0 \in \mathbb{Q} \text{ with } j_E = j_{12,4}(u_0).$$

We define the coefficients $a_{4;12,i}(u), a_{6;12,i}(u) \in \mathbb{Q}(u)$ by

$$a_{4;12,i}(u) := a_{4;3,1}\left(-\frac{27}{u^2}\right), \quad a_{6;12,i} := a_{6;3,1}\left(-\frac{27}{u^2}\right), \qquad (i \in \{1,2,3\}),$$
$$a_{4;12,4}(u) := a_{4;3,1}\left(\frac{1}{27u^2}\right), \quad a_{6;12,4} := a_{6;3,1}\left(\frac{1}{27u^2}\right)$$

and consider the elliptic curves $\mathcal{E}_{12,i}$ over $\mathbb{Q}(u,D)$ defined by

$$\mathcal{E}_{12,i} : Dy^2 = x^3 + a_{4;12,i}(u)x + a_{6;12,i}(u) \qquad (i \in \{1,2,3,4\}).$$

(Note that $\mathcal{E}_{12,1} = \mathcal{E}_{12,2} = \mathcal{E}_{12,3}$.)

Applying Lemma 4.2.13 with $\frac{u^4-18u^2-27}{u}$ substituted for the variable, we find that

$$\mathbb{Q}\left(i, \Delta_{\mathcal{E}_{12,i}}^{1/4}\right) = \mathbb{Q}\left(i, \sqrt{\frac{Du(u^2-27)(u^2-3)}{u^4-18u^2-27}}\right) \qquad (i \in \{1,2,3\}).$$

By (Equation 5.19) and Corollary 4.2.5, we see that, for any specialization $\mathcal{E}_{12,1}(u_0, D_0)$ that is an elliptic curve,

$$\begin{aligned}\rho_{\mathcal{E}_{12,1}(u_0,D_0)}(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,1,1} &\iff \mathbb{Q}\left(\sqrt{\pm\frac{D_0u_0(u_0^2-27)(u_0^2-3)}{u_0^4-18u_0^2-27}}\right) = \mathbb{Q}\left(\sqrt{-3}\right) \\ &\iff D_0 \in \mp\frac{3u_0(u_0^2-27)(u_0^2-3)}{u_0^4-18u_0^2-27}(\mathbb{Q}^\times)^2.\end{aligned}$$

By (Equation 5.19) and (Equation 5.20), and noting that $u \mapsto -\frac{3u(u^2-27)(u^2-3)}{u^4-18u^2-27}$ is an odd function of u, we are led to the twist choice

$$d_{12,1,1}(u) := -\frac{3u(u^2-27)(u^2-3)}{u^4-18u^2-27}$$

and the model $\mathcal{E}_{12,1,1}$ over $\mathbb{Q}(u)$, defined by

$$\mathcal{E}_{12,1,1}: \; d_{12,1,1}(u)y^2 = x^3 + a_{4;12,1}(u)x + a_{6;12,1}(u).$$

Regarding the groups $G_{12,2,1}$ and $G_{12,3,1}$, we apply Lemma 4.2.10 with $-\frac{27}{u^2}$ substituted for the variable, obtaining

$$\mathbb{Q}(t,D)\left(\mathcal{E}_{12,2}[3]\right)^{\ker \psi_3^{(2,1)}} = \mathbb{Q}(t,D)\left(\sqrt{\frac{6D(u^2-27)(u^2-3)}{u^4-18u^2-27}}\right),$$
$$\mathbb{Q}(t,D)\left(\mathcal{E}_{12,3}[3]\right)^{\ker \psi_3^{(3,1)}} = \mathbb{Q}(t,D)\left(\sqrt{-\frac{2D(u^2-27)(u^2-3)}{u^4-18u^2-27}}\right).$$

Noting also that for $i \in \{2,3\}$, the Weierstrass coefficients satisfy $a_{4;12,i}(-u) = a_{4;12,i}(u)$ and $a_{6;12,i}(-u) = a_{6;12,i}(u)$, we are thus led to the models $\mathcal{E}_{12,2,1}$, $\mathcal{E}_{12,3,1}$ over $\mathbb{Q}(v,D)$

$$\mathcal{E}_{12,2,1} : Dy^2 = x^3 + a_{4;12,2}(6v^2)x + a_{6;12,2}(6v^2),$$
$$\mathcal{E}_{12,3,1} : Dy^2 = x^3 + a_{4;12,3}(-2v^2)x + a_{6;12,3}(-2v^2).$$

2
For any elliptic curve E over $\mathbb{Q}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,1,1} \iff \exists u_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{12,1,1}(u_0),$$
$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,2,1} \iff \exists v_0, D_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{12,2,1}(v_0, D_0),$$
$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,3,1} \iff \exists v_0, D_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{12,3,1}(v_0, D_0).$$

We now find models for the remaining two groups $G_{12,4,1}$, $G_{12,4,2}$. Applying Lemma 4.2.10 with $\frac{1}{27u^2}$ substituted for the variable, we find that

$$\mathbb{Q}(t, D)\left(\mathcal{E}_{12,4}[3]\right)^{\ker \psi_3^{(4,1)}} = \mathbb{Q}(t, D)\left(\sqrt{-\frac{6D(27u^2+1)(243u^2+1)}{19683u^4+486u^2-1}}\right),$$
$$\mathbb{Q}(t, D)\left(\mathcal{E}_{12,4}[3]\right)^{\ker \psi_3^{(4,2)}} = \mathbb{Q}(t, D)\left(\sqrt{\frac{2D(27u^2+1)(243u^2+1)}{19683u^4+486u^2-1}}\right).$$

By (Equation 5.19) and (Equation 5.20), we obtain the appropriate twist classes by setting each of these fields equal to $\mathbb{Q}(i)$, which leads to the definitions

$$d_{12,4,1}(u) := \frac{6(27u^2+1)(243u^2+1)}{19683u^4+486u^2-1}, \qquad d_{12,4,2}(u) := -\frac{2(27u^2+1)(243u^2+1)}{19683u^4+486u^2-1}.$$

We define the elliptic curves $\mathcal{E}_{12,4,k}$ over $\mathbb{Q}(u)$ by

$$\mathcal{E}_{12,4,k}: \; d_{12,4,k}(u)y^2 = x^3 + a_{4;12,4}(u)x + a_{6;12,4}(u) \qquad (k \in \{1,2\}).$$

It follows from our discussion that, for any elliptic curve E over $\mathbb{Q}$,

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,4,1} \iff \exists u_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{12,4,1}(u_0),$$
$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{12,4,2} \iff \exists u_0 \in \mathbb{Q} \text{ for which } E \text{ is isomorphic over } \mathbb{Q} \text{ to } \mathcal{E}_{12,4,2}(u_0).$$

5.1.11 The level $m = 14$

We have

$$\mathfrak{G}_{MT}^{max}(0,14) = \mathfrak{G}_{MT,2}^{max}(0,14) \sqcup \mathfrak{G}_{MT,3}^{max}(0,14),$$

with

$$\mathfrak{G}_{MT,2}^{max}(0,14) = \{G_{14,1,1}, G_{14,2,1}, G_{14,2,1}, G_{14,2,2}, G_{14,3,1}, G_{14,3,2}, G_{14,4,1}\},$$
$$\mathfrak{G}_{MT,3}^{max}(0,14) = \{G_{14,5,1}, G_{14,6,1}, G_{14,6,2}, G_{14,7,1}, G_{14,7,2}\},$$

where the groups $G_{14,i,k}(14) \subseteq \mathrm{GL}_2(\mathbb{Z}/14\mathbb{Z})$ for $G_{14,i,k} \in \mathfrak{G}_{MT,2}^{\max}(0,14)$ are given by

$$
\begin{aligned}
G_{14,1,1}(14) &= \left\langle \begin{pmatrix} 9 & 2 \\ 1 & 9 \end{pmatrix}, \begin{pmatrix} 12 & 5 \\ 11 & 6 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(1,1)}} \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\}, \\
G_{12,1,2}(14) &= \left\langle \begin{pmatrix} 13 & 0 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 6 & 1 \\ 9 & 7 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(1,2)}} \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\}, \\
G_{14,2,1}(14) &= \left\langle \begin{pmatrix} 1 & 11 \\ 4 & 7 \end{pmatrix}, \begin{pmatrix} 9 & 4 \\ 13 & 7 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(2,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\}, \\
G_{14,2,2}(14) &= \left\langle \begin{pmatrix} 0 & 9 \\ 9 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 6 \\ 7 & 13 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(2,2)}} \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\}, \\
G_{14,3,1}(14) &= \left\langle \begin{pmatrix} 9 & 4 \\ 3 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 7 \\ 11 & 6 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(3,1)}} \left\{ \begin{pmatrix} a & * \\ 0 & \pm a \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\}, \\
G_{12,3,2}(14) &= \left\langle \begin{pmatrix} 7 & 13 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 12 \\ 3 & 13 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(3,2)}} \left\{ \begin{pmatrix} a & * \\ 0 & \pm a \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\}, \\
G_{14,4,1}(14) &= \left\langle \begin{pmatrix} 9 & 3 \\ 13 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 6 \\ 7 & 3 \end{pmatrix} \right\rangle \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi^{(4,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},
\end{aligned}
\tag{5.22}
$$

the groups $G_{14,i,k}(14) \subseteq GL_2(\mathbb{Z}/14\mathbb{Z})$ for $G_{14,i,k} \in \mathfrak{G}^{\max}_{MT,3}(0,14)$ are given by

$$
\begin{aligned}
G_{14,5,1}(14) &= \left\langle \begin{pmatrix} 3 & 7 \\ 9 & 2 \end{pmatrix}, \begin{pmatrix} 6 & 13 \\ 7 & 11 \end{pmatrix} \right\rangle \simeq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times_{\phi^{(5)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\
G_{14,6,1}(14) &= \left\langle \begin{pmatrix} 5 & 1 \\ 7 & 4 \end{pmatrix}, \begin{pmatrix} 7 & 13 \\ 9 & 10 \end{pmatrix} \right\rangle \simeq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times_{\phi^{(6)}} \left\{ \begin{pmatrix} a^2 & * \\ 0 & * \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\}, \\
G_{14,6,2}(14) &= \left\langle \begin{pmatrix} 9 & 11 \\ 7 & 12 \end{pmatrix}, \begin{pmatrix} 7 & 11 \\ 9 & 12 \end{pmatrix} \right\rangle \simeq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times_{\phi^{(6)}} \left\{ \begin{pmatrix} * & * \\ 0 & d^2 \end{pmatrix} : d \in (\mathbb{Z}/7\mathbb{Z})^\times \right\}, \\
G_{14,7,1}(14) &= \left\langle \begin{pmatrix} 3 & 1 \\ 1 & 10 \end{pmatrix}, \begin{pmatrix} 9 & 7 \\ 11 & 6 \end{pmatrix} \right\rangle \simeq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times_{\phi^{(7)}} \left\{ \begin{pmatrix} a^2 & * \\ 0 & * \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\}, \\
G_{14,7,2}(14) &= \left\langle \begin{pmatrix} 0 & 3 \\ 9 & 13 \end{pmatrix}, \begin{pmatrix} 9 & 11 \\ 13 & 4 \end{pmatrix} \right\rangle \simeq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times_{\phi^{(7)}} \left\{ \begin{pmatrix} * & * \\ 0 & d^2 \end{pmatrix} : d \in (\mathbb{Z}/7\mathbb{Z})^\times \right\},
\end{aligned}
\tag{5.23}
$$

and each $G_{14,i,k} = \pi^{-1}_{GL_2}(G_{14,i,k}(14))$. In all cases, the representations of the groups on the right-hand are to be understood via the Chinese Remainder Theorem as subgroups of $GL_2(\mathbb{Z}/2\mathbb{Z}) \times GL_2(\mathbb{Z}/7\mathbb{Z})$. For each group $G \in \mathfrak{G}^{\max}_{MT,2}(0,14)$, the associated common quotient $\psi_2^{(i,k)}(GL_2(\mathbb{Z}/2\mathbb{Z}))$ is a cyclic group of order 2, whereas for each group $G \in \mathfrak{G}^{\max}_{MT,3}(0,14)$ the associated common quotients $\phi_2^{(i)}\left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle\right)$ is a cyclic group of order 3 (i.e. $\phi_2^{(i)}$ is a group isomorphism).

These homomorphisms are defined as follows: the maps $\psi_2^{(i,k)} : \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \{\pm 1\}$ are all equal to the map ε as in (Equation 4.28), whereas the maps $\psi_7^{(i,k)}$ are given by

$$\begin{aligned}
&\psi_7^{(1,k)} : \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}; \quad \psi_7^{(1,1)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{d}{7} \right), \quad \psi_7^{(1,2)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{a}{7} \right), \\
&\psi_7^{(2,k)} : \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \quad \psi_2^{(2,1)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{d}{7} \right), \quad \psi_2^{(2,2)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{a}{7} \right), \\
&\psi_7^{(3,k)} : \left\{ \begin{pmatrix} a & * \\ 0 & \pm a \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \quad \psi_2^{(3,1)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{d}{7} \right), \quad \psi_2^{(3,2)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{a}{7} \right), \\
&\psi_7^{(4,1)} : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_2^{(4,1)}(g) := \left(\frac{\det g}{7} \right).
\end{aligned} \tag{5.24}$$

For $G \in \mathfrak{G}^{\max}_{MT,3}(0,14)$, the common quotient will be $((\mathbb{Z}/7\mathbb{Z})^\times)^2$, which is cyclic of order 3. The map $\phi_2^{(i)} : \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \longrightarrow ((\mathbb{Z}/7\mathbb{Z})^\times)^2$ is any isomorphism, whereas the maps $\phi_7^{(i)}$ are defined by

$$\begin{aligned}
\phi_7^{(5)} : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} &\longrightarrow \left((\mathbb{Z}/7\mathbb{Z})^\times\right)^2, \qquad \phi_7^{(5)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := (a/d)^2, \\
\phi_7^{(6)} : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} &\longrightarrow \left((\mathbb{Z}/7\mathbb{Z})^\times\right)^2, \qquad \phi_7^{(6)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := d^2, \qquad (5.25) \\
\phi_7^{(7)} : \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} &\longrightarrow \left((\mathbb{Z}/7\mathbb{Z})^\times\right)^2, \qquad \phi_7^{(7)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := a^2.
\end{aligned}$$

We note that $-I \in G_{14,4,1}, G_{14,5,1}$, whereas $-I \notin G_{14,i,k}$ for $i \in \{1,2,3,6,7\}$ and $k \in \{1,2\}$. For $i \in \{1,2,3\}$, $G_{14,i,k} \in \mathfrak{G}^{\max}_{MT,2}(0,14)$, and in this case we have

$$\begin{aligned}
\tilde{G}_{14,1}(14) := \tilde{G}_{14,1,1}(14) = \tilde{G}_{14,1,2}(14) &\simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \times \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\}, \\
\tilde{G}_{14,2}(14) := \tilde{G}_{14,2,1}(14) = \tilde{G}_{14,2,2}(14) &\simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \times \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\}, \qquad (5.26) \\
\tilde{G}_{14,3}(14) := \tilde{G}_{14,3,1}(14) = \tilde{G}_{14,3,2}(14) &\simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \times \left\{ \begin{pmatrix} a & * \\ 0 & \pm a \end{pmatrix} : \ a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\}.
\end{aligned}$$

By contrast, for $i \in \{6,7\}$ and $k \in \{1,2\}$, the group $G_{14,i,k} \in \mathfrak{G}^{\max}_{MT,3}(0,14)$, and in this case the fibering does not disappear under $G \mapsto \tilde{G}$. Indeed, we have

$$\begin{aligned}\tilde{G}_{14,6}(14) = \tilde{G}_{14,6,k}(14) &\simeq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times_{\phi^{(6)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\ \tilde{G}_{14,7}(14) = \tilde{G}_{14,7,k}(14) &\simeq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times_{\phi^{(7)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}.\end{aligned} \tag{5.27}$$

Since the arguments are quite different, we will handle separately the levels of $G \in \mathfrak{G}^{\max}_{MT,2}(0,14)$ and $G \in \mathfrak{G}^{\max}_{MT,3}(0,14)$.

5.1.11.1 The case $G \in \mathfrak{G}^{\max}_{MT,2}(0,14)$: quadratic entanglements.

34

Let E be an elliptic curve defined over $\mathbb{Q}$. By virtue of (Equation 5.26), we have

$$\begin{aligned}\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{14,1} &\iff \rho_{E,7}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix} \right\}, \\ \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{14,2} &\iff \rho_{E,7}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix} \right\}, \\ \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{14,3} &\iff \rho_{E,7}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} a & * \\ 0 & \pm a \end{pmatrix} : a \in (\mathbb{Z}/7\mathbb{Z})^{\times} \right\}, \\ \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{14,4} &\implies \rho_{E,7}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}.\end{aligned} \tag{5.28}$$

Comparing (Equation 5.28) with (Equation 5.9) and considering (Equation 5.11), we are thus led to define the j-invariants $j_{14,i}(t) \in \mathbb{Q}(t)$ by

$$\begin{aligned} j_{14,i}(t) &:= j_{7,i}(t) \qquad (i \in \{1,2,3\}), \\ j_{7,4}(t) &:= \frac{(t^2+245t+2401)^3(t^2+13t+49)}{t^7}, \end{aligned} \tag{5.29}$$

where $j_{7,i}(t) \in \mathbb{Q}(t)$ are as in (Equation 5.10). Combining results in (30) with (Equation 5.28), for each E over $\mathbb{Q}$ with j-invariant j_E, we have

$$\begin{aligned} &\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{14,i} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{14,i}(t_0) \quad (i \in \{1,2,3\}), \\ &\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{14,4} \implies \rho_{E,7}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\ &\rho_{E,7}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{7,4}(t_0). \end{aligned} \tag{5.30}$$

We further define the Weierstrass coefficients $a_{4;14,i}(t)$, $a_{6;14,i}(t)$ for $i \in \{1,2,3\}$ (resp. for $i = 4$ the coefficients $a_{4;7,4}(t)$ and $a_{6;7,4}(t)$) by (Equation 5.29) and (Equation 1.9) and the elliptic curves $\mathcal{E}_{14,i}$ and $\mathcal{E}_{7,4}$ over $\mathbb{Q}(t, D)$ by

$$\begin{aligned} \mathcal{E}_{14,i} &: Dy^2 = x^3 + a_{4;14,i}(t)x + a_{6;14,i}(t) \qquad (i \in \{1,2,3\}), \\ \mathcal{E}_{7,4} &: Dy^2 = x^3 + a_{4;7,4}(t)x + a_{6;7,4}(t), \end{aligned} \tag{5.31}$$

By computing directly the discriminants $\Delta_{\mathcal{E}_{14,i}}$ and $\Delta_{\mathcal{E}_{7,4}}$, we find that

$$\begin{aligned}
\mathbb{Q}\left(\sqrt{\Delta_{\mathcal{E}_{14,i}}}\right) &= \mathbb{Q}\left(\sqrt{t(t-1)(t^3-8t^2+5t+1)}\right) \qquad (i \in \{1,2\}),\\
\mathbb{Q}\left(\sqrt{\Delta_{\mathcal{E}_{14,3}}}\right) &= \mathbb{Q}\left(\sqrt{-7(t^3-2t^2-t+1)(t^3-t^2-2t+1)}\right), \qquad (5.32)\\
\mathbb{Q}\left(\sqrt{\Delta_{\mathcal{E}_{7,4}}}\right) &= \mathbb{Q}\left(\sqrt{t}\right).
\end{aligned}$$

We now note that the j-invariant functions $j_{14,i}(t) \in \mathbb{Q}(t)$ satisfy

$$j_{14,i}(t) = j_{7,4}(u_i(t)) \qquad (i \in \{1,2,3\}),$$

where

$$u_1(t) := \frac{49t(t-1)}{t^3-8t^2+5t+1}, \qquad u_2(t) := \frac{t^3-8t^2+5t+1}{t(t-1)}, \qquad u_3(t) := -\frac{7(t^3-t^2-2t+1)}{t^3-2t^2-t+1}.$$

Applying Lemma 4.2.15 with $u_i(t)$ in place of t, we find that

$$\mathbb{Q}(t,D)(\mathcal{E}_{14},1[7])^{\ker\psi_7^{(1,1)}} = \mathbb{Q}(t,D)\left(\sqrt{\frac{14D(t^2-t+1)(t^6-11t^5+30t^4-15t^3-10t^2+5t+1)}{\left(t^{12}-18t^{11}+117t^{10}-354t^9+570t^8-486t^7+273t^6-222t^5+174t^4-46t^3-15t^2+6t+1\right)}}\right),$$

$$\mathbb{Q}(t,D)(\mathcal{E}_{14},2[7])^{\ker\psi_7^{(2,1)}} = \mathbb{Q}(t,D)\left(\sqrt{\frac{-2D(t^2-t+1)(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)}{\left(t^{12}-522t^{11}-8955t^{10}+37950t^9-70998t^8+131562t^7-253239t^6+316290t^5-218058t^4+80090t^3-14631t^2+510t+1\right)}}\right)$$

$$\mathbb{Q}(t,D)(\mathcal{E}_{14},3[7])^{\ker\psi_7^{(3,1)}} = \mathbb{Q}(t,D)\left(\sqrt{\frac{14D(t^2-3t-3)(t^2-t+1)(3t^2-9t+5)(3t^4-4t^3-5t^2-2t-1)}{(5t^2-t-1)(t^4-6t^3+17t^2-24t+9)(9t^4-12t^3-t^2+8t-3)}}\right).$$

Thus, by (Equation 5.32), (Equation 5.22) and (Equation 5.24), we are led to the twist parameters

$$d_{14,1,1}(t) := \frac{14\left(t^{12}-18t^{11}+117t^{10}-354t^{9}+570t^{8}-486t^{7}+273t^{6}-222t^{5}+174t^{4}-46t^{3}-15t^{2}+6t+1\right)(t^2-t+1)}{t(t-1)(t^3-8t^2+5t+1)(t^6-11t^5+30t^4-15t^3-10t^2+5t+1)},$$

$$d_{14,2,1}(t) := \frac{\left(t^{12}-522t^{11}-8955t^{10}+7950t^{9}-70998t^{8}+131562t^{7}-253239t^{6}+316290t^{5}-218058t^{4}+80090t^{3}-14631t^{2}+510t+1\right)(t^2-t+1)}{-2t(t-1)(t^3-8t^2+5t+1)(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)},$$

$$d_{14,3,1}(t) := \frac{-2(t^2-3t-3)(t^2-t+1)(3t^2-9t+5)(3t^4-4t^3-5t^2-2t-1)(t^3-2t^2-t+1)}{(5t^2-t-1)(t^4-6t^3+17t^2-24t+9)(9t^4-12t^3-t^2+8t-3)(t^3-t^2-2t+1)},$$

and

$$d_{14,i,2}(t) := -7d_{14,i,1}(t) \qquad (i \in \{1,2,3\}).$$

Defining the elliptic curves $\mathcal{E}_{14,i,k}$ over $\mathbb{Q}(t)$ by

$$\mathcal{E}_{14,i,k}: \ d_{14,i,k}(t)y^2 = x^3 + a_{4;14,i}(t)x + a_{6;14,i}(t) \qquad (i \in \{1,2,3\},\ k \in \{1,2\}),$$

we see that, for each E over $\mathbb{Q}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{14,i,k} \iff \exists t_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{14,i,k}(t_0) \qquad \begin{pmatrix} i \in \{1,2,3\} \\ k \in \{1,2\} \end{pmatrix}.$$

Finally, we see from (Equation 5.32), (Equation 5.22) and (Equation 5.24), that, defining the elliptic curve $\mathcal{E}_{14,4,1}$ over $\mathbb{Q}(u, D)$ by

$$\mathcal{E}_{14,4,1}: \; Dy^2 = x^3 + a_{4;7,4}(-7u^2)x + a_{6;7,4}(-7u^2),$$

we have, for any elliptic curve E over $\mathbb{Q}$,

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{14,4,1} \iff \exists u_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{14,4,1}(u_0, D_0).$$

5.1.11.2 The case $G \in \mathfrak{G}^{\max}_{MT,3}(0, 14)$: cubic entanglements.

By (Equation 5.27), we have

$$\tilde{G}_{14,i}(14) \subseteq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subseteq GL_2(\mathbb{Z}/2\mathbb{Z}) \times GL_2(\mathbb{Z}/7\mathbb{Z}) \qquad (i \in \{5, 6, 7\}).$$

As outlined in (30), we have

$$\begin{aligned} \rho_{E,2}(G_{\mathbb{Q}}) \dot{\subseteq} \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle &\iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = t_0^2 + 1728, \\ \rho_{E,7}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} &\iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = j_{7,4}(t_0). \end{aligned} \tag{5.33}$$

where $j_{7,4}(t)$ as in (Equation 5.29). We further define the Weierstrass coefficients $a_{4;7,4}(t)$, $a_{6;7,4}(t) \in \mathbb{Q}(t)$ as usual by (Equation 1.9), the twist parameters $d'_{7,1}(t), d'_{7,2}(t) \in \mathbb{Q}(t)$ by

$$\begin{aligned} d'_{7,1}(t) &:= \frac{(t^4 - 490t^3 - 21609t^2 - 235298t - 823543)(t^2 + 13t + 49)}{14(t^2 + 245t + 2401)}, \\ d'_{7,2}(t) &:= \frac{(t^4 - 490t^3 - 21609t^2 - 235298t - 823543)(t^2 + 13t + 49)}{-2(t^2 + 245t + 2401)} \end{aligned} \tag{5.34}$$

and the elliptic curves $\mathcal{E}'_{7,6}, \mathcal{E}'_{7,7}$ over $\mathbb{Q}(t)$ by

$$\mathcal{E}'_{7,i} : \ d'_{7,i}(t)y^2 = x^3 + a_{4;7,4}(t)x + a_{6;7,4}(t) \qquad (i \in \{1,2\}),$$

As demonstrated in (30), for any elliptic curve E over $\mathbb{Q}$ we have

$$\begin{aligned} \rho_{E,7}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} a^2 & * \\ 0 & * \end{pmatrix} : \ a \in (\mathbb{Z}/7\mathbb{Z})^\times \right\} &\iff \exists t_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}'_{7,1}(t_0), \\ \rho_{E,7}(G_{\mathbb{Q}}) \dot{\subseteq} \left\{ \begin{pmatrix} * & * \\ 0 & d^2 \end{pmatrix} : \ d \in (\mathbb{Z}/7\mathbb{Z})^\times \right\} &\iff \exists t_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}'_{7,2}(t_0). \end{aligned} \tag{5.35}$$

To first obtain a model for the modular curve corresponding to the level 14 group

$$\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},$$

we consider the equation

$$s^2 + 1728 = \frac{(t^2 + 245t + 2401)^3(t^2 + 13t + 49)}{t^7}, \tag{5.36}$$

which is a singular conic. Resolving the singularities via MAGMA, we are led to the substitutions

$$t = \frac{1}{u^2}, \qquad s = \frac{823543u^8 + 235298u^6 + 21609u^4 + 490u^2 - 1}{u}; \tag{5.37}$$

this gives rise to the j-invariant $j'_{14}(u) \in \mathbb{Q}(u)$, Weierstrass coefficients $a'_{4;14}(u)$, $a'_{6,14}(u) \in \mathbb{Q}(u)$ and twist parameters $d'_{14,1}(u)$, $d'_{14,2}(u) \in \mathbb{Q}(u)$, given by

$$\begin{aligned} j'_{14}(u) &= j_{7,4}(1/u^2) = \frac{(49u^4 + 13u^2 + 1)(2401u^4 + 245u^2 + 1)^3}{u^2}, \\ a'_{4;14}(u) &= a_{4;7,4}(1/u^2), \qquad a'_{6;14}(u) = a_{6;7,4}(1/u^2), \\ d'_{14,1}(u) &= d'_{7,1}(1/u^2), \qquad d'_{14,2}(u) = d'_{7,2}(1/u^2), \end{aligned} \tag{5.38}$$

(where $d'_{7,i}(t)$ are as in (Equation 5.34)) and to the elliptic curves $\mathcal{E}'_{14,5}$ over $\mathbb{Q}(u, D)$ and $\mathcal{E}'_{14,6}$ and $\mathcal{E}'_{14,7}$ over $\mathbb{Q}(u)$, defined by

$$\begin{aligned} \mathcal{E}'_{14,5} &: \; Dy^2 = x^3 + a'_{4;14}(u)x + a'_{6;14}(u), \\ \mathcal{E}'_{14,*,i} &: \; d'_{14,i}(u)y^2 = x^3 + a'_{4;14}(u)x + a'_{6;14}(u) \qquad (i \in \{1, 2\}). \end{aligned} \tag{5.39}$$

By (Equation 5.33) and (Equation 5.35), for any elliptic curve E over $\mathbb{Q}$ we have

$$\begin{aligned}
&\rho_{E,14}(G_{\mathbb{Q}}) \dot{\subseteq} \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \iff \exists u_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}'_{14,5}(u_0, D_0), \\
&\rho_{E,14}(G_{\mathbb{Q}}) \dot{\subseteq} \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times \left\{ \begin{pmatrix} a^2 & * \\ 0 & * \end{pmatrix} \right\} \iff \exists u_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}'_{14,*,1}(u_0), \\
&\rho_{E,14}(G_{\mathbb{Q}}) \dot{\subseteq} \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times \left\{ \begin{pmatrix} * & * \\ 0 & d^2 \end{pmatrix} \right\} \iff \exists u_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}'_{14,*,2}(u_0).
\end{aligned} \tag{5.40}$$

Fixing an elliptic curve E over $\mathbb{Q}$ satisfying $\rho_{E,14}(G_{\mathbb{Q}}) \dot{\subseteq} \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$, we will next identify conditions under which

$$\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[7]).$$

By (Equation 5.40), such an elliptic curve E must satisfy $E \simeq_{\mathbb{Q}} \mathcal{E}'_{14,5}(u_0, D_0)$ for some $u_0, D_0 \in \mathbb{Q}$. We define the homomorphisms $\eta_i : B(7) \longrightarrow ((\mathbb{Z}/7\mathbb{Z})^\times)^2$ for $i \in \{1, 2, 3, 4\}$ by

$$\eta_1(g) := \det(g)^2, \quad \eta_2(g) := \phi_7^{(7)}(g), \quad \eta_3(g) := \phi_7^{(6)}(g), \quad \eta_4(g) := \phi_7^{(5)}(g), \tag{5.41}$$

where $\phi_7^{(i)}$ are as in (Equation 5.25). The following lemma specializes Lemma 4.2.7 to the present case, allowing us to exhibit explicit polynomials for generators of each of the four

cyclic cubic subfields $\mathbb{Q}(u, D)\left(\mathcal{E}'_{14,5}[7]\right)^{\ker \eta_i} \subseteq \mathbb{Q}(u, D)\left(\mathcal{E}'_{14,5}[7]\right)$. Define the polynomials $f_i(x) \in \mathbb{Q}(u)[x]$ by

$$\begin{aligned} f_1(x) &= x^3 + x^2 - 2x - 1, \\ f_2(x) &= x^3 - T_1(u)x^2 + R_2(u)x - S_3(u), \\ f_3(x) &= x^3 - T_1(u)x^2 + T_2(u)x - R_3(u), \\ f_4(x) &= x^3 - T_1(u)x^2 + T_2(u)x - T_3(u), \end{aligned} \tag{5.42}$$

where

$$\begin{aligned} T_1(u) &:= 3\left(u^4 + \frac{13}{49}u^2 + \frac{1}{49}\right), \\ R_2(u) &:= 3\left(u^4 + \frac{13}{49}u^2 + \frac{1}{49}\right)\left(u^4 + \frac{13}{49}u^2 + \frac{33}{2401}\right), \\ S_3(u) &:= \left(u^4 + \frac{13}{49}u^2 + \frac{1}{49}\right)\left(u^8 + \frac{26}{49}u^6 + \frac{219}{2401}u^4 + \frac{778}{117649}u^2 + \frac{881}{5764801}\right), \\ T_2(u) &:= 3\left(u^4 + \frac{13}{49}u^2 + \frac{1}{49}\right)\left(u^4 + \frac{13}{49}u^2 - \frac{9}{343}\right), \\ R_3(u) &:= \left(u^4 + \frac{13}{49}u^2 + \frac{1}{49}\right)\left(u^8 + \frac{26}{49}u^6 - \frac{69}{2401}u^4 - \frac{506}{16807}u^2 - \frac{3289}{823543}\right), \\ T_3(u) &:= \left(u^4 + \frac{13}{49}u^2 + \frac{1}{49}\right)\left(u^8 + \frac{26}{49}u^6 - \frac{69}{2401}u^4 - \frac{506}{16807}u^2 - \frac{223}{117649}\right). \end{aligned} \tag{5.43}$$

Lemma 5.1.1. *Let $\mathcal{E}'_{14,5}$ be the elliptic curve over $\mathbb{Q}(u, D)$ defined by* (Equation 5.39). *The four cyclic cubic subfields of $\mathbb{Q}(u, D)\left(\mathcal{E}'_{14,5}[7]\right)$ are as follows. For each $i \in \{1, 2, 3, 4\}$, the field*

$$\mathbb{Q}(u, D)\left(\mathcal{E}'_{14,5}[7]\right)^{\ker \eta_i},$$

where η_i *is as in* (Equation 5.41)*, is equal to the splitting field of* $f_i(x)$*, where* $f_i(x)$ *is defined by* (Equation 5.42) *and* (Equation 5.43)*.*

Proof. Setting $t := 1/u^2$ in Lemma 4.2.7 and performing variable substitutions of the form $x \mapsto g(u)x$ proves the lemma. □

Turning back to our elliptic curve

$$E : y^2 = x^3 + D_0^2 a_{4;14,5}(u_0)x + D_0^3 a_{6;14,5}(u_0) \qquad (u_0, D_0 \in \mathbb{Q})$$

over $\mathbb{Q}$ satisfying $\rho_{E,14}(G_{\mathbb{Q}}) \dot{\subseteq} \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}$, we have the polynomials

$$\psi_{E,2}(x) = x^3 + D_0^2 a_{4;14,5}(u_0)x + D_0^3 a_{6;14,5}, \quad f_i(x) \qquad (i \in \{1,2,3,4\}),$$

(where $f_i(x)$ is as in (Equation 5.42)); we would like to determine conditions under which their splitting fields agree. To illustrate how we use the above results to compute explicit models of the modular curves X_G associated to groups $G \in \mathfrak{G}^{\max}_{MT,3}(0,14)$, we will go through the details for the first of the groups in (Equation 5.23); the other computations are done similarly. We wish to find a rational function $g(v) \in \mathbb{Q}(v)$ so that, defining the elliptic curve $\mathcal{E}_{14,5,1}$ over $\mathbb{Q}(v, D)$ by

$$\mathcal{E}_{14,5,1} : \; Dy^2 = x^3 + a'_{4;14}(g(v))x + a'_{6;14}(g(v)), \tag{5.44}$$

we have, for each elliptic curve E over $\mathbb{Q}$,

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{14,5,1} \iff \exists v_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{14,5,1}(v_0, D_0).$$

In other words, we need

$$\begin{aligned}\mathbb{Q}\left(\mathcal{E}_{14,5,1}[2]\right) &= \mathbb{Q}\left(\mathcal{E}_{14,5,1}[7]\right)^{\ker \phi_7^{(5)}} \\ &= \mathbb{Q}\left(\mathcal{E}_{14,5,1}[7]\right)^{\ker \eta_4}.\end{aligned}$$

By Lemma 5.1.1 we are led to apply Lemma 4.2.8 to the polynomials

$$\begin{aligned}f_S(x) &= x^3 + a'_{4;14}(u)x + a'_{6;14}(u), \\ f_T(x) &= x^3 - T_1(u)x^2 + T_2(u)x - T_3(u),\end{aligned}$$

where the coefficient functions $T_i(u)$ are as in (Equation 5.43) (the twist parameter D occurring in (Equation 5.44) has been absorbed into the variable). Setting $S_1(u) := 0$, $S_2(u) := a'_{4;14}(u)$ and $S_3(u) := -a'_{6;14}(u)$, the condition (Equation 4.20) now reads

$$\begin{aligned}T_1(u) &= -2aS_2(u) + 3c, \\ T_2(u) &= a^2S_2(u)^2 - 3abS_3(u) - 4acS_2(u) + b^2S_2(u) + 3c^2, \\ T_3(u) &= a^3S_3(u)^2 + a^2bS_2(u)S_3(u) + a^2cS_2(u)^2 - 3abcS_3(u) \\ &\quad - 2ac^2S_2(u) + b^3S_3(u) + b^2cS_2(u) + c^3.\end{aligned} \tag{5.45}$$

Setting $c := (T_1(u) + 2aS_2(u))/3$, the first equation above is satisfied. Inserting this into the second equation, we obtain a quadratic equation of the form

$$A(u)b^2 + B(u)ab + C(u)a^2 + c(u) = 0. \tag{5.46}$$

Viewing the left-hand side as a quadratic polynomial in b with coefficients in $\mathbb{Q}(a,u)$, its discriminant

$$\Delta(a,u) := (B(u)a)^2 - 4A(u)\left(C(u)a^2 + c(u)\right)$$

is equal to

$$\begin{aligned} &-\frac{2^{14}3^{11}u^2\left(u^4+\frac{13}{49}u^2+\frac{1}{49}\right)^2\left(u^4+\frac{5}{49}u^2+\frac{1}{2401}\right)^6}{7^{14}\left(u^8+\frac{2}{7}u^6+\frac{9}{343}u^4+\frac{10}{16807}u^2-\frac{1}{823543}\right)^6}a^2 \\ &+\frac{2^8 3^4\left(u^4+\frac{13}{49}u^2+\frac{1}{49}\right)^2\left(u^4+\frac{5}{49}u^2+\frac{1}{2401}\right)^3}{7^3\left(u^8+\frac{2}{7}u^6+\frac{9}{343}u^4+\frac{10}{16807}u^2-\frac{1}{823543}\right)^2}; \end{aligned} \tag{5.47}$$

we would like this to be a perfect square. Under the substitution

$$\tilde{a} := \frac{2^3 3^3 u\left(u^4+\frac{5}{49}u^2+\frac{1}{2401}\right)^2 a}{7^3\left(u^8+\frac{2}{7}u^6+\frac{9}{343}u^4+\frac{10}{16807}u^2-\frac{1}{823543}\right)^2}, \tag{5.48}$$

we see that $\Delta(a,u)$ is equal modulo $(\mathbb{Q}(a,u)^\times)^2$ to

$$-3\tilde{a}^2 + 7^5\left(u^4+\frac{5}{49}u^2+\frac{1}{2401}\right).$$

Further substituting $u = \tilde{u}/7$ and setting this expression equal to a perfect square, we arrive at the equation

$$X^2 + 3\tilde{a}^2 = 7\left(\tilde{u}^4 + 5\tilde{u}^2 + 1\right),$$

which we view as a conic over $\mathbb{Q}(u)$. Since $7 = 2^2 + 3 \cdot 1^2$ and $\tilde{u}^4 + 5\tilde{u}^2 + 1 = (\tilde{u}^2 + 1)^2 + 3\tilde{u}^2$ are each represented by the left-hand norm form, we discover the $\mathbb{Q}(u)$-rational point

$$(X, \tilde{a}) = \left(2\tilde{u}^2 - 3\tilde{u} + 2, (\tilde{u} + 1)^2\right)$$

on this conic. Projecting from this point, we arrive at the $\mathbb{Q}(u, v)$-rational point

$$\begin{aligned} X &:= 2\frac{\tilde{u}^6 - \frac{3}{2}\tilde{u}^5 - \tilde{u}^4 v + 6\tilde{u}^4 - \frac{15}{2}\tilde{u}^3 + \frac{1}{7}\tilde{u}^2 v^2 - 5\tilde{u}^2 v + 6\tilde{u}^2 - \frac{3}{14}\tilde{u}v^2 - \frac{3}{2}\tilde{u} + \frac{1}{7}v^2 - v + 1}{\tilde{u}^4 - \frac{4}{7}\tilde{u}^2 v + 5\tilde{u}^2 + \frac{6}{7}\tilde{u}v + \frac{1}{7}v^2 - \frac{4}{7}v + 1}, \\ \tilde{a} &:= \frac{(\tilde{u} + 1)^2\left(\tilde{u}^4 + 5\tilde{u}^2 - \frac{1}{7}v^2 + 1\right)}{\tilde{u}^4 - \frac{4}{7}\tilde{u}^2 v + 5\tilde{u}^2 + \frac{6}{7}\tilde{u}v + \frac{1}{7}v^2 - \frac{4}{7}v + 1} \\ &= \frac{(7u + 1)^2\left(16807u^4 + 1715u^2 - v^2 + 7\right)}{16807u^4 - 196u^2 v + 1715u^2 + 42uv + v^2 - 4v + 7}. \end{aligned} \tag{5.49}$$

Inserting this into (Equation 5.48), we find that

$$a = a(u, v) = \frac{7^3(7u + 1)^2\left(16807u^4 + 1715u^2 - v^2 + 7\right)\left(u^8 + \frac{2}{7}u^6 + \frac{9}{343}u^4 + \frac{10}{16807}u^2 - \frac{1}{823543}\right)^2}{2^3 3^3 u\left(u^4 + \frac{5}{49}u^2 + \frac{1}{2401}\right)^2 (16807u^4 - 196u^2 v + 1715u^2 + 42uv + v^2 - 4v + 7)};$$

inserting this into (Equation 5.47) (or alternatively working from the expression for X in (Equation 5.49)), we find that the discriminant $\Delta(u, a(u,v)) \in \mathbb{Q}(u,v)$ of the original quadratic (Equation 5.46) is now equal to

$$\left(\frac{2^5 3^2 \left(u^4 + \frac{13}{49}u^2 + \frac{1}{49}\right)\left(u^4 + \frac{5}{49}u^2 + \frac{1}{2401}\right) f(u,v)}{7h(u,v)g(u,v)} \right)^2$$

where

$$\begin{aligned} f(u,v) = \; & u^6 - \frac{3}{14}u^5 - \frac{1}{49}u^4 v + \frac{6}{49}u^4 - \frac{15}{686}u^3 + \frac{1}{16807}u^2v^2 - \frac{5}{2401}u^2 v \; + \\ & \frac{6}{2401}u^2 - \frac{3}{235298}uv^2 - \frac{3}{33614}u + \frac{1}{823543}v^2 - \frac{1}{117649}v + \frac{1}{117649} \end{aligned}$$

$$g(u,v) = u^4 - \frac{4}{343}u^2 v + \frac{5}{49}u^2 + \frac{6}{2401}uv + \frac{1}{16807}v^2 - \frac{4}{16807}v + \frac{1}{2401}$$

$$h(u,v) = u^8 + \frac{2}{7}u^6 + \frac{9}{343}u^4 + \frac{10}{16807}u^2 - \frac{1}{823543}$$

In particular, we have $\Delta(u,v) = \Delta(u,v)^2 \in (\mathbb{Q}(u,v)^\times)^2$, and applying the quadratic formula to (Equation 5.46), we obtain functions

$$b_\pm(u,v) := \frac{-B(u) \pm \Delta(u,v)}{2A(u)} \in \mathbb{Q}(u,v).$$

By construction, the first two equations of (Equation 5.45) are satisfied when $a = a(u,v)$, $b = b_\pm(u,v)$ and $c := (T_1(u) + 2a(u,v)S_2(u))/3$. We now insert these rational functions into

the third equation in (Equation 5.45). For instance, choosing to insert $b_+(u,v)$, gathering all terms to one side and factoring into irreducible polynomials leads to an equation of the form

$$\left(u^4+\frac{13}{49}u^2+\frac{1}{49}\right) f_1(u,v)f_2(u,v)=0, \tag{5.50}$$

where

$$\begin{aligned} f_1(u,v) :=& u^{13}-\frac{1}{7}u^{12}-\frac{1}{7^2}u^{11}v+\frac{15}{7^2}u^{11}-\frac{15}{7^3}u^{10}+\frac{1}{7^5}u^9v^2-\frac{16}{7^4}u^9v+\frac{78}{7^4}u^9-\frac{3}{7^6}u^8v^2\\ &-\frac{1}{7^5}u^8v-\frac{78}{7^5}u^8+\frac{1}{7^8}u^7v^3+\frac{18}{7^7}u^7v^2-\frac{87}{7^6}u^7v+\frac{155}{7^6}u^7+\frac{6}{7^9}u^6v^3-\frac{32}{7^8}u^6v^2\\ &-\frac{10}{7^7}u^6v-\frac{155}{7^7}u^6+\frac{1}{7^{10}}u^5v^3+\frac{81}{7^9}u^5v^2-\frac{172}{7^8}u^5v+\frac{78}{7^8}u^5+\frac{55}{7^{11}}u^4v^3-\frac{81}{7^{10}}u^4v^2\\ &-\frac{27}{7^9}u^4v-\frac{78}{7^9}u^4+\frac{1}{7^{12}}u^3v^3+\frac{88}{7^{11}}u^3v^2-\frac{61}{7^{10}}u^3v+\frac{15}{7^{10}}u^3+\frac{55}{7^{13}}u^2v^3+\frac{18}{7^{12}}u^2v^2\\ &-\frac{10}{7^{11}}u^2v-\frac{15}{7^{11}}u^2+\frac{8}{7^{14}}uv^3+\frac{15}{7^{13}}uv^2-\frac{6}{7^{12}}uv+\frac{1}{7^{12}}u-\frac{1}{7^{14}}v^3+\frac{1}{7^{13}}v^2-\frac{1}{7^{13}}v\\ &-\frac{1}{7^{13}} \end{aligned}$$

and $f_2(u,v)\in\mathbb{Q}[u,v]$ is another polynomial of degree 13. The polynomial equation $f_1(u,v)=0$ defines a singular conic $\mathfrak{S}$ that is found (by a computation in MAGMA) to be birational to the smooth conic

$$C:\ r^2-\frac{9}{49}s^2+600250r+32242s+90392079680=0;$$

we denote by $\tau : \mathfrak{S} \longrightarrow C$ be the birational map produced by our MAGMA calculation. Projecting from the rational point $(r_0, s_0) = (-300125, 184877)$ gives rise to a isomorphism $\mathbb{P}^1(w) \to C$ with coordinate functions

$$r = r(w) = -\frac{300125(9w^2 - 47w - 3920)}{(3w-79)(3w+46)},$$
$$s = s(w) = -\frac{84035(w^2 - 11w + 8624)}{(3w-79)(3w+46)}.$$

Furthermore, composing this isomorphism with $\tau^{-1} : C \longrightarrow \mathfrak{S}$, we obtain

$$u = u_5(w) := -\frac{w^3 + 546w^2 - 10003w - 205807}{13w^3 - 777w^2 - 43414w + 504259}. \tag{5.51}$$

We define the elliptic curve $\mathcal{E}_{14,5,1}$ over $\mathbb{Q}(w, D)$ by

$$\mathcal{E}_{14,5,1} : \; Dy^2 = x^3 + a'_{4,14}\left(u_5(w)\right)x + a'_{6,14}\left(u_5(w)\right), \tag{5.52}$$

where the Weierstrass coefficients $a'_{4,14}(u), a'_{6,14}(u) \in \mathbb{Q}(u)$ are as in (Equation 5.38) and $u_5(w) \in \mathbb{Q}(w)$ is as in (Equation 5.51). It follows from our discussion that, for each elliptic curve E over $\mathbb{Q}$, we have

$$\exists w_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{14,5,1}(w_0, D_0) \implies \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{14,5,1}. \tag{5.53}$$

Now suppose we instead consider the singular conic $\mathfrak{S}_2$ defined by $f_2(u, v) = 0$ (where $f_2(u, v)$ is as in (Equation 5.50)), and obtain a degree three function $u_2(w) \in \mathbb{Q}(w)$ similar to (Equation 5.51),

and thus to an elliptic curve $\mathcal{E}^{(2)}_{14,5,1}$ over $\mathbb{Q}(w, D)$ as in (Equation 5.52) with $u(w)$ replaced by $u_2(w)$. The elliptic curve $\mathcal{E}^{(2)}_{14,5,1}$ then satisfies property (Equation 5.53), and by considering the degrees of the associated j-invariants, it follows that $u_2(w) = u(\mu(w))$, where $\mu(w)$ is a linear fractional transformation, i.e. an automorphism of $\mathbb{P}^1$. The same is true if we instead use the function $b_-(u, v)$ in place of $b_+(u, v)$ and consider any irreducible factor resulting from the third equation of (Equation 5.45). We have thus established that, for any elliptic curve E over $\mathbb{Q}$,

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{14,5,1} \iff \exists w_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{14,5,1}(w_0, D_0).$$

The arguments and computations that lead to explicit models associated to the groups $G_{14,6,k}$ and $G_{14,7,k}$ are similar, and we skip most of the details, only summarizing the results. An analogous computation for the group $\tilde{G}_{14,6}(14)$ involves applying Lemma 4.2.8 to the polynomials

$$f_S(x) := x^3 + a'_{4;14}(u)x + a'_{6;14}(u)$$
$$f_T(x) := x^3 - T_1(u)x^2 + T_2(u)x - R_3(u),$$

where $T_1(u)$, $T_2(u)$ and $R_3(u)$ are as in (Equation 5.43). Continuing as above, we are led to the rational function

$$u_6(w) := -\frac{4(w+2)(w+25)(5w+33)}{71w^3 + 357w^2 - 5243w - 23513}, \tag{5.54}$$

and we define the elliptic curve $\mathcal{E}_{14,6}$ over $\mathbb{Q}(w, D)$ by

$$\mathcal{E}_{14,6}: \; Dy^2 = x^3 + a'_{4;14}(u_6(w))\,x + a'_{6;14}(u_6(w)). \tag{5.55}$$

For each elliptic curve E over $\mathbb{Q}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{14,6} \iff \exists w_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{14,6}(w_0, D_0). \tag{5.56}$$

Considering (Equation 5.35) and (Equation 5.23), we are led to define the twist families $\mathcal{E}_{14,6,1}$ and $\mathcal{E}_{14,6,2}$ over $\mathbb{Q}(w)$ by

$$\mathcal{E}_{14,6,k}: \; d'_{14,k}(u_6(w))y^2 = x^3 + a'_{4;14}(u_6(w))\,x + a'_{6;14}(u_6(w)) \qquad (k \in \{1,2\}), \tag{5.57}$$

where $d'_{14,k}(u) := d'_{7,k}(1/u^2)$ and $d'_{7,k}(t)$ is defined by (Equation 5.34). By (Equation 5.56) and (Equation 5.40), for any elliptic curve E over $\mathbb{Q}$ we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{14,6,k} \iff \exists w_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{14,6,k}(w_0) \qquad (k \in \{1,2\}).$$

Similarly, the group $\tilde{G}_{14,7}(14)$ leads us to apply Lemma 4.2.8 to the polynomials

$$f_S(x) := x^3 + a'_{4;14}(u)x + a'_{6;14}(u)$$

$$f_T(x) := x^3 - T_1(u)x^2 + R_2(u)x - S_3(u),$$

where $T_1(u)$, $R_2(u)$ and $S_3(u)$ are as in (Equation 5.43). Continuing as above, we are led to the rational function

$$u_7(w) := \frac{91w^3 - 42w^2 - 28w + 8}{28w(w-2)(5w-2)}, \tag{5.58}$$

and we define the elliptic curve $\mathcal{E}_{14,7}$ over $\mathbb{Q}(w, D)$ by

$$\mathcal{E}_{14,7} : \; Dy^2 = x^3 + a'_{4;14}(u_7(w))\,x + a'_{6;14}(u_7(w)). \tag{5.59}$$

For each elliptic curve E over $\mathbb{Q}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{14,7} \iff \exists w_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{14,7}(w_0, D_0). \tag{5.60}$$

We define the twist families $\mathcal{E}_{14,7,1}$ and $\mathcal{E}_{14,7,2}$ over $\mathbb{Q}(w)$ by

$$\mathcal{E}_{14,7,k} : \; d'_{14,k}(u_7(w))y^2 = x^3 + a'_{4;14}(u_7(w))\,x + a'_{6;14}(u_7(w)) \qquad (k \in \{1,2\}), \tag{5.61}$$

where $d'_{14,k}(u)$ is as before. By (Equation 5.56) and (Equation 5.40), for any elliptic curve E over $\mathbb{Q}$ we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{14,7,k} \iff \exists w_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{14,7,k}(w_0) \qquad (k \in \{1,2\}).$$

5.1.12 The level $m = 28$

We have $\mathfrak{G}_{MT}^{max}(0, 28) = \{G_{28,1,1}, G_{28,2,1}, G_{28,2,2}, G_{28,3,1}, G_{28,3,2}\}$, where $G_{28,i,k}(28) \subseteq GL_2(\mathbb{Z}/28\mathbb{Z})$ are given by

$$G_{28,1,1}(28) = \left\langle \begin{pmatrix} 5 & 19 \\ 21 & 8 \end{pmatrix}, \begin{pmatrix} 9 & 3 \\ 14 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 10 \\ 0 & 17 \end{pmatrix} \right\rangle \simeq GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times_{\psi^{(1,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{28,2,1}(28) = \left\langle \begin{pmatrix} 5 & 9 \\ 19 & 10 \end{pmatrix}, \begin{pmatrix} 2 & 23 \\ 13 & 5 \end{pmatrix}, \begin{pmatrix} 27 & 10 \\ 14 & 11 \end{pmatrix} \right\rangle \simeq \pi_{GL_2}^{-1} \left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \times_{\psi^{(2,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{28,2,2}(28) = \left\langle \begin{pmatrix} 4 & 19 \\ 11 & 9 \end{pmatrix}, \begin{pmatrix} 3 & 12 \\ 2 & 5 \end{pmatrix}, \begin{pmatrix} 22 & 9 \\ 9 & 19 \end{pmatrix} \right\rangle \simeq \pi_{GL_2}^{-1} \left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \times_{\psi^{(2,2)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{28,3,1}(28) = \left\langle \begin{pmatrix} 20 & 1 \\ 5 & 7 \end{pmatrix}, \begin{pmatrix} 15 & 14 \\ 2 & 11 \end{pmatrix}, \begin{pmatrix} 7 & 12 \\ 10 & 21 \end{pmatrix} \right\rangle \simeq \pi_{GL_2}^{-1} \left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \times_{\psi^{(3,1)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},$$

$$G_{28,3,2}(28) = \left\langle \begin{pmatrix} 17 & 5 \\ 3 & 24 \end{pmatrix}, \begin{pmatrix} 26 & 19 \\ 1 & 23 \end{pmatrix}, \begin{pmatrix} 0 & 13 \\ 27 & 5 \end{pmatrix} \right\rangle \simeq \pi_{GL_2}^{-1} \left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \times_{\psi^{(3,2)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \tag{5.62}$$

and $G_{28,i,k} = \pi_{GL_2}^{-1}(G_{28,i,k}(28))$. In all cases, the representations of the groups on the right-hand are to be understood via the Chinese Remainder Theorem as subgroups of $GL_2(\mathbb{Z}/4\mathbb{Z}) \times GL_2(\mathbb{Z}/7\mathbb{Z})$, and as before, we are making the usual use of the abbreviation $GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} :=$

$\{g \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) : \chi_4(\det g) = \varepsilon(g \bmod 2)\}$. In the fibered products $\psi^{(i,k)}$, the underlying homomorphisms are as follows: the maps $\psi_4^{(i,k)}$ are defined by

$$\psi_4^{(1,1)} : \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \longrightarrow \{\pm 1\},$$

$$\ker \psi_4^{(1,1)} = \left\langle \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \right\rangle,$$

$$\psi_4^{(i,k)} : \pi_{\mathrm{GL}_2}^{-1}\left(\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \right) \longrightarrow (\mathbb{Z}/7\mathbb{Z})^\times, \tag{5.63}$$

$$\ker \psi_4^{(i,k)} = \left\langle \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \right\rangle \quad \begin{pmatrix} i \in \{2,3\} \\ k \in \{1,2\} \end{pmatrix},$$

Note that, by Corollary 4.2.6, we need only specify the kernels of these automorphisms, since if we post-compose (say) $\psi_4^{(i,k)}$ by an automorphism of $(\mathbb{Z}/7\mathbb{Z})^\times$, the resulting fibered product

group would be $\mathrm{GL}_2(\mathbb{Z}/28\mathbb{Z})$-conjugate to the original group. On the "7 side," the maps $\psi_7^{(1,1)}$, $\psi_7^{(2,1)}$, $\psi_7^{(2,2)}$, $\psi_7^{(3,1)}$ and $\psi_7^{(3,2)}$ are defined by

$$\begin{aligned}
\psi_7^{(1,1)} &: \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow \{\pm 1\}, \qquad \psi_7^{(1,1)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := \left(\frac{ad}{7} \right), \\
\psi_7^{(2,1)} &: \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow (\mathbb{Z}/7\mathbb{Z})^\times, \qquad \psi_7^{(2,1)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := a^3 d^2, \\
\psi_7^{(2,2)} &: \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow (\mathbb{Z}/7\mathbb{Z})^\times, \qquad \psi_7^{(2,2)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := d, \\
\psi_7^{(3,1)} &: \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow (\mathbb{Z}/7\mathbb{Z})^\times, \qquad \psi_7^{(3,1)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := a, \\
\psi_7^{(3,2)} &: \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \longrightarrow (\mathbb{Z}/7\mathbb{Z})^\times, \qquad \psi_7^{(3,2)} \left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) := a^2 d^3.
\end{aligned} \tag{5.64}$$

We note that $-I \notin G_{28,i,k}$ for each $i \in \{1,2,3\}$ and $k \in \{1,2\}$, and we have $\tilde{G}_{28,2,1} = \tilde{G}_{28,2,2} = \tilde{G}_{14,6}$, and $\tilde{G}_{28,3,1} = \tilde{G}_{28,3,2} = \tilde{G}_{14,7}$. In particular, denoting by $\tilde{G}_{28,2}$ the common value of the two groups $\tilde{G}_{28,2,k}$ and by $\tilde{G}_{28,3}$ the common value of the two groups $\tilde{G}_{28,3,k}$, we see that each

of the groups $\tilde{G}_{28,2}$ and $\tilde{G}_{28,3}$ have GL_2-level 14, whereas $\tilde{G}_{28,1} := \tilde{G}_{28,1,1}$ has GL_2-level 28. Precisely, we have

$$\begin{aligned}
\tilde{G}_{28,1}(28) = \tilde{G}_{28,1,1}(28) &\simeq GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \times \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\
\tilde{G}_{28,2}(14) = \tilde{G}_{28,2,k}(14) &\simeq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times_{\phi^{(6)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\}, \\
\tilde{G}_{28,3}(14) = \tilde{G}_{28,3,k}(14) &\simeq \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \times_{\phi^{(7)}} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},
\end{aligned} \tag{5.65}$$

where the fibering maps $\phi_2^{(6)}$ and $\phi_2^{(7)}$ are isomorphisms $\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \longrightarrow ((\mathbb{Z}/7\mathbb{Z})^\times)^2$ and $\phi_7^{(6)}$, $\phi_7^{(7)}$ are as in (Equation 5.25). By (Equation 5.27), it is then natural to define the elliptic curves $\mathcal{E}_{28,2}$ and $\mathcal{E}_{28,3}$ over $\mathbb{Q}(w, D)$ by

$$\mathcal{E}_{28,2} := \mathcal{E}_{14,6}, \qquad \mathcal{E}_{28,3} := \mathcal{E}_{14,7},$$

where $\mathcal{E}_{14,6}$ is as in (Equation 5.55) and $\mathcal{E}_{14,7}$ is as in (Equation 5.59). By (Equation 5.56) and (Equation 5.60), for each elliptic curve E over $\mathbb{Q}$ we have

$$\begin{aligned}
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{28,2} &\iff \exists w_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{28,2}(w_0, D_0), \\
\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{28,3} &\iff \exists w_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{28,3}(w_0, D_0).
\end{aligned}$$

We note by (Equation 5.63) that, for each $i \in \{2,3\}$ and $k \in \{1,2\}$, $\ker \psi_4^{(i,k)} \subseteq \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$, and it follows that

$$\mathbb{Q}(u,D)\left(\mathcal{E}_{28,i}[4]\right)^{\ker \psi_4^{(i,k)}} = \mathbb{Q}(u,D)\left(\mathcal{E}_{28,i}[2],i\right) \qquad \begin{pmatrix} i \in \{2,3\} \\ k \in \{1,2\} \end{pmatrix}.$$

26
On the other hand, a computation shows that

$$\mathbb{Q}(u,D)\left(\mathcal{E}_{28,i}[7]\right)^{\ker \psi_7^{(i,k)}} = \mathbb{Q}(u,D)\left(\mathcal{E}_{28,i}[7]\right)^{\ker \phi_7^{(4+i)}} \cdot \mathbb{Q}(u,D)\left(\sqrt{Df_k(u)}\right) \qquad \begin{pmatrix} i \in \{2,3\} \\ k \in \{1,2\} \end{pmatrix},$$

where

$$f_1(u) := \frac{-14(49u^4+13u^2+1)(2401u^4+245u^2+1)}{823543u^8+235298u^6+21609u^4+490u^2-1},$$
$$f_2(u) := \frac{2(49u^4+13u^2+1)(2401u^4+245u^2+1)}{823543u^8+235298u^6+21609u^4+490u^2-1}.$$

This leads us to define the twist parameters $d_k(u) \in \mathbb{Q}(u)$ by

$$d_1(u) := -f_1(u) = \frac{14(49u^4+13u^2+1)(2401u^4+245u^2+1)}{823543u^8+235298u^6+21609u^4+490u^2-1},$$
$$d_2(u) := -f_2(u) = \frac{-2(49u^4+13u^2+1)(2401u^4+245u^2+1)}{823543u^8+235298u^6+21609u^4+490u^2-1},$$

and the elliptic curves $\mathcal{E}_{28,i,k}$ over $\mathbb{Q}(w)$ by

$$\mathcal{E}_{28,2,k} : d_k(u_6(w))y^2 = x^3 + a'_{4;14,4}(u_6(w))x + a'_{6;14,4}(u_6(w)),$$

$$\mathcal{E}_{28,3,k} : d_k(u_7(w))y^2 = x^3 + a'_{4;14,4}(u_7(w))x + a'_{6;14,4}(u_7(w)),$$

where $a'_{4;14,4}(u)$, $a'_{6;14,4}(u)$ are as in (Equation 5.38), $u_6(w)$ is as in (Equation 5.54) and $u_7(w)$ is as in (Equation 5.58). By the above discussion taken together with Corollary 4.2.6, for each elliptic curve E over $\mathbb{Q}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{28,i,k} \iff \exists w_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{28,i,k}(w_0) \qquad \begin{pmatrix} i \in \{2,3\} \\ k \in \{1,2\} \end{pmatrix}.$$

To handle the group $G_{28,1,1}$, we first recall that, as detailed in (25), one has

$$\rho_{E,4}(G_{\mathbb{Q}}) \dot{\subseteq} GL_2(\mathbb{Z}/4\mathbb{Z})_{\chi_4=\varepsilon} \iff \exists t_0 \in \mathbb{Q} \text{ for which } j_E = -t_0^2 + 1728. \tag{5.66}$$

This, together with (Equation 5.65) and (Equation 5.30), leads us to the equation

$$-s^2 + 1728 = \frac{(t^2 + 245t + 2401)^3(t^2 + 13t + 49)}{t^7} =: j_{7,4}(t) \tag{5.67}$$

which is quite close to (Equation 5.36). The replacement $u \mapsto iu$ in (Equation 5.37) leads us to the substitutions

$$t = -\frac{1}{u^2}, \qquad s = \frac{823543u^8 - 235298u^6 + 21609u^4 - 490u^2 - 1}{u}, \tag{5.68}$$

which satisfy the equation (Equation 5.67). We set

$$j_{28,1}(u) := j_{7,4}(-1/u^2),$$

where $j_{7,4}(t)$ is as in (Equation 5.67), we define $a_{4;28,1}(u), a_{6;28,1}(u) \in \mathbb{Q}(u)$ as usual by (Equation 1.9) and finally the elliptic curve $\mathcal{E}_{28,1}$ over $\mathbb{Q}(u, D)$ by

$$\mathcal{E}_{28,1} : \; Dy^2 = x^3 + a_{4;28,1}(u)x + a_{6;28,1}(u).$$

By (Equation 5.65), (Equation 5.66) and (Equation 5.30), we see that, for any elliptic curve E over $\mathbb{Q}$, we have

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} \tilde{G}_{28,1} \iff \exists u_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{28,1}(u_0, D_0).$$

Applying the substitution (Equation 5.68) to Lemma 4.2.13 and using (Equation 5.64), we find that

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{28,1,1} \iff \begin{array}{c} \exists u_0, D_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{28,1}(u_0, D_0) \text{ and} \\ \mathbb{Q}\left(\sqrt{\frac{Du(49u^4-13u^2+1)(2401u^4-245u^2+1)}{823543u^8-235298u^6+21609u^4-490u^2-1}}\right) = \mathbb{Q}\left(\sqrt{-7}\right), \end{array}$$

and this happens if and only if

$$D = d_{28,1,1}(u) := \frac{-7u(49u^4 - 13u^2 + 1)(2401u^4 - 245u^2 + 1)}{823543u^8 - 235298u^6 + 21609u^4 - 490u^2 - 1}$$

modulo $(\mathbb{Q}^\times)^2$. We define the elliptic curve $\mathcal{E}_{28,1,1}$ over $\mathbb{Q}(u)$ by

$$\mathcal{E}_{28,1,1} : d_{28,1,1}(u)y^2 = x^3 + a_{4;28,1}(u)x + a_{6;28,1}(u).$$

We have verified that, for any elliptic curve E over $\mathbb{Q}$,

$$\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{28,1,1} \iff \exists u_0 \in \mathbb{Q} \text{ for which } E \simeq_{\mathbb{Q}} \mathcal{E}_{28,1,1}(u_0).$$

CHAPTER 6

TABLES OF J-INVARIANTS AND TWIST PARAMETERS ASSOCIATED TO $G \in \mathfrak{G}_{MT}^{max}(0)$

We first define the auxiliary rational functions $f_{m,i}(t)$, $g_{m,i}(t)$ and $h_{m,i}(t)$ in Table I. These functions allow us to express some of the j-invariants in the subsequent tables in a reasonably compact way (these functions would otherwise not have fit on the page). Next, we define the j-invariants $j_{m,i}(t) \in \mathbb{Q}(t)$ in Table II and Table III. Finally, in Table IV, Table V, and Table VI we define the relevant twist parameters $d_{m,i,k} \in \mathbb{Q}(t, D)$.

(m,i)	$f_{m,i}(t)$	$g_{m,i}(t)$	$h_{m,i}(t)$
$(9,1)$	$\frac{(t+3)^3(t+27)}{t}$	$\frac{729}{t^3-27}$	$\frac{-6(t^3-9t)}{t^3+9t^2-9t-9}$
$(9,2)$		$t(t^2+9t+27)$	$\frac{-3(t^3+9t^2-9t-9)}{t^3+3t^2-9t-3}$
$(9,3)$		t^3	$\frac{3(t^3+3t^2-9t-3)}{t^3-3t^2-9t+3}$
$(10,3)$	$t^3(t^2+5t+40)$	$\frac{3t^6+12t^5+80t^4+50t^3-20t^2-8t+8}{(t-1)^2(t^2+3t+1)^2}$	
$(14,1)$	$\frac{(49t^4+13t^2+1)(2401t^4+245t^2+1)^3}{t^2}$		
$(14,2)$	$\frac{(49t^4+13t^2+1)(823543t^8+235298t^6+21609t^4+490t^2-1)}{-14t^8(2401t^4+245t^2+1)}$		
$(14,5)$		$-\frac{t^3+546t^2-10003t-205807}{13t^3-777t^2-43414t+504259}$	
$(14,6)$		$-\frac{4(t+2)(5t+33)(t+25)}{71t^3+357t^2-5243t-23513}$	
$(14,7)$		$\frac{91t^3-42t^2-28t+8}{28t(t-2)(5t-2)}$	

TABLE I: Some auxiliary rational functions

(m, i)	$j_{m,i}(t)$
$(2, 1)$	$256\frac{(t+1)^3}{t}$
$(3, 1)$	$27\frac{(t+1)(t+9)^3}{t^3}$
$(4, 1)$	$-t^2 + 1728$
$(5, 1)$	$\frac{(t^4-12t^3+14t^2+12t+1)^3}{t^5(t^2-11t-1)}$
$(5, 2)$	$\frac{(t^4+228t^3+494t^2-228t+1)^3}{t(t^2-11t-1)^5}$
$(6, 1)$	$2^{10}3^3t^3(1-4t^3)$
$(6, 2)$	$\frac{-27(t^2-9)^3(t^2-1)}{t^6}$
$(6, 3)$	$27\frac{(t+1)(t+9)^3}{t^3}$
$(7, 1)$	$\frac{(t^2-t+1)^3(t^6-11t^5+30t^4-15t^3-10t^2+5t+1)^3}{t^7(t-1)^7(t^3-8t^2+5t+1)}$
$(7, 2)$	$\frac{(t^2-t+1)^3(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)^3}{t(t-1)(t^3-8t^2+5t+1)^7}$
$(7, 3)$	$-\frac{(t^2-3t-3)^3(t^2-t+1)^3(3t^2-9t+5)^3(5t^2-t-1)^3}{(t^3-2t^2-t+1)(t^3-t^2-2t+1)^7}$
$(8, 1)$	$\frac{-4(t^2+2t-2)^3(t^2+10t-2)}{t^4}$
$(9, 1)$	$f_{9,1}(g_{9,1}(h_{9,1}(t)))$
$(9, 2)$	$f_{9,1}(g_{9,2}(h_{9,2}(t)))$
$(9, 3)$	$f_{9,1}(g_{9,3}(h_{9,3}(t)))$
$(9, 4)$	$\frac{3^7(t^2-1)^3(t^6+3t^5+6t^4+t^3-3t^2+12t+16)^3(2t^3+3t^2-3t-5)}{(t^3-3t-1)^9}$

TABLE II: j-invariants associated to maximal genus zero missing trace groups for $m < 10$ (see Table I for the definitions of $f_{m,i}(t)$, $g_{m,i}(t)$ and $h_{m,i}(t)$)

(m,i)	$j_{m,i}(t)$
$(10,1)$	$\frac{(t^4-12t^3+14t^2+12t+1)^3}{t^5(t^2-11t-1)}$
$(10,2)$	$\frac{(t^4+228t^3+494t^2-228t+1)^3}{t(t^2-11t-1)^5}$
$(10,3)$	$f_{10,3}\,(g_{10,3}(t))$
$(12,1)$	$-\frac{(t^2-27)(t^2-3)^3}{t^2}$
$(12,2)$	$-\frac{(36t^2-27)(36t^2-3)^3}{36t^2}$
$(12,3)$	$-\frac{(4t^2-27)(4t^2-3)^3}{4t^2}$
$(12,4)$	$\frac{(27t^2+1)(243t^2+1)^3}{t^2}$
$(14,1)$	$j_{7,1}(t)$
$(14,2)$	$j_{7,2}(t)$
$(14,3)$	$j_{7,3}(t)$
$(14,4)$	$-\frac{(49t^4-1715t^2+2401)^3(49t^4-91t^2+49)}{823543t^{14}}$
$(14,5)$	$f_{14,1}(g_{14,5}(t))$
$(14,6)$	$f_{14,1}(g_{14,6}(t))$
$(14,7)$	$f_{14,1}(g_{14,7}(t))$
$(28,1)$	$-\frac{(49t^4-13t^2+1)(2401t^4-245t^2+1)^3}{t^2}$
$(28,2)$	$f_{14,1}(g_{14,6}(t))$
$(28,3)$	$f_{14,1}(g_{14,7}(t))$

TABLE III: j-invariants associated to maximal genus zero missing trace groups for $m \geq 10$ (see Table I for the definitions of $f_{m,i}(t)$, $g_{m,i}(t)$ and $h_{m,i}(t)$)

(m,i,k)	$d_{m,i,k}$
$(2,1,1)$	D
$(3,1,1)$	$\frac{6(t+1)(t+9)}{t^2-18t-27}$
$(3,1,2)$	$-3d_{3,1,1}$
$(4,1,1)$	$t(t^2-1728)$
$(5,1,1)$	$-\frac{(t^2+1)(t^4-18t^3+74t^2+18t+1)}{2(t^4-12t^3+14t^2+12t+1)}$
$(5,1,2)$	$5d_{5,1,1}$
$(5,2,1)$	$-\frac{(t^2+1)(t^4-522t^3-10006t^2+522t+1)}{2(t^4+228t^3+494t^2-228t+1)}$
$(5,2,2)$	$5d_{5,2,1}$
$(6,1,1)$	D
$(6,2,1)$	D
$(6,3,1)$	$-td_{3,1,1}$
$(6,3,2)$	$3td_{3,1,1}$
$(7,1,1)$	$-\frac{t^{12}-18t^{11}+117t^{10}-354t^9+570t^8-486t^7+273t^6-222t^5+174t^4-46t^3-15t^2+6t+1}{2(t^2-t+1)(t^6-11t^5+30t^4-15t^3-10t^2+5t+1)}$
$(7,1,2)$	$-7d_{7,1,1}$
$(7,2,1)$	$-\frac{t^{12}-522t^{11}-8955t^{10}+37950t^9-70998t^8+131562t^7-253239t^6+316290t^5-218058t^4+80090t^3-14631t^2+510t+1}{2(t^2-t+1)(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)}$
$(7,2,2)$	$-7d_{7,2,1}$
$(7,3,1)$	$\frac{7(t^4-6t^3+17t^2-24t+9)(3t^4-4t^3-5t^2-2t-1)(9t^4-12t^3-t^2+8t-3)}{2(t^2-3t-3)(t^2-t+1)(3t^2-9t+5)(5t^2-t-1)}$
$(7,3,2)$	$-7d_{7,3,1}$

TABLE IV: j-invariants associated to maximal genus zero missing trace groups for $m \leq 7$

(m, i, k)	$d_{m,i,k}$
$(8,1,1)$	$\frac{(t^2+2t-2)(t^2+10t-2)}{(t^2+2)(t^2+8t-2)}$
$(9,1,1)$	D
$(9,2,1)$	D
$(9,3,1)$	D
$(9,4,1)$	D
$(10,1,1)$	$\frac{-2t(t^2-11t-1)(t^4-12t^3+14t^2+12t+1)}{(t^2+1)(t^4-18t^3+74t^2+18t+1)}$
$(10,1,2)$	$5d_{10,1,1}$
$(10,2,1)$	$\frac{-2t(t^2-11t-1)(t^4+228t^3+494t^2-228t+1)}{(t^2+1)(t^4-522t^3-10006t^2+522t+1)}$
$(10,2,2)$	$5d_{10,2,1}$
$(10,3,1)$	D
$(12,1,1)$	$-\frac{3t(t^2-27)(t^2-3)}{t^4-18t^2-27}$
$(12,2,1)$	D
$(12,3,1)$	D
$(12,4,1)$	$\frac{6(27t^2+1)(243t^2+1)}{19683t^4+486t^2-1}$
$(12,4,2)$	$-3d_{12,4,1}$

TABLE V: j-invariants associated to maximal genus zero missing trace groups for $7 < m < 14$

(m,i,k)	$d_{m,i,k}$
$(14,1,1)$	$-\frac{t^{12}-522t^{11}-8955t^{10}+37950t^9-70998t^8+131562t^7-253239t^6+316290t^5-218058t^4+80090t^3-14631t^2+510t+1}{2(t^2-t+1)(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)}$
$(14,1,2)$	$-7d_{7,2,1}$
$(14,2,1)$	$\frac{t^{12}-522t^{11}-8955t^{10}+37950t^9-70998t^8+131562t^7-253239t^6+316290t^5-218058t^4+80090t^3-14631t^2+510t+1}{-2t(t-1)(t^2-t+1)(t^3-8t^2+5t+1)(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)}$
$(14,2,2)$	$-7d_{14,2,1}$
$(14,3,1)$	$\frac{7(t^4-6t^3+17t^2-24t+9)(3t^4-4t^3-5t^2-2t-1)(9t^4-12t^3-t^2+8t-3)}{2(t^2-3t-3)(t^2-t+1)(3t^2-9t+5)(5t^2-t-1)}$
$(14,3,2)$	$-7d_{14,3,1}$
$(14,4,1)$	D
$(14,5,1)$	D
$(14,6,1)$	$f_{14,2}(g_{14,6}(t))$
$(14,6,2)$	$-7d_{14,6,1}$
$(14,7,1)$	$f_{14,2}(g_{14,7}(t))$
$(14,7,2)$	$-7d_{14,7,1}$
$(28,1,1)$	$\frac{-7t(49t^4-13t^2+1)(2401t^4-245t^2+1)}{823543t^8-235298t^6+21609t^4-490t^2-1}$
$(28,2,1)$	$-d_{14,6,1}$
$(28,2,2)$	$-7d_{28,2,1}$
$(28,3,1)$	$-d_{14,7,1}$
$(28,3,2)$	$-7d_{28,3,1}$

TABLE VI: j-invariants associated to maximal genus zero missing trace groups for $m \geq 14$ (see Table I for the definitions of $f_{m,i}(t)$, $g_{m,i}(t)$ and $h_{m,i}(t)$)

CHAPTER 7

CONCLUSION

Serre's open image theorem may be stated as follows: for each number field K and each elliptic curve E defined over K, there is a constant $C_{E,K} > 0$ such that, for each prime $\ell \geq C_{E,K}$, we have $\rho_{E,\ell}(G_K) = GL_2(\mathbb{Z}/\ell\mathbb{Z})$. Serre's uniformity question asks whether the constant $C_{E,K}$ above may be chosen independent of E, i.e. it asks whether, for each number field K there exists a constant C_K such that, for each elliptic curve E defined over K and for each prime $\ell \geq C_K$, we have $\rho_{E,\ell}(G_K) = GL_2(\mathbb{Z}/\ell\mathbb{Z})$. In case $K = \mathbb{Q}$, it is generally believed that Serre's uniformity question has an affirmative answer with $C_{\mathbb{Q}} = 41$. Furthermore, assuming that it does, then as a corollary of (13, Lemma 4.10), we may see that, for any non-CM elliptic curve E over $\mathbb{Q}$, $SL_2\text{-level}(\rho_E(G_{\mathbb{Q}})) \mid \prod_{\ell \leq C_{\mathbb{Q}}} \ell^{\infty}$. This, taken together with Proposition 4.1.1 implies that that

$$G \in \mathfrak{G}_{MT}^{max} \implies GL_2\text{-level}(G) \mid \prod_{\ell \leq C_{\mathbb{Q}}} \ell^{\infty}, \tag{7.1}$$

Recent work establishes vertical bounds on the largest possible n for which ℓ^n divides m_G when $G = \rho_E(G_{\mathbb{Q}})$ when $\ell = 2$ (see (22)) and it is of general interest to establish such vertical bounds for all ℓ; clearly such bounds are relevant to the problem of determining the set $\mathfrak{G}_{MT}^{max}$, even conditionally on an affirmative answer to Serre's uniformity question. In any event, together with the tables of Cummins-Pauli, (Equation 7.1) reduces the determination of $\mathfrak{G}_{MT}^{max}(g)$ to a targeted computer search, for any fixed genus g. It would be interesting to extend the results

in the present paper to $\mathsf{g} = 1$, in the spirit of Sutherland-Zywina, to find all modular curves (or Weierstrass models in case $-\mathrm{I} \notin \mathsf{G}$) that have infinitely many rational points. We leave this to future work.

Vissuet_Kevin_PP1-144.PDF

ORIGINALITY REPORT

10%

SIMILARITY INDEX

PRIMARY SOURCES

1	www.tandfonline.com Internet	462 words — 2%
2	Murty, M.. "On Artin's conjecture", Journal of Number Theory, 198304 Crossref	233 words — 1%
3	epdf.pub Internet	138 words — 1%
4	Zywina, D.. "Elliptic curves with maximal Galois action on their torsion points", Bulletin of the London Mathematical Society, 2010. Crossref	124 words — < 1%
5	Harris B. Daniels, Enrique González-Jiménez. "Serre's Constant of Elliptic Curves Over the Rationals", Experimental Mathematics, 2019 Crossref	89 words — < 1%
6	www.ideals.illinois.edu Internet	70 words — < 1%
7	"Modular Forms and Fermat's Last Theorem", Springer Nature, 1997 Crossref	56 words — < 1%
8	ANDREW V. SUTHERLAND. "COMPUTING IMAGES OF GALOIS REPRESENTATIONS ATTACHED TO ELLIPTIC CURVES", Forum of Mathematics, Sigma, 2016 Crossref	47 words — < 1%

9	Dolan, F.A.. "Conformal partial wave expansions for N=4 chiral four-point functions", Annals of Physics, 200603 Crossref	44 words — < 1%
10	www.journals.cms.math.ca Internet	41 words — < 1%
11	www.researchgate.net Internet	40 words — < 1%
12	"Computational Algebra and Number Theory", Springer Science and Business Media LLC, 1995 Crossref	40 words — < 1%
13	Ayerst, Stephen. "Essays in Macroeconomic Growth.", University of Toronto (Canada), 2020 ProQuest	39 words — < 1%
14	Harris B. Daniels, Álvaro Lozano-Robledo, Filip Najman, Andrew V. Sutherland. "Torsion subgroups of rational elliptic curves over the compositum of all cubic fields", Mathematics of Computation, 2017 Crossref	37 words — < 1%
15	arxiv.org Internet	36 words — < 1%
16	A. C. Cojocaru, M. R. Murty. "Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik?s problem", Mathematische Annalen, 2004 Crossref	35 words — < 1%
17	Abdelkerim, Richard Jo. "Geometry of the Dual Grassmannian", Proquest, 2012. ProQuest	35 words — < 1%
18	Graduate Texts in Mathematics, 2009. Crossref	34 words — < 1%
19	Chris Hall. International Mathematics Research Notices, 2005	34 words — < 1%

Crossref

20	Chang, Zhihua. "Automorphisms and twisted forms of differential lie conformal superalgebras.", Proquest, 2014. ProQuest	33 words	< 1%
21	www.ist-africa.org Internet	29 words	< 1%
22	Yang Zhang. "Factoring and decomposing ore polynomials over F_q (t)", Proceedings of the 2003 international symposium on Symbolic and algebraic computation - ISSAC 03 ISSAC 03, 2003 Crossref	29 words	< 1%
23	L. Magnin. "Determination of 7-Dimensional Indecomposable Nilpotent Complex Lie Algebras by Adjoining a Derivation to 6-Dimensional Lie Algebras", Algebras and Representation Theory, 12/12/2009 Crossref	27 words	< 1%
24	Özkan, Fehmi. "Lévy processes in credit risk and market models", Universität Freiburg, 2002. Publications	27 words	< 1%
25	www.freepatentsonline.com Internet	26 words	< 1%
26	Natalia Garcia-Fritz, Hector Pasten. "Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points", Mathematische Annalen, 2020 Crossref	26 words	< 1%
27	Andrea Bandini, Laura Paladino. "Fields generated by torsion points of elliptic curves", Journal of Number Theory, 2016 Crossref	26 words	< 1%
28	Communications and Control Engineering, 2016. Crossref	25 words	< 1%

29	V. Vatsal. "MULTIPLICATIVE SUBGROUPS OF J 0(N) AND APPLICATIONS TO ELLIPTIC CURVES", Journal of the Institute of Mathematics of Jussieu, 2005 Crossref	24 words — < 1%
30	M. Yang, L. Wang, A.E.A. Almaini. "Fast Conversion for Large Canonical OR-Coincidence Functions", APCCAS 2006 - 2006 IEEE Asia Pacific Conference on Circuits and Systems, 2006 Crossref	22 words — < 1%
31	Liam O'Carroll, Francesc Planas-Vilanova. "Minimal free resolutions of lattice ideals of digraphs", Algebraic Combinatorics, 2018 Crossref	22 words — < 1%
32	drops.dagstuhl.de Internet	21 words — < 1%
33	tel.archives-ouvertes.fr Internet	21 words — < 1%
34	www.mat.uniroma2.it Internet	21 words — < 1%
35	emis.kaist.ac.kr Internet	20 words — < 1%
36	web2.mat.uniroma3.it Internet	19 words — < 1%
37	Morteza H. Bagheri, Kazem Esmailpour, Seyyed Mostafa Hoseinalipour, Arun S. Mujumdar. "Numerical study and POD snapshot analysis of flow characteristics for pulsating turbulent opposing jets", International Journal of Numerical Methods for Heat & Fluid Flow, 2019 Crossref	18 words — < 1%
38	Álvaro Lozano-Robledo. "On the field of definition of $$p$$ -torsion points on elliptic curves over the rationals", Mathematische Annalen, 2013	18 words — < 1%

Crossref

39	www.manchester.ac.uk Internet	16 words — < 1%
40	Krivts, . "Open-Loop Pneumatic Actuating Systems", Pneumatic Actuating Systems for Automatic Equipment Structure and Design, 2006. Crossref	16 words — < 1%
41	mafiadoc.com Internet	16 words — < 1%
42	www.goaegis.com Internet	16 words — < 1%
43	www.security-essen.de Internet	16 words — < 1%
44	Ralph Greenberg. "Iwasawa theory for elliptic curves", Lecture Notes in Mathematics, 1999 Crossref	16 words — < 1%
45	Ebrahim Ebrahim. "The prime spectrum and representation theory of the 2 × 2 reflection equation algebra", Communications in Algebra, 2019 Crossref	16 words — < 1%
46	D. S. Kubert. "Universal Bounds on the Torsion of Elliptic Curves", Proceedings of the London Mathematical Society, 09/01/1976 Crossref	16 words — < 1%
47	B. Mazur. "Modular curves and the eisenstein ideal", Publications mathématiques de l'IHÉS, 1977 Crossref	15 words — < 1%
48	Francesco Pappalardi. International Mathematics Research Notices, 1999 Crossref	14 words — < 1%
49	trace.tennessee.edu Internet	14 words — < 1%

50	www.flsepi.es Internet	13 words — < 1%
51	research.library.mun.ca Internet	13 words — < 1%
52	polen.itu.edu.tr Internet	12 words — < 1%
53	Junmin Liu. "A modified differential evolution algorithm and its application in the training of BP neural network", 2008 IEEE/ASME International Conference on Advanced Intelligent Mechatronics, 07/2008 Crossref	12 words — < 1%
54	Pilar Bayer. "Jean-Pierre Serre: An Overview of His Work", The Abel Prize, 2010 Crossref	10 words — < 1%
55	www.mfo.de Internet	10 words — < 1%
56	Tonny A. Springer, Ferdinand D. Veldkamp. "Octonions, Jordan Algebras and Exceptional Groups", Springer Science and Business Media LLC, 2000 Crossref	10 words — < 1%
57	idoc.pub Internet	10 words — < 1%
58	Xudong Li, Liming Ma, Chaoping Xing. "Optimal locally repairable codes via elliptic curves", IEEE Transactions on Information Theory, 2018 Crossref	10 words — < 1%
59	Jacques Tits, Richard M. Weiss. "Moufang Polygons", Springer Science and Business Media LLC, 2002 Crossref	9 words — < 1%
60	www.sec.gov.qa	

	Internet	9 words — < 1%
61	library.wur.nl Internet	9 words — < 1%
62	L. Foissy. "The infinitesimal Hopf algebra and the poset of planar forests", Journal of Algebraic Combinatorics, 11/28/2008 Crossref	9 words — < 1%
63	J. S. WILSON. "Conjugacy separability of certain Bianchi groups and HNN extensions", Mathematical Proceedings of the Cambridge Philosophical Society, 03/1998 Crossref	9 words — < 1%
64	Ryan, Dani. "Fitness dependent dispersal in intraguild predation communities", Proquest, 2012. ProQuest	9 words — < 1%
65	orca.cf.ac.uk Internet	9 words — < 1%
66	Kelly, . "Free Vibrations of Conservative Systems", Dekker Mechanical Engineering, 2006. Crossref	8 words — < 1%
67	lia.epfl.ch Internet	8 words — < 1%
68	Odasso, C.. "Ergodicity for the stochastic Complex Ginzburg-Landau equations", Annales de l'Institut Henri Poincare / Probabilites et statistiques, 200607/08 Crossref	8 words — < 1%
69	Jiajun Zhang, Zhanjiang Yuan, Tianshou Zhou. "Geometric characteristics of dynamic correlations for combinatorial regulation in gene expression noise", Physical Review E, 2009 Crossref	8 words — < 1%

70	milne.ruc.dk Internet	8 words — < 1%
71	Ramesh Ramachandran, Józef R. Lewandowski, Patrick C. A. van der Wel, Robert G. Griffin. "Multipole-multimode Floquet theory of rotational resonance width experiments: C13–C13 distance measurements in uniformly labeled solids", The Journal of Chemical Physics, 2006 Crossref	8 words — < 1%
72	www.fhwa.dot.gov Internet	8 words — < 1%
73	G.A. Miller. " XIX. ", The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 2009 Crossref	8 words — < 1%
74	Berestovskii, V.. "Covering group theory for topological groups", Topology and its Applications, 20010731 Crossref	8 words — < 1%
75	A. Di Nola, M. Holcapek, G. Jenca. "The category of MV-pairs", Logic Journal of IGPL, 2009 Crossref	8 words — < 1%
76	N. Bel Haj Rhouma, M. Mosbah. "On the Existence of Positive Eigenvalues for Linear and Nonlinear Equations with Indefinite Weight", Applicable Analysis, 2002 Crossref	8 words — < 1%
77	"Chapter 1 Elementary theory of one-parameter semigroups", Springer Science and Business Media LLC, 2007 Crossref	8 words — < 1%
78	Wielogorski, Jerzy W. J.. "Influence of a Dip Plate on the Discharge of Water over a Sharp Crested Rectangular Weir.", University of Surrey (United Kingdom), 2018 ProQuest	8 words — < 1%

79 Hum Chi Tso, Norman J. Morgenstern Horing. "Nonequilibrium Green's-function field equations for the coupled electron-hole-phonon system: A generalization of the shielded-potential approximation", Physical Review B, 1991 — 7 words — < 1%
Crossref

80 Mehmet Koca. "Quaternionic root systems and subgroups of the Aut(F[sub 4])", Journal of Mathematical Physics, 2006 — 7 words — < 1%
Crossref

81 Jan Andres, Lech Górniewicz. "Chapter 3 Application to Differential Equations and Inclusions", Springer Science and Business Media LLC, 2003 — 7 words — < 1%
Crossref

82 Robert C. Vaughan, Trevor D. Wooley. "The asymptotic formula in Waring's problem: Higher order expansions", Journal für die reine und angewandte Mathematik (Crelles Journal), 2018 — 7 words — < 1%
Crossref

83 David Ayala, John Francis. "Poincaré/Koszul Duality", Communications in Mathematical Physics, 2019 — 7 words — < 1%
Crossref

84 Xiangdong Lin, Y. Bar-Shalom, T. Kirubarajan. "Multisensor-multitarget bias estimation for general asynchronous sensors", IEEE Transactions on Aerospace and Electronic Systems, 2005 — 7 words — < 1%
Crossref

85 B. Sarath, K. Varadarajan. "Dual goldie dimension - II", Communications in Algebra, 2007 — 7 words — < 1%
Crossref

86 George E. P. Box, Gwilym M. Jenkins, Gregory C. Reinsel. "Time Series Analysis", Wiley, 2008 — 6 words — < 1%
Crossref

87 Alexei Oblomkov, Zhiwei Yun. "Geometric — 6 words — < 1%

representations of graded and rational Cherednik algebras",
Advances in Mathematics, 2016
Crossref

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		