THE UNIVERSITY OF CHICAGO

MODULI SPACES OF ABELIAN VARIETIES ASSOCIATED TO MOD-P GALOIS REPRESENTATIONS

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY
SHIVA CHIDAMBARAM

CHICAGO, ILLINOIS
JUNE 2021

To Ganesh and my teachers

TABLE OF CONTENTS

LIST OF TABLES

LIST OF SUPPLEMENTARY FILES

All supplementary files are available online as part of the dissertation

1. `CodeRationality.txt`
   Code to study the Galois module $\mathrm{Pic}_{\overline{\mathbb{Q}}}(\mathcal{A}_2(\rho))$.

2. `CodeRationality.out`
   Output file containing data about order in Burnside cokernel, and cohomology of the Galois module $\mathrm{Pic}_{\overline{\mathbb{Q}}}(\mathcal{A}_2(\rho))$.

3. `code_3torsion.txt`
   Code to compute invariants, covariants, contravariants and the new Weierstrass coefficients A, B, C, D.

4. `ABCD.txt`
   The polynomials A, B, C, D giving Weierstrass coefficients of the universal curve over the moduli space $\mathcal{M}_2^w(\rho)$.

5. `ABCDstar.txt`
   Specialisation of the polynomials A^*, B^*, C^*, D^* giving Weierstrass coefficients of the curve over the point $(s : t : u : v) = (1 : 0 : 0 : 0)$ in the moduli space $\mathcal{M}^*_{a,b,c,d}$.

6. `p40.txt`
   The polynomial of degree 240 over $\mathbb{Q}[a, b, c, d]$ described in Section 2.3.1

7. `mat240-and-matstar240.txt`
   The two 240×240 matrices in the computation in Section 2.3.5

ACKNOWLEDGMENTS

I thank my advisor Frank Calegari for his constant guidance and unwavering support throughout my graduate study. I am grateful to him for the confidence he showed in me during long periods of slow progress. His enthusiasm for mathematics, computation, chess and most things in life is inspiring. I thank him for teaching me a lot of beautiful mathematics.

I thank Matt Emerton for serving as my secondary advisor and for his wonderful seminars and courses on automorphic forms and Langlands program. His insight and the clarity of his explanations make his lectures extremely enjoyable.

My gratitude also goes to my collaborators Dave Roberts and Alexandru Ghitza. I especially thank Dave for conversations that helped straighten my thoughts. He set the ball rolling on our project and was instrumental in writing up the paper quickly when we were working on a close deadline.

I want to thank my cohort-mates and friends in the department for being great comrades. Thanks to Claudio Gonzales, Dylan Quintana, Duc Ho, Weinan Lin, Mariya Sardarli, Ronno Das, Santiago Chavez Aguilar, Karl Schaefer, Tung Nguyen. Special thanks to Eric Stubley and Noah Taylor for our mathematical discussions, and for their resourcefulness and initiative in organizing learning seminars. I also want to thank all the speakers and participants of No Theory seminar which I have consistently enjoyed.

I thank Sarah Ziesler, Tim Black, John Boller and Jitka Stehnova for helping me in my teaching. I also want to thank Joe Lampert from the Chicago Center for Teaching for an excellent course in pedagogy. The projects provided a great avenue to share perspectives and I greatly enjoyed the discussions with Dylan Quintana and Murphykate Montee.

My friends from other departments in the University have been a great source of support and joy. I thank Krithika Mohan, Soudeep Deb, Debsouri Kundu, Preeti Poddar, Upasana Dutta, Sanjukta Poddar and Shubham Shivang. They have been good friends and have helped me grow in various ways. I also want to thank my dear friends Kavya Smitha Pillai, Abhirup Guha, Shankar Menon, Chaitra Agrahar, Poojya Ravishankar, Mihir Kulkarni and

Sainath Gupta whose company and support were vital in navigating the pandemic.

I thank my parents for their love and unwavering belief in me. Their dedication to my education is beyond words. Thanks also to my brother whose support has been key to living far away from home with little worry. Finally, I want to thank Hemalatha Thiagarajan for firmly believing in me and giving me the crucial push to mathematics, when I had only started to feel its beautiful contours.

ABSTRACT

This thesis consists of four research papers stapled together. In this work, we study moduli spaces of principally polarised abelian varieties of dimension $g > 1$ with p-torsion structure for prime p. In particular, given a Galois representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GSp}(2g, \mathbf{F}_p)$ with cyclotomic similitude character, we study various rationality aspects of the twist $\mathcal{A}_g(\overline{\rho})$ of the Siegel modular variety $\mathcal{A}_g(p)$ of genus g and level p.

Using a description of the cohomology of the compactification $\mathcal{A}_2^*(3)$ given by Hoffman and Weintraub, we show that the variety $\mathcal{A}_2(\overline{\rho})$ is not rational in general (Theorem 1.1.1). When $\overline{\rho}$ is surjective, the minimal degree of a rational cover is 6 (Theorem 1.1.2). Boxer, Calegari, Gee and Pilloni have shown the existence of a rational cover $\mathcal{A}_2^w(\overline{\rho})$ of degree 6. We find explicit formulae parametrizing the pullback $\mathcal{M}_2^w(\overline{\rho})$ of $\mathcal{A}_2^w(\overline{\rho})$ under the Torelli map $\mathcal{M}_2 \to \mathcal{A}_2$ (Theorem 2.3.1). This describes the universal family of genus 2 curves with a rational Weierstrass point, having fixed 3-torsion of Jacobian. This exploits Shioda's work on Mordell-Weil lattices and the invariant theory of the complex reflection group $C_3 \times \mathrm{Sp}_4(\mathbf{F}_3)$. We also outline how similar results can be obtained for $(g, p) = (2, 2), (3, 2), (4, 2)$.

By making use of the modularity lifting theorem for abelian surfaces proved by Boxer, Calegari, Gee and Pilloni, we produce some explicit examples of modular abelian surfaces A with $\mathrm{End}_{\mathbf{C}}(A) = \mathbf{Z}$ (Theorems 3.3.1, 3.3.2). Using the explicit formulae describing families of abelian surfaces with fixed 3-torsion, and transferring modularity in the family yields infinitely many such examples (Corollary 2.4.1).

When $g = 1$ and $p > 5$, the existence of mod-p Galois representations not arising from elliptic curves over $\mathbf{Q}$ is known. For $g > 1$ and $(g, p) \neq (2, 2), (2, 3), (3, 2)$, we investigate a local obstruction to the existence of rational points on $\mathcal{A}_g(\overline{\rho})$, and thus construct Galois representations $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GSp}(2g, \mathbf{F}_p)$ with cyclotomic similitude character, that do not arise from the p-torsion of any g-dimensional abelian variety over $\mathbf{Q}$ (Theorem 4.1.1). This is accomplished by solving embedding problems with local conditions at suitably chosen auxiliary primes $l \neq p$, with the help of Galois cohomological machinery.

CHAPTER 1

RATIONALITY OF TWISTS OF THE SIEGEL MODULAR VARIETY OF GENUS 2 AND LEVEL 3

1.1 Introduction

Let p be a prime and suppose that $A/\mathbf{Q}$ is an abelian variety of dimension g with a polarization of degree prime to p. Associated to the action of the absolute Galois group $G_{\mathbf{Q}}$ on $A[p]$ there exists a Galois representation

$$\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GSp}_{2g}(\mathbf{F}_p)$$

such that the corresponding similitude character is the mod-p cyclotomic character ε. One can ask, conversely, whether any such representation comes from an abelian variety in infinitely many ways. When $g = 1$, this question is well-studied, and has a positive answer exactly for $p = 2$, 3, and 5. Indeed, the corresponding twists $X(\overline{\rho})$ of the modular curve $X(p)$ are rational over $\mathbf{Q}$ for $p = 2$, 3, and 5, and have higher genus for larger p.

In [7], this question arose for abelian surfaces ($g = 2$) when $p = 3$. (The case $p = 2$, which is also discussed in that paper, is understood by analyzing the branch points of the hyperelliptic involution.) Let $\mathcal{A}_2(3)$ denote the Siegel modular variety of genus 2 and level 3. It is the moduli space of principally polarized abelian surfaces together with a symplectic isomorphism $A[3] \simeq (\mathbf{Z}/3\mathbf{Z})^2 \oplus (\mu_3)^2$. Given a $\overline{\rho}$ as above, one can form the corresponding moduli space $\mathcal{A}_2(\overline{\rho})$ where now one insists that there is a symplectic isomorphism $A[3] \simeq V$, where V is the representation space of $\overline{\rho}$ with its symplectic structure. The variety $\mathcal{A}_2(3)$ is well-known to be birational to the Burkhardt quartic, which is rational over $\mathbf{Q}$ ([9]). It is clear that $\mathcal{A}_2(\overline{\rho})$ is isomorphic to $\mathcal{A}_2(3)$ over $\mathbf{C}$ (and even over the fixed field of the kernel of $\overline{\rho}$), and hence $\mathcal{A}_2(\overline{\rho})$ is *geometrically* rational. If $\mathcal{A}_2(\overline{\rho})$ was in fact *rational* (by which we always mean rational over the base field), then indeed the answer to the question above

would be positive, just as for elliptic curves when $p \leq 5$. In [7, Prop 10.2.3], a weaker result was established: The variety $\mathcal{A}_2(\overline{\rho})$ is unirational over $\mathbf{Q}$ via a map of degree at most 6. As a consequence, any such $\overline{\rho}$ *does* arise from (infinitely many) abelian surfaces. We refer the reader to [15] which produces explicit polynomials describing the universal family over a rational cover of $\mathcal{A}_2(\overline{\rho})$ of degree 6. However, the question as to whether $\mathcal{A}_2(\overline{\rho})$ was actually rational was left open. We address this question here.

Theorem 1.1.1. *Let $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GSp}_4(\mathbf{F}_3)$ be a representation with cyclotomic similitude character. Suppose that the order of $\mathrm{im}(\overline{\rho})$ is greater than 96. Then $\mathcal{A}_2(\overline{\rho})$ is not rational over $\mathbf{Q}$.*

More refined results can be extracted directly from Table 1.2 in §1.3. Since $\overline{\rho}$ has cyclotomic similitude character, the restriction of $\overline{\rho}$ to G_E, where $E = \mathbf{Q}(\sqrt{-3})$, has image contained in $\mathrm{Sp}_4(\mathbf{F}_3)$. If we let H denote the projection of $\mathrm{im}(\overline{\rho}|_{G_E})$ to the simple group $\mathrm{PSp}_4(\mathbf{F}_3)$, then we prove that $\mathcal{A}_2(\overline{\rho})$ is not rational over $\mathbf{Q}$ for all but 26 of the 116 conjugacy classes of subgroups of $\mathrm{PSp}_4(\mathbf{F}_3)$. With the exception of three cases (including when H is trivial) where the methods of [9] may be applied (see §1.2.3), we do not know what happens in the remaining 23 cases, nor do we even know whether the rationality of $\mathcal{A}_2(\overline{\rho})$ depends only on $\mathrm{im}(\overline{\rho})$ or not. One easy remark is that, for a quadratic character χ, there is an isomorphism $\mathcal{A}_2(\overline{\rho}) \simeq \mathcal{A}_2(\overline{\rho} \otimes \chi)$, and so the rationality of $\mathcal{A}_2(\overline{\rho})$ depends only on the image of $\overline{\rho}$ in $\mathrm{PGSp}_4(\mathbf{F}_3)$.

The case of a surjective representation $\overline{\rho}$ is of special interest, since this is what happens generically for the three-torsion Galois representations of abelian surfaces.

Theorem 1.1.2. *Suppose that $\overline{\rho}$ is surjective. Then $\mathcal{A}_2(\overline{\rho})$ is not rational over $\mathbf{Q}$, and the minimal degree of any rational cover is 6.*

In light of the result [7, Prop 10.2.3] mentioned above, the constant 6 is best possible in this case.

The key ingredient in our results is the explicit description of the cohomology of the compactified Siegel modular variety $\mathcal{A}_2^*(3)$ given in [23]. We use it to study the Galois module $\mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(\overline{\rho}))$. The Galois action over $E = \mathbf{Q}(\sqrt{-3})$ factors through the projectivization of $\overline{\rho}$ turning it into a H-module. We then calculate group cohomology of this module for various subgroups $P \subset H$, and employ a necessary criterion for rationality (see Theorem 1.2.1) to deduce our results.

1.1.1 Acknowledgments

We thank Jason Starr and Yuri Tschinkel for discussions about rationality versus geometric rationality for smooth varieties over number fields, Steven Weintraub for a suggestion on how to explicitly extract a description of $H^2(\mathcal{A}_2^*(3), \mathbf{Z})$ as a $G = \mathrm{PSp}_4(\mathbf{F}_3)$-module from Theorem 4.9 of [23], and Mark Watkins with help using `Magma`. We thank the anonymous referees for useful comments and corrections, and we also thank Nils Bruin for explaining to us many of the ideas in section 1.2.3.

1.2 Strategy

The main idea behind the proof is to follow a strategy employed by Manin for cubic surfaces. Recall [28, §A.1] that a continuous G_K-module with the discrete topology is called a *permutation module* if it admits a finite free $\mathbf{Z}$-basis on which G_K acts (via a finite quotient) via permutations, and that two G_K-modules M and N are *similar* if $M \oplus P \simeq N \oplus Q$ for some permutation modules P and Q. In particular, we employ the following theorem.

Theorem 1.2.1. *[28, §A.1 Theorem 2] Let Z be a smooth projective algebraic variety over a number field K. Suppose that Z is rational over K. Then $\mathrm{Pic}_{\overline{K}} Z$ as a G_K-module is stably permutation. In other words, it is similar to the zero module.*

The Shimura variety $\mathcal{A}_2(3)$ admits a smooth toroidal projective compactification $\mathcal{A}_2^*(3)$, the (canonical) toroidal compactification constructed by Igusa [26]. The automorphism group

of $\mathcal{A}_2^*(3)$ over $\overline{\mathbf{Q}}$ is the group $G = \mathrm{PSp}_4(\mathbf{F}_3)$, the simple group of order 25920, which acts over the field $E = \mathbf{Q}(\sqrt{-3})$. It will be convenient from this point onwards to always work over the field E. (Certainly rationality over $\mathbf{Q}$ implies rationality over E, so non-rationality over E implies non-rationality over $\mathbf{Q}$.) This action on $\mathcal{A}_2(3)$ arises explicitly from the action of G on the 3-torsion $A[3] = (\mathbf{Z}/3\mathbf{Z})^2 \oplus (\mu_3)^2 \simeq (\mathbf{Z}/3\mathbf{Z})^4$ over E. We will apply Theorem 1.2.1 to the corresponding twist $\mathcal{A}_2^*(\overline{\rho})$. We then make crucial use of very explicit description of the cohomology of this compactification given by Hoffman and Weintraub [23]. We recall some facts from that paper here now.

1.2.1 Picard group

The Picard group of $\mathcal{A}_2^*(3)$ over $\overline{\mathbf{Q}}$ is a free $\mathbf{Z}$-module of rank 61. It is generated by two natural sets of classes. The first is a 40-dimensional space explained by the 40 connected components of the boundary. The second is a 45-dimensional space explained by divisors coming from Humbert surfaces. These are also in one to one correspondence with the 45 nodes on the Burkhardt quartic. Together, these generate the Picard group of $\mathcal{A}_2^*(3)$ over $\overline{\mathbf{Q}}$, which is free of rank 61. Indeed, the Betti cohomology of $\mathcal{A}_2^*(3)$ over $\mathbf{Z}$ is free of degrees $1, 0, 61, 0, 61, 0, 1$ for $i = 0, \ldots 6$ by [23, Theorem 1.1]. Furthermore, all of these classes are trivial under the action of G_E.

Let $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GSp}_4(\mathbf{F}_3)$ be a continuous Galois representation with cyclotomic similitude character. The assumption on the similitude character implies that the restriction of $\overline{\rho}$ to E is valued in $\mathrm{Sp}_4(\mathbf{F}_3)$. Let

$$\varrho : G_E \to G = \mathrm{PSp}_4(\mathbf{F}_3)$$

denote the projectivization of the representation $\overline{\rho}$ restricted to E. The group G acts over E on $\mathcal{A}_2^*(3)$ via automorphisms, and $\mathcal{A}_2^*(\overline{\rho})$ is the twist of $\mathcal{A}_2^*(3)$ by ϱ. The group $\mathrm{Pic}_{\overline{\mathbf{Q}}} \mathcal{A}_2^*(\overline{\rho})$ as a G_E-module is obtained by considering $\mathrm{Pic}_{\overline{\mathbf{Q}}} \mathcal{A}_2^*(3)$ as a G-module and then obtaining the Galois action via the map $\varrho : G_E \to G$. Thus it remains to closely examine $\mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(3))$

as a G-module over $\mathbf{Z}$. In fact, we can quickly prove a weaker version of Theorem 1.1.2 by studying this G-module over $\mathbf{Q}$. The group G admits a unique conjugacy class G_{45} of subgroups of index 45, but two conjugacy classes of index 40; let G_{40} denote the (conjugacy class of) subgroups which fix a point in the tautological action of $G \subset \mathrm{PGL}_4(\mathbf{F}_3)$ on $\mathbf{P}^3(\mathbf{F}_3)$. The following is an easy consequence of the calculations of [23] (and is also confirmed by our `Magma` code).

Lemma 1.2.1. *As $\mathbf{Q}[G]$-modules, there is an equality of virtual representations*

$$H^2(\mathcal{A}_2^*(3), \mathbf{Q}) \simeq \mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(3)) \otimes \mathbf{Q} = \mathbf{Q}[G/G_{40}] + \mathbf{Q}[G/G_{45}] - [\chi_{24}],$$

where $\chi_{24} \otimes_{\mathbf{Q}} \mathbf{C}$ is the unique absolutely irreducible 24-dimensional representation of G.

Now, assuming that ϱ is *surjective*, we can prove that $\mathcal{A}_2^*(\overline{\rho})$ is not rational simply by proving that χ_{24} is not virtually equal to a sum of permutation representations. If $R_{\mathbf{Q}}(G)$ denotes the representation ring of G, this is equivalent to proving that $\chi_{24} \in R_{\mathbf{Q}}(G)$ does not lie in the Burnside subring generated by permutation representations. But one may compute (using `Magma` or otherwise) that the Burnside cokernel of G has order 2 and is generated by χ_{24}. This proves a weaker version of Theorem 1.1.2 showing that any rational cover of $\mathcal{A}_2(\overline{\rho})$ should have degree at least 2, although it is softer in that it only needs the $\mathbf{Q}[G]$-representation rather than the $\mathbf{Z}[G]$-module. This argument also applies if one only assumes that the image of ϱ is $H \subset G$, as long as the restriction of χ_{24} to H is still non-trivial in the Burnside cokernel, which it is for precisely 8 of the 116 conjugacy classes of subgroups of G.

1.2.2 Cohomological Obstructions

From now on, we let H denote the image of $\varrho : G_E \to G = \mathrm{PSp}_4(\mathbf{F}_3)$. A second way to prove that a Galois module is not similar to the zero module is to use cohomology. If M is a permutation module of H, then the restriction of M to any subgroup P is also a permutation

module, and thus a direct sum of P-modules of the form $\mathbf{Z}[P/Q]$ for subgroups Q of P. (Note that since a permutation module of a group G arises from a finite G-set, it always decomposes over $\mathbf{Z}$ into a direct sum of such irreducible permutation modules.) Then, Shapiro's Lemma implies that $H^1(P, M)$ is a direct sum of groups of the form

$$H^1(P, \mathbf{Z}[P/Q]) = H^1(Q, \mathbf{Z}) = 0,$$

where the second group vanishes because Q is finite. Moreover, the $\mathbf{Z}$-dual $M^\vee = \mathrm{Hom}(M, \mathbf{Z})$ of a permutation module is isomorphic to the same permutation module (a permutation matrix is its own inverse transpose). Thus one immediately has the following elementary criterion.

Lemma 1.2.2 (Cohomological Criterion for non-rationality)**.** *Let M denote the G-module* $\mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(3))$. *Suppose $\mathcal{A}_2^*(\overline{\rho})$ is rational over $E = \mathbf{Q}(\sqrt{-3})$, and $\varrho|_{G_E}$ has image $H \subset G$. Then*

$$H^1(P, M^\vee) = H^1(P, M) = 0$$

for every subgroup $P \subset H$.

We note that this is not an "if and only if" criterion. In the language of [18], the lemma is saying that M as a G_E-module is *flasque* and *coflasque* respectively. In general, this is weaker than being stably permutation (which itself is not enough to formally imply rationality).

In order to test this criterion in practice, we need an explicit description of M as a $\mathbf{Z}[G]$-module rather than a $\mathbf{Q}[G]$-module. In order to do this, we explain how an explicit description of M can be extracted from Theorem 4.9 of [23]. That theorem describes a set of elements which generate both $H_4(\mathcal{A}_2^*(3), \mathbf{Z})$ and $H^2(\mathcal{A}_2^*(3), \mathbf{Z})$, and explicitly gives the intersection pairing between them. Moreover, the basis comes with a transparent action of the group G. Specifically, $H^2(\mathcal{A}_2^*(3), \mathbf{Z})$ is given as a quotient of $\mathbf{Z}[G/G_{40}] \oplus \mathbf{Z}[G/G_{45}]$. Hence to compute $H^2(\mathcal{A}_2^*(3), \mathbf{Z})$ as a G-module, it suffices to compute the quotient of $\mathbf{Z}[G/G_{40}] \oplus \mathbf{Z}[G/G_{45}]$ by the saturated subspace which pairs trivially with all elements of $H_4(\mathcal{A}_2^*(3), \mathbf{Z})$. Having

carried out this computation, we obtain a free abelian group of rank 61 with an explicit action of G. We then do the following for every conjugacy class of subgroups $H \subset G$.

1. Determine whether χ_{24} is non-trivial in the Burnside cokernel of H.
2. Determine whether $H^1(P, M) \neq 0$ for any subgroup $P \subset H$.
3. Determine whether $H^1(P, M^\vee) \neq 0$ for any subgroup $P \subset H$.

If any of these is non-trivial, this proves that $\mathcal{A}_2^*(\overline{\rho})$ is not rational. Moreover, the computation of these cohomology groups allows us to deduce our result about the minimal degree of any rational covering.

Lemma 1.2.3. *Let M denote the G-module $\mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(3))$. Suppose $\varrho|_{G_E}$ has image $H \subset G$. Let n denote the least common multiple of the exponents of $H^1(P, M)$ and $H^1(P, M^\vee)$ as P varies over all subgroups of H. Suppose $f : X \to \mathcal{A}_2^*(\overline{\rho})$ is a rational cover of degree d defined over $\mathbf{Q}$. Then n divides d.*

Proof. The induced pullback map $f^* : \mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(\overline{\rho})) \to \mathrm{Pic}_{\overline{\mathbf{Q}}}(X)$ and pushforward map $f_* : \mathrm{Pic}_{\overline{\mathbf{Q}}}(X) \to \mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(\overline{\rho}))$ are Galois equivariant since f is defined over $\mathbf{Q}$. The composite map $g = f_* \circ f^*$ on $\mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(\overline{\rho}))$ is multiplication by d. The discussion in §1.2.1 shows that the G_E-module $\mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(\overline{\rho}))$ can be thought of as the H-module M.

By Theorem 1.2.1, we know that $\mathrm{Pic}_{\overline{\mathbf{Q}}}(X)$ is stably permutation as a Galois module and hence the Galois cohomology group $H^1(G_{\mathbf{Q}}, \mathrm{Pic}_{\overline{\mathbf{Q}}}(X)) = 0$. Therefore, the maps induced by g on the cohomology groups $H^1(P, M)$ and $H^1(P, M^\vee)$ are the zero maps for every subgroup $P \subset H$. Since the map g is multiplication by d, the induced map on cohomology is also multiplication by d, and hence we deduce that the exponent of each of these cohomology groups divides d. □

We give one final statement which can be extracted from the `Magma` code given in the supplementary file `CodeRationality.txt`, but not directly from Table 1.2. In order to

represent elements of $G = \mathrm{PSp}_4(\mathbf{F}_3)$ by matrices, we follow the conventions of `Magma` by fixing $\mathrm{Sp}_4(\mathbf{F}_3) \subset \mathrm{GL}_4(\mathbf{F}_3)$ to be the matrices preserving the symplectic form

$$J = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Lemma 1.2.4. *Suppose that the image of $\overline{\rho}$ contains an element conjugate in $\mathrm{PSp}_4(\mathbf{F}_3)$ to*

$$\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $\mathcal{A}_2(\overline{\rho})$ is not rational, and the minimal degree of any rational cover is divisible by 3.

Proof. It suffices to note that this element generates the subgroup labelled as subgroup 6 in Table 1.2 below, and then to apply Lemma 1.2.3. □

1.2.3 Other cases where rationality can be established

The analysis of Baker's parametrization [1] undertaken in [9, §4] allows one to deduce the rationality of certain twists of the Burkhardt quartic B (and hence of $\mathcal{A}_2(\overline{\rho})$) in a few more cases. (We thank Nils Bruin for pointing this out to us, as well as explaining the geometric construction below.) The rational parametrization $\mathbf{P}^3 \dashrightarrow B$ over $\mathbf{Q}$ constructed in [9] is not equivariant with respect the action of $\mathrm{PSp}_4(\mathbf{F}_3)$. If it were, then the twists $\mathcal{A}_2(\overline{\rho})$ we are considering would all be birational to Brauer–Severi varieties. However, because they are also unirational over $\mathbf{Q}$ by [7, Prop 10.2.3], they would be rational over $\mathbf{Q}$, which we prove in this paper to be false in general. On the other hand, the parametrization $\mathbf{P}^3 \dashrightarrow B$ *is*

equivariant with respect to the (unique up to conjugacy) cyclic group of order 9 [9, §4.3], and also the corresponding group scheme over $\mathbf{Q}$ whose E points are this group of order 9 (c.f. [15, §2.3]), which controls the descent from E to $\mathbf{Q}$. In particular, the same argument implies that $\mathcal{A}_2(\overline{\rho})$ is rational in two further cases, namely, the subgroups labelled $n = 4$ (of order 3) and $n = 24$ (of order 9) in Table 1.2 below. One can also arrive at this rational parametrization more geometrically, following [9, §4], whose notation we now freely follow. The variety of lines L_{J_1,J_2,J_3} incident with 3-distinct planes $J_i \subset \mathbf{P}^4$ is geometrically rational. If these planes are mutually skew and lie on B, there is a dominant map $L_{J_1,J_2,J_3} \dashrightarrow B$ defined by noting that a line will generically intersect B in four points and each J_i in one point, and hence one can send the line to the fourth point of intersection with B. There are 40 Jacobi planes J_i on B, and 2880 triples of mutually skew such planes. The stabilizer under $\mathrm{PSp}_4(\mathbf{F}_3)$ on these 2880 triples is the cyclic group of order 9. The assumption that H is contained inside this group then implies that there exists a triple of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-invariant mutually skew planes on the twist of B corresponding to $\overline{\rho}$. The result then follows after noting that L_{J_1,J_2,J_3} is rational over $\mathbf{Q}$ whenever this triple is defined over $\mathbf{Q}$. (We omit a direct proof of this last claim in light of the alternate argument given above.)

1.3 Computation

Let M denote the G-module $\mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(3)) \simeq H^2(\mathcal{A}_2^*(3), \mathbf{Z})$. We have, by Poincaré duality, an isomorphism $M^\vee = H^4(\mathcal{A}_2^*(3), \mathbf{Z})$, Below we present in Table 1.2 the result of our computation for all 116 conjugacy classes of subgroups $H \subset G$, indicating the following data:

1. An ordering $n = 1 \ldots 116$ of the conjugacy class of the subgroup H as determined by `Magma`.

2. The group H in the small groups database [3]. The first element of the pair gives the order of H.

3. The order of M in the Burnside cokernel of H over $\mathbf{Q}$ (if it is non-trivial). If this is

greater than 1, then the corresponding twist is not rational over E (or $\mathbf{Q}$).

4. The least common multiple of the exponents of $H^1(P, M)$ and $H^1(P, M^\vee)$ as P ranges over subgroups $P \subset H$. If this is greater than 1, then the corresponding twist is not rational over E (or $\mathbf{Q}$). In particular, the fact that this number is 6 for G itself proves Theorem 1.1.2.

5. The pre-image of H in $\mathrm{Sp}_4(\mathbf{F}_3)$ acts on $\mathbf{F}_3^4$. Is this action absolutely irreducible? (That is, is the action on $\overline{\mathbf{F}}_3^4$ irreducible.)

6. A list of the conjugacy class of maximal subgroups of H (as indexed in the table). This allows one to compute the LCM column directly. The table is separated into blocks to reflect the geometry of the corresponding poset of subgroups. In particular, all maximal subgroups of H occur in blocks before that of H.

7. The last two columns give $H^1(H, M)$ and $H^1(H, M^\vee)$.

One must be careful while reading Table 1.2 because the ordering of the conjugacy classes of subgroups is not evident. The Small Group tag and the indices of the maximal subgroups given in the second and sixth columns of the table do determine the ordering uniquely once we distinguish between the conjugacy classes indexed by $n = 2, 3$, $n = 4, 5, 6$, $n = 9, 11$ and $n = 10, 12$. This can be done by considering the length of each of these conjugacy classes (i.e., the number of subgroups in each conjugacy class) as shown in Table 1.1.

n	Length
2	45
3	270
4	40
5	120
6	240

n	Length
9	270
11	405
10	270
12	540

Table 1.1: Distinguishing conjugacy classes of subgroups of $\mathrm{PSp}_4(\mathbf{F}_3)$ based on length.

The `Magma` code in the supplementary file `CodeRationality.txt` computes G and M directly from the description given by Hoffman and Weintraub [23]. This leads to a representation of G as generated by two sparse 61×61 matrices x and y in $\mathrm{GL}_{61}(\mathbf{Z})$ such that the underlying module on which G acts (on the right, by `Magma` conventions) is M. The matrices x and y are also printed in the output file `CodeRationality.out` of our `Magma` script.

n	SmallGroup	B	LCM	irred	maximal subgroups	$H^1(M)$	$H^1(M^\vee)$
1	<1,1>		1	no			
2	<2,1>		1	no	1		
3	<2,1>		1	no	1		
4	<3,1>		1	no	1		
5	<3,1>		1	no	1		
6	<3,1>		3	no	1	$\mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/3\mathbf{Z}$
7	<5,1>		1	no	1		
8	<4,1>		1	no	2		
9	<4,2>		1	no	2 3		
10	<4,2>		2	no	3		$(\mathbf{Z}/2\mathbf{Z})^2$
11	<4,2>		2	no	2 3		$\mathbf{Z}/2\mathbf{Z}$
12	<4,2>		1	no	3		
13	<4,1>		1	no	3		
14	<6,1>		3	no	2 6	$\mathbf{Z}/3\mathbf{Z}$	
15	<6,2>		1	no	2 4		
16	<6,2>		3	no	2 6		
17	<6,1>		3	no	3 6		$\mathbf{Z}/3\mathbf{Z}$
18	<6,1>		1	no	3 5		
19	<6,2>		1	no	2 5		
20	<6,2>		1	no	3 5		
21	<9,2>		3	no	5 6		$(\mathbf{Z}/3\mathbf{Z})^2$
22	<9,2>		3	no	4 6		$(\mathbf{Z}/3\mathbf{Z})^2$
23	<9,2>		3	no	4 5 6		
24	<9,1>		1	no	4		
25	<10,1>		1	no	3 7		
26	<8,4>		1	no	8		
27	<8,5>		2	no	11 12		$(\mathbf{Z}/2\mathbf{Z})^2$
28	<8,5>		2	no	10 11		$(\mathbf{Z}/2\mathbf{Z})^2$

Table 1.2: Subgroup lattice structure of $G = \mathrm{PSp}_4(\mathbf{F}_3)$ and computational results for the G-module $M = \mathrm{Pic}_{\overline{\mathbf{Q}}}(\mathcal{A}_2^*(3))$: order in Burnside cokernel; cohomological data.

n	SmallGroup	B	LCM	irred	maximal subgroups	$H^1(M)$	$H^1(M^\vee)$
29	<8,5>		2	no	9 10 11		
30	<8,2>		2	no	8 11		
31	<8,2>		2	no	11 13	$\mathbf{Z}/2\mathbf{Z}$	$\mathbf{Z}/2\mathbf{Z}$
32	<8,3>		2	no	8 11		$\mathbf{Z}/2\mathbf{Z}$
33	<8,3>		2	no	10 12 13		$\mathbf{Z}/2\mathbf{Z}$
34	<8,3>		1	no	9 12 13		
35	<12,3>		2	no	5 10		
36	<12,3>		3	no	6 12	$\mathbf{Z}/3\mathbf{Z}$	$\mathbf{Z}/3\mathbf{Z}$
37	<12,4>		3	no	9 14 16 17		
38	<12,5>		1	no	9 19 20		
39	<12,1>		1	no	13 20		
40	<12,2>		1	no	8 15		
41	<12,4>		1	no	12 18 20		
42	<18,4>		3	no	17 18 21		$(\mathbf{Z}/3\mathbf{Z})^2$
43	<18,3>		3	no	14 16 21		
44	<18,3>		3	no	14 19 23		
45	<18,3>		3	no	14 15 22		
46	<18,3>		3	no	18 20 21		$\mathbf{Z}/3\mathbf{Z}$
47	<18,3>		3	no	17 20 23		
48	<18,5>		3	no	15 16 19 23		
49	<20,3>		1	yes	13 25		
50	<27,5>		3	no	21 22 23		$\mathbf{Z}/3\mathbf{Z}$
51	<27,3>		3	no	22		$(\mathbf{Z}/3\mathbf{Z})^2$
52	<27,4>		3	no	22 24		$\mathbf{Z}/3\mathbf{Z}$
53	<16,14>		2	yes	28 29		
54	<16,13>		2	no	26 30 32		
55	<16,11>		2	yes	27 28 30 32		$\mathbf{Z}/2\mathbf{Z}$
56	<16,3>		2	no	28 31		$(\mathbf{Z}/2\mathbf{Z})^2$
57	<16,11>		2	yes	27 29 31 33 34		$\mathbf{Z}/2\mathbf{Z}$
58	<16,3>		2	no	29 30 31		
59	<24,3>		1	no	15 26		
60	<24,13>		2	no	20 29 35		
61	<24,3>		3	no	16 26		
62	<24,3>		1	no	19 26		
63	<24,11>	2	1	no	26 40		
64	<24,13>		2	no	19 28 35		
65	<24,13>		6	no	16 27 36		
66	<24,12>		2	no	18 33 35		
67	<24,12>		6	no	17 33 36		$\mathbf{Z}/6\mathbf{Z}$

Table 1.2 continued

n	SmallGroup	B	LCM	irred	maximal subgroups	$H^1(M)$	$H^1(M^\vee)$
68	<24,12>		3	no	14 34 36	$\mathbf{Z}/3\mathbf{Z}$	
69	<24,8>		1	no	34 38 39 41		
70	<36,10>		3	no	37 42 43		
71	<36,10>		3	no	41 42 46		$\mathbf{Z}/3\mathbf{Z}$
72	<36,9>		3	no	13 42		$\mathbf{Z}/3\mathbf{Z}$
73	<36,12>		3	no	37 38 44 47 48		
74	<54,8>		3	no	45 51		
75	<54,13>		3	no	42 46 47 50		$\mathbf{Z}/3\mathbf{Z}$
76	<54,12>		3	no	43 44 45 48 50		
77	<60,5>		2	no	18 25 35		
78	<60,5>		3	no	17 25 36		$\mathbf{Z}/3\mathbf{Z}$
79	<81,7>		3	no	50 51 52		$\mathbf{Z}/3\mathbf{Z}$
80	<32,49>		2	no	54 56		
81	<32,6>		2	yes	55 56		$\mathbf{Z}/2\mathbf{Z}$
82	<32,27>		2	yes	53 55 56 57 58		
83	<48,30>		2	no	39 58 60		
84	<48,49>		2	yes	38 53 60 64		
85	<48,33>		2	yes	40 54 59		
86	<48,48>		2	no	41 57 60 66		$\mathbf{Z}/2\mathbf{Z}$
87	<48,48>		6	yes	37 57 65 67 68		
88	<72,40>		3	no	34 70 71 72		
89	<72,25>	2	3	no	48 59 61 62 63		
90	<80,49>		2	yes	7 53		
91	<108,40>		3	no	71 75		$\mathbf{Z}/3\mathbf{Z}$
92	<108,15>		3	no	40 74		
93	<108,38>		3	no	70 73 75 76		
94	<108,37>		3	no	39 72 75		
95	<120,34>		3	yes	37 49 68 78		
96	<120,34>		2	yes	41 49 66 77		
97	<162,10>		3	no	74 76 79		
98	<64,138>		2	yes	80 81 82		
99	<96,204>		2	no	62 64 80		
100	<96,204>		6	no	61 65 80		
101	<96,201>	2	2	no	63 80 85		
102	<96,195>		2	yes	69 82 83 84 86		
103	<160,234>		2	yes	25 82 90		
104	<216,88>	2	3	no	63 92		
105	<216,158>		3	no	69 88 91 93 94		
106	<324,160>		3	no	36 79 91		$\mathbf{Z}/3\mathbf{Z}$

Table 1.2 continued

n	SmallGroup	B	LCM	irred	maximal subgroups	$H^1(M)$	$H^1(M^\vee)$
107	<360,118>		6	no	66 67 72 77 78		$\mathbf{Z}/3\mathbf{Z}$
108	<192,1493>		6	yes	87 98 100		
109	<192,201>		2	yes	84 98 99		
110	<288,860>	2	6	no	89 99 100 101		
111	<648,533>	2	3	no	89 97 104		
112	<648,704>		3	no	68 97 105 106		
113	<720,763>		6	yes	86 87 88 95 96 107		
114	<576,8277>	2	6	yes	73 108 109 110		
115	<960,11358>		2	yes	77 102 103 109		
116	G	2	6	yes	111 112 113 114 115		

Table 1.2 continued

CHAPTER 2

ABELIAN SURFACES WITH FIXED 3-TORSION

2.1 Introduction

2.1.1 Overview

Consider a genus two curve X over $\mathbf{Q}$ given by an affine equation

$$y^2 = x^5 + ax^3 + bx^2 + cx + d. \tag{2.1.1}$$

The representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GSp}_4(\mathbf{F}_3)$ on the three-torsion $\mathrm{Jac}(X)[3]$ of its Jacobian is given by an explicit degree 80 polynomial with coefficients in $\mathbf{Q}[a, b, c, d]$. The polynomial can be extracted from [36], or following the recipe given in §2.3.1. The main theorem of this paper parametrizes all pairs (Y, i) consisting of a curve

$$Y : \quad y^2 = x^5 + Ax^3 + Bx^2 + Cx + D \tag{2.1.2}$$

and a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivariant symplectic isomorphism, $i : \mathrm{Jac}(X)[3] \to \mathrm{Jac}(Y)[3]$. The curves in (2.1.2) all have a rational Weierstrass point at ∞. The reader may wonder why we did not instead try to parametrize pairs (Y, i) for *all* genus two curves Y. The answer is that the corresponding moduli space, while rational over $\mathbf{C}$, will not typically be rational over $\mathbf{Q}$ (see the discussion towards the end of §2.1.2).

Analogous problems for genus one curves and their mod-p representations for $p \leq 5$ were solved by Rubin and Silverberg [33]. In Section 2.2, we explain how the mod 3 formulas of [27] can be reconstructed by using that $\mathrm{Sp}_2(\mathbf{F}_3)$ has a two-dimensional complex reflection representation, summarizing the result in Theorem 2.2.1.

Section 2.3 contains our main result, Theorem 2.3.1. It follows Section 2.2 closely, using now that $\mathrm{Sp}_4(\mathbf{F}_3)$ is the main factor in the complex reflection group $C_3 \times \mathrm{Sp}_4(\mathbf{F}_3)$. We

write the new curves as $Y = X(s,t,u,v)$ with $X(1,0,0,0) = X$. The new coefficients A, B, C and D are polynomials in a, b, c, d, s, t, u, and v. While the genus one and two cases are remarkably similar theoretically, the computations in the genus two case are orders of magnitude more complicated. For example, A, B, C, and D have 14604, 112763, 515354, and 1727097 terms respectively, while the corresponding two coefficients in the genus one case have only 6 and 9 terms. We give all these coefficients and other information the reader may find helpful in *Mathematica* files in the supplementary material.

Section 2.4 provides four independent complements. §2.4.1 sketches an alternative method for computing the above (A, B, C, D). §2.4.2 presents a family of examples involving Richelot isogenies. §2.4.3 gives an application to modularity which was one of the motivations for this paper. §2.4.4 illustrates that much of what we do works for arbitrary complex reflection groups; in particular, it sketches direct analogs of our main result in the computationally yet more difficult settings of 2-torsion in the Jacobians of certain curves of genus 3 and 4.

2.1.2 Moduli spaces

Theorems 2.2.1 and 2.3.1 and the analogs sketched in §2.4.4 are all formulated in terms of certain *a priori* complicated moduli spaces being actually open subvarieties of projective space. To underscore this perspective, we consider a whole hierarchy of standard moduli spaces as follows.

Let A be an abelian variety over $\mathbf{Q}$ of dimension g with a principal polarization λ. If $V_A = A[p]$ is the set of p-torsion points with coefficients in $\overline{\mathbf{Q}}$, then V_A is a $2g$-dimensional vector space over $\mathbf{F}_p$ with a symplectic form $\wedge^2_A$ induced by the Weil pairing $A[p] \times A[p] \to \mu_p$. This structure is preserved by $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and so gives rise to a Galois representation:

$$\overline{\rho}_A : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GSp}_{2g}(\mathbf{F}_p);$$

here the similitude character $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_p^\times$ is the mod-p cyclotomic character.

Conversely, if $\overline{\rho}$ is any such representation on a symplectic space $(V, \wedge^2)$, coming from an abelian variety or not, there exists a moduli space $\mathcal{A}_g(\overline{\rho})$ over $\mathbf{Q}$ parametrizing triples (A, λ, ι) consisting of a principally polarized abelian variety A together with an isomorphism $\iota : (V, \wedge^2) \simeq (V_A, \wedge^2_A)$ of symplectic representations.

Via $(A, \lambda, \iota) \mapsto (A, \lambda)$, one has a covering map $\mathcal{A}_g(\overline{\rho}) \to \mathcal{A}_g$ to the moduli space of principally polarized g-dimensional abelian varieties. For the split Galois representation $\overline{\rho}_0$, corresponding to the torsion structure $(\mathbf{Z}/p\mathbf{Z})^g \oplus (\mu_p)^g$ with its natural symplectic form, the cover $\mathcal{A}_g(\overline{\rho}_0)$ is the standard "full level p" cover $\mathcal{A}_g(p)$ of $\mathcal{A}_g$. In general, $\mathcal{A}_g(\overline{\rho})$ is a twisted version of $\mathcal{A}_g(p)$, meaning that the two varieties become isomorphic after base change from $\mathbf{Q}$ to $\overline{\mathbf{Q}}$.

The varieties $\mathcal{A}_g(\overline{\rho})$ become rapidly more complicated as either g or p increases. In particular, they are geometrically rational exactly for the cases $(g, p) = (1, 2)$, $(1, 3)$, $(1, 5)$ $(2, 2)$, $(2, 3)$, and $(3, 2)$ [24, Thm II.2.1]. In the three cases when $g = 1$, the curves $\mathcal{A}_1(\overline{\rho})$ are always rational. In the main case of interest $(2, 3)$ for this paper, the three-dimensional variety $\mathcal{A}_2(3) = \mathcal{A}_2(\overline{\rho}_0)$ is rational [9]. However, for many $\overline{\rho}$, including all surjective representations, it is proven in [13] that the variety $\mathcal{A}_2(\overline{\rho})$ is never rational. It *is* true, however, that there exists a degree 6 cover $\mathcal{A}^w_2(\overline{\rho})$ which is rational ([7, Lemma 10.2.4]). Thus while Theorem 2.2.1 corresponds to a parametrization of $\mathcal{A}_1(\overline{\rho})$ for $p = 3$, Theorem 2.3.1 corresponds to a parametrization of $\mathcal{A}^w_2(\overline{\rho})$. More precisely, the Torelli map $\mathcal{M}_2 \to \mathcal{A}_2$ is an open immersion, and the pullback of $\mathcal{A}^w_2(\overline{\rho})$ is the moduli space $\mathcal{M}^w_2(\overline{\rho})$ of genus two curves of the form (2.1.1) whose Jacobians give rise to $\overline{\rho}$, and it is $\mathcal{M}^w_2(\overline{\rho})$ which we explicitly parametrize. The retreat to this cover is optimal in the sense that six is generically the minimal degree of any dominant rational map from $\mathbf{P}^3_{\mathbf{Q}}$ to $\mathcal{A}_2(\overline{\rho})$ [13]. We mention in passing that our arguments give an alternative proof of [7, Lemma 10.2.4].

There is a natural generalization of the varieties $\mathcal{A}_g(\overline{\rho})$. Namely, for any $m \in \mathbf{F}_p^\times$, one can require instead an isomorphism $i : (V, \wedge^2) \simeq (V_A, m\wedge^2_A)$. For m/m' a square, the corresponding varieties are canonically isomorphic, so that one gets a new moduli space

only in the case of p odd. We denote this new moduli space involving "antisymplectic" isomorphisms by $\mathcal{A}_g^*(\overline{\rho})$. Our policy throughout this paper is to focus on $\mathcal{A}_g(\overline{\rho})$ and be much briefer about parallel results for $\mathcal{A}_g^*(\overline{\rho})$.

2.1.3 Acknowledgments

We thank Tom Fisher and the anonymous referees for corrections and other improvements.

2.2 Elliptic curves with fixed 3-torsion

In this section, as a warm up to Section 2.3, we rederive the formulas in [27] describing elliptic curves with fixed 3-torsion from the invariant theory of the group $\mathrm{Sp}_2(\mathbf{F}_3)$ as in [20]. Many of the steps in the derivation transfer with no theoretical change to our main case of abelian surfaces. We present these steps in greater detail here, because space allows us to give explicit formulas right in the text. Throughout this section and the next, we present the derivations in elementary language which stays very close to the computations involved. Only towards the end of the sections do we recast the results in the moduli language of the introduction.

2.2.1 Elliptic curves and their 3-torsion

Let a and b be rational numbers such that the polynomial discriminant $\Delta_{\mathrm{poly}} = -4a^3 - 27b^2$ of $x^3 + ax + b$ is nonzero and consider the elliptic curve X over $\mathbf{Q}$ with affine equation

$$y^2 = x^3 + ax + b. \tag{2.2.1}$$

We emphasize the discriminant $\Delta(a, b) = \Delta = 2^4\Delta_{\mathrm{poly}}$ in the sequel, because it makes §2.2.7 cleaner.

By a classical division polynomial formula, the eight primitive 3-torsion points $(x, y) \in \mathbf{C}^2$

are exactly the points satisfying both (2.2.1) and

$$3x^4 + 6ax^2 + 12bx - a^2 = 0. \tag{2.2.2}$$

Equations (2.2.1) and (2.2.2) together define an octic algebra over $\mathbf{Q}$. Rather than work with the two generators x and y and the two relations (2.2.1) and (2.2.2), we will work with z, the slope of a tangent line to the elliptic curve at the 3-torsion point (x, y). Then $z^2 = 3x$ and assuming $a \neq 0$ to avoid inseparability issues, the algebra in question is the quotient $K := K_{a,b}$ of $\mathbf{Q}[z]$ coming from the equation

$$F(a, b, z) := z^8 + 18az^4 + 108bz^2 - 27a^2 = 0. \tag{2.2.3}$$

2.2.2 $\mathrm{Sp}_2(\mathbf{F}_3)$ and related groups

For generic (a, b), the Galois group of the polynomial $F(a, b, z)$ is $\mathrm{GSp}_2(\mathbf{F}_3) = \mathrm{GL}_2(\mathbf{F}_3)$. The discriminant of $F(a, b, z)$ is $-2^8 3^{21} a^2 \Delta^4$. Thus the splitting field $K'_{a,b}$ of $F(a, b, z)$ contains $E = \mathbf{Q}(\sqrt{-3})$ for all a, b. The relative Galois group $\mathrm{Gal}(K'_{a,b}/E)$ is $\mathrm{Sp}_2(\mathbf{F}_3) = \mathrm{SL}_2(\mathbf{F}_3)$. We will generally use symplectic rather than linear language in the sequel, to harmonize our notation with our main case of genus two. Also we will systematically use $\omega = \exp(2\pi i/3) = (-1 + \sqrt{-3})/2$ as our preferred generator for E.

To describe elliptic curves with fixed 3-torsion, we use that (2.2.3) arises as a generic polynomial in the invariant theory of $\mathrm{Sp}_2(\mathbf{F}_3)$. The invariant theory is simple because $\mathrm{Sp}_2(\mathbf{F}_3) = \langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$ can be realized as a complex reflection group by sending the generators in order to

$$g_1 = \begin{pmatrix} \bar{\omega} & \bar{\omega} - 1 \\ 0 & 1 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} 1 & 0 \\ (\omega - 1)/3 & \omega \end{pmatrix}. \tag{2.2.4}$$

The matrices g_1 and g_2 are indeed complex reflections because all but one eigenvalue is

1. In our study of the image ST4 $= G = \langle g_1, g_2 \rangle$, the subgroup $H = \langle g_1 \rangle$ will play an important role. Here our notation ST4 refers to the placement of G in the Shephard–Todd classification of the thirty-seven exceptional irreducible complex reflection groups sorted roughly by increasing size [35, Table VII].

For both the current case of $n = 2$ and the main case of $n = 4$, we are focused principally on three irreducible characters of $\mathrm{Sp}_n(\mathbf{F}_3)$, the unital character χ_1 and a complex conjugate pair χ_{na} and χ_{nb}. Here χ_{na} corresponds to the representations (2.2.4) and (2.3.2) on $V = E^n$. Just as *invariant* is used for polynomials associated to χ_1, we will use the terms *covariant* and *contravariant* for polynomials similarly associated to χ_{na} and χ_{nb} respectively.

The left half of Table 2.1 shows how the three characters 1, χ_{2a}, and χ_{2b} fit into the entire character theory of $\mathrm{Sp}_2(\mathbf{F}_3)$. For example, via $\bar{\omega} + 1 = -\omega$ and its conjugate, g_1 and g_2 lie in the classes $3A$ and $3B$ respectively. While this information is clarifying, it is not strictly speaking needed for our arguments.

$\lvert C\rvert$:	1	1	4	4	6	4	4	$\langle \chi_i, \phi_k \rangle$								
C :	$1A$	$2A$	$3A$	$3B$	$4A$	$6A$	$6B$	0	1	2	3	4	5	6	7	8	$N_i(x)$
χ_1	1	1	1	1	1	1	1	1				1		1		1	1
χ_{1a}	1	1	$\bar{\omega}$	ω	1	$\bar{\omega}$	ω					1				1	x^4
χ_{1b}	1	1	ω	$\bar{\omega}$	1	ω	$\bar{\omega}$									1	x^8
χ_2	2	-2	-1	-1	0	1	1						1		1		$x^5 + x^7$
χ_{2a}	2	-2	$-\omega$	$-\bar{\omega}$	0	ω	$\bar{\omega}$		1		1		1		2		$x + x^3$
χ_{2b}	2	-2	$-\bar{\omega}$	$-\omega$	0	$\bar{\omega}$	ω				1		1		1		$x^3 + x^5$
χ_3	3	3	0	0	-1	0	0			1		1		2		2	$x^2 + x^4 + x^6$

Table 2.1: Character table of $\mathrm{Sp}_2(\mathbf{F}_3)$ and invariant-theoretic information.

The right half of Table 2.1 gives numerical information that will guide our calculation with explicit polynomials in the next subsections. The characters are orthonormal with respect to the Hermitian inner product $\langle f, g \rangle = |G|^{-1} \sum_C |C| f(C) \overline{g(C)}$. Let $\phi_k = \sum_i \langle \chi_i, \phi_k \rangle \chi_i$ be the character of the k^{th} symmetric power $\mathrm{Sym}^k V$. The multiplicities $\langle \chi_i, \phi_k \rangle$ for $k \leq 8$ are given in the right half of Table 2.1. These numbers are given for arbitrary k by $\sum_{k=0}^{\infty} \langle \chi_i, \phi_k \rangle x^k = N_i(x)/((1-x^4)(1-x^6))$. The character of the permutation representation of G on the coset

space G/H is $\phi_{G/H} = \chi_1 + \chi_3 + \chi_{2a} + \chi_{2b}$. If W has character χ_i then the dimension of the subspace W^H of H-invariants is $\langle \chi_i, \phi_{G/H} \rangle$. So $\dim(W^H) = 1$ if $i \in \{1, 2a, 2b, 3\}$ and $\dim(W^H) = 0$ if $i \in \{1a, 1b, 2\}$.

2.2.3 Rings of invariants

The group G acts on the polynomial ring $E[u, z]$ by the formulas induced from the matrices in (2.2.4),

$$\begin{aligned} g_1 u &= \bar{\omega} u + (\bar{\omega} - 1) z, & g_2 u &= u, \\ g_1 z &= z, & g_2 z &= (\omega - 1) u/3 + \omega z. \end{aligned}$$

Despite the appearance of the irrationality ω in these formulas, there is an important rationality present. Namely we have arranged in (2.2.4) that $g_1^2 = \overline{g}_1$ and $g_2^2 = \overline{g}_2$. Accordingly G is stable under complex conjugation, a stability not present in either the original Shephard–Todd paper [35, §4] or in *Magma*'s implementation `ShephardTodd(4)`.

We can use stability under complex conjugation to interpret G and H as the E-points of group schemes $\underline{G}$ and $\underline{H}$ over $\mathbf{Q}$. Then actually $\underline{G}$ acts on $\mathbf{Q}[u, z]$. All seven irreducible representations of $\underline{G}$ are defined over $\mathbf{Q}$, just like all three representations of the familiar group scheme $\underline{H} \cong \mu_3$, are defined over $\mathbf{Q}$. In practice, we continue thinking almost exclusively in terms of ordinary groups; these group schemes just provide a conceptually clean way of saying that in our various choices below we can and do always take all coefficients rational.

Define

$$w = \frac{u^3}{3} + u^2 z + u z^2, \qquad a = \frac{wz}{9}, \qquad b = \frac{w^2 - 6wz^3 - 3z^6}{324} \tag{2.2.5}$$

in $\mathbf{Q}[u,z]$. Then the subrings of $\underline{H}$- and $\underline{G}$-invariants are respectively

$$\mathbf{Q}[u,z]^{\underline{H}} = \mathbf{Q}[w,z], \qquad\qquad \mathbf{Q}[u,z]^{\underline{G}} = \mathbf{Q}[a,b]. \tag{2.2.6}$$

Giving u and z weight one, the elements w, a, and b clearly have weights 3, 4, and 6 respectively. If one eliminates w from the last two equations of (2.2.5), then one gets the polynomial relation $F(a,b,z) = 0$ of (2.2.3), explaining our choice of overall scale factors in (2.2.5). The fact that the rings on the right in (2.2.6) are polynomial rings, rather than more complicated rings requiring relations to describe, comes exactly from the fact that H and G are complex reflection groups, by the Chevalley–Shephard–Todd Theorem [17].

2.2.4 Covariants and contravariants

The graded ring $\mathbf{Q}[w,z]$ is free of rank eight over the graded ring $\mathbf{Q}[a,b]$. Moreover there is a homogeneous basis 1, z^2, z^4, z^6, α_1, α_3, β_3, β_5 with the following properties. The exponent or index d gives the weight, and the elements α_d and β_d are in the isotypical piece of $\mathbf{Q}[u,z]_d$ corresponding to χ_{2a} and χ_{2b} respectively.

The covariants α_d and the contravariants β_d are each well-defined up to multiplication by a nonzero rational scalar. Explicit formulas for particular choices can be found by simultaneously imposing the G-equivariance condition and the H-invariance condition. We take

$$\alpha_1 = z, \qquad \alpha_3 = \frac{w+z^3}{6}, \qquad \beta_3 = \frac{w-z^3}{2}, \qquad \beta_5 = \frac{5wz^2+3z^5}{18}. \tag{2.2.7}$$

Ideas from classical invariant theory are useful in finding these quantities. For example, the polynomials in $\mathbf{Q}[u,z]_3$ which have the required G-equivariance property for contravariance are exactly the linear combinations of the partial derivatives $\partial_u a$ and $\partial_z a$. The subspace fixed by H is the line spanned by $(\partial_u - \partial_z)a$. Thus $\beta_3 \propto (\partial_u - \partial_z)a$ and, in the same way, $\beta_5 \propto (\partial_u - \partial_z)b$. Further the covariant $\alpha_3 \propto \partial_u D$, where $D^3 = \Delta(a,b)$.

2.2.5 New coefficients

While we call the unique (up to scalar) homogeneous H-invariant elements α_1, α_3 generating the χ_{2a} isotypical pieces as covariants, Fisher in [20] defines a covariant to be a tuple defining an equivariant map $\mathbf{Q}[u,z]_1 \to \mathbf{Q}[u,z]_d$. For $d=1$, a covariant tuple is given by $l_1 = (u,z)$ corresponding to the identity map. For $d=3$, a covariant tuple is given as $l_3 = (\alpha_{3,1}, \alpha_{3,2})$, where $\alpha_{3,2} := \alpha_3$ and the first entry $\alpha_{3,1}$ is uniquely determined because of the required G-equivariance. Following [20], one can obtain new coefficients by evaluating the invariants a and b at the general covariant tuple $(u,z) = s \cdot l_1 + t \cdot l_3 = (su + t\alpha_{3,1}, sz + t\alpha_{3,2})$. This approach yields our answer immediately in the case of $g=1$, but becomes computationaly difficult for $g=2$. So we continue to treat covariants as polynomials as in §2.2.4 and describe two approaches to obtain new coefficients.

The octic $\mathbf{Q}[a,b]$-algebra $\mathbf{Q}[w,z]$ acts on itself by multiplication and so every element e in $\mathbf{Q}[w,z]$ has an octic characteristic polynomial $\phi(e,u) \in \mathbf{Q}[a,b,u]$. One has $\phi(z,u) = F(a,b,u)$ from (2.2.3). To obtain the characteristic polynomial for a general e, one can express e as an element of $\mathbf{Q}(a,b,z)$ via (2.2.7) and $w = 9a/z$. Then one removes z by a resultant to get the desired octic relation on e. Alternatively, we could have calculated these characteristic polynomials by using 8-by-8 matrices; in §2.3.5 we use the matrix approach.

Carrying out this procedure for the general covariant and contravariant gives

$$\phi(s\alpha_1 + t\alpha_3, u) = F(A(a,b,s,t), B(a,b,s,t), u),$$
$$\phi(s\beta_3 + t\beta_5, u) = F(A^*(a,b,s,t), B^*(a,b,s,t), u),$$

with

$$\begin{aligned} 3A(a,b,s,t) &= 3as^4 + 18bs^3t - 6a^2s^2t^2 - 6abst^3 - (a^3 + 9b^2)t^4, \\ 9B(a,b,s,t) &= 9bs^6 - 12a^2s^5t - 45abs^4t^2 - 90b^2s^3t^3 + 15a^2bs^2t^4 \\ &\quad -2a(2a^3 + 9b^2)st^5 - 3b(a^3 + 6b^2)t^6, \end{aligned}$$

and A^* and B^* in the accompanying computer file. As stated in the introduction, A and B when fully expanded have 6 and 9 terms respectively and agree exactly with expressions in [27, §2].

The polynomials A and B and their starred versions are respectively of degrees four and six in s and t. Also in the main case assign weights $(4, 6, -1, -3)$ to (a, b, s, t) and in the starred case make these weights $(4, 6, -3, -5)$ instead. Then all four polynomials are homogeneous of weight zero.

2.2.6 Geometric summary

The following theorem summarizes our calculations in terms of moduli spaces. The $\overline{\rho}$ of the introduction is the mod 3 representation of the initial elliptic curve, so to be more explicit we write $\mathcal{A}_{a,b}$ rather than $\mathcal{A}_1(\overline{\rho})$.

Theorem 2.2.1. *Fix an equation $y^2 = x^3 + ax + b$ defining an elliptic curve X over $\mathbf{Q}$. Let $\mathcal{A}_{a,b}$ be the moduli space of pairs (Y, i) with Y an elliptic curve and $i : X[3] \to Y[3]$ a symplectic isomorphism. Then $\mathcal{A}_{a,b}$ can be realized as the complement of a discriminant locus $\mathcal{Z}_{a,b}$ in the projective line* Proj $\mathbf{Q}[s, t]$. *The natural map to the j-line $\mathcal{A}_1 \subset$ Proj $\mathbf{Q}[A, B]$ has degree twelve and is given by*

$$(A, B) = (A(a, b, s, t), B(a, b, s, t)). \tag{2.2.8}$$

The formula $y^2 = x^3 + A(a, b, s, t)x + B(a, b, s, t)$ gives the universal elliptic curve $X(s, t)$ over $\mathcal{A}_{a,b}$.

The discriminant locus $\mathcal{Z}_{a,b}$ is given by the vanishing of the discriminant

$$\Delta(A, B) = \Delta(a, b)\delta(a, b, s, t)^3/27, \quad \delta(a, b, s, t) = 3s^4 + 6as^2t^2 + 12bst^3 - a^2t^4. \tag{2.2.9}$$

It thus consists of four geometric points. Comparing with (2.2.2), one sees that these

points are permuted by $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ according to the projective mod 3 representation into $\mathrm{PGL}_2(\mathbf{F}_3) \cong S_4$. Theorem 2.2.1 has a direct analog for the covers $\mathcal{A}^*_{a,b} \to \mathcal{A}_1$.

2.2.7 Finding (s,t)

Let $X : y^2 = x^3 + ax + b$ and $Y : y^2 = x^3 + Ax + B$ be elliptic curves over $\mathbf{Q}$ with isomorphic 3-torsion. Then, in contrast with the analogous situation for the genus two case described in §2.3.7, it is very easy to find associated $(s,t) \in \mathbf{Q}^2$. Namely, (2.2.8) and its analog $(A,B) = (A^*(a,b,s,t), B^*(a,b,s,t))$ each have twenty-four solutions in $\mathbf{C}^2$. One just extracts the rational ones, say by eliminating s and factoring the resulting degree twenty-four polynomials $f(t)$ and $f^*(t)$. If the image of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is all of $\mathrm{GSp}_2(\mathbf{F}_3) = \mathrm{GL}_2(\mathbf{F}_3)$, then one of these polynomials factors as $1+1+6+8+8$ and the other as $12+12$. The two 1's correspond to the desired solutions $\pm(s,t)$.

Discriminants are useful in distinguishing the two moduli spaces as follows. If Y has the form $X(s,t)$ then Δ_X/Δ_Y is a perfect cube by (2.2.9). If it has the form $X^*(s,t)$ then $\Delta_X\Delta_Y$ is a perfect cube by the starred analog of (2.2.9). These implications determine a unique space on which Y represents a point unless Δ_X and Δ_Y are both perfect cubes. Since $x^3 - \Delta$ is a resolvent cubic of the octic (2.2.3), this ambiguous case arises if and only if the image Γ of $\overline{\rho}_X$ has order dividing 16.

As an example, let $(a,b) = (-1,0)$ so that X has conductor 2^5 and discriminant 2^6. Let $(A,B) = (-27,-162)$ so that Y has conductor $2^5 3^3$ and discriminant $-2^9 3^9$. The octic polynomials $F(a,b,z)$ and $F(A,B,z)$ define the same field because under *Pari*'s `polredabs` they each become z^8+6z^4-3. This polynomial has Galois group of order 16. The procedure in the first paragraph yields solutions only in the starred case, these being $(s,t) = \pm(-1/2, 3/2)$.

An elliptic curve Y can give rise to a point on both moduli spaces constructed from X if and only if the two moduli spaces coincide. The spaces coincide exactly when there is an equivariant isomorphism $(X[3], \wedge) \simeq (X[3], -\wedge)$ where $\wedge$ is the Weil pairing. Such an isomorphism exists if and only if $X[3]$ is either a twist of $\overline{\rho}_0 = \mathbf{Z}/3\mathbf{Z} \oplus \mu_3$ or when $X[3]$

is irreducible but not absolutely irreducible. (The latter occurs precisely when the image factors through the non-split Cartan subgroup $\mathbf{F}_9^\times$ and has order > 2; this case does not arise over $\mathbf{Q}$.) An instance over $\mathbf{Q}$ is $X = Y$ coming from $(a, b) = (5805, -285714)$ which is the modular curve $X_0(14)$ of genus one and discriminant $-2^{18}3^{12}7^3$; here $(s, t) = \pm(1, 0)$ in the main case and $2^6 3^4 7^2 (s, t) = \pm(435, 11)$ in the starred case.

2.3 Abelian surfaces with fixed 3-torsion

In this section, we present our main theorem on abelian surfaces with fixed 3-torsion. We are brief on parts of the derivation which closely follow steps described in the previous section, and concentrate on steps which have a new feature.

2.3.1 Weierstrass curves and their 3-torsion

By a *Weierstrass curve* in this paper we will mean a genus two curve together with a distinguished Weierstrass point. Placing this marked point at infinity and shifting the variable x, one can always present a Weierstrass curve via the affine equation (2.1.1), which we call a *Weierstrass equation*. Replacing (a, b, c, d) by $(u^4 a, u^6 b, u^8 c, u^{10} d)$ yields an isomorphic Weierstrass curve via the compensating change $(x, y) \mapsto (u^2 x, u^5 y)$. The standard discriminant of the genus two curve (2.1.1) is $\Delta(a, b, c, d) = \Delta = 2^8 \Delta_{\text{poly}}$, where Δ_{poly} is the discriminant of the quintic polynomial on the right of (2.1.1). It is best for our purposes to give the parameters a, b, c, and d weights 12, 18, 24, and 30. In this system, Δ is homogeneous of weight 120. The (coarse) moduli space of Weierstrass curves $\mathcal{M}_2^w$ is then the complement of the hypersurface $\Delta = 0$ in the weighted projective space $\mathbf{P}^3(12, 18, 24, 30) = \mathbf{P}^3(2, 3, 4, 5)$. As explained at the end of §1.2, rather than describing moduli spaces mapping to $\mathcal{A}_2$, we will be describing their base changes to $\mathcal{M}_2^w$.

The group law in terms of effective divisors on the Jacobian of a general genus two curve $X : y^2 = f(x)$ yields a classical $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivariant bijection [16] from the non-zero

3-torsion points to decompositions of the form

$$f(x) = (b_4x^3 + b_3x^2 + b_2x + b_1)^2 - b_7(x^2 + b_6x + b_5)^3.$$

In the quintic case of (2.1.1), one has $b_4^2 = b_7$. The minimal polynomial of b_4^{-2} is a degree 40 polynomial p_{40} such that $p_{40}(x^2)$ describes the 3-torsion representation of X.

In our reflection group approach, it is actually $p_{40}(z^6)$ which appears naturally. It has 1673 terms and begins as

$$\begin{aligned} F(a,b,c,d,z) &= z^{240} + 15120az^{228} + 2620800bz^{222} \\ &\quad -504\left(70227a^2 - 831820c\right)z^{216} - 1965600z^{210}(2529ab - 33550d)z^{210} + \cdots \end{aligned} \tag{2.3.1}$$

The splitting field of $F(a,b,c,d,z)$ is the compositum of the splitting fields of $p_{40}(x^2)$ and $x^3 - \Delta$. In particular, having chosen a *Weierstrass equation*, the field $E(\Delta^{1/3})$ remains constant throughout our family of Weierstrass equations, even though $E(\Delta^{1/3})$ is *not* determined by the 3-torsion representation. On the other hand, the change of coordinates $(x,y) \mapsto (u^2x, u^5y)$ maps Δ to $u^{40}\Delta$, and so this auxiliary choice places no restrictions on the *Weierstrass curves* which can occur in the family. In contrast, when $g = 1$, the field $E(\Delta^{1/3})$ also remains constant, but in this case it *is* determined by the 3-torsion representation as it is the fixed field of the 2-Sylow of the image of $\mathrm{Gal}(\overline{\mathbf{Q}}/E)$ in $\mathrm{Sp}_2(\mathbf{F}_3)$.

2.3.2 $\mathrm{Sp}_4(\mathbf{F}_3)$ and related groups

Define g_1, g_2, g_3, and g_4 to be

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \omega & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & -\bar{\alpha} & -\bar{\alpha} & 0 \\ -\bar{\alpha} & \alpha & -\bar{\alpha} & 0 \\ -\bar{\alpha} & -\bar{\alpha} & \alpha & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & \bar{\alpha} & 0 & \bar{\alpha} \\ \bar{\alpha} & \alpha & 0 & -\bar{\alpha} \\ 0 & 0 & 1 & 0 \\ \bar{\alpha} & -\bar{\alpha} & 0 & \alpha \end{pmatrix}, \tag{2.3.2}$$

where $\alpha = \omega/\sqrt{-3}$. Define $H = \langle g_1, g_2, g_3\rangle$ and $G = \langle g_1, g_2, g_3, g_4\rangle$. The matrices g_i are all complex reflections of order 3, and they are exactly the matrices given in [35, 10.5]. As with $H = C_3$ and $G = \mathrm{ST4} = \mathrm{Sp}_2(\mathbf{F}_3)$ of the last section, the new groups $H = \mathrm{ST25}$ and $G = \mathrm{ST32}$ are also complex reflection groups. The group G has the structure $C_3 \times \mathrm{Sp}_4(\mathbf{F}_3)$ and it is the extra C_3 that is the reason that Δ behaves differently in the two cases.

Again numeric identities guide polynomial calculations as we discussed around Table 2.1. For example, orders are products of degrees of fundamental invariants. Analogous to the old cases $|C_3| = 3$ and $|\mathrm{Sp}_2(\mathbf{F}_3)| = 4\cdot 6$, the new cases are $|H| = 6\cdot 9\cdot 12$ and $|G| = 12\cdot 18\cdot 24\cdot 30$. Thus again the index $|G|/|H| = 240$ matches the degree of the main polynomial (2.3.1). The character table of G has size 102×102, so we certainly will not present the analog of Table 2.1. The most important information is that the degrees in which co- and contravariants live, previously 1, 3 and 3, 5, are now 1, 7, 13, 19 and 11, 17, 23, 29 for G.

2.3.3 Rings of invariants

One has the rationality condition $g_i^2 = \overline{g}_i$ for all four i, allowing us again to interpret H and G as E-points of group schemes $\underline{H}$ and $\underline{G}$ over $\mathbf{Q}$. The matrices g_i together give an action of $\underline{G}$ on $\mathbf{Q}[z_1, z_2, z_3, z_4]$. The variable $z = z_4$ plays a role which is different from the other z_i.

Define, following [25, 4.72],

$$\begin{aligned} p &= z_1^6 + z_2^6 + z_3^6 - 10\left(z_2^3z_3^3 + z_2^3z_1^3 + z_3^3z_1^3\right), \\ q &= (z_1^3 - z_2^3)(z_2^3 - z_3^3)(z_3^3 - z_1^3), \\ r &= (z_1^3 + z_2^3 + z_3^3)\left[(z_1^3 + z_2^3 + z_3^3)^3 + 216z_1^3z_2^3z_3^3\right]. \end{aligned}$$

Define also a, b, c, and d by taking $(2^4 3^7 5a, 2^6 3^9 5^2 b, 2^8 3^{12} 5^3 c, 2^{10} 3^{16} 5^5 d)$ to be

$$(-p^2 - 5r + 1320qz^3 - 132pz^6 - 6z^{12},$$
$$p^3 - 400q^2 - 5pr - 680pqz^3 + 323p^2z^6 - 255rz^6 - 7480qz^9 + 68pz^{12} - 4z^{18},$$
$$2p^4 - 800pq^2 - 5p^2r + 320p^2qz^3 - 3000qrz^3 - 722p^3z^6 + 175200q^2z^6 + 990prz^6$$
$$+33040pqz^9 - 953p^2z^{12} + 3495rz^{12} + 15720qz^{15} + 268pz^{18} - 3z^{24},$$
$$13p^5 - 6000p^2q^2 - 25p^3r + 21600p^3qz^3 - 9600000q^3z^3 - 45000pqrz^3 + 11790p^4z^6$$
$$-4572000pq^2z^6 - 37575p^2rz^6 + 28125r^2z^6 - 247200p^2qz^9 - 945000qrz^9$$
$$+37155p^3z^{12} + 234000q^2z^{12} - 150075prz^{12} - 214200pqz^{15} + 30855p^2z^{18}$$
$$-143775rz^{18} + 354600qz^{21} + 2340pz^{24} - 12z^{30}).$$

Because H and G are complex reflection groups, the rings of invariants are freely generated, explicit formulas being

$$\mathbf{Q}[z_1, z_2, z_3, z]^{\underline{H}} = \mathbf{Q}[p, q, r, z], \qquad \mathbf{Q}[z_1, z_2, z_3, z]^{\underline{G}} = \mathbf{Q}[a, b, c, d].$$

When one removes p, q, r from the equations defining a, b, c, d, one gets exactly the degree 240 equation (2.3.1) for z.

2.3.4 Covariants and contravariants

As mentioned before, group-theoretic calculations like those in Table 2.1 say that covariants lie in degrees 1, 7, 13, and 19. Formulas for H-invariant covariants in these degrees are

$$\alpha_1 = z, \qquad 2^2 3^3 5\alpha_7 = 7pz - 3z^7, \qquad 2^4 3^6 \alpha_{13} = (11r - 3p^2)z + 216qz^4 + 72pz^7,$$
$$2^4 3^{10} \alpha_{19} = (p^3 - pr - 468q^2)z - 24pqz^4 + (66r - 6p^2)z^7 - 288qz^{10} - 12pz^{13}.$$

Here, unlike in the genus one case, there is an ambiguity beyond multiplying by a nonzero scalar. Namely rather than working with α_{13} we could work with any linear combination of $a\alpha_1$ and α_{13} that involves α_{13} nontrivially. Similarly we could replace α_{19} by $c_1 b\alpha_1 +$

$c_7 a\alpha_7 + c_{19}\alpha_{19}$ for any nonzero c_{19}. The choices involved in picking particular contravariants β_k mirror the choices involved in picking α_{k-10}. Our choice of $(\beta_{11}, \beta_{17}, \beta_{23}, \beta_{29})$ is given in the accompanying computer file. Just as in §2.2.4, the contravariants β_k can be described in terms of partial derivatives of the invariants. To be precise, we take $(\beta_{11}, \beta_{17}, \beta_{23}, \beta_{29}) = (\partial_z a, \partial_z b, \partial_z c, \partial_z d)$.

2.3.5 New coefficients

Each covariant element α_d is the last entry of a uniquely determined covariant tuple l_d of length 4 defining an equivariant map $\mathbf{Q}[z_1, z_2, z_3, z]_1 \to \mathbf{Q}[z_1, z_2, z_3, z]_d$. By evaluating the invariants a, b, c, d at the general covariant tuple i.e., by setting $(z_1, z_2, z_3, z) = s \cdot l_1 + t \cdot l_7 + u \cdot l_{13} + v \cdot l_{19}$, one can theoretically obtain the new coefficients. For computational reasons, we instead follow the matrix approach as stated in §2.2.5.

Our key computation takes place in the algebra $\mathbf{Q}[p, q, r, z]$ of $\underline{H}$-invariants viewed as a graded module over the algebra $\mathbf{Q}[a, b, c, d]$ of $\underline{G}$-invariants. As a graded basis we use $p^i q^j r^k z^l$ with $0 \leq i, j, k < 2$ and $0 \leq l < 30$. Repeatedly using the vector equation in §2.3.3, we expand the products

$$\alpha_e p^i q^j r^k z^l = \sum_{I,J,K,L} M(e)^{i,j,k,l}_{I,J,K,L} p^I q^J r^K z^L$$

to represent the covariants α_e as 240-by-240 matrices $M(e)$ with entries in $\mathbf{Q}[a, b, c, d]$. The general covariant

$$Z = s\alpha_1 + t\alpha_7 + u\alpha_{13} + v\alpha_{19} \tag{2.3.3}$$

satisfies the characteristic polynomial of $M = sM(1) + tM(7) + uM(13) + vM(19)$. In other words, Z satisfies a degree 240 polynomial equation

$$F(A, B, C, D, Z) = Z^{240} + c_2 Z^{228} + c_3 Z^{222} + c_4 Z^{216} + c_5 Z^{210} + \cdots = 0$$

with F from (2.3.1). We need to calculate A, B, C, D in terms of the free parameters a, b, c, d, s, t, u, and v. Define normalized traces τ_n by

$$6\tau_n = \mathrm{Tr}(M^{6n}) = \sum_{i+j+k+l=6n} \binom{6n}{i,j,k,l} s^i t^j u^k v^l \mathrm{Tr}(M(1)^i M(7)^j M(13)^k M(19)^l).$$

Because the first trace τ_1 is 0, standard symmetric polynomial formulas simplify, giving $(c_2, c_3, c_4, c_5) = (-\tau_2/2, \tau_3/3, \tau_2^2/8 - \tau_4/4, \tau_2\tau_3/6 - \tau_5/5)$. Then (2.3.1) yields

$$(A, B, C, D) = \left(\frac{-\tau_2}{30240}, \frac{-\tau_3}{7862400}, \frac{3667\tau_2^2 - 5600\tau_4}{9390915072000}, \frac{2521\tau_2\tau_3 - 2688\tau_5}{886312627200000} \right). \tag{2.3.4}$$

The matrices M^k have entries in $\mathbf{Q}[a, b, c, d, s, t, u, v]$ and for $k = 1, \ldots, 6$ they take approximately 2, 10, 40, 125, 300, and 675 megabytes to store. The matrix M^6 suffices to determine A because the evaluation of $\mathrm{Tr}(M^{12}) = \mathrm{Tr}(M^6 \cdot M^6)$ does not require the full matrix multiplication on the right. However we would not be able to continue in this way to the needed M^{15}. In contrast, the $M(e)$ have entries only in $\mathbf{Q}[a, b, c, d]$ and take less space to store. The worst of the $M(e)^j$ that we actually use in the above expansion is $M(19)^{15}$, which requires about 210 megabytes to store. By getting the terms in smaller batches and discarding matrix products when no longer needed, we can completely compute all of A, B, C, and D without memory overflow. In principle, one could repeat everything in the contravariant case, although here the initial matrix M^* takes twice as much space to store as M.

The polynomials A, B, C, and D have respectively degrees 12, 18, 24, and 30 in s, t, u, and v. Also, assign weights $(12, 18, 24, 30, -1, -7, -13, -19)$ to (a, b, c, d, s, t, u, v). Then all four polynomials are homogeneous of weight zero. The bigradation allows A, B, C, and D to have 14671, 112933, 515454, and 1727921 terms respectively. With our choice of α_{13} and α_{19}, respectively 67, 170, 100, and 824 of these terms vanish, so A, B, C, and D have the number of terms reported in the introduction. Not only do the polynomials have many

terms, but the coefficients can have moderately large numerators. The largest absolute value of all the numerators is achieved by the term

$$2^{30} \cdot 3^3 \cdot 5^{23} \cdot 1381131815224116413 \cdot a^3bc^5d^{10}u^{16}v^{14}$$

in D. On the another hand, denominators of the coefficients in A, B, C, and D always divide 5, 5^2, 5^3, and 5^5 respectively.

2.3.6 Geometric summary

We now summarize our results in the following theorem. The $\overline{\rho}$ of §1.2 is the mod 3 representation of the initial genus two curve (2.1.1). So, to be more explicit, we write $\mathcal{M}_{a,b,c,d} = \mathcal{M}_2^w(\overline{\rho})$ below.

Theorem 2.3.1. *Fix an equation $y^2 = x^5+ax^3+bx^2+cx+d$ defining a curve X over $\mathbf{Q}$. Let $\mathcal{M}_{a,b,c,d}$ be the moduli space of pairs (Y, i) with Y a Weierstrass curve and $i : \mathrm{Jac}(X)[3] \to \mathrm{Jac}(Y)[3]$ a symplectic isomorphism on the 3-torsion points of their Jacobians. Then $\mathcal{M}_{a,b,c,d}$ can be realized as the complement of a discriminant locus $\mathcal{Z}_{a,b,c,d}$ in the projective three-space $\mathrm{Proj}\ \mathbf{Q}[s,t,u,v]$. The covering maps to the moduli space $\mathcal{M}_2^w \subset \mathrm{Proj}\ \mathbf{Q}[A,B,C,D]$ have degree 25920 and are given by*

$$(A, B, C, D) = (A(a, \ldots, v), B(a, \ldots, v), C(a, \ldots, v), D(a, \ldots, v)). \tag{2.3.5}$$

The formula

$$y^2 = x^5 + A(a, \ldots, v)x^3 + B(a, \ldots, v)x^2 + C(a, \ldots, v)x + D(a, \ldots, v) \tag{2.3.6}$$

gives the universal Weierstrass curve $X(s,t,u,v)$ over $\mathcal{M}_{a,b,c,d}$.

The discriminant locus $\mathcal{Z}_{a,b,c,d}$ is given by the vanishing of the discriminant

$$\Delta(A(a,\ldots,v),\ldots,D(a,\ldots,v)) = \Delta(a,b,c,d)\delta(a,b,c,d,s,t,u,v)^3. \tag{2.3.7}$$

where δ is homogeneous of degree 40 in s, t, u, v. Geometrically, $\mathcal{Z}_{a,b,c,d}$ is the union of forty planes and these planes are permuted by $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ according to the roots of p_{40} from the end of §2.3.1. While the fibres of $\mathcal{M}_{a,b,c,d}$ over $\mathcal{M}_2^w$ are projective spaces, the entire space defines a non-trivial projective bundle which can be determined explicitly from our equations in terms of $\mathrm{Pic}(\mathcal{M}_2^w)$ (for more details, see the blog post [11], in particular the comments of Najmuddin Fakhruddin). In principle, Theorem 2.3.1 has a direct analog for $\mathcal{M}^*_{a,b,c,d} \to \mathcal{M}_2^w$. The computer file only gives the starred coefficients evaluated at $(a,b,c,d,1,0,0,0)$, as this is sufficient for moving from one moduli space to the other.

2.3.7 Finding (s,t,u,v)

Let X and Y be Weierstrass curves over $\mathbf{Q}$ having isomorphic 3-torsion and given by coefficient sequences (a,b,c,d) and (A,B,C,D) respectively. Then finding associated rational (s,t,u,v) is both theoretically and computationally more complicated than in the genus one case of §2.2.7.

As in the genus one case, for (2.3.5) to have a solution, the ratio Δ_X/Δ_Y must be a perfect cube by (2.3.7). Similarly, for the starred version of (2.3.5) to have a solution the product $\Delta_X\Delta_Y$ must be a perfect cube. The theoretical complication was introduced at the end of §2.3.1: the class modulo cubes of the discriminant now depends on the model via $\Delta(u^4A,u^6B,u^8C,u^{10}D) = u^{40}\Delta(A,B,C,D)$. So as a preparatory step one needs to adjust the model of Y to some new (A,B,C,D) before seeking solutions to (2.3.5), and also to some typically different (A^*,B^*,C^*,D^*) before seeking solutions to the starred analog of (2.3.5).

Having presented Y properly, one then encounters the computational problem. Namely both (2.3.5) and its starred version have 155520 solutions $(s,t,u,v) \in \mathbf{C}^4$, and so one cannot

expect to find the rational ones by algebraic manipulations. Working numerically instead, one gets 240 solutions $(p, q, r, z) \in \mathbf{C}^4$ to the large vector equation in §2.3.3. Eight of these solutions are in $\mathbf{R}^4$. These vectors yield eight vectors $(\alpha_1, \alpha_7, \alpha_{13}, \alpha_{19}) \in \mathbf{R}^4$ from the covariants in §2.3.4, and also eight vectors $(\beta_{11}, \beta_{17}, \beta_{23}, \beta_{29}) \in \mathbf{R}^4$. Let Z and Z^* respectively run over the eight real roots of $F(A, B, C, D, U)$ and $F(A^*, B^*, C^*, D^*, U)$. Then one can apply the LLL algorithm to find low height relations of the form (2.3.3) and its starred variant

$$Z^* = s\beta_{11} + t\beta_{17} + u\beta_{23} + v\beta_{29}.$$

When the image of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on 3-torsion is sufficiently large then there will just be a single pair of solutions $\pm(s, t, u, v)$ from the eight equations of one type and none from the other eight equations. The supplementary file `code_3torsion.txt` provides a *Mathematica* program `findisos` to do all steps at once. Examples are given in §2.4.2 and §2.4.3.

2.4 Complements

The four subsections of this section can be read independently.

2.4.1 A matricial identity

The polynomials A, B, C, and D in Theorem 2.3.1 satisfy the matricial identity

$$\mathcal{E}(A(a, \ldots, v), B(a, \ldots, v), C(a, \ldots, v), D(a, \ldots, v), S, T, U, V) = \mathcal{E}(a, b, c, d, M(S, T, U, V)^t),$$

where $\mathcal{E}$ can be any one of A, B, C, D, and M is a 4×4 matrix with entries in $\mathbf{Q}[a, b, c, d, s, t, u, v]$ whose first column is $(s, t, u, v)^t$. The columns of M are homogeneous of degrees $1, 7, 13, 19$ in s, t, u, v, and the rows are homogeneous of degrees $-1, -7, -13, -19$ with respect to the weights assigned in §2.3.5.

The situation in the $g = 1$ case is analogous but enormously simpler:

$$\begin{aligned} A(A(a,b,s,t),B(a,b,s,t),S,T) &= A(a,b,M(S,T)^t), \\ B(A(a,b,s,t),B(a,b,s,t),S,T) &= B(a,b,M(S,T)^t), \end{aligned} \qquad M = \begin{pmatrix} s & -as^2t - 3bst^2 + a^2t^3/3 \\ t & s^3 + ast^2 + bt^3 \end{pmatrix}.$$

Here, as is visible, columns of M have degrees 1 and 3 in s, t, while rows have weights -1 and -3 with respect to the weights assigned in §2.2.5. The second column is in fact proportial to $[-\partial_t\delta, \partial_s\delta]^t$, where δ is as in (2.2.9). Hence M is the matrix found in Lemma 8.4 of [20], up to rescaling of the columns.

The identities say that changing the initial Weierstrass curve to a different one in $\mathcal{M}_{a,b,c,d}$ has the effect of changing the parametrization of the family through a linear transformation M of the covariants. In fact, our first method of calculating the quantities $\mathcal{E}(a,\ldots,v)$ exploited this ansatz. Starting from a few curves with $a = b = 0$, computing covariants numerically, and changing bases so as to meet the bigradation conditions of §2.3.5, we obtained the polynomials $\mathcal{E}(0,0,c,d,s,t,u,v)$. We then examined the matricial identity with $a = b = 0$. Comparing certain monomial coefficients, we determined the second column of M precisely, the third column up to one free parameter, and the fourth column up to two free parameters. This corresponds to the ambiguity in the covariants in degrees 13 and 19 described in §2.3.4. Once a choice of M was made, comparing coefficients again and solving the resulting linear equations determined the polynomials $\mathcal{E}(a,\ldots,v)$ completely.

2.4.2 Examples involving Richelot isogenies

Let X and Y be Weierstrass curves and let $I : \mathrm{Jac}(X) \to \mathrm{Jac}(Y)$ be an isogeny with isotropic kernel of type (m,m) with m prime to 3. Then I induces an isomorphism $\iota : \mathrm{Jac}(X)[3] \to \mathrm{Jac}(Y)[3]$ which is symplectic if $m \equiv 1\ (3)$ and antisymplectic if $m \equiv 2\ (3)$. In the following examples, $m = 2$.

Let $X_{e,f,g}$ be defined by (2.1.1) with $(a,b,c,d) =$

$$\Big(-5(7e^2-2f), -10e(3e^2-2f), 5(32e^4-39e^2f+g), -4e(24e^4+115e^2f-5g)\Big).$$

The discriminant of $X_{e,f,g}$ is

$$\Delta_X = -2^{12}5^5\left(125e^4+20f^2-4g\right)^2\left(25e^2f-g\right)\left(25e^2f+g\right)^2.$$

Define $Y_{e,f,g}$ to be the quadratic twist by 2 of $X_{e,-f,g}$. The form of (a,b,c,d) has been chosen so that there is a Richelot isogeny from $\mathrm{Jac}(X_{e,f,g})$ to $\mathrm{Jac}(Y_{e,f,g})$.

Let $\bar{\cdot}$ be the involution of $\mathbf{Q}[e,f,g]$ given by $(\bar{e},\bar{f},\bar{g}) = (e,-f,g)$. To make $\Delta_X\Delta_Y$ a cube and avoid denominators in (s,t,u,v), present $Y_{e,f,g}$ via $(A,B,C,D) = (\bar{a}z^2, \bar{b}z^3, \bar{c}z^4, \bar{d}z^5)$ with $z = 2^3 5^4\left(125e^4+20f^2-4g\right)^4\left(25e^2f+g\right)^6$. Applying the numeric method of §2.3.7 and interpolating strongly suggests $(s,t,u,v) =$

$$\pm\Big(-4e(80e^4+7e^2f-g), 2(40e^4-9e^2f-g), -4e(5e^2+2f), 5e^2+2f\Big).$$

Specializing the contravariant matrix $M(a,b,c,d,s,t,u,v)^*$ of §2.3.5 to $M(e,f,g)^*$ allows direct computation of its powers up through the needed fifteenth power. Applying (2.3.4) indeed recovers (A,B,C,D) so that the interpolation was correct.

The examples of this subsection are already much simpler than the general case with its millions of terms. For a smaller family of even simpler examples, now with all mod 3 representations non-surjective, one can set $e = 0$. Then b, d, B, D, s, and u are all 0, while a, c, A, C, t, and v are given by tiny formulas.

2.4.3 Explicit families of modular abelian surfaces

Our main theorem gives a process by which modularity of a genus two curve can be transferred to modularity of infinitely many other genus two curves:

Corollary 2.4.1. *Suppose the genus two curve $X : y^2 = x^5 + ax^3 + bx^2 + cx + d$ has good reduction at 3, and assume that $A = \mathrm{Jac}(X)$ satisfies all the conditions of [7, Prop. 10.1.1, 10.1.3], so that X is modular. Then all the curves $X(s,t,u,v)$ or $X^*(s,t,u,v)$ having good reduction at 3 are also modular.*

The conclusion follows simply because the hypotheses imply that the new Jacobians also satisfy the conditions of [7, Prop. 10.1.1, 10.1.3] and are thus modular. In particular, for any $(s,t,u,v) \in \mathbf{P}^3(\mathbf{Q})$ reducing to $(1,0,0,0) \in \mathbf{P}^3(\mathbf{F}_3)$, the curves X and $X(s,t,u,v)$ are identical modulo 3 and therefore $X(s,t,u,v)$ is modular.

The hypotheses of [7, Prop. 10.1.1, 10.1.3] include that the mod 3 representation $\overline{\rho}$ is not surjective. The easiest way to satisfy the hypotheses is to look among X for which the geometric endomorphism ring of $\mathrm{Jac}(X)$ is larger than $\mathbf{Z}$. One such X, appearing in [14, Example 3.3], is given by

$$(a,b,c,d) = \left(12/5, 12/5^2, 292/5^3, -3672/5^5\right),$$

having arisen from the simple equation $y^2 = (x^2+2x+2)(x^2+2)x$. This curve has conductor 2^{15} and discriminant $\Delta_X = 2^{23}$. Applying the corollary, one gets infinitely many modular genus two curves $X(s,t,u,v)$. For generic parameters, the geometric endomorphism ring of $\mathrm{Jac}(X(s,t,u,v))$ is just $\mathbf{Z}$.

It is much harder to directly find curves Y satisfying the hypotheses of [7, Prop 10.1.1, 10.1.3] and also satisfying $\mathrm{End}(\mathrm{Jac}(Y)_{\overline{\mathbf{Q}}}) = \mathbf{Z}$. A short list was found in [14]. The curve Y in Example 3.3 there has

$$(A,B,C,D) = \left(2^7/5, 2^{11}\cdot 57/5^2, -2^{12}\cdot 503/5^3, 2^{17}\cdot 17943/5^5\right)$$

and comes from the simple equation $y^2 = (2x^4 + 2x^2 + 1)(2x + 3)$. It has conductor $2^{15}5$ and Example 3.3 also observes that its 3-torsion is isomorphic to that of X.

While Y was found in [14] via an *ad hoc* search, it now appears as just one point in an

infinite family. To see this explicitly, note that $\Delta_Y = 2^{83}5^6$ so that Δ_Y/Δ_X is a perfect cube. Numerical computation as in §2.3.7 followed by algebraic verification yields

$$Y = X(129/125, 11/25, 3/100, 1/20).$$

If this procedure had failed, we would have found the proper $X^*(s,t,u,v)$ by dividing (A,B,C,D) by $(2^4, 2^6, 2^8, 2^{10})$ to make $\Delta_X\Delta_Y$ a cube.

2.4.4 Analogs for $p = 2$

Complex reflection groups also let one respond to the problem of the introduction for residual prime $p = 2$ and dimensions $g = 2$, 3, and 4 via descriptions of moduli spaces related to $\mathcal{A}_g(\overline{\rho})$. A conceptual simplification is that since $p = 2$ one does not have the second collection of spaces $\mathcal{A}_g^*(\overline{\rho})$. Correspondingly, the relevant groups are actually reflection groups defined over $\mathbf{Q}$, so that covariants and contravariants coincide. The cases of dimension $g = 3$, 4 make fundamental use of work of Shioda [36].

We begin with the easiest case $g = 2$, because it shows clearly that our approach has classical roots in Tschirnhausen transformations. Greater generality would be possible by using the symmetric group S_6, but we describe things instead using S_5 to stay in the uniform context of Weierstrass curves. Let α_1 be a companion matrix of $x^5 + ax^3 + bx^2 + cx + d$. For $j = 2$, 3, 4, let $\alpha_j = \alpha_1^j - k_j I$ where k_j is chosen to make α_j traceless. Then the curve

$$y^2 = \det(xI - s\alpha_1 - t\alpha_2 - u\alpha_3 - v\alpha_4)$$

has the same 2-torsion as the original curve. From this fact follows a very direct analog of Theorem 2.3.1, with the new $\mathcal{M}_{a,b,c,d} \subset \text{Proj } \mathbf{Q}[s,t,u,v]$ now mapping to the same $\mathcal{M}_2^w \subset \text{Proj } \mathbf{Q}[A,B,C,D]$ with degree 120. Carrying out this easy computation, the elements A, B, C, and D of $\mathbf{Q}[a,b,c,d,s,t,u,v]$ respectively have 24, 86, 235, and 535 terms. Of course there is nothing special about degree 5, and the analogous computations in degrees $2g+1$

and $2g+2$ give statements about genus g hyperelliptic curves with fixed 2-torsion.

For $g = 3$, we work with the moduli space $\mathcal{M}_3^q$ of smooth plane quartics which maps isomorphically to an open subvariety of $\mathcal{A}_3$. From the analog addressed in [13], we suspect that the varieties $\mathcal{A}_3(\overline{\rho})$ are in general not rational. To place ourself in a clearly rational setting, we work with the moduli space $\mathcal{M}_3^f$ of smooth plane quartics with a rational flex. This change is analogous to imposing a rational Weierstrass point on a genus two curve, although now the resulting cover $\mathcal{M}_3^f \to \mathcal{M}_3^q$ has degree twenty-four. A quartic curve with a rational flex can always be given in affine coordinates by

$$y^3 + (x^3 + a_8 x + a_{12})y + (a_2 x^4 + a_6 x^3 + a_{10} x^2 + a_{14} x + a_{18}) = 0. \tag{2.4.1}$$

Here the flex in homogeneous coordinates is at $(x, y, z) = (0, 1, 0)$ and its tangent line is the line at infinity $z = 0$. Changing a_d to $u^d a_d$ gives an isomorphic curve via $(x, y) \mapsto (u^4 x, u^6 y)$. The variety $\mathcal{M}_3^f$ is the complement of a discriminant locus in the weighted projective space Proj $\mathbf{Q}[a_2, \ldots, a_{18}] = \mathbf{P}^6(2, \ldots, 18)$. The invariant theory of the reflection group ST36 $= W(E_7) = C_2 \times \mathrm{Sp}_6(\mathbf{F}_2)$ gives polynomials $A_i(a_2, \ldots, a_{18}, s_{-1}, \ldots, s_{-17})$ of degree i in the s_{-j} and total weight 0. Following the template of the previous cases, for fixed $(a_2, \ldots, a_{18})$ one has a six-dimensional variety $\mathcal{M}_{a_2,\ldots,a_{18}} \subset$ Proj $\mathbf{Q}[s_{-1}, \ldots, s_{-17}]$ parametrizing genus three curves with a rational flex and 2-torsion identified with that of (2.4.1). The covering maps $\mathcal{M}_{a_2,\ldots,a_{18}} \to \mathcal{M}_3^f$ now have degree $|\mathrm{Sp}_6(\mathbf{F}_2)| = 1451520$. The number of terms allowed in $A_i(a_2, \ldots, a_{18}, s_{-1}, \ldots, s_{-17})$ by the bigradation is the coefficient of $x^i t^{19i}$ in

$$\prod_{d \in \{2,6,8,10,12,14,18\}} \frac{1}{(1-t^d)(1-xt^d)}. \tag{2.4.2}$$

For $i = 18$, this number is $11,617,543,745$, so complete computations in the style of this paper seem infeasible.

For $g = 4$, one needs to go quite far away from the 10-dimensional variety $\mathcal{A}_4$ to obtain a statement parallel to the previous ones. Even the nine-dimensional variety $\mathcal{M}_4$ is too large

because for a generic genus four curve X corresponding to a point in $\mathcal{M}_4$, the image of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in its action on $\mathrm{Jac}(X)[2]$ is $\mathrm{Sp}_8(\mathbf{F}_2)$, and this group is not a complex reflection group. However, one can work with the smooth curves

$$y^3 + (a_2x^3 + a_8x^2 + a_{14}x + a_{20})y + (x^5 + a_{12}x^3 + a_{18}x^2 + a_{24}x + a_{30}) = 0 \qquad (2.4.3)$$

and a corresponding seven-dimensional moduli space $\mathcal{M}_4^s \subset \mathbf{P}^7(2, \ldots, 30)$. For a generic curve in (2.4.3), the image of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is the index 136 subgroup $\mathrm{O}_8^+(\mathbf{F}_2) : 2$ of $\mathrm{Sp}_8(\mathbf{F}_2)$. Now from the invariant theory of the largest Shephard–Todd group ST37 $= W(E_8) = 2.\,\mathrm{O}_8^+(\mathbf{F}_2){:}2$, one gets polynomials $A_i(a_2, \ldots, a_{30}, s_{-1}, \ldots, s_{-29})$ and covering maps $\mathcal{M}_{a_2,\ldots,a_{30}} \to \mathcal{M}_4^s$ of degree $|\,\mathrm{O}_8^+(\mathbf{F}_2){:}2| = 348,364,800$. Aspects of this situation are within computational reach; for example Shioda computed the degree 240 polynomial $F(a_2, \ldots, a_{30}, z)$ analogous to (2.2.3) and (2.3.1). However the number of allowed terms in $A_i(a_2, \ldots, a_{30}, s_{-1}, \ldots, s_{-29})$ is even larger than in the previous $g = 3$ case, being the coefficient of $x^i t^{31i}$ in the analog of (2.4.2) where d runs over $\{2, 8, 12, 14, 18, 20, 24, 30\}$. For $i = 30$, this number is $100,315,853,630,512$. We close the paper with this $W(E_8)$ case because it is here that the paper actually began: the polynomial (2.3.1) for our main case $C_3 \times \mathrm{Sp}_4(\mathbf{F}_3)$ is also the specialization $F(0, 0, a_{12}, 0, a_{18}, 0, a_{24}, a_{30}, z)$ of Shioda's polynomial.

CHAPTER 3

SOME MODULAR ABELIAN SURFACES

3.1 Introduction

Let $C/\mathbf{Q}$ be a smooth projective curve of genus g. Let[1] $\Gamma_{\mathbf{C}}(s) = (2\pi)^{-s}\Gamma(s)$. Associated to C and its Jacobian $A = \mathrm{Jac}(C)$ is a completed L-function

$$\Lambda(C, s) = \Gamma_{\mathbf{C}}(s)^g \prod_p L_p(C, p^{-s})^{-1},$$

where, for any $\ell \neq p$, $L_p(C, T) = \det\left(I_{2g} - T \cdot \mathrm{Frob}_p \mid H^1_{\mathrm{et}}(C, \mathbf{Q}_\ell)^{I_p}\right)$. We say that C is automorphic if $\Lambda(C, s) = \Lambda(\pi, s)$, where π is an automorphic form for $\mathrm{GL}_{2g}(\mathbf{Q})$, and $\Lambda(\pi, s)$ is the completed L-function associated to the standard representation of GL_{2g}. If C is automorphic, then

$$\Lambda(C, s) = \pm N^{1-s}\Lambda(C, 2 - s),$$

where N is the conductor of A. One conjectures that all smooth projective curves C over $\mathbf{Q}$ are automorphic. When $g = 0$ and $g = 1$, one knows that C is automorphic by theorems of Riemann [32] and Wiles et al. [38, 37, 8] respectively. The conjecture seems completely hopeless with current technology for general curves when $g \geq 3$, but for $g = 2$ it was recently proved in [7] that all such curves over $\mathbf{Q}$ (and even over totally real fields) were potentially automorphic. For abelian surfaces over $\mathbf{Q}$, let us additionally say that $A = \mathrm{Jac}(C)$ is *modular* of level N if there exists a cuspidal Siegel modular form f of weight two such that $\Lambda(C, s) = \Lambda(f, s)$, where $\Lambda(f, s)$ is the completed L-function associated to the degree four spin representation of GSp_4. If A is modular in this sense, then it is also automorphic in the sense above by taking π to be the transfer of the automorphic representation associated

1. There is some ambiguity in the literature as to whether one defines $\Gamma_{\mathbf{C}}(s)$ to be $(2\pi)^{-s}\Gamma(s)$ or $\Gamma_{\mathbf{R}}(s)\Gamma_{\mathbf{R}}(s+1) = 2\cdot(2\pi)^{-s}\Gamma(s)$. It makes no difference as long as one uses the same choice for both $\Lambda(C, s)$ and $\Lambda(\pi, s)$. To be safe, we make the same choice as Serre [34, §3(20)].

to f from $\mathrm{GSp}(4)/\mathbf{Q}$ to $\mathrm{GL}(4)/\mathbf{Q}$. It was also shown in [7] that certain classes of abelian surfaces over $\mathbf{Q}$ were actually modular (see Theorem 3.1.1 below), and even that there were infinitely many modular abelian surfaces over $\mathbf{Q}$ up to twist with $\mathrm{End}_{\mathbf{C}}(A) = \mathbf{Z}$. However, no explicit examples of such surfaces were given in that paper.

The aim of this note is to give explicit examples of modular abelian surfaces $A/\mathbf{Q}$ with $\mathrm{End}_{\mathbf{C}}(A) = \mathbf{Z}$ and such that A has good reduction outside a set S that is either $S = \{2, 5\}$, $S = \{2, 5, 7\}$, or $S = \{2, 3, 7\}$. Previous explicit examples of modular abelian surfaces with trivial endomorphisms were found by [10] (in 2015) and also by [2]; these results relied heavily on very delicate and explicit computations of spaces of low weight Siegel modular forms following [31, 30]. In particular, they rely on the conductor being relatively small and also take advantage of the fact that the conductor is odd and squarefree. (The examples in those papers are of conductors 277, 353, 587, and $731 = 17 \cdot 43$.) In contrast, the examples of this paper only require verifying some local properties of A at the prime p (with $p = 3$ or $p = 5$) and showing that the image of the action of $G_{\mathbf{Q}}$ on the p-torsion of $A = \mathrm{Jac}(C)$ is of a suitable form. Although the conductors of our examples have only small factors, the conductors themselves are quite large — the smallest of our examples has conductor $98000 = 2^4 \cdot 5^3 \cdot 7^2$. The modularity of the examples in this paper follows by applying the following result (with either $p = 3$ or $p = 5$) proved in [7, Propositions 10.1.1 and 10.1.3].

Theorem 3.1.1. *Let $A/\mathbf{Q}$ be an abelian surface with good ordinary reduction at $v|p$ and a polarization of degree prime to p, and suppose that the eigenvalues of Frobenius on $A[p](\overline{\mathbf{F}}_p)$ are distinct. Let*

$$\overline{\rho}_{A,p} : G_F \to \mathrm{GSp}_4(\mathbf{F}_p)$$

denote the mod-p Galois representation associated to $A[p]$, and assume that $\overline{\rho}_{A,p}$ has vast and tidy image in the notation of [7]. Suppose that either:

1. *$p = 3$, and $\overline{\rho}_{A,3}$ is induced from a 2-dimensional representation over a real quadratic*

extension $F/\mathbf{Q}$ in which 3 is unramified.

2. *$p = 5$, and $\overline{\rho}_{A,5}$ is induced from a 2-dimensional representation valued in $\mathrm{GL}_2(\mathbf{F}_5)$ over a real quadratic extension $F/\mathbf{Q}$ in which 5 is unramified.*

Then A is modular.

A precise definition of what representations are vast and tidy is included in §7.5 of [7], but we content ourselves with the following list which exhausts all of our examples:

Lemma 3.1.1 (Examples of vast and tidy representations from [7, Lemmas 7.5.13 and 7.5.21])**.** The representation $\overline{\rho}_{A,p}$ is automatically vast and tidy when the image of $\overline{\rho}_{A,p}$ is one of the following conjugacy classes of subgroups of $\mathrm{GSp}_4(\mathbf{F}_p)$:

1. The groups G_{2304}, G_{768}, G'_{768} or G_{480} in $\mathrm{GSp}_4(\mathbf{F}_3)$ of orders 2304, 768, 768, and 480, where:

   (a) The group G_{2304} is a semi-direct product $\Delta \rtimes \mathbf{Z}/2\mathbf{Z}$ where

   $$\Delta = \left\{(A, B) \in \mathrm{GL}_2(\mathbf{F}_3)^2 \mid \det(A) = \det(B)\right\};$$

   it is (up to conjugacy) the unique subgroup of order 2304 of $\mathrm{GSp}_4(\mathbf{F}_3)$.

   (b) The groups G_{768} and G'_{768} are subgroups of G_{2304} of index 3, and are (up to conjugacy) the only two subgroups of order 768 of $\mathrm{GSp}_4(\mathbf{F}_3)$. They are isomorphic as abstract groups, but they are distinguished up to conjugacy inside $\mathrm{GSp}_4(\mathbf{F}_3)$ by their intersections H_{384} and H'_{384} with $\mathrm{Sp}_4(\mathbf{F}_3)$. In particular, $(H_{384})^b \simeq \mathbf{Z}/6\mathbf{Z}$ and $(H'_{384})^b \simeq \mathbf{Z}/2\mathbf{Z}$. According to the small groups database of `magma` (cf. [4]),

   $$G_{768} \simeq G'_{768} \simeq \texttt{SmallGroup(768,1086054)},$$

   whereas

   $$H_{384} \simeq \texttt{SmallGroup(384, 18130)}, \quad H'_{384} \simeq \texttt{SmallGroup(384, 618)}.$$

These groups can also be distinguished by their images P_{192} and P'_{192} in $\mathrm{PSp}_4(\mathbf{F}_3) \subset \mathrm{PGSp}_4(\mathbf{F}_3)$, namely

$$P_{192} \simeq \texttt{SmallGroup(192, 1493)}, \quad P'_{192} \simeq \texttt{SmallGroup(192, 201)}.$$

(c) The group G_{480} is a semi-direct product $\widetilde{A}_5 \rtimes \langle\sigma\rangle$ where $\widetilde{A}_5 \subset \mathrm{GL}_2(\mathbf{F}_9)$ is a central extension of A_5 by $\mathbf{Z}/4\mathbf{Z}$. There are precisely two subgroups of this order up to conjugacy in $\mathrm{GSp}_4(\mathbf{F}_3)$. The second subgroup G'_{480} also contains $\widetilde{A}_5$ with index two, but it is not a semi-direct product. According to the small groups database of `magma`,

$$G_{480} \simeq \texttt{SmallGroup(480, 948)}, \quad G'_{480} \simeq \texttt{SmallGroup(480, 947)}.$$

2. The group G_{115200} in $\mathrm{GSp}_4(\mathbf{F}_5)$ is a semi-direct product $\Delta \rtimes \mathbf{Z}/2\mathbf{Z}$ where

$$\Delta = \left\{(A, B) \in \mathrm{GL}_2(\mathbf{F}_5)^2 \mid \det(A) = \det(B)\right\};$$

it is (up to conjugacy) the unique subgroup of order 115200 of $\mathrm{GSp}_4(\mathbf{F}_5)$.

The conditions of the theorem are all very easy to verify in any given example (once found) with the possible exception of computing the image of the mod-p representation for $p = 3$ or 5. We describe how we computed this in the section below. The second problem is then to find a list of candidate curves. Our original approach involved searching for curves in a large box, which did indeed result in a number of examples. However, we then switched to using a collection of curves provided to us by Andrew Sutherland, all of which had the property that they had good reduction outside the set $\{2, 3, 5, 7\}$ (these were found during the construction of [5] but discarded because their minimal discriminants were too large). This list consisted of some 20 million curves, so the next task was to identify examples to which we could apply Theorem 3.1.1. For a genus two curve C on Sutherland's list, we

applied the following algorithm.

1. Fix a real quadratic field F of fundamental discriminant D dividing Δ_C in which $p \in \{3, 5\}$ is unramified. Since Δ_C is only divisible by primes in $\{2, 3, 5, 7\}$, there are at most seven such F. Let χ_D denote the quadratic character associated to F.

2. Check whether $a_q \equiv 0 \mod p$ for all primes $q \leq 100$ of good reduction for C with $\chi_D(q) = -1$.

3. Check that $a_q \neq 0$ for at least one prime $q \leq 100$ of good reduction for C with $\chi_D(q) = -1$.

Any C that passes this test is likely to have the following two properties: $\overline{\rho}_{A,p}$ is induced from F, but the p-adic representation $\rho_{A,p}$ itself is not induced. The third condition in particular guarantees that A itself is not isogenous to a base change of an elliptic curve defined over F. Note that this test is very fast — one can discard a C as soon as one finds a prime q with $\chi_D(q) = -1$ and $a_q \not\equiv 0 \mod p$, so for almost all curves C, one only has to compute a_q for very small primes q. In addition, the following postage stamp calculation with the Chebotarev density theorem suggests that false positives will be few in number: for each of the allowable discriminants D (there are 7 such D for either $p = 3$ or $p = 5$), there are at least $M \geq 10$ primes in the interval $[10, 100]$ with $\chi_D(q) = -1$. A "random" abelian surface A will have $a_q \equiv 0 \mod p$ for any such prime q approximately $1/p$ of the time (the exact expectation depends on $A[p]$ — if the mod-p representation is surjective, the exact expectation that $a_q \equiv 0 \mod p$ for a random prime q is $231/640$ for $p = 3$ and $3095/14976$ for $p = 5$), and so one might expect a false positive to occur with probability approximately $1/p^M$. On the other hand, false positives are certainly not impossible. In our original box search, we did find the one curve $C : y^2 = x^5 - 2x^4 + 6x^3 + 5x^2 + 10x + 5$ that "passed" the test for $\overline{\rho}_{A,3}$ to be induced from $\mathbf{Q}(\sqrt{7})$, whereas it turns out instead to be induced from $\mathbf{Q}(\sqrt{85})$ — requiring only an accidental vanishing of a_q for $q = 23$, 73, 89,

and 97. The smallest prime guaranteeing that $\overline{\rho}_{A,3}$ is not induced from $\mathbf{Q}(\sqrt{7})$ in this case is $a_{151} = 5 \not\equiv 0 \mod 3$.

3.1.1 Acknowledgments

We would like to thank Andrew Booker, Andrew Sutherland, and John Voight for useful discussions about this project. We would also like to thank Andrew Sutherland for providing us with a large list of genus two curves over $\mathbf{Q}$ with good reduction outside $\{2, 3, 5, 7\}$. Finally, we would like to thank Andrew Sutherland and Andrew Booker for help computing the 2-part of the conductors of our curves.

3.2 Determining the mod-p representation

Consider a genus two curve

$$C : Y^2 = f(X),$$

with $\deg(f) = 6$. The desingularization of the corresponding projective curve has two points $\mathfrak{b}_1$ and $\mathfrak{b}_2$ at infinity. The canonical class $\mathfrak{D}$ in $\mathrm{Pic}^2(C)$ is represented by the divisor $\mathfrak{b}_1 + \mathfrak{b}_2$, and the Jacobian $A = \mathrm{Jac}(C)$ can be identified with $\mathrm{Pic}^2(C)$ under addition of the canonical class. By Riemann–Roch, every class in $\mathrm{Pic}^2(C)$ except $\mathfrak{D}$ has precisely one effective divisor. Thus, we may represent any point of A as an unordered pair $\{P, Q\}$ of points on C.

If we assume $f(X)$ has a rational root, then, by suitably transforming the variables X and Y, we can make $\deg(f) = 5$; then, there will be exactly one point $\mathfrak{b}$ at infinity, and the canonical class will be represented by $2\mathfrak{b}$. We will not need this assumption, however, and several of our examples do not have any Weierstrass points over $\mathbf{Q}$.

3.2.1 $p = 3$

Let $K/\mathbf{Q}$ denote the Galois closure of the corresponding projective representation. It will contain the field $\mathbf{Q}(x+u, xu, yv)$ for any 3-torsion point $\{P, Q\}$ of A, where $P = (x, y)$ and $Q = (u, v)$. There exist polynomials B_{ij}, given in [16, Theorem 3.4.1 and Appendix II], using which the multiplication-by-n map can be described explicitly at the level of the Kummer surface of A. Writing the equation $[2]\{P, Q\} = -\{P, Q\}$ in terms of the Kummer coordinates explicitly, taking resultants, and eliminating spurious solutions, one can compute the minimal polynomials of $x+u$, xu and yv in any particular case, as well as determine the Galois group of the corresponding extension.

Note that the first coordinates determine the $\mathrm{GSp}_4(\mathbf{F}_3)/\langle \pm 1 \rangle = \mathrm{PGSp}_4(\mathbf{F}_3)$-representation, so this determines the image of $\overline{\rho}_{A,3}$ modulo the central subgroup of order 2 as an abstract group. One can similarly compute the field $\mathbf{Q}(y+v, yv)$ if one wants to know the full $\mathrm{GSp}_4(\mathbf{F}_3)$-representation. In any case of interest, this is enough (purely by considering possible orders) to determine the order of the image of $\overline{\rho}_{A,3}$ itself. It then remains to determine the precise subgroup of $\mathrm{GSp}_4(\mathbf{F}_3)$ in the cases where this is ambiguous. The group $\mathrm{PGSp}_4(\mathbf{F}_3)$ has a natural permutation representation on 40 points, corresponding to the non-zero points of $A[3]$ up to sign (warning: the group $\mathrm{PGSp}_4(\mathbf{F}_3)$ has a second non-conjugate representation on 40 points). From this data, one can distinguish between G_{480} and G'_{480} purely based on the degrees of the polynomials arising from the computation above. Table 3.1 gives the corresponding decomposition in the cases of interest:

G	Orbits
G_{2304}	8, 32
G_{768}	8, 32
G'_{768}	8, 32
G_{480}	20, 20
G'_{480}	40

Table 3.1: Orbit decomposition for subgroups of $\mathrm{PGSp}_4(\mathbf{F}_3)$.

The groups G_{768} and G'_{768} cannot be distinguished by this method. This is not important for establishing modularity since both groups give representations with vast and tidy image. However, in order to complete the tables, we distinguish between these cases as follows: we *explicitly* compute (using `magma`) the Galois group of the corresponding degree 32 polynomial over the field $\mathbf{Q}(\sqrt{-3})$, and see whether the resulting group is P_{192} or P'_{192} (in which case the group is G_{768} or G'_{768} respectively).

3.2.2 $p = 5$

Similar to the $p = 3$ case, for an arbitrary point $\{P = (x, y), Q = (u, v)\}$ of A, we write the equation $3\{P, Q\} = -2\{P, Q\}$ in terms of the Kummer coordinates of the point, and take resultants to find the minimal polynomials of $x + u, xu$ and yv of 5-torsion points on A. The splitting field of these polynomials is the Galois closure $K/\mathbf{Q}$ of the representation to $\mathrm{PGSp}_4(\mathbf{F}_5) = \mathrm{GSp}_4(\mathbf{F}_5)/\langle \pm 1 \rangle$.

We describe an algorithm for showing that the image $\overline{\rho}_{A,5}$ of a mod-5 representation in $\mathrm{GSp}_4(\mathbf{F}_5)$ with cyclotomic determinant has image G_{115200}. The group $\mathrm{GSp}_4(\mathbf{F}_5)$ has a representation on $312 = (5^4 - 1)/2$ points, given by the action on the non-trivial 5-torsion points up to sign (which factors through $\mathrm{PGSp}_4(\mathbf{F}_5)$).

Lemma 3.2.1. *Let $G \subset \mathrm{GSp}_4(\mathbf{F}_5)$ be a subgroup, and suppose that the similitude character is surjective on G, or equivalently that $[G : G \cap \mathrm{Sp}_4(\mathbf{F}_5)] = 4$. Suppose, in addition, that G acts on the degree 312 permutation representation above with two orbits of size 288 and 24 respectively. Then:*

1. *G is one of four groups, distinguished by their orders: 2304, 4608, 57600, and 115200.*
2. *The degree 24 permutation representation of G factors through a group of order 576, 1152, 14400, and 28800 respectively.*

In particular, we can distinguish these representations by computing the Galois group of the factor of size 24. Hence by computing the corresponding polynomials of order 24 and 288

we can verify that the image is indeed G_{115200}.

3.2.3 Checking the Sato–Tate group

For all the residual representations we consider, it turns out that the image of $\overline{\rho}$ is big enough to guarantee that the Sato–Tate group is either $\mathrm{USp}(4)$ or the normalizer of $\mathrm{SU}(2) \times \mathrm{SU}(2)$. More precisely:

Lemma 3.2.2. *Suppose that $p = 3$ and that $\overline{\rho}_{A,p}$ has image either G_{480}, G_{768}, G'_{768}, G_{2304}, or that $p = 5$, and $\overline{\rho}_{A,p}$ has image G_{115200}. Then the Sato–Tate group of A is either $\mathrm{USp}(4)$ or $N(\mathrm{SU}(2) \times \mathrm{SU}(2))$. Moreover, if the Sato–Tate group is $N(\mathrm{SU}(2) \times \mathrm{SU}(2))$, the quadratic extension $F/\mathbf{Q}$ over which A has Sato–Tate group $\mathrm{SU}(2) \times \mathrm{SU}(2)$ is the quadratic field F from which $\overline{\rho}$ is induced.*

Proof. The image of $\overline{\rho}_{A,p}$ is constrained by the Sato–Tate group, and thus the fact that the Sato–Tate group can only be $\mathrm{USp}(4)$ or $N(\mathrm{SU}(2)\times\mathrm{SU}(2))$ follows directly from a classification of all such groups in [21]. (In fact, when the image is G_{480}, only the first case can occur.) In the latter case, the representation becomes reducible over the quadratic extension F where A has Sato–Tate group $\mathrm{SU}(2) \times \mathrm{SU}(2)$, and (for the given $\overline{\rho}$) this forces F to be the field from which $\overline{\rho}$ is induced. □

In particular, in all our examples, our initial selection process requires the existence of a prime q of good reduction with $\chi(q) = -1$ and $a_q \neq 0$, which implies that $\rho_{A,p}$ cannot be induced from F, and thus the Sato–Tate group in each example below is $\mathrm{USp}(4)$.

3.3 Examples

Of the curves we consider, a number satisfy the conditions of the main theorem, and are thus provably modular. For any curve C that is modular, so too are any quadratic twists. Hence we only list a single representative curve for each equivalence class of abelian surfaces under both $\mathbf{Q}$-isogenies and twisting by quadratic characters.

3.3.1 Inductions from $\mathrm{GL}_2(\mathbf{F}_3)$ and $\mathrm{GL}_2(\mathbf{F}_9)$

We first give the examples of modular curves whose mod-3 representation is induced from either $\mathrm{GL}_2(\mathbf{F}_3)$ or $\mathrm{GL}_2(\mathbf{F}_9)$-representations of G_F for real quadratic fields F. It turns out that, in the range of our computation, the representation $\overline{\rho}$ up to twist determined the representation ρ up to twist — after applying our other desiderata, including that $A/\mathbf{Q}$ had good reduction at p and had Sato–Tate group $\mathrm{USp}(4)$. In particular, all the examples below give rise to mod-3 representations that are not twist equivalent. The examples C we choose to list in Table 3.2 are of minimal conductor amongst all those with Jacobian isogenous to a twist of $\mathrm{Jac}(C)$. The conductors were computed rigorously away from 2 using `magma`. The conductors at 2 were computed for us by Andrew Sutherland using an analytic algorithm discussed in §5.2 of [5]. This computation *assumes* the analytic continuation and functional equation for $L(A, s)$, which we know to be true in this case. (More precisely, as explained to us by Andrew Booker, one version of this program gives a non-rigorous computation of these conductors and a second slower but more rigorous version then confirms these values.) In the case of ties, we chose the curve with smaller minimal discriminant. In the case of subsequent ties, we eyeballed the different forms and chose the one that looked the prettiest.

Theorem 3.3.1. *The Jacobians $A = \mathrm{Jac}(C)$ of the following smooth genus two curves C over $\mathbf{Z}[1/70]$ given in Table 3.2 are modular. In particular, the L-function $L(A, s)$ is holomorphic in $\mathbf{C}$ and satisfies the corresponding functional equation. Each A has good ordinary reduction at 3 and is 3-distinguished and $\mathrm{End}_{\mathbf{C}}(A) = \mathbf{Z}$. Moreover, the representation $\overline{\rho}_{A,3}$ is induced from a $\mathrm{GL}_2(\overline{\mathbf{F}}_3)$-valued representation of G_F that is vast and tidy.*

Curve	Cond	Disc	$\mathrm{im}(\overline{\rho})$	Δ_F
$y^2 = x^6 - 10x^4 + 2x^3 + 31x^2 - 13x - 18$	$2^4 5^3 7^2$	$2^8 5^3 7^3$	G_{480}	5
$y^2 = -5x^6 - 20x^5 - 10x^4 + 36x^3 + 22x^2 - 20x$	$2^{10} 5^3 7$	$2^{20} 5^4 7^3$	G'_{768}	5
$y^2 + y = -4x^5 - 23x^4 - 22x^3 + 74x^2 - 40x + 6$	$2^8 5^3 7^2$	$2^{19} 5^7 7^2$	G_{2304}	5
$y^2 = 16x^6 - 46x^4 + 10x^3 + 46x^2 - 9x - 17$	$2^{12} 5^2 7^4$	$2^{19} 5^9 7^4$	G_{480}	5
$y^2 = 2x^5 - 8x^4 + 26x^2 - 7x - 26$	$2^{15} 5$	$2^{16} 5^3$	G_{2304}	8
$y^2 = x^5 - x^4 - 4x^3 - 44x^2 - 60x - 100$	$2^{14} 5 \cdot 7$	$2^{33} 5^3 7$	G_{2304}	8
$y^2 = x^5 - 17x^4 + 70x^3 + 26x^2 - 35x - 29$	$2^{16} 5 \cdot 7$	$2^{37} 5^3 7$	G_{2304}	8
$y^2 + x^2 y = 13x^6 - 29x^5 - 10x^4 + 41x^3 + 6x^2 + 20x + 20$	$2^7 5^2 7^4$	$2^{16} 5^2 7^{16}$	G_{2304}	8
$y^2 = x^5 - 11x^4 - 2x^3 - 34x^2 - 5x - 25$	$2^{20} 5 \cdot 7$	$2^{21} 5^3 7^3$	G_{768}	8
$y^2 = -2x^6 - 41x^5 - 48x^4 + 54x^3 + 42x^2 - 49x$	$2^{14} 5^2 7^4$	$2^{32} 5^2 7^{11}$	G_{2304}	8
$y^2 = 2x^5 + 34x^4 - 16x^3 - 52x^2 - 13x - 1$	$2^{19} 5^3 7^2$	$2^{20} 5^5 7^6$	G'_{768}	8
$y^2 = 8x^6 - 24x^5 - 4x^4 + 20x^3 + 49x^2 - 21x - 28$	$2^{15} 5^2 7^4$	$2^{23} 5^6 7^9$	G_{2304}	8
$y^2 + (x+1)y = 64x^5 - 8x^4 + 39x^3 + x^2 + 2x + 1$	$2^7 5^3 7^3$	$2^{27} 5^6 7^6$	G_{480}	40
$y^2 = 15x^5 + 23x^4 + 20x^3 + 28x^2 + 12x - 4$	$2^{14} 3 \cdot 5^3$	$2^{33} 3^2 5^4$	G_{2304}	40
$y^2 = 3x^5 + 7x^4 + 28x^3 + 20x^2 + 28x - 36$	$2^{14} 3 \cdot 5^3$	$2^{36} 3^2 5^4$	G_{2304}	40

Table 3.2: Some smooth genus 2 curves with Jacobians A that are modular, 3-distinguished, and have good ordinary reduction at 3 and $\mathrm{End}_{\mathbf{C}}(A) = \mathbf{Z}$.

Example 3.3.1. *Precisely one curve in Table 3.2 is actually smooth over a smaller ring, namely the curve of conductor* $163840 = 2^{15} \cdot 5$ *which is smooth over* $\mathbf{Z}[1/10]$. *This curve has a quadratic twist with particularly small naïve height, namely the curve:*

$$y^2 = 4x^5 + 6x^4 + 4x^3 + 6x^2 + 2x + 3$$

which also has conductor $163840 = 2^{15} \cdot 5$ *but larger minimal discriminant*

$$131072000000 = 2^{23} \cdot 5^6$$

rather than $8192000 = 2^{16} \cdot 5^3$ *as the curve in the table. The mod-*3 *representation of both of these curves is actually unramified at* 5*, and is congruent up to twist to the mod-*3 *representation attached to the curve* $y^2 = 4x^5 - 4x^4 + 4x^3 - 2x^2 + x$ *of conductor* 2^{15}*. The Jacobian of this latter curve is isogenous to* $\mathrm{Res}_{\mathbf{Q}(\sqrt{2})/\mathbf{Q}}(E)$*, where* E *is the elliptic curve:*

$$y^2 + \sqrt{2}xy = x^3 + (-1 - \sqrt{2})x^2 + 2(\sqrt{2} + 1)x - 3\sqrt{2} - 5.$$

3.3.2 Inductions from $\mathrm{GL}_2(\mathbf{F}_5)$

We now consider the case $p = 5$.

Theorem 3.3.2. *The Jacobians* $A = \mathrm{Jac}(C)$ *of the following smooth genus two curves* C *over* $\mathbf{Z}[1/42]$ *are modular. In particular, the L-function* $L(A, s)$ *is holomorphic in* $\mathbf{C}$ *and satisfies the corresponding functional equation. Each* A *has good ordinary reduction at* 5 *and is* 5*-distinguished and* $\mathrm{End}_{\mathbf{C}}(A) = \mathbf{Z}$*. Moreover, the representation* $\overline{\rho}_{A,5}$ *is induced from a* $\mathrm{GL}_2(\mathbf{F}_5)$*-valued representation of* G_F *that is vast and tidy.*

Curve	Cond	Disc	$\mathrm{im}(\overline{\rho})$	Δ_F
$y^2 + xy = 7x^6 - 22x^5 - 7x^4 + 61x^3 - 3x^2 - 54x - 12$	$2^7 3^2 7^3$	$2^{11} 3^9 7^4$	G_{115200}	8
$y^2 = 8x^6 - 24x^5 - 30x^4 + 8x^3 - 24x^2 - 48x - 8$	$2^6 3^8 7$	$2^{51} 3^8 7$	G_{115200}	8

Table 3.3: Some smooth genus 2 curves with Jacobians A that are modular, 5-distinguished, and have good ordinary reduction at 5 and $\mathrm{End}_{\mathbf{C}}(A) = \mathbf{Z}$.

The second curve also admits a quadratic twist of smaller naïve height, namely

$$y^3 + x^2 y = x^6 - 3x^5 - 4x^4 + x^3 - 3x^2 - 6x - 1$$

of conductor $5878656 = 2^7 \cdot 3^8 \cdot 7$ and minimal discriminant $96315899904 = 2^{21} \cdot 3^8 \cdot 7$.

CHAPTER 4

MOD-P GALOIS REPRESENTATIONS NOT ARISING FROM ABELIAN VARIETIES

4.1 Introduction

Let $g \geq 1$ and p be a prime. Let $\mathcal{A}_g(p)$ be the Siegel modular variety which is the moduli space of principally polarized abelian varieties of dimension g with full level p structure. The space $\mathcal{A}_g(p)$ is geometrically rational only for $(g,p) = (1,2)$, $(1,3)$, $(1,5)$, $(2,2)$, $(2,3)$, $(3,2)$ [24]. Furthermore, in all the genus 1 cases above, it is known that $\mathcal{A}_1(p)$ and its twists $\mathcal{A}_1(\rho)$ corresponding to two dimensional mod-p Galois representations ρ with cyclotomic determinant, are in fact rational over $\mathbf{Q}$. That is, if $\rho : G_{\mathbf{Q}} \to \mathrm{GL}(2, \mathbf{F}_p)$ with $p = 2, 3, 5$ is any representation with cyclotomic determinant, then it arises from an elliptic curve over $\mathbf{Q}$, and in fact from infinitely many elliptic curves [33]. In the three exceptional cases with $g \geq 2$, the corresponding moduli spaces $\mathcal{A}_g(p)$ and their twists are all unirational, as explained in [7, Lemma 10.2.4] and [15, §4.4]. Hence, in these cases, all representations $\rho : G_{\mathbf{Q}} \to \mathrm{GSp}(2g, \mathbf{F}_p)$ with cyclotomic similitude character do arise from g-dimensional abelian varieties over $\mathbf{Q}$.

In this paper, we consider the cases where $g \geq 2$ and $\mathcal{A}_g(p)$ is not geometrically rational. The main theorem we prove is:

Theorem 4.1.1. *Let $g \geq 2$ and p be a prime number. Suppose (g,p) is not one of $(2,2)$, $(2,3)$, $(3,2)$. Then there exists a Galois representation $\rho : G_{\mathbf{Q}} \to \mathrm{GSp}(2g, \mathbf{F}_p)$ with cyclotomic similitude character such that ρ does not arise from the p-torsion of any abelian variety over $\mathbf{Q}$.*

The case $g = 1, p > 5$ has been studied earlier in [12], [19] which show the existence of non-elliptic mod-p Galois representations. The representations constructed in [12] for $p \geq 11$ are modular, semistable Galois representations of weight 2 and level $\Gamma_0(N)$. For $p = 7$, one

desired representation is constructed explicitly, with image contained in the normalizer of the non-split Cartan subgroup. We extend this idea to higher genus situations.

Our approach is as follows. Let $l \neq p$ be any prime. For any mod-p representation arising from an abelian variety, we use Raynaud's inertial criteria for semistable reduction and deduce that there exists a constant K_g only depending on g such that the prime to p part of the order of image of the inertia subgroup at l divides K_g. On the other hand, we can easily show using Zsigmondy's theorem that there exists $q > 1$ coprime to p such that q divides $\#\,\mathrm{GSp}(2g, \mathbf{F}_p)$ and does not divide K_g. If one could construct Galois representations valued in $\mathrm{GSp}(2g, \mathbf{F}_p)$ with cyclotomic similitude and such that the image of inertia at l had order q, we could then deduce that such Galois representations did not come from abelian varieties. But the inverse Galois problem (with local conditions) for $\mathrm{GSp}(2g, \mathbf{F}_p)$ is unknown — indeed the standard approach to constructing such groups as Galois groups is to use abelian varieties which is the opposite of what we want. We instead describe various *solvable* subgroups of $\mathrm{GSp}(2g, \mathbf{F}_p)$ which have an element of order q and are also big enough so that the restriction of the similitude character is surjective. We then attempt to construct these groups as Galois representations using class field theory. The condition that the similitude character is cyclotomic leads to some non-split embedding problems which we solve using Galois cohomological machinery related to the Grunwald-Wang theorem.

In Section 4.2, we recall basic notions about abelian varieties and semistable reduction. Let $K_g = \gcd_{\text{primes } r \neq 2} \#\,\mathrm{GSp}(2g, \mathbf{F}_r)$. We show that if ρ is the p-torsion representation of a g-dimensional abelian variety over $\mathbf{Q}$, then the prime to p part of $\#\rho(I_l)$ divides K_g.

Let $d \geq 1$. In Section 4.3, we study several solvable subgroups inside $\mathrm{GSp}(2d, \mathbf{F}_p)$. We consider a symplectic pairing on k^2 valued in $\mathbf{F}_p$, where $k = \mathbf{F}_{p^d}$. The natural action of $\mathrm{SL}(2, k)$ on k^2 gives us a map $\mathrm{SL}(2, k) \to \mathrm{Sp}(2d, \mathbf{F}_p)$. Let $C_1 \subset \mathrm{Sp}(2d, \mathbf{F}_p)$ denote the image of the non-split Cartan subgroup of $\mathrm{SL}(2, k)$, and N denote a certain subgroup of the normalizer of C_1 in $\mathrm{GSp}(2d, \mathbf{F}_p)$. Then C_1 is a cyclic group of order $p^d + 1$, $[N, N] = C_1$, and $N^{ab} \simeq \mathbf{Z}/(p-1) \times \mathbf{Z}/2d$. The quotient on to the first factor $\mathbf{Z}/(p-1) \simeq \mathbf{F}_p^\times$ in

fact corresponds to the similitude character. Conjugation action of N^{ab} on $[N,N]$ factors through the $\mathbf{Z}/2d$ factor, and it is given by multiplication by p. When $p=2$, N is in fact a semi-direct product.

In Section 4.4, we consider odd primes p and study the embedding problem

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbf{Q}} & & \\ & & & & & \overset{?}{\swarrow} & \downarrow{\scriptstyle \phi} & & \\ 0 & \longrightarrow & [N,N] = \mathbf{Z}/(p^d+1) & \longrightarrow & N & \longrightarrow & \mathbf{Z}/(p-1)\times\mathbf{Z}/2d & \longrightarrow & 0 \end{array} \tag{4.1.1}$$

for some ϕ with $\mathrm{pr}_1 \circ \phi$ equal to the p-cyclotomic character. We choose ϕ carefully so that all local obstructions to the embedding problem vanish. We then show that global obstructions vanish as well, and that ϕ can be lifted to a proper solution $\tilde{\phi} : G_{\mathbf{Q}} \to N$.

In Section 4.5, we finish the proof of the main theorem. We twist $\tilde{\phi}$ to obtain representations ρ such that $\rho(I_l) \subset [N,N]$ has prime power order q not dividing K_g. By allowing ourselves to consider reducible representations landing inside $\mathrm{GSp}(2d, \mathbf{F}_p) \subset \mathrm{GSp}(2g, \mathbf{F}_p)$ for $d \leq g$, we can deal with all cases except $(g,p) = (3,3)$ using this approach. We deal with the exceptional case explicitly, by producing a representation whose image in $\mathrm{GSp}(6, \mathbf{F}_3)$ has order 78, with $\rho(I_l)$ being the unique cyclic subgroup of order 13.

4.1.1 Acknowledgments

I would like to thank Frank Calegari for suggesting this problem, and for many helpful discussions.

4.2 Semistable reduction of abelian varieties

Let X be an abelian variety of dimension g defined over a field F. Let v be a discrete valuation on F, and $\mathcal{X}$ denote the Neron model of X at v. Let l be the residue characteristic of v.

Definition 4.2.1. *1. X is said to have good reduction at v, if the identity component of the special fiber of $\mathcal{X}$ is an abelian variety*

2. X is said to have semistable reduction at v, if the identity component of the special fiber of $\mathcal{X}$ is an extension of an abelian variety by an affine torus.

Let I_v denote the absolute inertia group at the finite prime v of F. For a rational prime p, let $X[p]$ and $T_p(X)$ denote the p-torsion subgroup and the p-adic Tate module of X respectively. The following are simple critera for semistable reduction in terms of inertial action on $T_p(X)$ and $X[p]$. The proofs can be found in Propositions 3.5 and 4.7 of [22], and Theorem 6 of [6, §7.4].

Theorem 4.2.1 (Grothendieck)**.** *Let $p \neq l$ be a prime. Then the following are equivalent.*

1. X has semistable reduction at v.

2. I_v acts unipotently on the Tate module $T_p(X)$.

Theorem 4.2.2 (Raynaud)**.** *Let $m \geq 3$ be an integer not divisible by l, and suppose that all the points of $X[m]$ are defined over an extension of F unramified at v. Then X has semistable reduction at v.*

Before describing the inertial condition alluded to in the introduction, we prove a few lemmas about the number $K_g = \gcd_{\text{primes } r \neq 2} \#\,\mathrm{GSp}(2g, \mathbf{F}_r)$. We repeatedly make use of Dirichlet's theorem about primes in arithmetic progression in the proofs. Let ν_p denote the p-adic valuation function normalized so that $\nu_p(p) = 1$.

Lemma 4.2.1. *All primes dividing K_g are less than or equal to $2g+1$. Further, if $g \geq 2$ and p is a prime such that $2 < p \leq 2g+1$, then $\nu_p(K_g) < g^2$.*

Proof. Suppose $p > 2g+1$ is a prime. Choose a primitive root $a \in \mathbf{Z}/p$ and let $r \equiv a \pmod{p}$ be a prime. Then, $r^{2i} - 1 \not\equiv 0 \pmod{p}$ for each $1 \leq i \leq g$ showing that p does not divide K_g.

For the second part of the lemma, choose a primitive root $a \in (\mathbf{Z}/p^{g^2})^\times$ and let $r \equiv a \pmod{p^{g^2}}$ be a prime. Then, for $n \leq g^2$, the order of $r \in (\mathbf{Z}/p^n)^\times$ is $p^{n-1}(p-1)$. So p^n divides a term $r^{2i}-1$ in the product below if and only if $p^{n-1}(p-1)$ dividies $2i$. Using this observation we count the powers of p to get that

$$\begin{aligned}\nu_p(\#\,\mathrm{GSp}(2g,\mathbf{F}_r)) &= \nu_p\left((r^2-1)(r^4-1)\cdots(r^{2g}-1)\right)\\ &= \left\lfloor\frac{2g}{p-1}\right\rfloor + \left\lfloor\frac{2g}{p(p-1)}\right\rfloor + \left\lfloor\frac{2g}{p^2(p-1)}\right\rfloor + \cdots\\ &\leq \left\lfloor\frac{2g}{2}\right\rfloor + \left\lfloor\frac{2g}{4}\right\rfloor + \left\lfloor\frac{2g}{8}\right\rfloor + \cdots < 2g \leq g^2\end{aligned}$$

since $g \geq 2$. Therefore, $\nu_p(K_g) < g^2$. □

Lemma 4.2.2. *For any $M > 2$, $K_g = \gcd_{\text{primes } r>M} \#\,\mathrm{GSp}(2g,\mathbf{F}_r)$.*

Proof. Let $L = \gcd_{\text{primes } r>M} \#\,\mathrm{GSp}(2g,\mathbf{F}_r)$. Clearly K_g divides L, and following the argument in the proof of Lemma 4.2.1, no prime greater than $2g+1$ divides L.

Let $p \leq 2g+1$ be a prime and suppose $\nu_p(K_g) = n$. Then, there exists some prime $r \neq 2$ such that $\nu_p(\#\,\mathrm{GSp}(2g,\mathbf{F}_r)) = n$. If $r > M$, it is clear that $\nu_p(L) = n$ as well. Suppose $r \leq M$. By the second part of Lemma 4.2.1, we know $r \neq p$ since $\nu_p(\#\,\mathrm{GSp}(2g,\mathbf{F}_p)) = g^2$. Choose a prime $l > M$ such that $l \equiv r \pmod{p^{n+1}}$. Then, it is clear that $\#\,\mathrm{GSp}(2g,\mathbf{F}_l) \equiv \#\,\mathrm{GSp}(2g,\mathbf{F}_r) \pmod{p^{n+1}}$ showing that $\nu_p(\#\,\mathrm{GSp}(2g,\mathbf{F}_l)) = n$. This shows that $\nu_p(L) = n$ as well. Hence, $K_g = L$ which is what we want. □

Proposition 4.2.1. *Let $p \neq l$ be a prime and let $\rho : G_F \to \mathrm{Aut}(X[p])$ denote the p-torsion representation coming from the g-dimensional abelian variety X. Then, the prime to p part of $\#\rho(I_v)$ divides K_g.*

Proof. Suppose X admits a polarization $X \to X^\vee$ of degree M. Thus for primes $r > M$, the mod r representation associated to $X[r]$ is valued in $\mathrm{GSp}(2g,\mathbf{F}_r)$. Let $r > M$ be a prime distinct from l. Let w be an extension of v to $K = F(X[r])$. By Theorem 4.2.2, we know X attains semistable reduction at w over K. Theorem 4.2.1 now implies that the absolute

inertia group at w acts unipotently on $T_p(X)$ and hence also on $X[p]$. So, $\rho(I_w)$ is a p-group. Thus the prime to p part of $\#\rho(I_v)$ divides $\#I_v(K|F)$ which in turn divides $\#\,\mathrm{GSp}(2g, \mathbf{F}_r)$. Since this is true for all primes $r > M$, $r \neq l$, we get by Lemma 4.2.2 that the prime to p part of $\#\rho(I_v)$ divides K_g. □

4.3 Certain subgroups inside $\mathrm{GSp}(2d, \mathbf{F}_p)$

Let k denote the finite field of order p^d. Consider the symplectic pairing $\wedge_k$ on k^2 valued in k, defined as follows. It is preserved by the action of $\mathrm{SL}(2, k)$.

$$\wedge_k(\mathbf{v}_1, \mathbf{v}_2) = ad - bc, \quad \text{if } \mathbf{v}_1 = [a\ b]^t,\ \mathbf{v}_2 = [c\ d]^t$$

Then, $\wedge = \mathrm{Tr}_{k|\mathbf{F}_p} \circ \wedge_k$ is a symplectic pairing on k^2 valued in $\mathbf{F}_p$, and we get an induced map

$$\mathrm{SL}(2, k) \to \mathrm{Sp}(2d, \mathbf{F}_p)$$

Let $G_d \subset \mathrm{GL}(2, k)$ denote the subgroup consisting of elements whose determinant lies in $\mathbf{F}_p^\times \subset k^\times$. This preserves $\wedge_k$ and $\wedge$ up to scalars, and hence induces a map $G_d \to \mathrm{GSp}(2d, \mathbf{F}_p)$. Further, the composite of this map with the similitude map to $\mathbf{F}_p^\times$ is surjective.

Let l be the finite field of order p^{2d}. Then $[l : k] = 2$, and we consider an identification of l with k^2 as vector spaces over k. This induces an inclusion $l^\times \subset \mathrm{GL}(2, k)$, and the image is called the non-split Cartan subgroup of $\mathrm{GL}(2, k)$. We consider the following subgroups

$$C = \{\ x \in l^\times \mid \mathrm{Nm}_{l|k}\ x \in \mathbf{F}_p^\times\ \} \subset G_d$$
$$C_1 = \{\ x \in l^\times \mid \mathrm{Nm}_{l|k}\ x = 1\ \} \subset \mathrm{SL}(2, k).$$

Then C_1 is the non-split Cartan subgroup of $\mathrm{SL}(2, k)$. Identifying C and C_1 with their

images under the inclusion $G_d \to \mathrm{GSp}(2d, \mathbf{F}_p)$, we see that $C \subset \mathrm{GSp}(2d, \mathbf{F}_p)$ is a cyclic subgroup of order $(p^d+1)(p-1)$ and $C_1 = C \cap \mathrm{Sp}(2d, \mathbf{F}_p)$ is the subgroup of order p^d+1.

The Galois group of l over $\mathbf{F}_p$ acts naturally on C, with Frobenius raising an element of C to its p^{th} power. The following lemmas, for $p = 2$ and odd p, let us describe a subgroup N inside the normalizer of C in $\mathrm{GSp}(2d, \mathbf{F}_p)$, such that the action of the quotient N/C on C is exactly this Galois action.

Lemma 4.3.1. *Let $p = 2$. Let $\eta \in l^\times$ be such that $\mathrm{Tr}_{l|k}(\eta) = -1$, i.e., the minimal polynomial over k of η is of the form $x^2 + x + u$ for some $u \in k$. Let us identify l with k^2 using the basis $1, \eta$. Let $\sigma = \mathrm{Frob}_p \in \mathrm{Gal}(l|\mathbf{F}_p)$. Then σ acts $\mathbf{F}_p$-linearly on $l = k^2$, and preserves the pairing $\wedge$.*

Proof. It is clear that σ acts $\mathbf{F}_p$-linearly. Let $a + b\eta$ and $c + d\eta$ be elements of l. With the given identification $l = k^2$, we have $\wedge(a + b\eta, c + d\eta) = \mathrm{Tr}_{k|\mathbf{F}_p}(ad - bc)$. Then, we get

$$\begin{aligned}
\wedge(\sigma(a + b\eta), \sigma(c + d\eta)) &= \wedge(a^2 + b^2(\eta^2), c^2 + d^2(\eta^2)) \\
&= \wedge((a^2 - ub^2) - b^2\eta, (c^2 - ud^2) - d^2\eta) \\
&= \mathrm{Tr}_{k|\mathbf{F}_p}(-a^2d^2 + b^2c^2) \\
&= \mathrm{Tr}_{k|\mathbf{F}_p}(\mathrm{Frob}_p(ad - bc)) \\
&= \mathrm{Tr}_{k|\mathbf{F}_p}(ad - bc) \\
&= \wedge(a + b\eta, c + d\eta)
\end{aligned}$$

showing that the action of σ preserves the pairing $\wedge$. □

It is clear that σ has order $2d$, and the conjugation action of σ on $x \in C$ sends it to $\sigma x \sigma^{-1} = \sigma(x) \cdot \sigma \circ \sigma^{-1} = \sigma(x) = x^2$. Let N denote the subgroup of $\mathrm{GSp}(2d, \mathbf{F}_2)$ generated by C and σ. Then, N is contained in the normalizer of C, and admits a split short exact

sequence

$$0 \longrightarrow [N,N] = C_1 = C \longrightarrow N \overset{\curvearrowleft}{\longrightarrow} N^{ab} = \mathbf{Z}/2d \longrightarrow 0. \tag{4.3.1}$$

Let x denote a generator of C, and $y = \sigma$ so that $\langle x, y | x^{2^d+1} = y^{2d} = 1, yxy^{-1} = x^2 \rangle$ is a presentation of N. Then the abelianization map above sends $x^a y^b \in N$ to $b \in \mathbf{Z}/2d$, with the obvious splitting $\mathbf{Z}/2d \to N$ sending $b \mapsto y^b$.

Lemma 4.3.2. *Let p be odd. Let $\eta \in l^\times$ such that $\eta^2 \in k^\times$ is a primitive root, and let us identify l with k^2 using the basis $1, \eta$. Let $\alpha \in l^\times$ and let $\sigma = \mathrm{Frob}_p \in \mathrm{Gal}(l|\mathbf{F}_p)$. Then $\tilde{\sigma} := \alpha\sigma$ acts $\mathbf{F}_p$-linearly on $l = k^2$, and it preserves the pairing $\wedge$ exactly if and only if*

$$\mathrm{Nm}_{l|k}(\alpha) = \eta^{1-p}.$$

Note this means that α can be taken to be in $k^\times$ if and only if $p \equiv 1 \pmod 4$.

Proof. It is clear that $\tilde{\sigma}$ acts $\mathbf{F}_p$-linearly, since both σ and multiplication by $\alpha \in l^\times$ are $\mathbf{F}_p$-linear operations. With the given identification $l = k^2$, we have $\wedge(a + b\eta, c + d\eta) = \mathrm{Tr}_{k|\mathbf{F}_p}(ad - bc)$. If $\alpha = \alpha_1 + \alpha_2\eta$, then we have

$$\begin{aligned}
\wedge(\alpha\sigma(a + b\eta), \alpha\sigma(c + d\eta)) &= \wedge((\alpha_1 + \alpha_2\eta)(a^p + b^p\eta^p), (\alpha_1 + \alpha_2\eta)(c^p + d^p\eta^p)) \\
&= \mathrm{Tr}_{k|\mathbf{F}_p}(\eta^{p-1}(\alpha_1^2 - \alpha_2^2\eta^2)(a^p d^p - b^p c^p)) \\
&= \mathrm{Tr}_{k|\mathbf{F}_p}(\eta^{p-1}\,\mathrm{Nm}_{l|k}(\alpha)\,\mathrm{Frob}_p(ad - bc))
\end{aligned}$$

This is equal to $\mathrm{Tr}_{k|\mathbf{F}_p}(ad - bc)$ for all $a, b, c, d \in k$ if and only if $\eta^{p-1}\,\mathrm{Nm}_{l|k}(\alpha) = 1$, which proves the lemma. □

The conjugation action of $\tilde{\sigma}$ on $x \in C$ sends it to $\alpha\sigma x\sigma^{-1}\alpha^{-1} = \alpha x^p \alpha^{-1} = x^p$. The next

question is what power of $\tilde{\sigma}$ lies in the image of C. We have

$$\tilde{\sigma}^n = (\alpha\sigma)^n = \alpha\alpha^p \dots \alpha^{p^{n-1}}\sigma^n = \alpha^{\frac{p^n-1}{p-1}}\sigma^n.$$

In particular, since the order of σ is $2d$ we have

$$\tilde{\alpha}^{2d} = \alpha^{\frac{p^{2d}-1}{p-1}}\sigma^{2d} = (\alpha^{1+p^d})^{\frac{p^d-1}{p-1}} = \mathrm{Nm}_{l|k}(\alpha)^{\frac{p^d-1}{p-1}} = \eta^{-(p^d-1)} = -1 \in C.$$

Hence, the element $\tilde{\sigma} \in \mathrm{Sp}(2d, \mathbf{F}_p)$ is of order $4d$, and normalizes C. Let N denote the subgroup of $\mathrm{GSp}(2d, \mathbf{F}_p)$ generated by C and $\tilde{\sigma}$. Then, N is contained in the normalizer of C, and admits a short exact sequence

$$0 \longrightarrow [N, N] = C_1 \longrightarrow N \longrightarrow N^{ab} = \mathbf{Z}/(p-1) \times \mathbf{Z}/2d \longrightarrow 0. \tag{4.3.2}$$

Unlike the case $p = 2$, this sequence does not split. Let x denote a generator of C, and $y = \tilde{\sigma}$ so that N has the presentation $\langle x, y | x^e = 1, y^{2d} = x^{e/2}, yxy^{-1} = x^p \rangle$ where $e = (p^d + 1)(p - 1)$. Then, C_1 is generated by x^{p-1} and the abelianization map above sends $x^a y^b \in N$ to $(a, b) \in \mathbf{Z}/(p-1) \times \mathbf{Z}/2d$. The similitude character $N \to \mathbf{F}_p^\times$ corresponds to the projection on to the first factor in N^{ab}, followed by the isomorphism $\mathbf{Z}/(p-1) \simeq \mathbf{F}_p^\times$ sending $1 \mapsto \mathrm{Nm}_{l|k}(x)$.

4.4 Embedding problem

In this section, we show the existence of a number field K with $\mathrm{Gal}(K|\mathbf{Q}) \simeq N$, such that the similitude character of N cuts out the subfield $\mathbf{Q}(\zeta_p) \subset K$. When $p = 2$, N was shown to be a semi-direct product of abelian groups in Section 4.3, and furthermore the similitude condition is trivial. Hence the existence of K in this case is immediate from known results on Inverse Galois problem. For example, Shafarevich's theorem says that every solvable group is a Galois group over $\mathbf{Q}$, though it is too strong for our need.

When p is odd, Shafarevich's theorem again yields that N is a Galois group over $\mathbf{Q}$ since it is solvable. But this is not enough since we need additionally that our number field have $\mathbf{Q}(\zeta_p)$ as the appropriate subfield. So we are forced to study the following embedding problem

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbf{Q}} & & \\ & & & & & \overset{?}{\swarrow} & \downarrow{\scriptstyle \phi} & & \\ 0 & \longrightarrow & [N,N] = \mathbf{Z}/(p^d+1) & \longrightarrow & N & \longrightarrow & \mathbf{Z}/(p-1)\times\mathbf{Z}/2d & \longrightarrow & 0 \end{array} \tag{4.4.1}$$

where the kernel of $\mathrm{pr}_1 \circ \phi$ corresponds to the p-cyclotomic field $\mathbf{Q}(\zeta_p)$. Suppose $F|\mathbf{Q}$ is a number field such that $F \cap \mathbf{Q}(\zeta_p) = \mathbf{Q}$ and $\mathrm{Gal}(F|\mathbf{Q}) \simeq \mathbf{Z}/2d$. Then, $F(\zeta_p)|\mathbf{Q}$ is Galois over $\mathbf{Q}$ with Galois group isomorphic to $\mathbf{Z}/(p-1)\times\mathbf{Z}/2d$. Let ϕ be the homomorphism cutting out $F(\zeta_p)$ i.e., $\overline{\mathbf{Q}}^{\ker\phi} = F(\zeta_p)$. The embedding problem of (4.4.1) asks whether ϕ can be lifted to a map $\tilde{\phi} : G_{\mathbf{Q}} \to N$ such that the diagram commutes. Such a lift $\tilde{\phi}$ describes an embedding of $F(\zeta_p)$ into a number field $L = \overline{\mathbf{Q}}^{\ker\tilde{\phi}}$ with $\mathrm{Gal}(L|\mathbf{Q}) \subseteq N$. A lift $\tilde{\phi}$ is called a proper solution to the embedding problem if it is surjective, i.e., if $\mathrm{Gal}(L|\mathbf{Q}) \simeq N$. We refer to [29, §3.5] for a detailed discussion of embedding problems.

The rest of this section is devoted to proving the existence of a proper solution to (4.4.1) for a suitably chosen initial field F. We follow the general strategy to study these types of problems. Let ϵ denote the cohomology class in $H^2(\mathbf{Z}/(p-1)\times\mathbf{Z}/2d, \mathbf{Z}/(p^d+1))$ corresponding to the group extension in (4.3.2). Then there exists a lift $\tilde{\phi}$ if and only if $\phi^*\epsilon = 0 \in H^2(\mathbf{Q}, \mathbf{Z}/(p^d+1))$ [29, Prop. 3.5.9.]. We show $\phi^*\epsilon = 0$ in two steps. First, we show that the restriction $\mathrm{res}_l(\phi^*\epsilon) = 0 \in H^2(\mathbf{Q}_l, \mathbf{Z}/(p^d+1))$ for all primes l including the infinite prime. Second, we show that Hasse principle holds in our case. That is, if all the local restrictions of a global cohomology class are trivial, then the class itself is trivial. Finally, we exploit the fact [29, Prop. 3.5.11.] that the space of solutions to (4.4.1) is a principal homogenous space over $H^1(\mathbf{Q}, \mathbf{Z}/(p^d+1))$, and twist using a suitable class to obtain properness.

We will choose F so that all ramification in F is tame and all the local embedding problems are solvable. Let $2d = 2^n d_1$ where d_1 is odd. Then, $\mathbf{Z}/2d \simeq \mathbf{Z}/2^n \times \mathbf{Z}/d_1$. We will choose Galois extensions F_1 and F_2 of $\mathbf{Q}$ with Galois groups $\mathbf{Z}/2^n$ and $\mathbf{Z}/d_1$ respectively, and define F to be their compositum. For $i = 1, 2$, we take F_i to be the unique subfield of the above mentioned degree inside the cyclotomic field $\mathbf{Q}(\zeta_{N_i})$, for certain primes N_i described below.

Let $N_2 \equiv 1 \pmod{d_1}$, so $N_2 = 2\alpha d_1 + 1$ for some $\alpha \in \mathcal{N}$. Let N_1 be a prime satisfying

(a) $N_1 \equiv 2^n + 1 \pmod{2^{n+1}}$.

(b) $N_1 \equiv 1 \pmod{N_2}$.

(c) $p \not\equiv \square \pmod{N_1}$.

The third condition can be rewritten as a congruence condition on N_1 modulo p using quadratic reciprocity. Dirichlet's theorem on primes in arithmetic progression guarantees the existence of such primes N_1, N_2.

We first study the local embedding problems at the infinite prime, and all ramified primes in $F(\zeta_p)|\mathbf{Q}$. Let us call this set S, so that $S = \mathrm{Ram}(F|\mathbf{Q}) \cup \{\infty, p\}$. With the choices made above, we have $\mathrm{Ram}(F|\mathbf{Q}) = \{N_1, N_2\}$, and $S = \{\infty, p, N_1, N_2\}$ and $F(\zeta_p)$ is tamely ramified at each finite prime in S.

4.4.1 Local obstruction at ∞

If F_1 is chosen as above, condition (a) on N_1 implies that F_1 is not a totally real extension of $\mathbf{Q}$. That is, complex conjugation is given by the non-trivial order 2 element in $\mathrm{Gal}(F_1|\mathbf{Q})$. Complex conjugation acts trivially on F_2 since the order of $\mathrm{Gal}(F_2|\mathbf{Q}) = \deg(F_2) = d_1$ is odd. Thus, complex conjugation in $\mathrm{Gal}(F(\zeta_p)|\mathbf{Q}) = \mathbf{Z}/(p-1) \times \mathbf{Z}/2d$ is given by the element $(\frac{p-1}{2}, d)$.

The element $x^{(p-1)/2} y^d$ is clearly a lift of complex conjugation to N. Recalling that

$e = (p^d + 1)(p-1)$, we further have

$$\left(x^{\frac{p-1}{2}} y^d\right)^2 = x^{\frac{p-1}{2}} \left(y^d x^{\frac{p-1}{2}} y^{-d}\right) y^{2d} = x^{\frac{p-1}{2}} x^{\frac{(p-1)p^d}{2}} y^{2d} = x^{\frac{e}{2}} y^{2d} = 1,$$

so the lift has order 2. This shows that there is no local obstruction at the infinite place to the embedding problem (4.4.1).

4.4.2 Local obstruction at p

The local obstruction at p is measured by whether or not the restriction of ϕ to the decomposition group $G_{\mathbf{Q}_p}$, can be lifted to a map $G_{\mathbf{Q}_p} \longrightarrow N$. The map $\phi|_{G_{\mathbf{Q}_p}}$ factors through the tame Galois group $G_{\mathbf{Q}_p}^{\text{tame}}$ which is a profinite group with presentation $\langle \sigma, \tau | \sigma\tau\sigma^{-1} = \tau^p \rangle$, where τ is a generator of tame inertia, and σ is a lift of the Frobenius of the maximal unramified extension. Without loss of generality, suppose that ϕ sends σ to $(0, a)$ and τ to $(1, 0)$ in $\text{Gal}(F(\zeta_p)|\mathbf{Q}) \simeq \mathbf{Z}/(p-1) \times \mathbf{Z}/2d$.

Proposition 4.4.1. *There exist $\tilde{\sigma}, \tilde{\tau} \in N$ lifting $(0, a)$ and $(1, 0)$ and satisfying $\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1} = \tilde{\tau}^p$ if and only if $a \equiv 1 \pmod 2$.*

Proof. Let $\tilde{\sigma} = x^{l(p-1)} y^a$ and $\tilde{\tau} = x^{1+k(p-1)}$ be any lifts. We have

$$\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1}\tilde{\tau}^{-p} = y^a x^{1+k(p-1)} y^{-a} x^{-(1+k(p-1))p} = x^{(1+k(p-1))(p^a - p)}$$

If $a = 0$, then the desired condition $\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1} = \tilde{\tau}^p$ cannot be met since the equation

$$1 + k(p-1) \equiv 0 \pmod{p^d + 1}$$

has no solution. If $a = 1$, any choice of k and l gives desired lifts.

Assume $a \geq 2$. We get a lift satisfying $\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1} = \tilde{\tau}^p$ if and only if there exists $k \in$

$\mathbf{Z}/(p^d+1)$ satisfying

$$(1+k(p-1))(p^a-p) \equiv 0 \pmod{e}$$
$$\text{i.e., } k(p-1) \equiv -1 \pmod{e'}$$

where

$$e' = \frac{e}{\gcd(e, p^a-p)} = \frac{p^d+1}{\gcd(p^d+1, 1+p+p^2+\cdots+p^{a-2})}.$$

This equation has a solution if and only if $p-1$ is invertible modulo e'. Since $\gcd(p-1, e')$ divides $\gcd(p-1, p^d+1) = 2$, this happens if and only if e' is odd.

Lemma 4.4.1. *e' is odd if and only if $a \equiv 1 \pmod 2$.*

Proof. If d is even, then the maximum power of 2 dividing p^d+1 is 2 itself. Hence e' is odd if and only if 2 divides $1+p+p^2+\cdots+p^{a-2}$, which happens if and only if $a \equiv 1 \pmod 2$.

Suppose d is odd. Let $m \geq 1$ be such that $p \equiv 2^m - 1 \pmod{2^{m+1}}$. Then,

$$p^d + 1 \equiv p + 1 \equiv 2^m \pmod{2^{m+1}}.$$

Hence, e' is odd if and only if 2^m divides $1+p+p^2+\cdots+p^{a-2}$. We have

$$1+p+\cdots+p^{a-2} \equiv 1-1+\cdots+(-1)^{a-2} \pmod{2^m}$$

Hence, e' is odd if and only if $a \equiv 1 \pmod 2$. □

This completes the proof of the proposition. □

The proposition says that the local obstruction at p to the embedding problem vanishes if and only if $\text{Frob}_p \in \text{Gal}(F|\mathbf{Q})$, equivalently $\text{Frob}_p \in \text{Gal}(F_1|\mathbf{Q})$, is not a square. This holds as a result of condition (c).

4.4.3 Local obstruction at N_1

The prime N_1 is unramified in $\mathbf{Q}(\zeta_p)$, totally tamely ramified in $F_1 \subset \mathbf{Q}(\zeta_{N_1})$, and split in F_2. The first two assertions are clear, and the third one follows from condition (b). Hence, the restriction of ϕ to the decomposition group $G_{\mathbf{Q}_{N_1}}$ factors through the profinite tame quotient $G_{\mathbf{Q}_{N_1}}^{\text{tame}} = \langle \sigma, \tau | \sigma\tau\sigma^{-1} = \tau^{N_1} \rangle$ as before, and without loss of generality, we may suppose that ϕ sends σ to $\text{Frob}_{N_1} = (a, 0)$ and τ to $(0, d_1)$ in $\text{Gal}(F(\zeta_p)|\mathbf{Q}) \simeq \mathbf{Z}/(p-1) \times \mathbf{Z}/2d$.

Note that the parity of a is already determined by conditions (a) and (c). To be precise, if d is even making $n \geq 2$ and hence $N_1 \equiv 1 \pmod 4$, or if $p \equiv 1 \pmod 4$, then by quadratic reciprocity we have that $N_1 \not\equiv \square \pmod p$ meaning that a is odd. Otherwise, that is, if d is odd and $p \equiv 3 \pmod 4$ then a is even. This will be used below.

Consider the elements $\tilde{\sigma} = x^{a+k(p-1)}$ and $\tilde{\tau} = y^{d_1}$ in the group N lifting the elements $\phi(\sigma)$ and $\phi(\tau)$. We will show that there is a choice of k so that $\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1} = \tilde{\tau}^{N_1}$. Hence these elements determine a map $G_{\mathbf{Q}_{N_1}} \longrightarrow N$ factoring through the tame Galois group, that lifts $\phi|_{G_{\mathbf{Q}_{N_1}}}$.

We first simplify both sides of the expression.

$$\begin{aligned}\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1} = x^{a+k(p-1)}y^{d_1}x^{-(a+k(p-1))} &= x^{a+k(p-1)}\left(y^{d_1}x^{-(a+k(p-1))}y^{-d_1}\right)y^{d_1} \\ &= x^{(a+k(p-1))(1-p^{d_1})}y^{d_1}.\end{aligned}$$

Since the order of $y \in N$ is $4d = 2^{n+1}d_1$, and condition (a) says that $N_1 \equiv 2^n + 1 \pmod{2^{n+1}}$,

$$\tilde{\tau}^{N_1} = y^{N_1 d_1} = y^{(2^n+1)d_1} = y^{2d}y^{d_1} = x^{e/2}y^{d_1}.$$

Thus, we need to show that there is a solution k to the equation

$$\begin{aligned}(a+k(p-1))(1-p^{d_1}) &\equiv e/2 \pmod{e}\\ \text{i.e., } k(p-1)(1-p^{d_1}) &\equiv e/2 - a(1-p^{d_1}) \pmod{(p-1)(p^d+1)}\\ \text{i.e., } k(1-p^{d_1}) &\equiv \frac{p^d+1}{2} + a(1+p+p^2+\cdots+p^{d_1-1}) \pmod{p^d+1}.\end{aligned}$$

Since d_1 divides d, it is clear that $\gcd(1-p^{d_1}, p^d+1) = 2$. Hence, there is a solution k to the above equation if and only if

$$\begin{aligned}\frac{p^d+1}{2} + a(1+p+p^2+\cdots+p^{d_1-1}) &\equiv 0 \pmod 2\\ \textit{i.e.,}\quad \frac{p^d+1}{2} + a &\equiv 0 \pmod 2 \quad \text{(since } d_1 \text{ is odd)}\end{aligned}$$

The parity condition on a we described earlier ensures that this holds. If d is even or $p \equiv 1 \pmod 4$, then both $\frac{p^d+1}{2}$ and a are odd. Otherwise, both are even. Hence there is no local obstruction to the embedding problem at the prime N_1.

4.4.4 Local obstruction at N_2

The prime N_2 is unramified in $\mathbf{Q}(\zeta_p)$ and F_1, and totally tamely ramified in $F_2 \subset \mathbf{Q}(\zeta_{N_2})$. Hence, the restriction of ϕ to the decomposition group $G_{\mathbf{Q}_{N_2}}$ factors through the profinite tame quotient $G^{\text{tame}}_{\mathbf{Q}_{N_2}} = \langle \sigma, \tau | \sigma\tau\sigma^{-1} = \tau^{N_2} \rangle$, and without loss of generality, we may suppose that ϕ sends σ to $\text{Frob}_{N_2} = (a, bd_1)$ and τ to $(0, 2^n)$ in $\text{Gal}(F(\zeta_p)|\mathbf{Q}) \simeq \mathbf{Z}/(p-1) \times \mathbf{Z}/2d$.

Consider the elements $\tilde{\sigma} = x^{a+k(p-1)}y^{bd_1}$ and $\tilde{\tau} = y^{2^n}$ in the group N lifting the elements $\phi(\sigma)$ and $\phi(\tau)$. We will show that there is a choice of k so that $\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1} = \tilde{\tau}^{N_2}$. Hence these elements determine a map $G_{\mathbf{Q}_{N_2}} \longrightarrow N$ factoring through the tame Galois group, that lifts $\phi|_{G_{\mathbf{Q}_{N_2}}}$.

We first simplify both sides of the expression, recalling that $N_2 = 2\alpha d_1 + 1$.

$$\begin{aligned}\tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1} = x^{a+k(p-1)}y^{2^n}x^{-(a+k(p-1))} &= x^{a+k(p-1)}\left(y^{2^n}x^{-(a+k(p-1))}y^{-2^n}\right)y^{2^n} \\ &= x^{(a+k(p-1))(1-p^{2^n})}y^{2^n}. \\ \tilde{\tau}^{N_2} = y^{2^n N_2} = y^{2^{n+1}d_1\alpha}y^{2^n} &= y^{4d\alpha}y^{2^n} = y^{2^n}.\end{aligned}$$

Thus, we need to show that there is a solution k to the equation

$$\begin{aligned}(a+k(p-1))(1-p^{2^n}) &\equiv 0 \pmod{e}. \\ k(1-p^{2^n}) &\equiv a(1+p+p^2+\cdots+p^{2^n-1}) \pmod{p^d+1}. \\ k(1-p^{2^{n-1}})(1+p^{2^{n-1}}) &\equiv a(1+p^{2^{n-1}})(1+p+\cdots+p^{2^{n-1}-1}) \pmod{p^d+1}. \\ k(1-p^{2^{n-1}}) &\equiv a(1+p+\cdots+p^{2^{n-1}-1}) \pmod{M},\end{aligned}$$

where

$$M = \frac{p^d+1}{p^{2^{n-1}}+1} = 1 - p^{2^{n-1}} + p^{2\cdot 2^{n-1}} - p^{3\cdot 2^{n-1}} + \cdots + p^{(d_1-1)\cdot 2^{n-1}}.$$

Now, it is easy to see that $\gcd(1-p^{2^{n-1}}, M) = 1$. If $l > 1$ divides $1 - p^{2^{n-1}}$, then

$$M \equiv 1 - 1 + 1 - 1 + \cdots + 1 \equiv 1 \pmod{l}.$$

This proves that there does exist a solution k to the above equation. Hence there is no local obstruction to the embedding problem at the prime N_2 either.

Since $F(\zeta_p)|\mathbf{Q}$ is unramified at primes not in S, the local embedding problems at these primes are trivially solvable. Thus, we have shown that there is no local obstruction to the embedding problem.

4.4.5 Global obstruction

Let A denote the $G_{\mathbf{Q}}$-module $[N,N] = \mathbf{Z}/(p^d+1)$ with Galois action factoring through the map ϕ and given by conjugation in N as in the short exact sequence (4.3.2). Note that this action further factors through $\mathrm{pr}_2 \circ \phi : G_{\mathbf{Q}} \to \mathrm{Gal}(F|\mathbf{Q}) = \mathbf{Z}/2d$. Global obstruction to the embedding problem is measured by the group $Ш^2_{\mathbf{Q}}(A)$ defined as

$$Ш^2_{\mathbf{Q}}(A) = \ker\left(H^2(\mathbf{Q}, A) \longrightarrow \prod_v H^2(\mathbf{Q}_v, A) \right),$$

where v runs over all places of $\mathbf{Q}$.

Proposition 4.4.2. *There is no global obstruction to this embedding problem, i.e.,* $Ш^2_{\mathbf{Q}}(A) = 0$.

Proof. By Poitou-Tate duality, we have $Ш^2_{\mathbf{Q}}(A) \simeq Ш^1_{\mathbf{Q}}(A^\vee)^\vee$, where $A^\vee = \mathrm{Hom}(A, \overline{\mathbf{Q}}^\times)$ is the dual module. If we let $m = p^d + 1$, then $A^\vee = \mathrm{Hom}(A, \mu_m)$. Let k be the trivializing extension of $A^\vee$. It is clear that k is contained in $F(\zeta_m)$. In fact it is easy to see that $A^\vee$ as a $\mathrm{Gal}(k|\mathbf{Q})$-module is isomorphic to μ_m as a $(\mathbf{Z}/m)^\times \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_m)|\mathbf{Q})$-module. That is, there is an isomorphism of pairs

$$\psi : \big(\mathrm{Gal}(k|\mathbf{Q}),\ A^\vee\big) \longrightarrow (\mathrm{Gal}(\mathbf{Q}(\zeta_m)|\mathbf{Q}), \mu_m) \tag{4.4.2}$$

The map $\mathrm{Gal}(F(\zeta_m)|\mathbf{Q}) \simeq \mathbf{Z}/2d \times (\mathbf{Z}/m)^\times \to (\mathbf{Z}/m)^\times \simeq \mathrm{Gal}(\mathbf{Q}(\zeta_m)|\mathbf{Q})$ sending $(a,b) \mapsto p^{-a}b$ induces the isomorphism ψ on the groups. Since inertia subgroup behaves well with respect to quotients, we deduce that for any prime unramified in $F|\mathbf{Q}$, the isomorphism ψ identifies the inertia subgroups of k and $\mathbf{Q}(\zeta_m)$ at that prime. In particular, the inertia subgroups at 2 get identified.

Consider the following commutative diagram

$$\begin{array}{ccccccc}
 & & & & H^1(k, A^\vee) & \longrightarrow & \prod_w H^1(k_w, A^\vee) \\
 & & & & \uparrow & & \uparrow \\
0 & \longrightarrow & Ш^1_{\mathbf{Q}}(A^\vee) & \longrightarrow & H^1(\mathbf{Q}, A^\vee) & \longrightarrow & \prod_v H^1(\mathbf{Q}_v, A^\vee) \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & Ш^1_{k|\mathbf{Q}}(A^\vee) & \longrightarrow & H^1(k|\mathbf{Q}, A^\vee) & \longrightarrow & \prod_v H^1(k_v|\mathbf{Q}_v, A^\vee) \\
 & & & & \uparrow & & \uparrow \\
 & & & & 0 & & 0
\end{array} \tag{4.4.3}$$

where the vertical maps are coming from the inflation restriction sequence. Since $A^\vee$ is trivial as a G_k-module, and w ranges over all places of k, Hasse principle holds for the G_k-module $A^\vee$ as per [29, Theorem 9.1.9.(i)]. That is, the horizontal map at the top is injective. Thus we get the isomorphism

$$Ш^1_{\mathbf{Q}}(A^\vee) \simeq Ш^1_{k|\mathbf{Q}}(A^\vee), \tag{4.4.4}$$

bringing us to the study of the cohomology of the module $A^\vee$ of the finite group $\mathrm{Gal}(k|\mathbf{Q})$. This will be done by using the isomorphism ψ in (4.4.2) and studying the familiar module μ_m. Before that, we relax local conditions slightly. Let T denote the set of all odd primes that are unramified in $k|\mathbf{Q}$. Let $\mathcal{L}$ denote the Selmer condition given by

$$L_v = \begin{cases} H^1_{ur}(k_v|\mathbf{Q}_v, A^\vee), & \text{if } v = 2 \\ 0, & \text{if } v \in T \\ H^1(k_v|\mathbf{Q}_v, A^\vee), & \text{otherwise} \end{cases}$$

In words, the local condition at 2 is relaxed from split to unramified, and the local conditions

at ramified primes are fully relaxed. The resulting Selmer group $H^1_{\mathcal{L}}(k|\mathbf{Q}, A^\vee)$ is given by

$$H^1_{\mathcal{L}}(k|\mathbf{Q}, A^\vee) = \ker\left(H^1(k|\mathbf{Q}, A^\vee) \longrightarrow \prod_v H^1(k_v|\mathbf{Q}_v, A^\vee)/L_v\right)$$

and it clearly contains $Ш^1_{k|\mathbf{Q}}(A^\vee)$. So, it is enough to show that $H^1_{\mathcal{L}}(k|\mathbf{Q}, A^\vee) = 0$.

The Selmer condition $\mathcal{L}$ amounts exactly to requiring that restriction to inertia subgroup at 2 of $k|\mathbf{Q}$, and to any cyclic subgroup of $\mathrm{Gal}(k|\mathbf{Q})$ is zero. As mentioned earlier, the isomorphism ψ in (4.4.2) identifies the inertia group at 2 of $k|\mathbf{Q}$ with that of $\mathbf{Q}(\zeta_m)|\mathbf{Q}$. Thus, the induced isomorphism in group cohomology $\psi^* : H^1(k|\mathbf{Q}, A^\vee) \simeq H^1(\mathbf{Q}(\zeta_m)|\mathbf{Q}, \mu_m)$ gives an isomorphism of Selmer subgroups

$$H^1_{\mathcal{L}}(k|\mathbf{Q}, A^\vee) \simeq H^1_{\mathcal{L}'}(\mathbf{Q}(\zeta_m)|\mathbf{Q}, \mu_m), \tag{4.4.5}$$

where $\mathcal{L}'$ is a similar set of Selmer conditions. To be precise, let T' denote the set of all odd primes that are unramified in $\mathbf{Q}(\zeta_m)|\mathbf{Q}$. Then, $\mathcal{L}'$ imposes the unramified condition at the prime 2, and the split condition at every prime in T'.

We temporarily forget the condition at 2, and consider a commutative diagram similar to (4.4.3) for the Galois module μ_m and the set T'.

$$\begin{array}{ccccccc}
 & & & & H^1(\mathbf{Q}(\zeta_m), \mu_m) & \longrightarrow & \prod_{w\in T'} H^1(\mathbf{Q}(\zeta_m)_w, \mu_m) \\
 & & & & \uparrow & & \uparrow \\
0 & \longrightarrow & Ш^1_{\mathbf{Q}}(T', \mu_m) & \longrightarrow & H^1(\mathbf{Q}, \mu_m) & \longrightarrow & \prod_{v\in T'} H^1(\mathbf{Q}_v, \mu_m) \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & Ш^1_{\mathbf{Q}(\zeta_m)|\mathbf{Q}}(T', \mu_m) & \longrightarrow & H^1(\mathbf{Q}(\zeta_m)|\mathbf{Q}, \mu_m) & \longrightarrow & \prod_{v\in T'} H^1(\mathbf{Q}(\zeta_m)_v|\mathbf{Q}_v, \mu_m) \\
 & & & & \uparrow & & \uparrow \\
 & & & & 0 & & 0
\end{array} \tag{4.4.6}$$

Then, [29, Theorem 9.1.9.] again says that the horizontal map at the top is injective, and

hence

$$Ш^1_{\mathbf{Q}(\zeta_m)|\mathbf{Q}}(T', \mu_m) \simeq Ш^1_{\mathbf{Q}}(T', \mu_m). \tag{4.4.7}$$

Furthermore, the same theorem says that Hasse principle for μ_m holds over $\mathbf{Q}$ as long as we are not in a special case. In fact, the obstruction to Hasse principle is described precisely.

$$Ш^1_{\mathbf{Q}}(T', \mu_m) = \begin{cases} 0, & \text{if } (\mathbf{Q}, m, T') \text{ is not a special case} \\ \mathbf{Z}/2, & \text{if } (\mathbf{Q}, m, T') \text{ is a special case} \end{cases}$$

As per the remarks following [29, Lemma 9.1.8.], the special case is equivalent to the statement that 8 divides m, since T' only consists of odd primes and has Dirichlet density 1.

If $(\mathbf{Q}, m, T')$ is not a special case, then we are done by (4.4.5), (4.4.7) and the inclusion

$$H^1_{\mathcal{L}'}(\mathbf{Q}(\zeta_m)|\mathbf{Q}, \mu_m) \subseteq Ш^1_{\mathbf{Q}(\zeta_m)|\mathbf{Q}}(T', \mu_m).$$

Suppose $(\mathbf{Q}, m, T')$ is a special case. Then 8 divides m. Let $m = 2^r m_1$ with m_1 odd and $r \geq 3$. Then the non-trivial element in $Ш^1_{\mathbf{Q}}(T', \mu_m) \simeq \mathbf{Z}/2$ is the inflation of the class in $H^1(\mathbf{Q}(\zeta_m)|\mathbf{Q}, \mu_m)$ represented by the cocycle

$$\mathrm{Gal}(\mathbf{Q}(\zeta_m)|\mathbf{Q}) \longrightarrow \mathrm{Gal}(\mathbf{Q}(\zeta_{2^r})|\mathbf{Q}) \longrightarrow \mathrm{Gal}(\mathbf{Q}(\sqrt{-2})|\mathbf{Q}) \xrightarrow{\simeq} \{\pm 1\} \subseteq \mu_m.$$

It is non-trivial when restricted to $\mathrm{Gal}(\mathbf{Q}(\zeta_m)|\mathbf{Q}(\zeta_{m_1}))$, which is the inertia group at 2 of $\mathbf{Q}(\zeta_m)|\mathbf{Q}$. Hence, this class fails the unramified condition at 2 of $\mathcal{L}'$. So, we get that $H^1_{\mathcal{L}'}(\mathbf{Q}(\zeta_m)|\mathbf{Q}, \mu_m) = 0$, and we are done by (4.4.5). □

We have therefore shown that the map $\phi : G_{\mathbf{Q}} \to \mathbf{Z}/(p-1) \times \mathbf{Z}/2d = \mathrm{Gal}(F(\zeta_p)|\mathbf{Q})$ in (4.4.1) lifts to some map $\tilde{\phi} : G_{\mathbf{Q}} \to N$. The map $\tilde{\phi}$ is not necessarily surjective. But we can twist it using a suitable cohomology class in $H^1(\mathbf{Q}, A)$ to get a surjective lift. If

$c : G_{\mathbf{Q}} \to A \subset N$ is a representing cocycle, then the twisted solution it determines is given by $c \cdot \tilde{\phi}$.

Choose a prime v that splits completely in both k and $F(\zeta_p)$. Cebotarev density theorem guarantees the existence of such a prime. The fact that v splits completely in $F(\zeta_p)$ implies that ϕ is trivial on $G_{\mathbf{Q}_v}$ and hence the restriction of $\tilde{\phi}$ to $G_{\mathbf{Q}_v}$ lands inside A. So, the map $\tilde{\phi}|_{G_{\mathbf{Q}_v}} \in \mathrm{Hom}(G_{\mathbf{Q}_v}, A) = H^1(\mathbf{Q}_v, A)$. Choose another homomorphism $c_v \in H^1(\mathbf{Q}_v, A)$ so that $c_v \cdot \tilde{\phi} : G_{\mathbf{Q}_v} \to A$ is surjective. If there is a global cohomology class in $H^1(\mathbf{Q}, A)$ which restricts to $c_v \in H^1(\mathbf{Q}_v, A)$, then twisting by this class gives us a proper solution. The existence of such a class is guaranteed by the following proposition.

Proposition 4.4.3. *The map $H^1(\mathbf{Q}, A) \longrightarrow H^1(\mathbf{Q}_v, A)$ is surjective.*

Proof. Let $\mathrm{coker}^1_{\mathbf{Q}}(T, M)$ denote the cokernel of the restriction map $H^1(\mathbf{Q}, M) \to \prod_{v \in T} H^1(\mathbf{Q}_v, M)$ for a $G_{\mathbf{Q}}$-module M and a set T of places of $\mathbf{Q}$. We want to show $\mathrm{coker}^1_{\mathbf{Q}}(\{v\}, A) = 0$. According to [29, Lemma 9.2.2.], there is a canonical short exact sequence

$$0 \longrightarrow Ш^1_{\mathbf{Q}}(A^\vee) \longrightarrow Ш^1_{\mathbf{Q}}(S \setminus \{v\}, A^\vee) \longrightarrow \mathrm{coker}^1_{\mathbf{Q}}(\{v\}, A)^\vee \longrightarrow 0$$

where S is the set of all places of $\mathbf{Q}$. So it is enough to show that $Ш^1_{\mathbf{Q}}(S \setminus \{v\}, A^\vee) = Ш^1_{\mathbf{Q}}(A^\vee)$.

Following a similar argument as in the proof of Proposition 4.4.2, we get that

$$Ш^1_{\mathbf{Q}}(S \setminus \{v\}, A^\vee) \simeq Ш^1_{k|\mathbf{Q}}(S \setminus \{v\}, A^\vee)$$

Since the prime v was chosen to be split in $k|\mathbf{Q}$, the decomposition group of v inside $\mathrm{Gal}(k|\mathbf{Q})$ is trivial. Hence, the restriction map at v on the finite group cohomology $H^1(\mathrm{Gal}(k|\mathbf{Q}), A^\vee)$ is automatically zero. So a local condition at v is vacuous. Thus we deduce from the isomorphism $Ш^1_{\mathbf{Q}}(S \setminus \{v\}, A^\vee) \simeq Ш^1_{k|\mathbf{Q}}(S \setminus \{v\}, A^\vee) = Ш^1_{k|\mathbf{Q}}(A^\vee) \simeq Ш^1_{\mathbf{Q}}(A^\vee)$ that $\mathrm{coker}^1_{\mathbf{Q}}(\{v\}, A) = 0$. □

4.5 Proof

We first discuss some preliminaries about the desired inertia condition at an auxiliary prime l. Recall the subgroups C, C_1 and N of $\mathrm{GSp}(2d, \mathbf{F}_p)$ introduced in Section 4.3. For every $1 \leq d \leq g$, since $\mathrm{GSp}(2d, \mathbf{F}_p) \subset \mathrm{GSp}(2g, \mathbf{F}_p)$, the group $\mathrm{GSp}(2g, \mathbf{F}_p)$ contains cyclic subgroups C, C_1 of orders $(p^d + 1)(p - 1)$ and $p^d + 1$, and a subgroup N of the normalizer of C as described in Section 4.3 such that $[N, N] = C_1$. We desire $\rho(I_l) \subset [N, N]$ to have a prime power order q not dividing K_g. So, we first need to look for prime powers q that divide $p^d + 1$ for some $1 \leq d \leq g$, but do not divide K_g.

Lemma 4.5.1. *Let $g \geq 7$ and p be any prime. Then, there exists a prime $q > 2g + 1$ such that q divides $p^d + 1$ for some $1 \leq d \leq g$.*

Proof. Zsigmondy's theorem implies that for any prime p and $n \geq 1$, with the exception of $p = 2, n = 3$, there is a prime divisor of $p^n + 1$ which does not divide $p^m + 1$ for any $m < n$.

Let π denote the prime counting function.

Case 1: $p \neq 2$.

If $g \geq 7$ then $\pi(2g + 1) \leq g - 1$. Zsigmondy's theorem implies that there are at least g distinct prime numbers that divide some number in the set $\{p^d + 1 : 1 \leq d \leq g\}$. So one of them has to be bigger than $2g + 1$.

Case 2: $p = 2$.

If $g = 7, 8, 9$, we may take $d = 7$ and $q = 43$. If $g \geq 10$ then $\pi(2g + 1) \leq g - 2$. Zsigmondy's theorem implies that there are at least $g - 1$ distinct prime numbers that divide some number in the set $\{2^d + 1 : 1 \leq d \leq g\}$. So one of them has to be bigger than $2g + 1$. □

Lemmas 4.2.1 and 4.5.1 ensure that when $g \geq 7$ there exists a prime q that divides $p^d + 1$ for some $1 \leq d \leq g$, and does not divide K_g. Suppose $2 \leq g \leq 6$. If p is a large enough prime, for example, if $p^g + 1 > K_g$, then there exists a prime power q that divides $p^g + 1$ and does not divide K_g. This leaves only finitely many cases (g, p) to be dealt with. For each

of them except $(g,p) = (2,2)$, $(2,3)$, $(3,2)$, $(3,3)$ we check explicitly that there exists some prime power q dividing $p^d + 1$ for some $1 \leq d \leq g$, such that q does not divide K_g.

We can now prove Theorem 4.1.1.

Proof. Suppose $(g,p) \neq (3,3)$. By the preceding discussion, we find a number d and a prime power q such that $1 \leq d \leq g$, q divides $p^d + 1$, and q does not divide K_g.

Let C, C_1, N denote the subgroups of $\mathrm{GSp}(2d, \mathbf{F}_p)$ of orders $(p^d+1)(p-1)$, p^d+1 and $2d(p^d+1)(p-1)$ as defined in Section 4.3. We will consider them as subgroups of $\mathrm{GSp}(2g, \mathbf{F}_p)$ by a fixed inclusion $\mathrm{GSp}(2d, \mathbf{F}_p) \subset \mathrm{GSp}(2g, \mathbf{F}_p)$ Choose a number field F and define k to be the trivializing extension of the dual module $A^\vee$, just as in Section 4.4. The calculations in Section 4.4 say that there is no obstruction to the embedding problem (4.4.1).

In order to get desired inertia at an auxiliary prime, we follow the same approach that was used in Section 4.4 to get properness. Let $\tilde{\phi}$ be a solution to the embedding problem (4.4.1). In addition to the prime v and the cohomology class $c_v \in H^1(\mathbf{Q}_v, A)$ chosen in Section 4.4 to get properness, choose an auxiliary prime $l \equiv 1 \pmod{q}$ that splits completely in k and $F(\zeta_p)$, and a homomorphism $c_l : G_{\mathbf{Q}_l} \to A = [N,N]$ so that the image of I_l under $c_l \cdot \tilde{\phi}$ is the cyclic subgroup of $[N,N]$ of order q. The proof of Proposition 4.4.3 goes through to show that the restriction map

$$H^1(\mathbf{Q}, A) \to H^1(\mathbf{Q}_v, A) \times H^1(\mathbf{Q}_l, A)$$

is surjective. Thus, there is a global cohomology class $c \in H^1(\mathbf{Q}, A)$ which restricts to c_v and c_l. Twisting $\tilde{\phi}$ by this class produces a representation $\rho : G_{\mathbf{Q}} \twoheadrightarrow N \subset \mathrm{GSp}(2d, \mathbf{F}_p) \subset \mathrm{GSp}(2g, \mathbf{F}_p)$ with $\#\rho(I_l) = q \nmid K_g$. Proposition 4.2.1 now implies that ρ does not arise from the p-torsion of an abelian variety over $\mathbf{Q}$.

Suppose $(g,p) = (3,3)$. We find that there is a subgroup $N \subset \mathrm{GSp}(6, \mathbf{F}_3)$ of order 78, with surjective similitude character. It is a semi-direct product of $\mathbf{Z}/13$ and $\mathbf{Z}/6$ with presentation $\langle x, y | x^{13} = y^6 = 1, yxy^{-1} = x^4 \rangle$. We take $\phi : G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}(\zeta_9)|\mathbf{Q}) \simeq \mathbf{Z}/6$.

Since N is a semi-direct product, the resulting embedding problem is trivially solvable. We twist as in Section 4.4 to get a proper solution ρ with $\#\rho(I_l) = 13$ for an auxiliary prime l. Proposition 4.2.1 again implies that ρ does not arise from the 3-torsion of an abelian threefold over $\mathbf{Q}$. $\square$

REFERENCES

[1] H. F. Baker. *A Locus with* 25920 *Linear Self-Transformations*. Cambridge Tracts in Mathematics and Mathematical Physics, no. 39. Cambridge, at the University Press; New York, The Macmillan Company, 1946.

[2] Tobias Berger and Krzysztof Klosin. Deformations of Saito-Kurokawa type and the Paramodular Conjecture (with an appendix by Cris Poor, Jerry Shurman, and David S. Yuen). arXiv:1710.10228 [math.NT], 2017.

[3] Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien. The groups of order at most 2000. *Electron. Res. Announc. Amer. Math. Soc.*, 7:1–4, 2001.

[4] Hans Ulrich Besche, Bettina Eick, and Eamonn A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.

[5] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki. A database of genus-2 curves over the rational numbers. *LMS J. Comput. Math.*, 19(suppl. A):235–254, 2016.

[6] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Neron Models*. Springer-Verlag Berlin Heidelberg, 1990.

[7] George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni. Abelian surfaces over totally real fields are potentially modular. arXiv:1812.09269 [math.NT], 2018.

[8] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[9] Nils Bruin and Brett Nasserden. Arithmetic aspects of the Burkhardt quartic threefold. *J. Lond. Math. Soc. (2)*, 98(3):536–556, 2018.

[10] Armand Brumer, Ariel Pacetti, Chris Poor, Gonzalo Tornaría, John Voight, and David S. Yuen. On the paramodularity of typical abelian surfaces. arXiv:1805.10873 [math.NT], 2018.

[11] Frank Calegari. Blog post (and comments): Picard groups of moduli stacks. https://www.galoisrepresentations.com/2020/04/30/picard-groups-of-moduli-stacks/.

[12] Frank Calegari. Mod p representations on elliptic curves. *Pacific J. Math.*, 225(1):1–11, 2006.

[13] Frank Calegari and Shiva Chidambaram. Rationality of twists of $\mathcal{A}_2(3)$. https://arxiv.org/abs/2009.00194, 2020.

[14] Frank Calegari, Shiva Chidambaram, and Alexandru Ghitza. Some modular abelian surfaces. *Math. Comp.*, 89(321):387–394, 2020.

[15] Frank Calegari, Shiva Chidambaram, and David P. Roberts. Abelian surfaces with fixed 3-torsion. In Steven Galbraith, editor, *Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV)*, Open Book Series 4, pages 91–108, Berkeley, 2020. Mathematical Sciences Publishers.

[16] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. LMS Lecture Note Series. Cambridge University Press, 1996.

[17] Claude Chevalley. Invariants of finite groups generated by reflections. *Amer. J. Math.*, 77:778–782, 1955.

[18] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. La R-équivalence sur les tores. *Ann. Sci. École Norm. Sup. (4)*, 10(2):175–229, 1977.

[19] Luis Dieulefait. Existence of nonelliptic mod ℓ galois representations for every $\ell > 5$. *Experiment. Math.*, 13(3):327–329, 2004.

[20] Tom Fisher. The Hessian of a genus one curve. *Proceedings of the London Mathematical Society*, 104(3):613–648, 2012.

[21] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.*, 148(5):1390–1442, 2012.

[22] A. Grothendieck and M. Raynaud. Modeles de neron et monodromie. In *Groupes de Monodromie en Géométrie Algébrique*, pages 313–523, Berlin, Heidelberg, 1972. Springer Berlin Heidelberg.

[23] J. William Hoffman and Steven H. Weintraub. The Siegel modular variety of degree two and level three. *Trans. Amer. Math. Soc.*, 353(8):3267–3305, 2001.

[24] Klaus Hulek and G. K. Sankaran. The geometry of Siegel modular varieties. In *Higher dimensional birational geometry (Kyoto, 1997)*, volume 35 of *Adv. Stud. Pure Math.*, pages 89–156. Math. Soc. Japan, Tokyo, 2002.

[25] Bruce Hunt. *The geometry of some special arithmetic quotients*, volume 1637 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1996.

[26] Jun-Ichi Igusa. A desingularization problem in the theory of siegel modular functions. *Mathematische Annalen*, 168(1):228–260, Dec 1967.

[27] Joan-C. Lario and Anna Rio. Elliptic modularity for octahedral Galois representations. *Math. Res. Lett.*, 3(3):329–342, 1996.

[28] Yu. I. Manin. *Cubic forms*, volume 4 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, second edition, 1986. Algebra, geometry, arithmetic, Translated from the Russian by M. Hazewinkel.

[29] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *The Absolute Galois Group of a Global Field*, pages 521–597. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[30] Cris Poor, Jerry Shurman, and David S. Yuen. Siegel paramodular forms of weight 2 and squarefree level. *Int. J. Number Theory*, 13(10):2627–2652, 2017.

[31] Cris Poor and David S. Yuen. Paramodular cusp forms. *Math. Comp.*, 84(293):1401–1438, 2015.

[32] Bernhard Riemann. Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsberichte der Berliner Akademie*, pages 671–680, 1859.

[33] K. Rubin and A. Silverberg. Families of elliptic curves with constant mod p representations. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 148–161. Int. Press, Cambridge, MA, 1995.

[34] Jean-Pierre Serre. Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, 11(2):1–15, 1969-1970.

[35] G. C. Shephard and J. A. Todd. Finite unitary reflection groups. *Canad. J. Math.*, 6:274–304, 1954.

[36] Tetsuji Shioda. Construction of elliptic curves with high rank via the invariants of the Weyl groups. *J. Math. Soc. Japan*, 43(4):673–719, 1991.

[37] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[38] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.