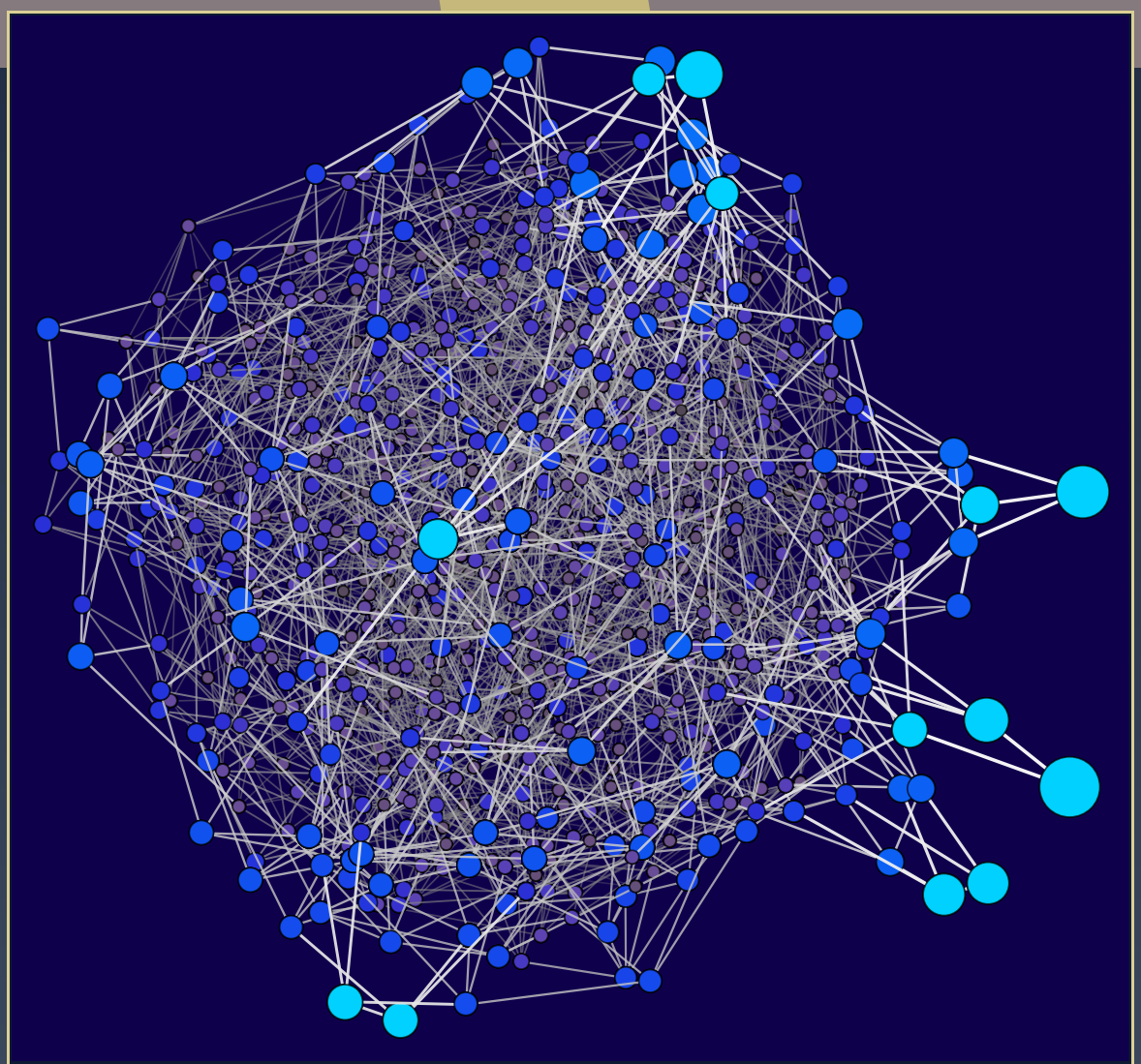
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Abelian surfaces with fixed 3-torsion

Frank Calegari, Shiva Chidambaram, and David P. Roberts



msp

THE OPEN BOOK SERIES 4 (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.91

Abelian surfaces with fixed 3-torsion

Frank Calegari, Shiva Chidambaram, and David P. Roberts

Given a genus two curve $X : y^2 = x^5 + ax^3 + bx^2 + cx + d$, we give an explicit parametrization of all other such curves Y with a specified symplectic isomorphism on three-torsion of Jacobians $\mathrm{Jac}(X)[3] \cong \mathrm{Jac}(Y)[3]$. It is known that under certain conditions modularity of X implies modularity of infinitely many of the Y, and we explain how our formulas render this transfer of modularity explicit. Our method centers on the invariant theory of the complex reflection group $C_3 \times \mathrm{Sp}_4(\mathbb{F}_3)$. We discuss other examples where complex reflection groups are related to moduli spaces of curves, and in particular motivate our main computation with an exposition of the simpler case of the group $\mathrm{Sp}_2(\mathbb{F}_3) = \mathrm{SL}_2(\mathbb{F}_3)$ and 3-torsion on elliptic curves.

1. Introduction

1.1. ***Overview.*** Consider a genus two curve X over $\mathbb{Q}$ given by an affine equation

$$y^2 = x^5 + ax^3 + bx^2 + cx + d. \tag{1-1}$$

The representation $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}_4(\mathbb{F}_3)$ on the three-torsion $\mathrm{Jac}(X)[3]$ of its Jacobian is given by an explicit degree 80 polynomial with coefficients in $\mathbb{Q}[a, b, c, d]$. The polynomial can be extracted from [Shi91], or by following the recipe given in Section 3.1. The main theorem of this paper parametrizes all pairs (Y, i) consisting of a curve

$$Y : \quad y^2 = x^5 + Ax^3 + Bx^2 + Cx + D \tag{1-2}$$

and a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant symplectic isomorphism, $i : \mathrm{Jac}(X)[3] \to \mathrm{Jac}(Y)[3]$. The curves in (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 $\mathbb{C}$, will not typically be rational over $\mathbb{Q}$ (see the discussion towards the end of Section 1.2).

FC and SC were supported in part by NSF grant DMS-1701703; DPR was supported in part by DMS-1601350.
MSC2020: primary 11F80; secondary 11G10, 20F55.
Keywords: abelian surfaces, three torsion, Galois representations.

Analogous problems for genus one curves and their mod p representations for $p \leq 5$ were solved by Rubin and Silverberg [RS95]. In Section 2, we explain how the mod 3 formulas of [LR96] can be reconstructed by using that $\mathrm{Sp}_2(\mathbb{F}_3)$ has a two-dimensional complex reflection representation, summarizing the result in Theorem 1.

Section 3 contains our main result, Theorem 2. It follows Section 2 closely, using now that $\mathrm{Sp}_4(\mathbb{F}_3)$ is the main factor in the complex reflection group $C_3 \times \mathrm{Sp}_4(\mathbb{F}_3)$. 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 online supplement.

Section 4 provides four independent complements. Section 4.1 sketches an alternative method for computing the above (A, B, C, D). Section 4.2 presents a family of examples involving Richelot isogenies. Section 4.3 gives an application to modularity which was one of the motivations for this paper. Section 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.

1.2. ***Moduli spaces.*** Theorems 1 and 2 and the analogs sketched in Section 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 $\mathbb{Q}$ of dimension g with a principal polarization λ. If $V_A = A[p]$ is the set of p-torsion points with coefficients in $\overline{\mathbb{Q}}$, then V_A is a $2g$-dimensional vector space over $\mathbb{F}_p$ 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and so gives rise to a Galois representation

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

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

Conversely, if $\bar{\rho}$ is any such representation on a symplectic space $(V, \wedge^2)$, coming from an abelian variety or not, there exists a moduli space $\mathcal{A}_g(\bar{\rho})$ over $\mathbb{Q}$ 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 $\mathcal{A}_g(\bar{\rho}) \to \mathcal{A}_g$ to the moduli space of principally polarized g-dimensional abelian varieties. For the split Galois representation $\bar{\rho}_0$, corresponding to the torsion structure $(\mathbb{Z}/p\mathbb{Z})^g \oplus (\mu_p)^g$ with its natural symplectic form, the cover $\mathcal{A}_g(\bar{\rho}_0)$ is the standard "full level p" cover $\mathcal{A}_g(p)$ of $\mathcal{A}_g$. In general, $\mathcal{A}_g(\bar{\rho})$ is a twisted version of $\mathcal{A}_g(p)$, meaning that the two varieties become isomorphic after base change from $\mathbb{Q}$ to $\overline{\mathbb{Q}}$.

The varieties $\mathcal{A}_g(\bar\rho)$ 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 $(3, 2)$ [HS02, Theorem II.2.1]. In the three cases when $g = 1$, the curves $\mathcal{A}_1(\bar\rho)$ are always rational. In the main case of interest $(2, 3)$ for this paper, the three-dimensional variety $\mathcal{A}_2(3) = \mathcal{A}_2(\bar\rho_0)$ is rational [BN18]. However, for many $\bar\rho$, including all surjective representations, it is proven in [CC20] that the variety $\mathcal{A}_2(\bar\rho)$ is never rational. It *is* true, however, that there exists a degree 6 cover $\mathcal{A}_2^w(\bar\rho)$ which is rational [BCGP18, Lemma 10.2.4]. Thus while Theorem 1 corresponds to a parametrization of $\mathcal{A}_1(\bar\rho)$ for $p = 3$, Theorem 2 corresponds to a parametrization of $\mathcal{A}_2^w(\bar\rho)$. More precisely, the Torelli map $\mathcal{M}_2 \to \mathcal{A}_2$ is an open immersion, and the pullback of $\mathcal{A}_2^w(\bar\rho)$ is the moduli space $\mathcal{M}_2^w(\bar\rho)$ of genus two curves of the form (1-1) whose Jacobians give rise to $\bar\rho$, and it is $\mathcal{M}_2^w(\bar\rho)$ 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 $\mathbb{P}^3_{\mathbb{Q}}$ to $\mathcal{A}_2(\bar\rho)$ [CC20]. We mention in passing that our arguments give an alternative proof of [BCGP18, Lemma 10.2.4].

There is a natural generalization of the varieties $\mathcal{A}_g(\bar\rho)$. Namely, for any $m \in \mathbb{F}_p^\times$, one can require instead an isomorphism $i : (V, \wedge^2) \simeq (V_A, m\wedge_A^2)$. 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 $\mathcal{A}_g^*(\bar\rho)$. Our policy throughout this paper is to focus on $\mathcal{A}_g(\bar\rho)$ and be much briefer about parallel results for $\mathcal{A}_g^*(\bar\rho)$.

2. Elliptic curves with fixed 3-torsion

In this section, as a warm up to Section 3, we rederive the formulas in [LR96] describing elliptic curves with fixed 3-torsion from the invariant theory of the group $\mathrm{Sp}_2(\mathbb{F}_3)$ as in [Fis12]. 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.

2.1. ***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 $\mathbb{Q}$ with affine equation

$$y^2 = x^3 + ax + b. \tag{2-1}$$

We emphasize the discriminant $\Delta(a, b) = \Delta = 2^4\Delta_{\mathrm{poly}}$ in the sequel, because it makes Section 2.7 cleaner.

By a classical division polynomial formula, the eight primitive 3-torsion points $(x, y) \in \mathbb{C}^2$ are exactly the points satisfying both (2-1) and

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

Equations (2-1) and (2-2) together define an octic algebra over $\mathbb{Q}$. Rather than work with the two generators x and y and the two relations (2-1) and (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 $\mathbb{Q}[z]$ coming from the equation

$$F(a, b, z) := z^8 + 18az^4 + 108bz^2 - 27a^2 = 0. \tag{2-3}$$

2.2. $\mathbf{Sp_2(\mathbb{F}_3)}$ *and related groups.* For generic (a, b), the Galois group of the polynomial $F(a, b, z)$ is $\mathrm{GSp}_2(\mathbb{F}_3) = \mathrm{GL}_2(\mathbb{F}_3)$. 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 $E = \mathbb{Q}(\sqrt{-3})$ for all a, b. The relative Galois group $\mathrm{Gal}(K'_{a,b}/E)$ is $\mathrm{Sp}_2(\mathbb{F}_3) = \mathrm{SL}_2(\mathbb{F}_3)$. 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 (2-3) arises as a generic polynomial in the invariant theory of $\mathrm{Sp}_2(\mathbb{F}_3)$. The invariant theory is simple because $\mathrm{Sp}_2(\mathbb{F}_3) = \left\langle \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$ can be realized as a complex reflection group by sending the generators in order to

$$g_1 = \begin{pmatrix} \bar{\omega} & \bar{\omega} - 1 \\ 0 & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 0 \\ (\omega - 1)/3 & \omega \end{pmatrix}. \tag{2-4}$$

The matrices g_1 and g_2 are indeed complex reflections because all but one eigenvalue is 1. In our study of the image $\mathrm{ST}\,4 = G = \langle g_1, g_2 \rangle$, the subgroup $H = \langle g_1 \rangle$ will play an important role. Here our notation $\mathrm{ST}\,4$ 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 [ST54, 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 $\mathrm{Sp}_n(\mathbb{F}_3)$, the unital character χ_1 and a complex conjugate pair χ_{na} and χ_{nb}. Here χ_{na} corresponds to the representations (2-4) and (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 1 shows how the three characters 1, χ_{2a}, and χ_{2b} fit into the entire character theory of $\mathrm{Sp}_2(\mathbb{F}_3)$. 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.

The right half of Table 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 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 $i \in \{1a, 1b, 2\}$.

$\lvert C\rvert$	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 1. Character table of $\mathrm{Sp}_2(\mathbb{F}_3)$ and invariant-theoretic information

2.3. ***Rings of invariants.*** The group G acts on the polynomial ring $E[u,z]$ by the formulas induced from the matrices in (2-4),

$$g_1u=\bar\omega u+(\bar\omega-1)z,\quad g_2u=u,$$
$$g_1z=z,\qquad\qquad g_2z=(\omega-1)u/3+\omega z.$$

Despite the appearance of the irrationality ω in these formulas, there is an important rationality present. Namely we have arranged in (2-4) that $g_1^2=\bar g_1$ and $g_2^2=\bar g_2$. Accordingly G is stable under complex conjugation, a stability not present in either the original Shephard and Todd paper [ST54, Section 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 $\mathbb{Q}$. Then actually $\underline{G}$ acts on $\mathbb{Q}[u,z]$. All seven irreducible representations of $\underline{G}$ are defined over $\mathbb{Q}$, just like all three representations of the familiar group scheme $\underline{H}\cong\mu_3$, are defined over $\mathbb{Q}$. 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

$$w=\frac{u^3}{3}+u^2z+uz^2,\quad a=\frac{wz}{9},\quad b=\frac{w^2-6wz^3-3z^6}{324}\tag{2-5}$$

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

$$\mathbb{Q}[u,z]^{\underline{H}}=\mathbb{Q}[w,z],\quad \mathbb{Q}[u,z]^{\underline{G}}=\mathbb{Q}[a,b].\tag{2-6}$$

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 (2-5), then one gets the polynomial relation $F(a,b,z)=0$ of (2-3), explaining our choice of overall scale factors in (2-5). The fact that the rings on the right in (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 [Che55].

2.4. ***Covariants and contravariants.*** The graded ring $\mathbb{Q}[w, z]$ is free of rank eight over the graded ring $\mathbb{Q}[a, b]$. Moreover there is a homogeneous basis $1, z^2, z^4, z^6, \alpha_1, \alpha_3, \beta_3, \beta_5$ 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 $\mathbb{Q}[u, z]_d$ 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

$$\alpha_1 = z, \quad \alpha_3 = \frac{w + z^3}{6}, \quad \beta_3 = \frac{w - z^3}{2}, \quad \beta_5 = \frac{5wz^2 + 3z^5}{18}. \tag{2-7}$$

Ideas from classical invariant theory are useful in finding these quantities. For example, the polynomials in $\mathbb{Q}[u, z]_3$ 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 $D^3 = \Delta(a, b)$.

2.5. ***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 defines in [Fis12] a covariant to be a tuple defining an equivariant map $\mathbb{Q}[u, z]_1 \to \mathbb{Q}[u, z]_d$. 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 [Fis12], 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 computationally difficult for $g = 2$. So we continue to treat covariants as polynomials as in Section 2.4 and describe two approaches to obtain new coefficients.

The octic $\mathbb{Q}[a, b]$-algebra $\mathbb{Q}[w, z]$ acts on itself by multiplication and so every element e in $\mathbb{Q}[w, z]$ has an octic characteristic polynomial $\phi(e, u) \in \mathbb{Q}[a, b, u]$. One has $\phi(z, u) = F(a, b, u)$ from (2-3). To obtain the characteristic polynomial for a general e, one can express e as an element of $\mathbb{Q}(a, b, z)$ via (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 Section 3.5 we use the matrix approach.

Carrying out this procedure for the general covariant and contravariant gives

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

with

$$3A(a, b, s, t) = 3as^4 + 18bs^3t - 6a^2s^2t^2 - 6abst^3 - (a^3 + 9b^2)t^4,$$
$$9B(a, b, s, t) = 9bs^6 - 12a^2s^5t - 45abs^4t^2 - 90b^2s^3t^3 + 15a^2bs^2t^4 - 2a(2a^3 + 9b^2)st^5 - 3b(a^3 + 6b^2)t^6,$$

and A^* and B^* in the online supplement. As stated in the introduction, A and B when fully expanded have 6 and 9 terms respectively and agree exactly with expressions in [LR96, Section 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.

2.6. ***Geometric summary.*** The following theorem summarizes our calculations in terms of moduli spaces. The $\bar\rho$ 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 $\mathcal{A}_1(\bar\rho)$.

Theorem 1. *Fix an equation $y^2 = x^3 + ax + b$ defining an elliptic curve X over $\mathbb{Q}$. 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* $\operatorname{Proj}\mathbb{Q}[s, t]$. *The natural map to the j-line $\mathcal{A}_1 \subset \operatorname{Proj}\mathbb{Q}[A, B]$ has degree twelve and is given by*

$$(A, B) = (A(a, b, s, t), B(a, b, s, t)). \tag{2-8}$$

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

$$\Delta(A, B) = \Delta(a, b)\delta(a, b, s, t)^3/27, \quad \delta(a, b, s, t) = 3s^4 + 6as^2t^2 + 12bst^3 - a^2t^4. \tag{2-9}$$

It thus consists of four geometric points. Comparing with (2-2), one sees that these points are permuted by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ according to the projective mod 3 representation into $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$. Theorem 1 has a direct analog for the covers $\mathcal{A}^*_{a,b} \to \mathcal{A}_1$.

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 $\mathbb{Q}$ with isomorphic 3-torsion. Then, in contrast with the analogous situation for the genus two case described in Section 3.7, it is very easy to find associated $(s, t) \in \mathbb{Q}^2$. Namely, (2-8) and its analog $(A, B) = (A^*(a, b, s, t), B^*(a, b, s, t))$ each have twenty-four solutions in $\mathbb{C}^2$. 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is all of $\mathrm{GSp}_2(\mathbb{F}_3) = \mathrm{GL}_2(\mathbb{F}_3)$, 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 (2-9). If it has the form $X^*(s, t)$ then $\Delta_X\Delta_Y$ is a perfect cube by the starred analog of (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 (2-3), this ambiguous case arises if and only if the image Γ of $\bar\rho_X$ 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 $(s,t) = \pm\left(-\frac{1}{2}, \frac{3}{2}\right)$.

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 $\bar{\rho}_0 = \mathbb{Z}/3\mathbb{Z} \oplus \mu_3$ or when $X[3]$ is irreducible but not absolutely irreducible. (The latter occurs precisely when the image factors through the nonsplit Cartan subgroup $\mathbb{F}_9^\times$ and has order > 2; this case does not arise over $\mathbb{Q}$.) An instance over $\mathbb{Q}$ 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.

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.

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 (1-1), which we call a *Weierstrass equation*. Replacing (a,b,c,d) by $(u^4a, u^6b, u^8c, u^{10}d)$ yields an isomorphic Weierstrass curve via the compensating change $(x,y) \mapsto (u^2x, u^5y)$. The standard discriminant of the genus two curve (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 (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 $\mathbb{P}^3(12,18,24,30) = \mathbb{P}^3(2,3,4,5)$. As explained at the end of Section 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 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-equivariant bijection [CF96] from the nonzero 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 (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

$$F(a,b,c,d,z) = z^{240} + 15120az^{228} + 2620800bz^{222} - 504(70227a^2 - 831820c)z^{216} - 1965600(2529ab - 33550d)z^{210} + \cdots. \quad (3\text{-}1)$$

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 $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$ in $\mathrm{Sp}_2(\mathbb{F}_3)$.

3.2. $\mathbf{Sp_4(\mathbb{F}_3)}$ *and related groups.* Define g_1, g_2, g_3, and g_4 to be

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&\omega&0\\0&0&0&1\end{pmatrix},\ \begin{pmatrix}\alpha&-\bar\alpha&-\bar\alpha&0\\-\bar\alpha&\alpha&-\bar\alpha&0\\-\bar\alpha&-\bar\alpha&\alpha&0\\0&0&0&1\end{pmatrix},\ \begin{pmatrix}1&0&0&0\\0&\omega&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\ \begin{pmatrix}\alpha&\bar\alpha&0&\bar\alpha\\\bar\alpha&\alpha&0&-\bar\alpha\\0&0&1&0\\\bar\alpha&-\bar\alpha&0&\alpha\end{pmatrix}, \tag{3-2}$$

where $\alpha=\omega/\sqrt{-3}$. Define

$$H=\langle g_1,g_2,g_3\rangle \quad\text{and}\quad G=\langle g_1,g_2,g_3,g_4\rangle.$$

The matrices g_i are all complex reflections of order 3, and they are exactly the matrices given in [ST54, 10.5]. As with $H=C_3$ and $G=\mathrm{ST}\,4=\mathrm{Sp}_2(\mathbb{F}_3)$ of the last section, the new groups $H=\mathrm{ST}\,25$ and $G=\mathrm{ST}\,32$ are also complex reflection groups. The group G has the structure $C_3\times\mathrm{Sp}_4(\mathbb{F}_3)$ 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 1. For example, orders are products of degrees of fundamental invariants. Analogous to the old cases $|C_3|=3$ and $|\mathrm{Sp}_2(\mathbb{F}_3)|=4\cdot6$, the new cases are $|H|=6\cdot9\cdot12$ and $|G|=12\cdot18\cdot24\cdot30$. Thus again the index $|G|/|H|=240$ matches the degree of the main polynomial (3-1). The character table of G has size 102×102, so we certainly will not present the analog of Table 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.

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

Define, following [Hun96, 4.72],

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

Also define a, b, c, and d by taking $(2^43^75a, 2^63^95^2b, 2^83^{12}5^3c, 2^{10}3^{16}5^5d)$ to be

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

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

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

When one removes p, q, r from the equations defining a, b, c, d, one gets exactly the degree 240 equation (3-1) for z.

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

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

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 online supplement. Just as in Section 2.4, the contravariants β_k can be described in terms of partial derivatives of the invariants. To be precise, we take $(\beta_{11}, \beta_{17}, \beta_{23}, \beta_{29}) = (\partial_z a, \partial_z b, \partial_z c, \partial_z d)$.

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 $\mathbb{Q}[z_1, z_2, z_3, z]_1 \to \mathbb{Q}[z_1, z_2, z_3, z]_d$. 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 Section 2.5.

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

$$Z = s\alpha_1 + t\alpha_7 + u\alpha_{13} + v\alpha_{19} \tag{3-3}$$

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 (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

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

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 (3-1) yields

$$(A, B, C, D) = \left(\frac{-\tau_2}{30240}, \frac{-\tau_3}{7862400}, \frac{3667\tau_2^2 - 5600\tau_4}{9390915072000}, \frac{2521\tau_2\tau_3 - 2688\tau_5}{886312627200000}\right). \tag{3-4}$$

The matrices M^k have entries in $\mathbb{Q}[a, b, c, d, s, t, u, v]$ 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 $\operatorname{Tr}(M^{12}) = \operatorname{Tr}(M^6 \cdot M^6)$ 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 $\mathbb{Q}[a, b, c, d]$ 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

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

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.

3.6. ***Geometric summary.*** We now summarize our results in the following theorem. The $\bar{\rho}$ of Section 1.2 is the mod 3 representation of the initial genus two curve (1-1). So, to be more explicit, we write $\mathcal{M}_{a,b,c,d} = \mathcal{M}_2^w(\bar{\rho})$ below.

Theorem 2. *Fix an equation $y^2 = x^5 + ax^3 + bx^2 + cx + d$ defining a curve X over $\mathbb{Q}$. 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 $\mathrm{Proj}\,\mathbb{Q}[s, t, u, v]$. The covering maps to the moduli space $\mathcal{M}_2^w \subset \mathrm{Proj}\,\mathbb{Q}[A, B, C, D]$ have degree 25920 and are given by*

$$(A, B, C, D) = (A(a, \ldots, v), B(a, \ldots, v), C(a, \ldots, v), D(a, \ldots, v)). \tag{3-5}$$

The formula

$$y^2 = x^5 + A(a, \ldots, v)x^3 + B(a, \ldots, v)x^2 + C(a, \ldots, v)x + D(a, \ldots, v) \tag{3-6}$$

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

$$\Delta(A(a, \ldots, v), \ldots, D(a, \ldots, v)) = \Delta(a, b, c, d)\delta(a, b, c, d, s, t, u, v)^3. \tag{3-7}$$

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 $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ according to the roots of p_{40} from the end of Section 3.1. While the fibers of $\mathcal{M}_{a,b,c,d}$ over $\mathcal{M}_2^w$ are projective spaces, the entire space defines a nontrivial 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 [Cal20], in particular the comments of Najmuddin Fakhruddin). In principle, Theorem 2 has a direct analog for $\mathcal{M}^*_{a,b,c,d} \to \mathcal{M}_2^w$. The online supplement 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.

3.7. ***Finding (s, t, u, v).*** Let X and Y be Weierstrass curves over $\mathbb{Q}$ 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 Section 2.7.

As in the genus one case, for (3-5) to have a solution, the ratio Δ_X/Δ_Y must be a perfect cube by (3-7). Similarly, for the starred version of (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 Section 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 (3-5), and also to some typically different (A^*, B^*, C^*, D^*) before seeking solutions to the starred analog of (3-5).

Having presented Y properly, one then encounters the computational problem. Namely both (3-5) and its starred version have 155520 solutions $(s, t, u, v) \in \mathbb{C}^4$, and so one cannot expect to find the rational

ones by algebraic manipulations. Working numerically instead, one gets 240 solutions $(p, q, r, z) \in \mathbb{C}^4$ to the large vector equation in Section 3.3. Eight of these solutions are in $\mathbb{R}^4$. These vectors yield eight vectors $(\alpha_1, \alpha_7, \alpha_{13}, \alpha_{19}) \in \mathbb{R}^4$ from the covariants in Section 3.4, and also eight vectors $(\beta_{11}, \beta_{17}, \beta_{23}, \beta_{29}) \in \mathbb{R}^4$. 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 (3-3) and its starred variant

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

When the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 online supplement provides a *Mathematica* program `findisos` to do all steps at once. Examples are given in Sections 4.2 and 4.3.

4. Complements

The four subsections of this section can be read independently.

4.1. ***A matricial identity.*** The polynomials A, B, C, and D in Theorem 2 satisfy the matricial identity

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

where $\mathcal{E}$ can be any one of A, B, C, D, and M is a 4×4 matrix with entries in $\mathbb{Q}[a, b, c, d, s, t, u, v]$ 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 Section 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 Section 2.5. The second column is in fact proportional to $[-\partial_t\delta, \partial_s\delta]^t$, where δ is as in (2-9). Hence M is the matrix found in Lemma 8.4 of [Fis12], 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 $\mathcal{E}(a, \dots, v)$ 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 Section 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 Section 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.

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 (1-1) with

$$(a, b, c, d) = (-5(7e^2 - 2f), -10e(3e^2 - 2f), 5(32e^4 - 39e^2 f + g), -4e(24e^4 + 115e^2 f - 5g)).$$

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

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

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 $\mathbb{Q}[e, f, g]$ 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

$$z = 2^3 5^4 (125e^4 + 20f^2 - 4g)^4 (25e^2 f + g)^6.$$

Applying the numeric method of Section 3.7 and interpolating strongly suggests

$$(s, t, u, v) = \pm(-4e(80e^4 + 7e^2 f - g), 2(40e^4 - 9e^2 f - g), -4e(5e^2 + 2f), 5e^2 + 2f).$$

Specializing the contravariant matrix $M(a, b, c, d, s, t, u, v)^*$ of Section 3.5 to $M(e, f, g)^*$ allows direct computation of its powers up through the needed fifteenth power. Applying (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 nonsurjective, 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.

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 3. *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* [BCGP18, Propositions 10.1.1 and 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 [BCGP18, Propositions 10.1.1, and 10.1.3] and are thus modular. In particular, for any $(s, t, u, v) \in \mathbb{P}^3(\mathbb{Q})$ reducing to $(1, 0, 0, 0) \in \mathbb{P}^3(\mathbb{F}_3)$, 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 [BCGP18, Propositions 10.1.1 and 10.1.3] include that the mod 3 representation $\bar{\rho}$ 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 $\mathbb{Z}$. One such X, appearing in [CCG20, Example 3.3], is given by

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

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 $\mathbb{Z}$.

It is much harder to directly find curves Y satisfying the hypotheses of [BCGP18, Propositions 10.1.1 and 10.1.3] and also satisfying $\mathrm{End}_{\bar{\mathbb{Q}}}(\mathrm{Jac}(Y)) = \mathbb{Z}$. A short list was found in [CCG20]. The curve Y in Example 3.3 there has

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

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 [CCG20] 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 Section 3.7 followed by algebraic verification yields

$$Y = X\left(\frac{129}{125}, \frac{11}{25}, \frac{3}{100}, \frac{1}{20}\right).$$

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.

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 $\mathcal{A}_g(\bar{\rho})$. A conceptual simplification is that since $p = 2$ one does not have the second collection of spaces $\mathcal{A}_g^*(\bar{\rho})$. Correspondingly, the relevant groups are actually reflection groups defined over $\mathbb{Q}$, so that covariants and contravariants coincide. The cases of dimension $g = 3$, 4 make fundamental use of work of Shioda [Shi91].

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 $\alpha_j=\alpha_1^j-k_jI$ 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, with the new $\mathcal{M}_{a,b,c,d}\subset \operatorname{Proj}\mathbb{Q}[s,t,u,v]$ now mapping to the same $\mathcal{M}_2^w\subset\operatorname{Proj}\mathbb{Q}[A,B,C,D]$ with degree 120. Carrying out this easy computation, the elements A, B, C, and D of $\mathbb{Q}[a,b,c,d,s,t,u,v]$ 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 [CC20], we suspect that the varieties $\mathcal{A}_3(\bar\rho)$ are in general not rational. To place ourselves 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

$$y^3+(x^3+a_8x+a_{12})y+(a_2x^4+a_6x^3+a_{10}x^2+a_{14}x+a_{18})=0. \tag{4-1}$$

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^da_d gives an isomorphic curve via $(x,y)\mapsto(u^4x,u^6y)$. The variety $\mathcal{M}_3^f$ is the complement of a discriminant locus in the weighted projective space $\operatorname{Proj}\mathbb{Q}[a_2,\dots,a_{18}]=\mathbb{P}^6(2,\dots,18)$. The invariant theory of the reflection group $\mathrm{ST}\,36=W(E_7)=C_2\times\mathrm{Sp}_6(\mathbb{F}_2)$ gives polynomials $A_i(a_2,\dots,a_{18},s_{-1},\dots,s_{-17})$ of degree i in the s_{-j} and total weight 0. Following the template of the previous cases, for fixed $(a_2,\dots,a_{18})$ one has a six-dimensional variety $\mathcal{M}_{a_2,\dots,a_{18}}\subset\operatorname{Proj}\mathbb{Q}[s_{-1},\dots,s_{-17}]$ parametrizing genus three curves with a rational flex and 2-torsion identified with that of (4-1). The covering maps $\mathcal{M}_{a_2,\dots,a_{18}}\to\mathcal{M}_3^f$ now have degree $|\mathrm{Sp}_6(\mathbb{F}_2)|=1451520$. The number of terms allowed in $A_i(a_2,\dots,a_{18},s_{-1},\dots,s_{-17})$ by the bigradation is the coefficient of x^it^{19i} in

$$\prod_{d\in\{2,6,8,10,12,14,18\}}\frac{1}{(1-t^d)(1-xt^d)}. \tag{4-2}$$

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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in its action on $\mathrm{Jac}(X)[2]$ is $\mathrm{Sp}_8(\mathbb{F}_2)$, and this group is not a complex reflection group. However, one can work with the smooth curves

$$y^3+(a_2x^3+a_8x^2+a_{14}x+a_{20})y+(x^5+a_{12}x^3+a_{18}x^2+a_{24}x+a_{30})=0 \tag{4-3}$$

and a corresponding seven-dimensional moduli space $\mathcal{M}_4^s \subset \mathbb{P}^7(2,\dots,30)$. For a generic curve in (4-3), the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is the index 136 subgroup $\mathrm{O}_8^+(\mathbb{F}_2) : 2$ of $\mathrm{Sp}_8(\mathbb{F}_2)$. Now from the invariant theory of the largest Shephard–Todd group $\mathrm{ST}\,37 = W(E_8) = 2.\mathrm{O}_8^+(\mathbb{F}_2) : 2$, one gets polynomials $A_i(a_2,\dots,a_{30},s_{-1},\dots,s_{-29})$ and covering maps $\mathcal{M}_{a_2,\dots,a_{30}} \to \mathcal{M}_4^s$ of degree $|\mathrm{O}_8^+(\mathbb{F}_2) : 2| = 348,364,800$. Aspects of this situation are within computational reach; for example Shioda computed the degree 240 polynomial $F(a_2,\dots,a_{30},z)$ analogous to (2-3) and (3-1). However the number of allowed terms in $A_i(a_2,\dots,a_{30},s_{-1},\dots,s_{-29})$ is even larger than in the previous $g = 3$ case, being the coefficient of $x^i t^{31i}$ in the analog of (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 (3-1) for our main case $C_3 \times \mathrm{Sp}_4(\mathbb{F}_3)$ is also the specialization $F(0,0,a_{12},0,a_{18},0,a_{24},a_{30},z)$ of Shioda's polynomial.

Acknowledgements

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

References

[BCGP18] George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni, *Abelian Surfaces over totally real fields are potentially modular*, preprint, 2018. arXiv 1812.09269

[BN18] Nils Bruin and Brett Nasserden, *Arithmetic aspects of the Burkhardt quartic threefold*, J. Lond. Math. Soc. (2) **98** (2018), no. 3, 536–556. MR 3893190

[Cal20] Frank Calegari, *Picard groups of moduli stacks*, blog post (and comments), 2020, https://tinyurl.com/FCalegariBlog.

[CC20] Frank Calegari and Shiva Chidambaram, *Rationality of twists of* $\mathcal{A}_2(3)$, preprint, 2020. arXiv 2009.00194

[CCG20] Frank Calegari, Shiva Chidambaram, and Alexandru Ghitza, *Some modular abelian surfaces*, Math. Comp. **89** (2020), no. 321, 387–394. MR 4011548

[CF96] 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.

[Che55] Claude Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782. MR 72877

[Fis12] Tom Fisher, *The Hessian of a genus one curve*, Proceedings of the London Mathematical Society **104** (2012), no. 3, 613–648.

[HS02] Klaus Hulek and G. K. Sankaran, *The geometry of Siegel modular varieties*, Higher dimensional birational geometry (Kyoto, 1997), Adv. Stud. Pure Math., vol. 35, Math. Soc. Japan, Tokyo, 2002, pp. 89–156. MR 1929793

[Hun96] Bruce Hunt, *The geometry of some special arithmetic quotients*, Lecture Notes in Mathematics, vol. 1637, Springer-Verlag, Berlin, 1996. MR 1438547

[LR96] Joan-C. Lario and Anna Rio, *Elliptic modularity for octahedral Galois representations*, Math. Res. Lett. **3** (1996), no. 3, 329–342. MR 1397682

[RS95] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod p representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 148–161. MR 1363500

[Shi91] Tetsuji Shioda, *Construction of elliptic curves with high rank via the invariants of the Weyl groups*, J. Math. Soc. Japan **43** (1991), no. 4, 673–719. MR 1126145

[ST54] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304. MR 59914

Received 23 Feb 2020. Revised 1 Sep 2020.

FRANK CALEGARI: fcale@math.uchicago.edu
Department of Mathematics, The University of Chicago, Chicago, IL, United States

SHIVA CHIDAMBARAM: shivac@math.uchicago.edu
Department of Mathematics, The University of Chicago, Chicago, IL, United States

DAVID P. ROBERTS: roberts@morris.umn.edu
Division of Science and Mathematics, University of Minnesota, Morris, MN, United States

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS