# Descent via $(3,3)$-isogeny on Jacobians of genus 2 curves

by

NILS BRUIN (Burnaby), E. VICTOR FLYNN (Oxford) and
DAMIANO TESTA (Coventry)

**1. Introduction.** In this article we consider curves $C$ of genus 2 over a field $k$ of characteristic not 2 or 3, that have special structure in the 3-torsion of their Jacobians $J$. In particular, we consider the situation where $J[3](k)$ contains a group $\Sigma(k)$ of order 9. As we show in Section 2, such a curve $C$ can be given by a model of the form

$$(1) \qquad\qquad y^2 = F(x) = G(x)^2 + \lambda H(x)^3,$$

where $G(x)$ is cubic and $H(x)$ is quadratic in $x$. The divisor $D = [(x, G(x)) + (x', G(x')) - \kappa]$, where $x, x'$ are the roots of $H(x)$ and $\kappa$ is a canonical divisor, represents a point in $J[3](k)$, as can be seen from the fact that $3D$ is linearly equivalent to the divisor of the function $y - G(x)$.

The curves of interest to us can be expressed as such a model in *several* ways. As we show in Lemma 5, the Weil pairing of the 3-torsion points can be easily expressed in terms of the corresponding polynomials $G(x)$ and $H(x)$. This allows us to fully describe the genus 2 curves that have a subgroup $\Sigma(k) \subset J[3](k)$ of size 9 on which the Weil pairing is trivial.

In Section 3 we phrase the question of classification of such curves in terms of *partial level structures* on principally polarized abelian surfaces. The relevant moduli space is $\mathcal{A}_2(\Sigma)$, with $\Sigma = \mathbb{Z}/3 \times \mathbb{Z}/3$. In Section 4 we determine a genus 2 curve $\mathcal{C}_{rst}$ over $k(r, s, t)$ such that a sufficiently general curve of the type we are interested in can be obtained by specializing $r, s, t$. Our construction identifies $k(r, s, t)$ with the function field of the moduli space $\mathcal{A}_2(\Sigma)$, thereby giving a particularly explicit proof of its rationality. Furthermore, we observe that if $J$ is equipped with a $\Sigma$-level structure, then the quadratic twist $J^{(d)}$ is naturally equipped with a $\Sigma^{(d)}$-level structure. Thus we find that $\mathcal{A}_2(\Sigma)$ and $\mathcal{A}_2(\Sigma^{(d)})$ are naturally isomorphic.

Since $\Sigma \subset J[3]$ is maximally isotropic with respect to the Weil pairing, we see that $\widetilde{J} = J/\Sigma$ is also principally polarized and in fact has a $\Sigma^{\vee}$-level structure. In Section 5 we identify a curve $\widetilde{\mathcal{C}}_{rst}$ such that its Jacobian $\widetilde{\mathcal{J}}_{rst}$ is $\mathcal{J}_{rst}/\Sigma$. In fact, we observe that $\Sigma^{\vee} = \Sigma^{(-3)}$ and hence that the quadratic twist satisfies $\widetilde{\mathcal{C}}_{rst}^{(-3)} \simeq \mathcal{C}_{r's't'}$, where $(r', s', t') = \psi_0(r, s, t)$ is a birational transformation that we explicitly determine. While the final formulas we find are quite manageable, the proof that they are correct requires some significant computation.

In Theorem 13 and Corollary 14 we observe some remarkable relations between the models for $\mathcal{C}_{rst}$ and $\widetilde{\mathcal{C}}_{rst}$. We also identify the natural action of $\mathrm{PGL}_2(\mathbb{F}_3)$ on $\mathcal{A}_2(\Sigma)$, as well as the involution $\mathcal{C}_{rst} \mapsto \widetilde{\mathcal{C}}_{rst}^{(-3)}$, as automorphisms of $k(r, s, t)$.

In Section 6 we get to the original motivation of this paper. If we take $J$ to be a Jacobian of a genus 2 curve with a $\Sigma$-level structure over a number field $k$, then it is particularly easy to compute interesting information about $J(k)$ and $\mathrm{III}(J/k)[3]$ via $(3, 3)$-isogeny descent, using ideas from [13] and [5]. This allows us to give examples of various absolutely simple abelian surfaces with interesting structures in $\mathrm{III}(J/k)[3]$; see Examples 19–21.

**2. Three-torsion on genus two Jacobians.** Let $k$ be a field of characteristic different from $2, 3$ and let $C$ be a smooth projective curve of genus 2 over $k$ given by an affine model
$$C\colon y^2 = F(x),$$
where $F(x) \in k[x]$ is of degree 6 (this only (mildly) restricts the admissible $C$ if $k$ is a finite field of 5 elements). Let $J$ be the Jacobian of $C$. The group $J(k)$ is isomorphic to the group of divisor classes of $k$-rational degree 0 divisors on $C$. Since $C$ is of genus 2, every degree 0 class contains a representative of the form
$$D - \kappa,$$
where $D$ is an effective divisor of degree 2, and $\kappa$ is an effective canonical divisor. Furthermore, for any non-principal class, the divisor $D$ is unique. For $\kappa$ we have choice, since effective canonical divisors are exactly the fibers of the hyperelliptic double cover $x\colon C \to \mathbb{P}^1$. We write $\iota\colon C \to C$ for the hyperelliptic involution, i.e., $\iota(x, y) = (x, -y)$.

LEMMA 1. *Let $\Sigma \subset \mathrm{Pic}(C/k)[3]$ be a subgroup of size 9. Then $\Sigma$ can be generated by a pair of divisors*
$$D_1 - \kappa_1, \quad D_2 - \kappa_2$$
*where $D_1, D_2$ are effective divisors of degree 2 and $\kappa_1, \kappa_2$ are effective canonical divisors, with the supports of $D_1, D_2, \kappa_1, \kappa_2$ pairwise disjoint. A fortiori, we can ensure that $x_*(D_1)$ and $x_*(D_2)$ are disjoint.*

*Proof.* First, note that we can choose each of $\kappa_1$ and $\kappa_2$ to be any fiber of $x\colon \mathcal{C} \to \mathbb{P}^1$ over points in $\mathbb{P}^1(k)$. Since $k$ has characteristic 0 or at least 5, we know that $\#\mathbb{P}^1(k) \geq 6$. Since $x_*(D_1 + D_2)$ is supported on at most 4 rational points, we can choose $\kappa_1, \kappa_2$ with disjoint support from $D_1, D_2$.

Let $\pm T_1, \ldots, \pm T_4$ be the non-zero elements of $\Sigma$. We write $T_i = [D_i - \kappa]$ where $D_i$ is an effective divisor of degree 2. We must show that two of the divisors $x_*(D_1), \ldots, x_*(D_4)$ have disjoint supports. Suppose for a contradiction that this is not the case. Simple combinatorics shows that either two of these divisors are equal, or there is a unique point common to the support of all 4 divisors. In the first case we may suppose $D_1 = P + Q$ and $D_2 = P + \iota Q$ for some $P, Q \in C(k)$. But then $T_1 + T_2 = [2P - \kappa]$, which brings us to the second case.

By switching the signs of the $T_i$ we may suppose $D_i = P + Q_i$ for some $P, Q_1, \ldots, Q_4 \in C(k)$. By re-ordering the $T_i$ we may suppose $P \notin \{Q_1, Q_2\}$ and $T_1 - T_2 = \pm T_3$. We obtain

$$[P + Q_3] = [\iota Q_1 + Q_2] \text{ or } [Q_1 + \iota Q_2].$$

Since non-canonical degree 2 divisor classes have a unique effective representative, we have either $P = \iota Q_1$, in which case $T_1 = 0$, or $P = \iota Q_2$, in which case $T_2 = 0$. This is the required contradiction. ∎

EXAMPLE 2. At this point it may be worth noting that rather exceptional configurations of support for 3-torsion do occur. For instance, for

$$C\colon y^2 = x^6 + rx^3 + 1$$

we see that $T_1 = [(0, 1) + \infty^+ - \kappa]$ and $T_2 = [(0, 1) + \infty^- - \kappa]$ are 3-torsion points. In fact, it is straightforward to check that any genus 2 Jacobian with two independent 3-torsion points such that the group generated by those 3-torsion points is supported on only four points of the curve, must be isomorphic to a curve of this form.

LEMMA 3. *Let $C$ be a curve of genus 2. Then $\mathrm{Pic}(C/k)[3]$ has a subgroup $\Sigma$ of size 9 if and only if $C$ admits a model of the form*

$$C\colon y^2 = F(x) = G_1(x)^2 + \lambda_1 H_1(x)^3 = G_2(x)^2 + \lambda_2 H_2(x)^3,$$

*where $H_1, H_2, G_1, G_2, F \in k[x]$ and $\lambda_1, \lambda_2 \in k^\times$ and $H_1, H_2$ are of degree 2 and $\gcd(H_1, H_2) = 1$.*

*Proof.* Suppose that $T \in \mathrm{Pic}(C/k)[3]$ is non-trivial. We assume that $T = [D - \kappa_\infty]$, where $\kappa_\infty$ is the fiber above $x = \infty$ and $D$ is an effective divisor with support disjoint from $\kappa_\infty$. Then $x_*(D)$ can be described by $H(x) = 0$, where $H(x) \in k[x]$ is a quadratic monic polynomial. Since $3T$ is the principal class, there is a function $g \in k(C)$ such that

$$\mathrm{div}(g) = 3D - 3\kappa_\infty$$

and it is straightforward to check that we must have $g = y - G(x)$ for some $G(x) \in k[x]$ with $\deg(G) \le 3$. It follows that

$$y^2 = F(x) = G(x)^2 + \lambda H(x)^3,$$

and conversely, any such decomposition of $F(x)$ gives rise to a 3-torsion point $T = [D - \kappa]$, where $D$ is the effective degree 2 divisor described by the vanishing of $\{y - G(x), H(x)\}$. The class $2T = -T$ is then described by the vanishing of $\{y + G(x), H(x)\}$.

The existence of $\Sigma$ as stated in the lemma would lead to four decompositions of the type described. If we let $\pm T_1$ and $\pm T_2$ be the points of order 3 corresponding to two of these decompositions, then these four decompositions correspond to $\pm T_1$, $\pm T_2$, $\pm(T_1 - T_2)$ and $\pm(T_1 + T_2)$. Lemma 1 shows we can find a pair of these for which the supports (and their images under the hyperelliptic involution) are disjoint; relabel them as $T_1$ and $T_2$. The corresponding decompositions will have $H_1, H_2$ with no common roots, as required. ∎

The torsion subgroup scheme $J[3]$ comes equipped with a non-degenerate, bilinear, alternating *Weil pairing*

$$e_3 \colon J[3] \times J[3] \to \mu_3,$$

where $\mu_3$ is the group scheme representing the cube roots of unity.

We say that a subgroup $\Sigma \subset J[3]$ is *isotropic* if $e_3$ restricts to the trivial pairing on $\Sigma$. If $\Sigma$ is of degree 9 then $\Sigma$ is *maximal isotropic*, meaning $\Sigma$ is not properly contained in an isotropic subgroup. The non-degeneracy of $e_3$ then induces an isomorphism $J[3]/\Sigma \to \Sigma^\vee = \mathrm{Hom}(\Sigma, \mu_3)$. In particular, if $\Sigma = \mathbb{Z}/3 \times \mathbb{Z}/3$ then we have $\Sigma^\vee = \mu_3 \times \mu_3$.

LEMMA 4. *Let*

$$C \colon y^2 = F(x) = G_1(x)^2 + \lambda_1 H_1(x)^3 = G_2(x)^2 + \lambda_2 H_2(x)^3$$

*be a genus* 2 *curve with* $H_1, H_2$ *quadratic monic polynomials and* $\gcd(H_1, H_2) = 1$. *For* $i \in \{1, 2\}$, *let* $D_i = \{y - G_i(x), H_i(x)\}$ *and let* $T_i = [D_i - \kappa] \in \mathrm{Pic}(C/k)[3]$. *Then*

$$e_3(T_1, T_2) = \frac{\lambda_2}{\lambda_1} \frac{\mathrm{Res}(G_2 - G_1, H_2)}{\mathrm{Res}(G_1 - G_2, H_1)}.$$

*Proof.* We choose canonical divisors $\kappa_1$ and $\kappa_2$ above $x = r_1$ and $x = r_2$ respectively, such that the divisors

$$D_1 - \kappa_1 \quad \text{and} \quad D_2 - \kappa_2$$

have disjoint support. We have the functions

$$g_i = \frac{y - G_i}{(x - r_i)^3} \quad \text{with} \quad \mathrm{div}(g_i) = 3D_i - 3\kappa_i.$$

We can compute the pairing via

$$e_3(T_1, T_2) = \frac{g_1(D_2 - \kappa_2)}{g_2(D_1 - \kappa_1)},$$

where evaluating a function on a divisor is defined as $g(\sum n_P P) = \prod g(P)^{n_P}$. Evaluating $y - G_1(x)$ at $D_2$ means evaluating $G_2(x) - G_1(x)$ at the roots of $H_2(x)$, yielding $\mathrm{Res}(G_2 - G_1, H_2)$. Evaluating $x - r_1$ at $D_2$ yields $H_2(r_1)$. Noting that $\kappa_2 = (r_2, \sqrt{F(r_2)}) + (r_2, -\sqrt{F(r_2)})$, we see that

$$g_1(\kappa_2) = \frac{G_1(r_2)^2 - F(r_2)}{(r_2 - r_1)^6} = \lambda_1 \frac{-H_1(r_2)^3}{(r_2 - r_1)^6}$$

and hence

$$g_1(D_2 - \kappa_2) = \frac{\mathrm{Res}(G_2 - G_1, H_2)(r_2 - r_1)^6}{-\lambda_1 H_1(r_2)^3 H_2(r_1)^3}.$$

Symmetry yields the result. ∎

We can characterize when $e_3(T_1, T_2) = 1$ in terms of the polynomials $G_i, H_i$ in the following way. First note that

$$G_2^2 - G_1^2 = \lambda_1 H_1^3 - \lambda_2 H_2^3.$$

Writing $\alpha_1, \alpha_2, \alpha_3$ for the cube roots of $\lambda_2/\lambda_1$ in an algebraic closure of $k$, we find that

$$(G_2 - G_1)(G_2 + G_1) = \lambda_1(H_1 - \alpha_1 H_2)(H_1 - \alpha_2 H_2)(H_1 - \alpha_3 H_2).$$

It follows that the roots of the quadratic polynomials $H_1 - \alpha_i H_2$ are the same as the roots of $G_2 - G_1$ and $G_2 + G_1$. The way in which they distribute determines the Weil pairing.

LEMMA 5. *The pairing $e_3(T_1, T_2)$ is trivial if and only if none of the polynomials $H_1 - \alpha_i H_2$ divide $G_2 - G_1$.*

*Proof.* First suppose that $G_2 - G_1 = L_1(H_1 - \alpha_1 H_2)$. Then

$$e_3(T_1, T_2) = \frac{\lambda_2}{\lambda_1} \frac{\mathrm{Res}(G_2 - G_1, H_2)}{\mathrm{Res}(G_1 - G_2, H_1)}$$

$$= \frac{\lambda_2}{\lambda_1} \frac{\mathrm{Res}((H_1 - \alpha_1 H_2)L_1, H_2)}{\mathrm{Res}((H_1 - \alpha_1 H_2)L_1, H_1)}$$

$$= \frac{\lambda_2}{\lambda_1 \alpha_1^2} \frac{\mathrm{Res}(L_1, H_2)}{\mathrm{Res}(L_1, H_1)}.$$

Observe that $L_1$ must divide one of the other factors $H_1 - \alpha_j H_2$, say for $j = 2$. Therefore, $\mathrm{Res}(L_1, H_1) = \mathrm{Res}(L_1, \alpha_2 H_2)$. Since $\deg(L_1) = 1$ and $\lambda_2/\lambda_1 = \alpha_1^3$ we obtain

$$e_3(T_1, T_2) = \alpha_1 \frac{\mathrm{Res}(L_1, H_2)}{\mathrm{Res}(L_1, H_1)} = \alpha_1 \frac{\mathrm{Res}(L_1, H_2)}{\mathrm{Res}(L_1, \alpha_2 H_2)} = \frac{\alpha_1}{\alpha_2},$$

which is indeed a primitive cube root of unity.

In the remaining situation we have $G_2 - G_1 = L_1 L_2 L_3$, where, for $i \in \{1, 2, 3\}$, the polynomial $L_i$ divides $H_1 - \alpha_i H_2$, and hence $\mathrm{Res}(L_i, H_1) = \mathrm{Res}(L_i, \alpha_i H_2)$. We obtain

$$\mathrm{Res}(G_2 - G_1, H_1) = \alpha_1 \alpha_2 \alpha_3 \mathrm{Res}(L_1 L_2 L_3, H_2) = \frac{\lambda_2}{\lambda_1} \mathrm{Res}(G_2 - G_1, H_2),$$

which indeed implies that $e_3(T_1, T_2) = 1$. ∎

**3. Level structure on principally polarized abelian surfaces.** Let $n$ be a positive integer. We need the analogues of the modular curves $Y(n)$, $Y_1(n)$ and $Y_0(n)$ for genus 2 Jacobians. The theory is most conveniently stated in terms of slightly more general objects, namely *principally polarized abelian surfaces* (PPAS). These include direct products of elliptic curves, equipped with the product polarization. The advantage is that the category of PPAS is closed under polarized isogenies.

Let $k$ be a field of characteristic not dividing $6n$. We write $\mathcal{A}_2(1)$ for the moduli space of isomorphism classes of PPAS over $k$. The coarse moduli space $\mathcal{A}_2(1)$ is a 3-dimensional variety. Note however that, for any extension $L$ of $k$, the set $\mathcal{A}_2(1)(L)$ of $L$-rational points of $\mathcal{A}_2(1)$ corresponds to $L$-rational isomorphism classes that need not contain an $L$-rational abelian surface; similarly two abelian surfaces defined over $L$ that are isomorphic over $\overline{k}$ need not be isomorphic over $L$.

Let $J$ be a principally polarized abelian surface over $k$. Then $J[n](\overline{k})$ has a non-degenerate bilinear alternating Galois covariant Weil pairing $J[n] \times J[n] \to \mu_n$. A *partial level $n$ structure* on $J$ consists of a finite étale group scheme $\Sigma$ with a pairing $\Sigma \times \Sigma \to \mu_n$ and an injective homomorphism $\Sigma \to J[n]$ that is compatible with the pairings. An isomorphism between $(J, \Sigma \to J[n])$ and $(J', \Sigma \to J'[n])$ is an isomorphism $\phi: J \to J'$ of PPAS such that the composition of $\Sigma \to J[n]$ with $\phi$ yields $\Sigma \to J'$. We write $\mathcal{A}_2(\Sigma)$ for the moduli space of PPAS equipped with a partial level $n$ structure involving $\Sigma$. If we take for example a sample abelian surface $J_0$ and set $\Sigma = J_0[n]$ then $\mathcal{A}_2(\Sigma)$ is the moduli space of PPAS with full level $n$ structure.

We will work with the case $n = 3$ and $\Sigma = \mathbb{Z}/3 \times \mathbb{Z}/3$ with trivial pairing (i.e., $\Sigma$ is *isotropic* with respect to its pairing). Note that the automorphism group of $\Sigma$ is the full $\mathrm{GL}_2(\mathbb{F}_3)$. However, since on every abelian surface $J$ the involution $-1: J \to J$ induces the automorphism $-1$ on level structures, we deduce that $(J, \Sigma \to J)$ and $(J, -\Sigma \to J)$ are isomorphic as level $n$ structures on $J$. Therefore we obtain an action of $\mathrm{PGL}_2(\mathbb{F}_3)$ on $\mathcal{A}_2(\Sigma)$.

In our case $\Sigma \subset J[3]$ is *maximal isotropic*, so the non-degeneracy of $e_3$ yields $J[3]/\Sigma \simeq \Sigma^\vee = \mathrm{Hom}(\Sigma, \mu_3)$. The fact that $\Sigma$ is maximal isotropic also means that the principal polarization on $J$ induces a principal polar-

ization on the isogenous abelian surface $J/\Sigma$. Furthermore, the Weil pairing determines an injection $\Sigma^\vee \to (J/\Sigma)[3]$. Thus we see that our maximal isotropic level structure leads to an isogeny $J \to J/\Sigma$, inducing an isomorphism $\mathcal{A}_2(\Sigma) \to \mathcal{A}_2(\Sigma^\vee)$, whose inverse is induced by the dual isogeny, using the principal polarizations to identify $J$ and $J/\Sigma$ with their duals.

The negation automorphism on $J$ also gives rise to a *quadratic twisting* operation. We write $J^{(d)}$ for the twist of $J$ by the quadratic character of discriminant $d$. A level structure under twisting gives rise to a twisted level structure $\Sigma^{(d)} \to J^{(d)}$, where $\Sigma^{(d)}$ is the quadratic twist of $\Sigma$. This gives rise to an isomorphism $\mathcal{A}_2(\Sigma) \to \mathcal{A}_2(\Sigma^{(d)})$.

We finish by making some observations about the covering degrees of the various moduli spaces of level structures we have introduced. Let us write $\mathcal{A}_2(3)$ for the space corresponding to full level 3 data (say, for $\mathbb{Z}/3 \times \mathbb{Z}/3 \times \mu_3 \times \mu_3$ with obvious pairing). This has a full $\mathrm{PSp}_4(\mathbb{F}_3)$ acting on it. The subgroups fixing a maximal isotropic space are all conjugate and have the group structure $(\mathbb{Z}/3)^3$. There are 40 of them. We see that $\mathcal{A}_2(3) \to \mathcal{A}_2(\Sigma)$ is finite of degree 27. The cover $\mathcal{A}_2(\Sigma) \to \mathcal{A}_2(1)$ is of degree $40 \cdot 24$, determined by the choice of isotropic space times the size of $\mathrm{PGL}_2(\mathbb{F}_3)$.

The variety $\mathcal{A}_2(3)$ is very well-known. Its completion is the Burkhardt quartic, defined by the homogeneous equation

$$(2) \qquad t^4 - t(w^3 + x^3 + y^3 + z^3) + 3wxyz = 0,$$

as is described in [6, 9]. In particular, it and its finite quotients are absolutely irreducible.

Note that most PPAS are Jacobians of genus 2 curves in the sense that outside a proper closed subvariety of $\mathcal{A}_2(1)$, any point can be represented by the Jacobian of a curve of genus 2. In what follows we will determine a genus 2 curve $\mathcal{C}_{rst}$ over the function field of $\mathcal{A}_2(\Sigma)$ together with a level structure on its Jacobian that makes it correspond to the generic point on $\mathcal{A}_2(\Sigma)$.

**4. Parametrization of genus 2 curves with a maximal isotropic $(\mathbb{Z}/3)^2$ in $J[3]$.** Let $k$ be a field of characteristic different from $2, 3$. In this section we derive a genus 2 curve $\mathcal{C}_{rst}$ over $k(r, s, t)$ with two non-trivial divisor classes $T_1, T_2 \in \mathrm{Pic}(\mathcal{C}_{rst}/k(r, s, t))[3]$ with $T_1 \neq \pm T_2$ and $e_3(T_1, T_2) = 1$. This specifies a $\Sigma$-level structure on the Jacobian $\mathcal{J}_{rst}$ of $\mathcal{C}_{rst}$. In the process we will see that any sufficiently general Jacobian with a $\Sigma$-level structure over $k$ can be obtained via specialization from $\mathcal{J}_{rst}$. This identifies $k(r, s, t)$ with the function field of $\mathcal{A}_2(\Sigma)$, verifying that this moduli space is indeed rational.

We use the notation from Lemmas 3 and 5. We consider the algebra $k[\alpha] = k[t]/(t^3 - \lambda_2/\lambda_1)$, which is only a field if $\lambda_2/\lambda_1$ is not a cube in $k$, but at least will always be an étale algebra because $\lambda_1, \lambda_2 \neq 0$. We write

$\mathrm{Nm} = \mathrm{Norm}_{k[x,\alpha]/k[x]}$. We have

$$(G_2 - G_1)(G_2 + G_1) = \lambda_1 \,\mathrm{Nm}(H_1 - \alpha H_2).$$

From Lemma 5 it follows that

(3) $\qquad H_1 - \alpha H_2 = LM \quad$ for some $L, M \in k[\alpha, x]$

and that for some $c \in k^\times$ we have

$$G_2 - G_1 = \tfrac{1}{c} \mathrm{Nm}(M), \qquad G_1 = \tfrac{1}{2}\big(c\lambda_1 \mathrm{Nm}(L) - \tfrac{1}{c}\mathrm{Nm}(M)\big),$$
$$G_2 + G_1 = c\lambda_1 \mathrm{Nm}(L), \qquad G_2 = \tfrac{1}{2}\big(c\lambda_1 \mathrm{Nm}(L) + \tfrac{1}{c}\mathrm{Nm}(M)\big).$$

We observe that

$$(cy)^2 = (cG_1)^2 + (c^2\lambda_1)H_1^3 = (cG_2)^2 + (c^2\lambda_2)H_2^3,$$

so by adjusting the values of $\lambda_1, \lambda_2$ we can assume $c = 1$. This shows that the isomorphism class of $\mathcal{C}$ is determined by $\lambda_1, \lambda_2, L, M$.

Furthermore, if $k$ has sufficiently many elements we can ensure that $L$ does not vanish at $x = \infty$ and that $L$ is monic, so that

$$L = x - (l_0 + \alpha l_1 + \alpha^2 l_2).$$

The fractional linear transformation

$$x \mapsto \frac{l_1 x + \alpha^3 l_2^2 - l_0 l_1}{l_2 x + l_1^2 - l_0 l_2},$$

with determinant $l_1^3 - \alpha^3 l_2^3$, sends $l_0 + l_1\alpha + l_2\alpha^2$ to $\alpha$. One can check that if $l_1^3 - \alpha^3 l_2^3 = 0$ then either $F$ has a repeated root, and hence our data does not specify a genus 2 curve, or $l_1 = l_2 = 0$. In the latter case, $L$ is already defined over $k$, so via $x \mapsto x - l_0$ we can move its root to 0. This shows that via a fractional linear transformation, we can assume that

(4) $\quad L = x - u\alpha \quad$ and $\quad M = (c_0 + c_1\alpha + c_2\alpha^2)x - (m_0 + m_1\alpha + m_2\alpha^2),$

where $u = 0$ corresponds to the case where $l_1 = l_2 = 0$. In order for $LM$ to be of the form $H_1 - \alpha H_2$, with $H_1, H_2 \in k[x]$, we need

(5) $\qquad c_2 = 0, \quad m_1 u = 0, \quad m_2 = -c_1 u.$

We set $\lambda_1 = s$, $\lambda_2 = st$ and observe that $c^2 F(x)$ is homogeneous with respect to the following gradings:

|  | $s$ | $t$ | $c_0$ | $c_1$ | $c_2$ | $m_0$ | $m_1$ | $m_2$ | $u$ | $x$ | $c$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| weights | 3 | 0 | $-1$ | $-1$ | $-1$ | 0 | 0 | 0 | 1 | 1 | $-3$ |
|  | 0 | 3 | 0 | $-1$ | $-2$ | 0 | $-1$ | $-2$ | $-1$ | 0 | 0 |
|  | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | $-3$ |

We can solve (5) either via $u = 0$ or via $m_1 = 0$. For $u = 0$ we find that $H_1$ and $H_2$ both have a root at $x = 0$. By Lemma 1 we know we can avoid this case by changing the basis for the 3-torsion subgroup. Thus we see that any $\mathrm{PGL}_2(\mathbb{F}_3)$-orbit has a representative that avoids this locus.

For the other case we take the affine open described by

$$(s,t,c_0,c_1,c_2,m_0,m_1,m_2,u) = (s,t,1,-1,0,-r,0,0,1),$$

leading to

$$H_1 = x^2 + rx + t, \quad H_2 = x^2 + x + r, \quad \lambda_1 = s, \quad \lambda_2 = st.$$

It is instructive to record which cases are excluded by the choices that we make here. We use the gradings to scale $c_0 = 1$, $c_1 = -1$, $u = 1$, so any curves that require any of these parameters to be 0 are ruled out. The gradings immediately show that setting any of $c_0, c_1, u$ to 0 yields at most a 2-dimensional family of curves. For $u = 0$ we have seen that $H_1, H_2$ have a common root. Furthermore, the gradings show that this forms at most a 2-dimensional family up to isomorphy. For $c_0 = 0$ we see that $H_1$ has a root at $\infty$, and for $c_1 = 0$ we see that $H_2$ has a root at infinity. Note that if $u \neq 0$, we have applied a linear transformation to normalize the form of $L$, so $\infty$ has geometric meaning. For instance, Example 2 describes a 1-dimensional family of curves that lie in this locus.

To summarize, we have established the following theorem, where we have scaled $s$ by 4 to avoid some denominators in coefficients.

THEOREM 6. *Let $k$ be a field of characteristic different from $2, 3$ and suppose that $(C, T_1, T_2)$ consists of a genus 2 curve $C$ over $k$ and $T_1, T_2 \in \operatorname{Pic}(\mathcal{C}/k)[3]$ such that $\#\langle T_1, T_2\rangle = 9$ and $e_3(T_1, T_2) = 1$. If the specified data is sufficiently general then $(C, T_1, T_2)$ is isomorphic to a suitable specialization of $r, s, t$ in the family described by the following data:*

$$H_1 = x^2 + rx + t,$$
$$\lambda_1 = 4s,$$
$$G_1 = (s - st - 1)x^3 + 3s(r - t)x^2 + 3sr(r - t)x - st^2 + sr^3 + t,$$
$$H_2 = x^2 + x + r,$$
$$\lambda_2 = 4st,$$
$$G_2 = (s - st + 1)x^3 + 3s(r - t)x^2 + 3sr(r - t)x - st^2 + sr^3 - t,$$
$$H_3 = sx^2 + (2sr - st - 1)x + sr^2,$$
$$\lambda_3 = 4t/(st + 1)^2,$$
$$G_3 = \frac{1}{st+1}\big((s^2t^2 - s^2t + 2st + s + 1)x^3 + (3s^2t^2 - 3s^2tr + 3st + 3sr)x^2$$
$$+ (3s^2t^2r - 3s^2tr^2 + 3str + 3sr^2)x + s^2t^3 - s^2tr^3 + 2st^2 + sr^3 + t\big),$$
$$H_4 = (str - st - sr^2 + sr + r)x^2 + (st^2 - str - st - sr^3 + 2sr^2 + t)x$$
$$+ st^2 - str^2 - str + sr^3 + t,$$

$$\lambda_4 = 4st/(st^2 - 3str + st + sr^3 + t)^2,$$

$$G_4 = \frac{1}{st^2 - 3str + st + sr^3 + t}\big((s^2t^3 - 3s^2t^2r - s^2tr^3 + 6s^2tr^2 - 3s^2tr$$
$$+s^2t - s^2r^3 + 2st^2 - 3str + 2st - sr^3 + t)x^3$$
$$+ (3s^2t^3 - 6s^2t^2r^2 - 3s^2t^2 + 9s^2tr^3 - 3s^2tr^2$$
$$+3s^2tr - 3s^2r^4 + 3st^2 - 6str^2 + 3str)x^2$$
$$+ (-3s^2t^3r + 6s^2t^3 - 9s^2t^2r + 3s^2tr^4$$
$$+3s^2tr^3 + 3s^2tr^2 - 3s^2r^5 - 3st^2r + 6st^2 - 3str^2)x$$
$$- s^2t^4 + 3s^2t^3r + s^2t^3 - 6s^2t^2r^2 + 3s^2tr^4$$
$$+s^2tr^3 - s^2r^6 - 2st^3 + 3st^2r + st^2 - 2str^3 - t^2\big).$$

*Here* $\mathcal{C}_{rst}\colon y^2 = F_{rst}(x) = G_i^2 + \lambda_i H_i^3$ *for* $i = 1,2,3,4$ *and* $T_i = [\{H_i(x) = 0,$
$y - G_i(x) = 0\} - \kappa]$ *and* $T_3 = T_1 + T_2$ *and* $T_4 = T_1 - T_2.$

For future reference we note that

(6) $$\mathrm{Disc}(F_{rst}) = -2^{12}3^6\delta_1^3\delta_2^3\delta_3^3\delta_4^3\delta_5^3\delta_6^3\delta_7^3,$$

where

$$\delta_1 = s,$$
$$\delta_2 = t,$$
$$\delta_3 = st + 1,$$
(7) $$\delta_4 = r^3 - 3rt + t^2 + t,$$
$$\delta_5 = r^3s - 3rst + st^2 + st + t,$$
$$\delta_6 = r^3s^2 - 3rs^2t - 3rs + s^2t^2 + s^2t + 2st + s + 1,$$
$$\delta_7 = r^3s^2t + r^3s - 3rs^2t^2 - 3rst + s^2t^3 + s^2t^2 + 2st^2 + t.$$

REMARK 7. Note that $\mathcal{C}_{rst}^{(d)}\colon dy^2 = F_{rst}(x)$ has exactly the same property for $\Sigma^{(d)}$-level structure.

**5. The isogeny.** We consider the curve $\mathcal{C}_{rst}$ as defined in Theorem 6 and its Jacobian $\mathcal{J}_{rst}$. In this section we determine a curve $\widetilde{\mathcal{C}}_{rst}$ whose Jacobian $\widetilde{\mathcal{J}}_{rst}$ is isogenous to $\mathcal{J}_{rst}$ via the isogeny $\mathcal{J}_{rst} \to \mathcal{J}_{rst}/\Sigma$. We do so by determining the corresponding map between their Kummer surfaces. There are various numerical methods to compute isogenous Jacobians (see for instance [8]), but since our computations are over $\mathbb{Q}(r,s,t)$, we needed to take some care to avoid coefficient explosion.

**5.1. Isogenies and the quartic model of the Kummer surface.** Let $J$ be a principally polarized abelian surface with theta divisor $\Theta_J$ and suppose that $\Sigma \subset J[3]$ is maximal isotropic. We consider $\widetilde{J} = J/\Sigma$ and

the isogeny $\phi\colon J \to \widetilde{J}$. By [11, Proposition 16.8] there exists a principal polarization on $\widetilde{J}$ with theta divisor $\Theta_{\widetilde{J}}$ such that $\phi^*(\Theta_{\widetilde{J}}) = 3\Theta_J$.

The classical theory of theta divisors tells us that $\mathcal{O}_J(2\Theta_J)$ is 4-dimensional and that the induced map $J \to \mathbb{P}^3$ yields a quartic model of the Kummer surface $\mathcal{K} = J/\langle -1 \rangle$. We write $\widetilde{\mathcal{K}}$ for the Kummer surface of $\widetilde{J}$. Similarly, the linear system $\mathcal{O}_{\widetilde{J}}(2\Theta_{\widetilde{J}})$ provides a quartic model of $\widetilde{\mathcal{K}}$.

REMARK 8. Note that this construction requires that we choose $2\Theta_J$ to be defined over the base field $k$. If $k$ is not algebraically closed, then there might not exist a $k$-rational divisor $\Theta_J$ in its class. For an abelian surface, however, $2\Theta_J$ is always linearly equivalent to a $k$-rational divisor.

The isogeny induces a map $\mathcal{K} \to \widetilde{\mathcal{K}}$ in the following way. First note that $\phi^*\mathcal{O}_{\widetilde{J}}(2\Theta_{\widetilde{J}}) \subset \mathcal{O}_J(6\Theta_J)$. The involution $-1\colon J \to J$ induces a linear transformation on $\mathcal{O}_J(6\Theta_J)$. We write $\mathcal{O}_J(6\Theta_J)^+$ for the fixed subspace. Similarly, the translation action of $\Sigma$ on $J$ induces a linear action on the same space. We write $\mathcal{O}_J(6\Theta_J)^\Sigma$ for its fixed space. It is straightforward to check that

$$\phi^*\mathcal{O}_{\widetilde{J}}(2\Theta_{\widetilde{J}}) = \mathcal{O}_J(6\Theta_J)^\Sigma \cap \mathcal{O}_J(6\Theta_J)^+.$$

If $\xi_0, \xi_1, \xi_2, \xi_3$ forms a basis for $\mathcal{O}_J(2\Theta_J)$ then $\mathcal{O}_J(6\Theta_J)^+$ is generated by the cubic forms in $\xi_0, \xi_1, \xi_2, \xi_3$. Thus we see that the isogeny $\phi\colon J \to \widetilde{J}$ induces a map $\mathcal{K} \to \widetilde{\mathcal{K}}$ which, between the quartic models, is given by cubic forms.

**5.2. Choice of model for Kummer surfaces.** Let $C$ be a curve of genus 2 given by a model

$$C\colon y^2 = f_6 x^6 + f_5 x^5 + \cdots + f_0,$$

with Jacobian $J$. We follow [7, p. 17] and choose a particular basis for $\mathcal{O}_J(2\Theta_J)$. We describe $\xi = \xi(D) = \xi_0, \ldots, \xi_3$ as functions on $J$ in terms of a divisor class $D = [(x_1, y_1) + (x_2, y_2) - \kappa]$ on $C$ as follows:

$$(8) \quad \xi_0 = 1, \quad \xi_1 = x_1 + x_2, \quad \xi_2 = x_1 x_2, \quad \xi_3 = \frac{\Phi(\xi_0, \xi_1, \xi_2) - 2y_1 y_2}{\xi_1^2 - 4\xi_0 \xi_2},$$

where

$$\Phi(\xi_0, \xi_1, \xi_2) = 2f_0\xi_0^3 + f_1\xi_0^2\xi_1 + 2f_2\xi_0^2\xi_2 + f_3\xi_0\xi_1\xi_2 + 2f_4\xi_0\xi_2^2 + f_5\xi_2^2\xi_1 + 2f_6\xi_2^3.$$

Note that for a Mumford representation $D = [\{x^2 - \xi_1 x + \xi_2, y - g_0 - g_1 x\} - \kappa]$ we have $y_1 y_2 = g_0^2 + g_0 g_1 \xi_1 + g_1^2 \xi_2$, so one can compute these coordinates readily from such a representation.

The quartic equation for the model of $\mathcal{K}$ arising from these coordinates has the shape

$$\mathcal{K}\colon (\xi_1^2 - 4\xi_0\xi_2)\xi_3^2 + \Phi(\xi_0, \xi_1, \xi_2)\xi_3 + \Psi(\xi_0, \xi_1, \xi_2) = 0,$$

where $\Psi(\xi_0, \xi_1, \xi_2)$ is a quartic form we do not need explicitly here. The important observation is that one can read off the coefficients $f_0, \ldots, f_6$ directly from $\Phi$ and thus recover $C$ from it.

In order to produce $\Sigma$-invariant forms on $\mathcal{K}$, we use biquadratic forms from [7, p. 23], arising from the addition structure on $J$. For $i, j = 0, \ldots, 3$ we have forms $B_{i,j} \in k[\xi_0, \ldots, \xi_3, \xi'_0, \ldots, \xi'_3]$, biquadratic in $(\xi_0, \ldots, \xi_3)$ and $(\xi'_0, \ldots, \xi'_3)$, such that for points $D_1, D_2$ on $J$ we have, as projective matrices,

$$(9) \quad \big(\xi_i(D_1 + D_2)\, \xi_j(D_1 - D_2) + \xi_i(D_1 - D_2)\, \xi_j(D_1 + D_2)\big)$$
$$= \big(B_{ij}(\xi(D_1), \xi(D_2))\big).$$

We fix two points $T_1, T_2 \in J[3]$ that generate $\Sigma$, write $\xi(T_1), \xi(T_2)$ for the coordinate vectors of their images on the quartic model of $\mathcal{K}$ and define

$$(10) \quad \begin{aligned} R_{ij}\big(\xi_0, \ldots, \xi_3\big) &= B_{ij}\big(\xi_0, \ldots, \xi_3, \xi(T_1)\big), \\ S_{ij}\big(\xi_0, \ldots, \xi_3\big) &= B_{ij}\big(\xi_0, \ldots, \xi_3, \xi(T_2)\big). \end{aligned}$$

We see that the cubic forms

$$R_{ijk} = \xi_i R_{jk} + \xi_j R_{ki} + \xi_k R_{ij} \quad \text{with } i, j, k \in \{0, \ldots, 3\}$$

are invariant under translation by $T_1$, and similarly that the forms

$$S_{ijk} = \xi_i S_{jk} + \xi_j S_{ki} + \xi_k S_{ij} \quad \text{with } i, j, k \in \{0, \ldots, 3\}$$

are invariant under translation by $T_2$. For $C = \mathcal{C}_{rst}$ the $R_{ijk}$ and $S_{ijk}$ each generate spaces of dimension 8 that intersect in a space of dimension 4. This intersection provides us with an explicit description of $\phi^*(\mathcal{O}_{\tilde{J}}(2\Theta_{\tilde{J}}))$.

Generally, we expect $\widetilde{J}$ to be the Jacobian of a curve of genus 2, say $\widetilde{\mathcal{C}}$. We can try to find a basis $\tilde{\xi}_0, \ldots, \tilde{\xi}_3$ for $\phi^*(\mathcal{O}_{\tilde{J}}(2\Theta_{\tilde{J}}))$ that is the pullback of a basis of the type described by (8). We can then read off the curve $\widetilde{\mathcal{C}}$, at least up to quadratic twist, from the resulting equation for $\tilde{\mathcal{K}}$. The basis choice can largely be characterized by the order of vanishing of each $\xi_i$ at the identity element. This leads us to conclude that, up to scalar multiples, we should take the basis choice

$$\begin{aligned} \tilde{\xi}_0 &= (1\xi_0 + 0\xi_1 + 0\xi_2)\xi_3^2 + \cdots, \\ \tilde{\xi}_1 &= (0\xi_0 + 1\xi_1 + 0\xi_2)\xi_3^2 + \cdots, \\ \tilde{\xi}_2 &= (0\xi_0 + 0\xi_1 + 1\xi_2)\xi_3^2 + \cdots. \end{aligned}$$

The determination of $\tilde{\xi}_3$ is a little more involved. The resulting forms for $\widetilde{\mathcal{C}} = \widetilde{\mathcal{C}}_{rst}$ are too voluminous to reproduce here, but we have made them available electronically at [4]. Via interpolation we find tentatively the following result.

THEOREM 9. *Let* $\mathcal{C}_{rst}$ *be as described by Theorem* 6. *Then* $\widetilde{\mathcal{J}}_{rst} = \mathcal{J}_{rst}/\Sigma$ *is the Jacobian of the genus* 2 *curve*

$$\widetilde{\mathcal{C}}_{rst} \colon -3y^2 = \widetilde{G}_4^2 + \tilde{\lambda}_4 \widetilde{H}_4^3,$$

*with*

$$\widetilde{G}_4 = \Delta \left( (s - st - 1)x^3 + 3s(r - t)x^2 + 3rs(r - t)x + (r^3 s - st^2 - t) \right),$$

$$\begin{aligned} \widetilde{H}_4 = {} & (r - 1)(rs - st - 1)x^2 + (r^3 s - 2r^2 s + rst + r - st^2 + st - t)x \\ & - (r^2 - t)(rs - st - 1), \end{aligned}$$

$$\tilde{\lambda}_4 = 4\Delta st,$$

*where*

$$\begin{aligned} (11) \qquad \Delta = {} & r^6 s^2 - 6r^4 s^2 t - 3r^4 s + 2r^3 s^2 t^2 + 2r^3 s^2 t + 3r^3 st + r^3 s + r^3 \\ & + 9r^2 s^2 t^2 + 6r^2 st - 6rs^2 t^3 - 6rs^2 t^2 - 9rst^2 - 3rst - 3rt \\ & + s^2 t^4 + 2s^2 t^3 + s^2 t^2 + 2st^3 + 3st^2 + t^2 + t. \end{aligned}$$

**5.3. Proof of Theorem 9.** Since we have completely explicit descriptions of $\mathcal{C}_{rst}$ and $\widetilde{\mathcal{C}}_{rst}$, we can write down explicit quartic models

$$\mathcal{K} \colon Q = (\xi_1^2 - 4\xi_0 \xi_2)\xi_3^2 + \Phi(\xi_0, \xi_1, \xi_2)\xi_3 + \Psi(\xi_0, \xi_1, \xi_2) = 0,$$
$$\widetilde{\mathcal{K}} \colon \tilde{Q} = (\tilde{\xi}_1^2 - 4\tilde{\xi}_0 \tilde{\xi}_2)\tilde{\xi}_3^2 + \tilde{\Phi}(\tilde{\xi}_0, \tilde{\xi}_1, \tilde{\xi}_2)\tilde{\xi}_3 + \tilde{\Psi}(\tilde{\xi}_0, \tilde{\xi}_1, \tilde{\xi}_2) = 0.$$

Furthermore, we have an explicit description at [4] of the map between them by expressions that give $\tilde{\xi}_0, \ldots, \tilde{\xi}_3$ as cubic forms in $\xi_0, \ldots, \xi_3$. We already know that $\widetilde{\mathcal{K}}$ is irreducible, because it is the Kummer surface of a Jacobian. Therefore, to check if $\widetilde{\mathcal{K}}$ is indeed the image of $\mathcal{K}$, we only need to substitute the cubic forms into the equation for $\widetilde{\mathcal{K}}$ and check that the resulting degree 12 equation is divisible by the quartic equation for $\mathcal{K}$. This is doable for specific specializations of $r, s, t$ in $\mathbb{Q}$, but the computers at our disposal were not able to do this directly.

We note that $Q$ and $\tilde{Q}$ (after substitution of the cubic forms) are polynomials in $r, s, t, \xi_0, \ldots, \xi_3$, of degrees 2 and 10 in $\xi_3$ respectively. Hence, long division yields unique polynomials $\sigma \in \mathbb{Q}[r, s, t, \xi_0, \ldots, \xi_3]$ and $\rho_0, \rho_1 \in \mathbb{Q}[r, s, t, \xi_0, \xi_1, \xi_2]$ such that

$$(\xi_1^2 - 4\xi_0 \xi_2)^9 \tilde{Q} = \sigma Q + \rho_1 \xi_3 + \rho_0.$$

We want to prove that $\rho_1$ and $\rho_0$ are identically zero. To this end, we analyze the appropriate Newton polygons (or do the required computation using polynomials with coefficients truncated to the appropriate leading terms) to verify that $\rho_0, \rho_1$ are of degrees at most $102, 67, 36$ in $r, s, t$. Hence, if we check that $Q$ indeed divides $\tilde{Q}$ for a grid of $103 \times 68 \times 37$ values for $(r, s, t)$ then a straightforward interpolation argument shows that $\rho_0, \rho_1$ must indeed

be identically 0. This is something that can easily be verified by a computer in less than 3 hours.

This computation shows that $\tilde{\mathcal{K}}$ is indeed the Kummer surface of $\tilde{J} = J/\Sigma$ and hence that $\tilde{\mathcal{C}}_{rst}$ is correct up to quadratic twist. Recall from Section 3 that $J/\Sigma$ comes equipped with a $\Sigma^\vee$-level structure. In our case, we have $\Sigma = (\mathbb{Z}/3)^2$, so $\Sigma^\vee = (\mu_3)^2 = \Sigma^{(-3)}$. Thus, it follows that $\tilde{\mathcal{J}}_{rst}^{(-3)}$ should have a $\Sigma$-level structure itself such that the isogeny corresponding to it brings us back to $\mathcal{J}_{rst}^{(-3)}$.

LEMMA 10. *Let $\mathcal{C}_{rst}$ be as in Theorem 6, let $\tilde{\mathcal{C}}_{rst}$ be as in Theorem 9, and let $\tilde{\mathcal{C}}_{rst}^{(-3)}$ be the quadratic twist of $\tilde{\mathcal{C}}_{rst}$ by $-3$, using the notation in Remark 7. Define $\psi_0$ by*

$$\psi_0(r,s,t)$$
$$= \left( \frac{-s(r-1)(r^2-t)(\delta_5-r)}{(rs-st-1)^2\delta_4}, \frac{(rs-st-1)^3\delta_4^2}{st(r-1)^3\Delta}, \frac{s^2(r-1)^3(r^2-t)^3}{(rs-st-1)^3\delta_4^2} \right).$$

*Then $\mathcal{C}_{r's't'}$ is birationally equivalent to $\tilde{\mathcal{C}}_{rst}^{(-3)}$, where $(r',s',t') = \psi_0(r,s,t)$. Furthermore, as a rational map we have $\psi_0(\psi_0(r,s,t)) = (r,s,t)$. The $\Sigma^{(-3)}$-level structure induced on $\tilde{\mathcal{J}}_{rst}$ determines the kernel of the dual isogeny $\tilde{\mathcal{J}}_{rst} \to \mathcal{J}_{rst}$.*

*Proof.* One can check directly that $\mathcal{C}_{r's't'}$ is birationally equivalent to $\tilde{\mathcal{C}}_{rst}^{(-3)}$ under the transformation

$$\theta_0 \colon (x,y) \mapsto \left( \frac{-(r^3-3rt+t^2+t)(rs-st-1)}{(r^2-t)(r-1)^2s}x + \frac{r-t}{r-1}, \right.$$
$$\left. \frac{\Delta t(rs-st-1)^3(r^3-3rt+t^2+t)^2}{s^2(r-1)^3(r^2-t)^3}y \right).$$

This naturally marks some $\Sigma^{(-3)}$-level structure on $\tilde{\mathcal{J}}_{rst}$. Note that it even does so over $\mathbb{Q}$, where we have no primitive cube root of unity. The Weil pairing implies that on $\tilde{\mathcal{J}}_{rst}^{(-3)}$, any two $\Sigma$-level structures must differ by a unique automorphism of $\Sigma$. It follows that the same holds for $\Sigma^{(-3)}$-level structures on $\tilde{\mathcal{J}}_{rst}$ itself. ∎

REMARK 11. A little more is true than we prove in Lemma 10: we have a *natural* $\Sigma^\vee$ structure on $\tilde{\mathcal{J}}_{rst}$. In Lemma 15 we identify this, and in Lemma 16 we identify the corresponding involution on $k(r,s,t)$, which is not *quite* $\psi_0$ as listed above. We selected $\psi_0$ because the corresponding transformation $\theta_0$ is easy to write down.

**5.4. Additional relations.** At this point, we have what we require for the applications in the next sections, since we only need the $\Sigma$-level structure up to $\Sigma$-automorphism. We shall devote the remainder of the section to a

more concise description of $\widetilde{\mathcal{C}}_{rst}$, which will also give the full natural $\Sigma^\vee$-level structure on $\widetilde{\mathcal{J}}_{rst}$.

REMARK 12. In the case of isotropic $(\mathbb{Z}/2)^2$-level structure, there is a very satisfying expression for the isogenous abelian variety in the general case (i.e., when it is a Jacobian), described in [2] (see also [7, Chapter 9]). An isotropic $(\mathbb{Z}/2)^2$-level structure on the Jacobian of a genus 2 curve can be expressed by a model of the curve of the form

$$C\colon y^2 = q_1(x)q_2(x)q_3(x),$$

where each $q_i$ is a quadratic polynomial in $x$. One forms a $3\times3$ matrix whose columns are the coefficients of $q_1, q_2, q_3$. If the determinant $\Delta$ of this matrix is non-zero, then the isogenous surface is a Jacobian and the associated curve can be expressed as

$$\widetilde{\mathcal{C}}\colon y^2 = \Delta\tilde{q}_1(x)\tilde{q}_2(x)\tilde{q}_3(x),$$

where the coefficients of the $\tilde{q}_i$ are easily expressible in terms of the cofactors of this same $3 \times 3$ matrix. Of particular note is that the curve is (naturally) again of the same form. Indeed, it is straightforward to verify that the same operation applied twice gives us back a model that is isomorphic to the curve we started with and that the quadrics satisfy the peculiar relation

$$(12) \qquad q_1(x)\tilde{q}_1(\tilde{x}) + q_2(x)\tilde{q}_2(\tilde{x}) + q_3(x)\tilde{q}_3(\tilde{x}) = \Delta(x - \tilde{x})^2,$$

given as identity (9.2.5) in [7]. In fact, this relation is the basis for the $(2, 2)$ correspondence between $C$ and $\widetilde{\mathcal{C}}$ that gives rise to the polarized isogeny between their Jacobians.

One might hope to find a similar relation in our case. Indeed, the general theory implies there is a correspondence between $\mathcal{C}_{rst}$ and $\widetilde{\mathcal{C}}_{rst}$ giving rise to the polarized isogeny between $\mathcal{J}_{rst}$ and $\widetilde{\mathcal{J}}_{rst}$. However, that general theory only predicts an $(18, 2)$ correspondence which lacks the desired symmetry and does not seem inviting from a computational point of view. The following theorem gives a possibly more attractive relation between the models for $\mathcal{C}_{rst}$ and $\widetilde{\mathcal{C}}_{rst}$ expressing the level structures on their Jacobians.

THEOREM 13. *For* $j = 1, \ldots, 4$ *let* $H_j(x) = h_{2j}x^2 + h_{1j}x + h_{0j}$ *be as in Theorem 6; for* $i = 1, \ldots, 7$, *let* $\delta_i$ *be as in* (7). *Define*

$$(13) \qquad A = \begin{pmatrix} h_{21} & h_{22} & h_{23} & h_{24} \\ h_{11} & h_{12} & h_{13} & h_{14} \\ h_{01} & h_{02} & h_{03} & h_{04} \\ -r/2 & -1/2 & -\delta_3/2 & -\delta_5/2 \end{pmatrix}.$$

*Then* $\det(A) = \Delta$ *(see (11)). Let $M$ be the cofactor matrix of $A$, i.e., $M^T = \det(A)A^{-1}$, and let $M_{ij}$ be its entry in the $i$th row and $j$th column. Define*

(14)
$$\widetilde{A} = \begin{pmatrix} M_{31} & M_{32} & M_{33} & M_{34} \\ -2M_{21} & -2M_{22} & -2M_{23} & -2M_{24} \\ M_{11} & M_{12} & M_{13} & M_{14} \\ \frac{1}{2}M_{41} & \frac{1}{2}M_{42} & \frac{1}{2}M_{43} & \frac{1}{2}M_{44} \end{pmatrix},$$

*and*

(15)      $\widetilde{H}_j(x) = \widetilde{A}_{1j}x^2 + \widetilde{A}_{2j}x + \widetilde{A}_{3j} \quad$ *for $j = 1, \dots 4$,*

*so that the $\widetilde{H}_j(x)$ bear the same relationship to the first three rows of $\widetilde{A}$ as the $H_j(x)$ bear to $A$. Also define*

(16)      $\tilde{\lambda}_1 = \lambda_1\Delta/\delta_6^2, \quad \tilde{\lambda}_2 = \lambda_2\Delta/\delta_7^2, \quad \tilde{\lambda}_3 = \lambda_3\Delta\delta_3^2/\delta_4^2, \quad \tilde{\lambda}_4 = \lambda_4\Delta\delta_5^2.$

*Finally define*

(17)                        $\widetilde{G}_4(x) = \Delta(G_1(x) - 2t),$

*and define $\widetilde{G}_1(x), \widetilde{G}_2(x), \widetilde{G}_3(x)$ up to $\pm$ (which is all we require for these) to be such that*

(18)      $\widetilde{G}_i(x)^2 = \widetilde{G}_4(x)^2 + \tilde{\lambda}_4\widetilde{H}_4(x)^3 - \tilde{\lambda}_i\widetilde{H}_i(x)^3,$ *for $i = 1, 2, 3$.*

*Then the curve $\widetilde{\mathcal{C}}_{rst}$ of Theorem 9 is the same as*

(19)        $\widetilde{\mathcal{C}}_{rst} : y^2 = -3(\widetilde{G}_i(x)^2 + \tilde{\lambda}_i\widetilde{H}_i(x)^3) \quad$ *for $i = 1, \dots, 4$.*

An immediate consequence the relationship between the matrices $A, \widetilde{A}$ is the following identity, which is strikingly similar to (12) for the Richelot isogeny.

COROLLARY 14. *Let the $H_i(x), \widetilde{H}_i(x)$ be as in Theorem 13. Then*

(20)      $H_1(x)\widetilde{H}_1(\tilde{x}) + H_2(x)\widetilde{H}_2(\tilde{x}) + H_3(x)\widetilde{H}_3(\tilde{x}) + H_4(x)\widetilde{H}_4(\tilde{x}) = \Delta(x - \tilde{x})^2.$

*Proof.* We first note that, if we take the matrix $\widetilde{A}$ of (14), divide the second row by $-2$, then swap the first and third rows, and then take the transpose, we obtain $A^{\text{adj}}$, the adjugate of the matrix $A$ of (13). We recall the standard identity $AA^{\text{adj}} = \Delta I_4$ from linear algebra and note that, in the left hand side of (20), the coefficients of $x^2, \tilde{x}^2$ are equal to diagonal entries of $AA^{\text{adj}}$ and so equal $\Delta$. Similarly, the coefficient of $x\tilde{x}$ is $-2$ times a diagonal entry of $AA^{\text{adj}}$ and so equals $-2\Delta$. The remaining coefficients on the left hand side of (20) equal non-diagonal entries of $AA^{\text{adj}}$, and so are all 0, as required. ∎

We can also formulate the relationship between the $H_i$ and the $\widetilde{H}_i$ in more intrinsic terms. Let $T_1, T_2, T_3, T_4 \in \mathcal{J}_{rst}[3]$ corresponding to $H_i$ be such that $T_1 + T_2 = T_3$ and $T_1 - T_2 = T_4$ and let $\widetilde{T}_i$ and $\widetilde{H}_i$ be related

analogously. Suppose we have a basis $T_1, T_2, U_1, U_2$ for $\mathcal{J}_{rst}[3]$ such that the Gram matrix of the Weil pairing (with values written additively) is

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

Then $U_1, U_2$ naturally provides a basis choice for $\mathcal{J}_{rst}[3]/\Sigma = \Sigma^\vee$. We find that $\phi(U_1) = \pm\widetilde{T}_1$ and that $\phi(U_2) = \pm\widetilde{T}_2$, with the same choice of sign (which is an ambiguity in $U_1, U_2$ already). This provides the following.

LEMMA 15. *The labeling for the* $\widetilde{T}_i$ *naturally marks the* $\Sigma^\vee$*-level structure on* $\widetilde{\mathcal{J}}_{rst}$ *in the sense that for* $i = 1, \ldots, 4$, *we have*

$$e_3(T_i, U) = 0 \quad \text{for any } U \in \widetilde{\mathcal{J}}_{rst}[3] \text{ such that } \phi(U) = \widetilde{T}_i.$$

*Proof.* We only have to check this statement for a particular specialization of $r, s, t$, for instance over a finite field where the full 3-torsion is pointwise defined. We have a completely explicit description of the map $\phi$ on the Kummer surfaces, which is sufficient to determine the appropriate elements $U$. One can then just verify the claim in the lemma by exhaustion. It is straightforward to check that the condition given indeed uniquely determines the structure (up to sign). ∎

**5.5. Automorphisms.** Recall from Section 3 that $\mathcal{A}_2(\Sigma)$ has $\mathrm{PGL}_2(\mathbb{F}_3)$ acting on it. Furthermore, because in our case we have $\Sigma^\vee \simeq \Sigma^{(-3)}$, we get an additional automorphism $J \mapsto \widetilde{J}^{(-3)}$. We identified the effect of this last automorphism on $r, s, t$ in Lemma 10. Here we describe generators for the other automorphisms as well. Note that $\psi_0$ is only a rational map, because the abelian surface $\widetilde{J}$ need not be a Jacobian if $J$ is: $\widetilde{J}$ may be a product of elliptic curves. In addition, while we have seen in Section 4 that every sufficiently general Jacobian with a $\Sigma$-level structure admits a model that is a specialization of $\mathcal{J}_{rst}$, this may involve a change of basis. Thus, we should also expect $\mathrm{PGL}_2(\mathbb{F}_3)$ to only act birationally on $(r, s, t)$.

LEMMA 16. *The transformations*

$$\psi_1(r, s, t) = \left( \frac{t}{r^2}, \frac{r^3 s}{t}, \frac{t^2}{r^3} \right),$$

$$\psi_2(r, s, t) = \left( r, \frac{1}{s(r^3 - 3rt + t^2 + t)}, t \right),$$

$$\psi_3(r, s, t) = \left( r, \frac{t(st + 1)}{r^3}, \frac{r^3 s}{st + 1} \right),$$

*have the property that, for each* $i = 1, 2, 3$, *if* $(r', s', t') = \psi_i(r, s, t)$ *then* $\mathcal{C}_{r's't'}$ *is birationally equivalent to* $\mathcal{C}_{rst}$. *The group generated by* $\psi_1, \psi_2, \psi_3$ *is isomorphic to* $\mathrm{PGL}_2(\mathbb{F}_3)$. *Furthermore, if* $\psi_0$ *is as in Lemma* 10 *then the group generated by* $\psi_0, \psi_1, \psi_2, \psi_3$ *is isomorphic to* $\mathbb{Z}/2 \times \mathrm{PGL}_2(\mathbb{F}_3)$.

*Proof.* We first note that, for each $i = 1, 2, 3$, if $(r', s', t') = \psi_i(r, s, t)$ then $\mathcal{C}_{r's't'}$ is birationally equivalent to $\mathcal{C}_{rst}$ under $\theta_i$, where

$$\theta_1(x, y) = \left( \frac{t}{rx}, \frac{ty}{x^3} \right),$$

$$\theta_2(x, y) = \left( \frac{(r-t)x + (r^2 - t)}{(r-1)x + (t-r)}, \frac{s(r^3 - 3rt + t^2 + t)^2 y}{(rx - x + t - r)^3} \right),$$

$$\theta_3(x, y) = \left( \frac{-rx}{x+r}, \frac{r^3 y}{(x+r)^3} \right).$$

It can also be checked that $\psi_1, \psi_2, \psi_3$ permute the roles of the $H_i$ and correspond, respectively, to:

$$(H_1, H_2, H_3, H_4) \leftrightarrow (H_2, H_1, H_3, H_4),$$
$$(H_1, H_2, H_3, H_4) \leftrightarrow (H_1, H_2, H_4, H_3),$$
$$(H_1, H_2, H_3, H_4) \leftrightarrow (H_3, H_2, H_1, H_4).$$

It follows that they can be identified with the transpositions $(12), (34), (13)$ in $S_4$, which generate all of $S_4$. Hence the group generated by $\psi_1, \psi_2, \psi_3$ is isomorphic to $S_4$, which in turn is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_3)$. Note also that $\psi_1, \psi_2, \psi_3$ give the same permutation of the roles of the $\widetilde{H}_i$. We finally note that $\psi_0$ corresponds to $(H_1, H_2, H_3, H_4) \leftrightarrow (\widetilde{H}_4, \widetilde{H}_3, \widetilde{H}_2, \widetilde{H}_1)$ and can be replaced by $\psi_0' = \psi_3 \psi_1 \psi_2 \psi_3 \psi_0$, which corresponds to $(H_1, H_2, H_3, H_4) \leftrightarrow (\widetilde{H}_1, \widetilde{H}_2, \widetilde{H}_3, \widetilde{H}_4)$, and is given explicitly by

$$\psi_0'(r, s, t) = \left( \frac{-(r^2 - t)(rs - st - 1)(\delta_5 - r)}{(r-1)^2 \delta_7}, \frac{(r-1)^3 s \delta_6 \delta_7^2}{(rs - st - 1)^3 \delta_5 \Delta}, \right.$$
$$\left. \frac{t(rs - st - 1)^3 (\delta_5 - r)^3}{(r-1)^3 \delta_6 \delta_7^2} \right).$$

This is an involution, and it commutes with $\psi_1, \psi_2, \psi_3$. Hence the group generated by the maps $\psi_0, \psi_1, \psi_2, \psi_3$, which is the same as the group generated by $\psi_0', \psi_1, \psi_2, \psi_3$, must be isomorphic to the group $\mathbb{Z}/2 \times \mathrm{PGL}_2(\mathbb{F}_3)$. ∎

**6. Isogeny descent.** Galois cohomology associates to an isogeny

$$0 \to J[\phi] \to J \xrightarrow{\phi} \widetilde{J} \to 0$$

between abelian varieties over a field $k$ an exact sequence

$$0 \to \frac{\widetilde{J}(k)}{\phi J(k)} \xrightarrow{\gamma} H^1(k, J[\phi]) \to H^1(k, J).$$

For $k$ a number field and $v$ a place of $k$, we consider the completion $k_v$ and its separable closure $k_v^{\mathrm{sep}}$ and identify $\mathrm{Gal}(k_v^{\mathrm{sep}}/k_v)$ with a relevant decomposition group inside $\mathrm{Gal}(k^{\mathrm{sep}}/k)$. This allows us to consider restriction maps $\mathrm{res}_v \colon H^i(k, \cdot) \to H^i(k_v, \cdot)$. Writing $\gamma_v$ for the relevant connecting homomorphism over the base field $k_v$, this allows us to define the *Selmer group*

$$(21) \qquad \mathrm{Sel}^\phi(J/k) = \{\delta \in H^1(k, J[\phi]) : \mathrm{res}_v(\delta) \in \mathrm{im}\,\gamma_v \text{ for all places } v \text{ of } k\}.$$

The Selmer group contains the image of $\gamma$. If this containment is strict then part of the Selmer group represents non-trivial elements in $\mathrm{III}(J/k)$. To be precise, we have

$$0 \to \frac{\widetilde{J}(k)}{\phi J(k)} \to \mathrm{Sel}^\phi(J/k) \to \mathrm{III}(J/k)[\phi] \to 0.$$

Therefore, the computation of Selmer groups can be used to exhibit non-trivial elements in Tate–Shafarevich groups. This is taking a historically backward view, since originally Tate–Shafarevich groups were introduced as a means to measure the failure of Selmer groups to provide sharp bounds on the size of $\widetilde{J}(k)/\phi J(k)$.

Let $\mathbb{G}_{\mathrm{m}}$ be the multiplicative group scheme over a field $k$ of characteristic not dividing 2. For $d \in k^\times$, we write $\mathbb{G}_{\mathrm{m}}^{(d)}$ for the *quadratic twist by $d$* of the multiplicative group. It is the group scheme that fits in the short exact sequence

$$1 \to \mathbb{G}_{\mathrm{m}}^{(d)}(L) \to L[\sqrt{d}]^\times \xrightarrow{\mathrm{Norm}} L^\times \to 1$$

for any extension $L$ of $k$. Similarly, for a positive integer $n$, we write $\mu_n^{(d)} \subset \mathbb{G}_{\mathrm{m}}^{(d)}$ for the kernel of the morphism $x \mapsto x^n$.

We begin by stating the following slight generalization of a classical result from Kummer theory.

LEMMA 17. *Let $n > 0$ be odd, let $k$ be a field of characteristic not dividing $2n$ and let $\mu_n$ be the $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-module of $n$th roots of unity in $k^{\mathrm{sep}}$. For $d \in k^\times$, we have*

$$H^1(k, \mu_n^{(d)}) = \frac{\mathbb{G}_{\mathrm{m}}^{(d)}(k)}{\mathbb{G}_{\mathrm{m}}^{(d)}(k)^n}.$$

LEMMA 18. *Let $\tilde{\phi} \colon \widetilde{J} \to J$ be a polarized isogeny between principally polarized abelian surfaces with kernel $\Sigma^{(-3d)} = \mu_3^{(d)} \times \mu_3^{(d)}$. Suppose that $J$ is the Jacobian of a genus 2 curve of the form*

$$C \colon y^2 = d(G_1(x)^2 + \lambda_1 H_1(x)^3) = d(G_2(x)^2 + \lambda_2 H_2(x)^3),$$

*where the 3-torsion subgroup with generators supported at $H_1(x) = 0$ and at $H_2(x) = 0$ is the kernel of an isogeny $\phi \colon J \to \widetilde{J}$ such that $\phi \circ \tilde{\phi} = 3$. Then*

*the connecting homomorphism*

$$\tilde{\gamma}\colon \frac{J(k)}{\tilde{\phi}\widetilde{J}(k)} \to H^1(k, \Sigma^{(-3d)}) = \frac{\mathbb{G}_{\mathrm{m}}^{(d)}(k)}{(\mathbb{G}_{\mathrm{m}}^{(d)}(k))^3} \times \frac{\mathbb{G}_{\mathrm{m}}^{(d)}(k)}{(\mathbb{G}_{\mathrm{m}}^{(d)}(k))^3}$$

*is induced by the partial map*

$$C \dashrightarrow \mathbb{G}_{\mathrm{m}}^{(d)} \times \mathbb{G}_{\mathrm{m}}^{(d)}, \qquad (x,y) \mapsto (y - \sqrt{d}\, G_1(x), y - \sqrt{d}\, G_2(x)).$$

*Proof.* This is a direct application of the theory developed in [13] and [5]. ∎

From Theorems 6 and 9 we can obtain isogenies $\phi\colon J \to \widetilde{J}$ and $\tilde{\phi}\colon \widetilde{J} \to J$ with kernels $\Sigma = \mathbb{Z}/3 \times \mathbb{Z}/3$ and $\Sigma^\vee = \mu_3 \times \mu_3$ respectively. We use Lemma 18 to compute $\mathrm{Sel}^\phi(J/\mathbb{Q})$ and $\mathrm{Sel}^{\tilde{\phi}}(\widetilde{J}/\mathbb{Q})$. As suggested by the lemma, we represent the cohomology classes by elements of $\mathbb{Q}(\sqrt{-3})^\times/\mathbb{Q}(\sqrt{-3})^{\times 3}$ and $\mathbb{Q}^\times/\mathbb{Q}^{\times 3}$ respectively.

We take $S$ to be the set of primes consisting of 3 and the primes of bad reduction of $C$. By [5, Proposition 9.2], the Selmer groups lie in the subgroups that are unramified outside $S$. We can represent those using $S$-units in $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}$. This already provides us with explicit finite groups that contain the Selmer groups. The remaining conditions come from the local images at $v \in S$ (note that $\mathbb{R}^\times/\mathbb{R}^{\times 3}$ is trivial, so the archimedian place does not provide any information). With the explicit description of the maps $\gamma_v$ and $\tilde{\gamma}_v$ we can generate elements in their images. Using [13, Lemma 3.8, Proposition 3.9] and some basic diagram chasing we have

$$(22) \qquad \#\frac{\widetilde{J}(\mathbb{Q}_v)}{\phi J(\mathbb{Q}_v)} \#\frac{J(\mathbb{Q}_v)}{\tilde{\phi}\widetilde{J}(\mathbb{Q}_v)} = \frac{\#\Sigma(\mathbb{Q}_v)\,\#\Sigma^\vee(\mathbb{Q}_v)}{|3|_p^2}$$

$$= \begin{cases} 81 & \text{if } v = 3 \text{ or } v \equiv 1 \ (\mathrm{mod}\, 3), \\ 9 & \text{if } v \equiv 2 \ (\mathrm{mod}\, 3), \end{cases}$$

so we know when we have found enough elements to generate the entire image. By explicitly computing the restriction maps $\mathbb{Q}^\times/\mathbb{Q}^{\times 3} \to \mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 3}$ and similarly for $\mathbb{Q}(\sqrt{-3})$, we can compute the Selmer groups using essentially the definition in (21).

We now apply the above theory to several examples, which combine the information of standard 2-descent and the above descent via $\Sigma$-isogeny and $\Sigma^\vee$-isogeny. In particular, this will give the first examples of non-trivial 3-part of the Tate–Shafarevich group on a non-reducible abelian surface.

The first example illustrates a situation where a 3-isogeny descent can be used to obtain a sharper rank bound than one can get from a 2-descent and hence exhibit some non-trivial 2-torsion elements in the Tate–Shafarevich group. There are alternative methods to do this, which show in the process that there is no 4-torsion, but obtaining unconditional results through these

is too computationally expensive at present. The computations involved in our examples are easily reproduced using Magma [1] and the software we have made available at [4]. Each of the examples is easily checked to be absolutely simple by checking that the reduction at 31 is absolutely simple, by [10, Proposition 3].

EXAMPLE 19. *Let $J$ be the Jacobian of the curve*

$$\mathcal{C}_{-3,-3,-3}\colon y^2 = (13x^3 - 105)^2 - 12(x^2 - 3x - 3)^3.$$

*Then $J(\mathbb{Q}) \simeq (\mathbb{Z}/3)^2 \times \mathbb{Z}^2$ and $\mathrm{III}(J/\mathbb{Q})[6] \simeq (\mathbb{Z}/2)^3$. Furthermore, conditional on the Generalized Riemann Hypothesis for a certain degree 12 number field, we have $\mathrm{III}(J/\mathbb{Q})[6^\infty] = (\mathbb{Z}/2)^3$.*

*Proof.* Using the isogenies $\phi\colon J \to \widetilde{J}$ and $\tilde{\phi}\colon \widetilde{J} \to J$ we find

$$\mathrm{Sel}^{\tilde{\phi}}(\widetilde{J}/\mathbb{Q}) = (\mathbb{Z}/3)^4 \quad \text{and} \quad \mathrm{Sel}^\phi(J/\mathbb{Q}) = 0.$$

We already know that $J[3](\mathbb{Q})$ is non-trivial and further computation shows that $J(\mathbb{Q})^{\mathrm{tors}} = (\mathbb{Z}/3)^2$. A height computation shows that divisors supported at $101x^2 + 21x + 147 = 0$ and at $x^2 - 6x - 45 = 0$ generate independent classes in $J(\mathbb{Q})$. From this one can deduce the structure of $J(\mathbb{Q})$ and that $\mathrm{III}(J/\mathbb{Q})[\phi]$ and $\mathrm{III}(\widetilde{J}/\mathbb{Q})[\tilde{\phi}]$ are trivial. From $3 = \tilde{\phi} \circ \phi$ it follows that $\mathrm{III}(J/\mathbb{Q})[3]$ is trivial as well.

A 2-descent on $J$ yields $\mathrm{Sel}^2(J/\mathbb{Q}) = (\mathbb{Z}/2)^5$, which shows that $\mathrm{III}(J/\mathbb{Q})[2] = (\mathbb{Z}/2)^3$. Indeed $J$ is *odd* in the sense of [12].

In order to prove there is no 4-torsion in $\mathrm{III}(J/\mathbb{Q})$, using a visibility argument [3] we observe that $J^{(-2)}(\mathbb{Q})$ has rank at least 3, which can be shown by exhibiting enough points and a height pairing computation. One can compute that $\mathrm{Sel}^2(J/\mathbb{Q}(\sqrt{-2})) = (\mathbb{Z}/2)^5$, provided one verifies a certain class group computation for which one presently requires the Generalized Riemann Hypothesis. Since the rank of $J(\mathbb{Q}(\sqrt{-2}))$ is the sum of the ranks of $J(\mathbb{Q})$ and $J^{(-2)}(\mathbb{Q})$, one concludes that $\mathrm{III}(J/\mathbb{Q}(\sqrt{-2}))[2]$ is trivial. Since the restriction map $\mathrm{III}(J/\mathbb{Q}) \to \mathrm{III}(J/\mathbb{Q}(\sqrt{-2}))$ can only kill elements of order 2, the statement follows.

It is worth noting that $\mathrm{Sel}^2(J^{(-2)}/\mathbb{Q}) = (\mathbb{Z}/2)^5$, so $\mathrm{III}(J^{(-2)}/\mathbb{Q})[2^\infty] = (\mathbb{Z}/2)^2$. ∎

Note that, for the last part of the above argument, we could alternatively have successfully used $\mathbb{Q}(\sqrt{2})$ instead of $\mathbb{Q}(\sqrt{-2})$.

EXAMPLE 20. *Let $\widetilde{J}$ be the Jacobian of the curve*

$$\tilde{\mathcal{C}}_{-2,1,2}\colon y^2 = -48(83x^3 + 498x^2 - 996x + 581)^2 - 3984(15x^2 - 26x + 10)^3.$$

*Then $\widetilde{J}(\mathbb{Q}) \simeq \mathbb{Z}$ and $\mathrm{III}(\widetilde{J}/\mathbb{Q})[3] \simeq (\mathbb{Z}/3)^2$.*

*Proof.* We find

$$\mathrm{Sel}^{\tilde{\phi}}(\widetilde{J}/\mathbb{Q}) = (\mathbb{Z}/3)^5 \quad \text{and} \quad \mathrm{Sel}^{\phi}(J/\mathbb{Q}) = 0.$$

With $J(\mathbb{Q})[3] = (\mathbb{Z}/3)^2$ and $\widetilde{J}(\mathbb{Q})[3] = 0$, this implies that $\widetilde{J}(\mathbb{Q})$ is of rank at most 3.

From a 2-descent we find $\mathrm{Sel}^2(J/\mathbb{Q}) = (\mathbb{Z}/2)$. Furthermore, we find a non-torsion point in $J(\mathbb{Q})$, so we deduce that $J(\mathbb{Q}) = (\mathbb{Z}/3)^2 \times \mathbb{Z}$ and $\widetilde{J}(\mathbb{Q}) = \mathbb{Z}$. Combined with the result above, this yields $\mathrm{III}(\widetilde{J}/\mathbb{Q})[3] = (\mathbb{Z}/3)^2$. ∎

EXAMPLE 21. *The Jacobian $\widetilde{J}$ of the curve*

$$\tilde{\mathcal{C}}_{2,-1,-2}\colon y^2 = -48(706x^3 + 2118x^2 + 4236x + 353)^2 + 16944(5x^2 - 14x - 30)^3$$

*has 6-torsion in $\mathrm{III}(\widetilde{J})$ and $\widetilde{J}(\mathbb{Q}) = \{0\}$.*

*Proof.* Let $J$ be the Jacobian of

$$\mathcal{C}_{2,-1,-2}\colon y^2 = 12x^6 + 72x^5 + 312x^4 + 688x^3 + 768x^2 + 192x + 68.$$

A direct computation shows that $\mathrm{Sel}^{\tilde{\phi}}(\widetilde{J}/\mathbb{Q}) = (\mathbb{Z}/3)^4$ and $\mathrm{Sel}^{\phi}(J/\mathbb{Q}) = 0$. The torsion $J(\mathbb{Q})^{\mathrm{tor}} = (\mathbb{Z}/3)^2$ explains two factors, so either $\widetilde{J}(\mathbb{Q})$ is of rank 2 or $\mathrm{III}(\widetilde{J}/\mathbb{Q})[3]$ is non-trivial. Similarly, a 2-descent shows that $\mathrm{Sel}^2(\widetilde{J}/\mathbb{Q}) \simeq \mathrm{Sel}^2(J/\mathbb{Q}) = (\mathbb{Z}/2)^2$.

In order to show that $J(\mathbb{Q})$ is actually of rank 0, we observe that $\mathrm{Sel}^2(J^{(3)}/\mathbb{Q}) = (\mathbb{Z}/2)^3$ and that $J^{(3)}(\mathbb{Q}) \simeq \mathbb{Z}^3$. Further computation shows that $\mathrm{Sel}^2(J/\mathbb{Q}(\sqrt{3})) = (\mathbb{Z}/2)^3$ as well, so base changing $J^{(3)}$ from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{3})$ does not increase the rank. It follows that $J(\mathbb{Q})$ is of rank 0, so $J(\mathbb{Q}) \simeq (\mathbb{Z}/3)^2$, and that $\mathrm{III}(J/\mathbb{Q})[2^\infty] = \mathrm{III}(\widetilde{J}/\mathbb{Q})[2^\infty] = (\mathbb{Z}/2)^2$. ∎

## References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[2] J.-B. Bost et J.-F. Mestre, *Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2*, Gaz. Math. 38 (1988), 36–64.

[3] N. Bruin and E. V. Flynn, *Exhibiting* SHA[2] *on hyperelliptic Jacobians*, J. Number Theory 118 (2006), 266–291.

[4] N. Bruin, E. V. Flynn, and D. Testa, *Genus 2 Jacobians with* (3,3) *level structure*, http://www.cecm.sfu.ca/~nbruin/c3xc3 (2013).

[5] N. Bruin, B. Poonen, and M. Stoll, *Generalized explicit descent and its application to curves of genus* 3, arXiv:1205.4456 (2012).

[6] H. Burkhardt, *Untersuchungen aus dem Gebiete der hyperelliptischen Modulfunctionen. Zweiter Theil*, Math. Ann. 38 (1891), 161–224.

[7] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, London Math. Soc. Lecture Note Ser. 230, Cambridge Univ. Press, Cambridge, 1996.

[8] I. Dolgachev and D. Lehavi, *On isogenous principally polarized abelian surfaces*, in: Curves and Abelian Varieties, Contemp. Math. 465, Amer. Math. Soc., Providence, RI, 2008, 51–69.

[9] J. W. Hoffman and S. H. Weintraub, *The Siegel modular variety of degree two and level three*, Trans. Amer. Math. Soc. 353 (2001), 3267–3305.

[10] E. W. Howe and H. J. Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field*, J. Number Theory 92 (2002), 139–163.

[11] J. S. Milne, *Abelian varieties*, in: Arithmetic Geometry (Storrs, CT, 1984), Springer, New York, 1986, 103–150.

[12] B. Poonen and M. Stoll, *The Cassels–Tate pairing on polarized abelian varieties*, Ann. of Math. (2) 150 (1999), 1109–1149.

[13] E. F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. 310 (1998), 447–471.

Nils Bruin
Department of Mathematics
Simon Fraser University
Burnaby, BC, Canada V5A 1S6
E-mail: nbruin@cecm.sfu.ca

Damiano Testa
Mathematics Institute, Zeeman Building
University of Warwick
Coventry CV4 7AL, United Kingdom
E-mail: D.Testa@warwick.ac.uk

E. Victor Flynn
Mathematical Institute
University of Oxford
24–29 St. Giles
Oxford OX1 3LB, United Kingdom
E-mail: flynn@maths.ox.ac.uk