VISIBILITY OF 4-COVERS OF ELLIPTIC CURVES

NILS BRUIN AND TOM FISHER

Abstract. Let C be a 4-cover of an elliptic curve E, written as a quadric intersection in $\mathbb{P}^3$. Let E' be another elliptic curve with 4-torsion isomorphic to that of E. We show how to write down the 4-cover C' of E' with the property that C and C' are represented by the same cohomology class on the 4-torsion. In fact we give equations for C' as a curve of degree 8 in $\mathbb{P}^5$.

We also study the K3-surfaces fibred by the curves C' as we vary E'. In particular we show how to write down models for these surfaces as complete intersections of quadrics in $\mathbb{P}^5$ with exactly 16 singular points. This allows us to give examples of elliptic curves over $\mathbb{Q}$ that have elements of order 4 in their Tate-Shafarevich group that are not visible in a principally polarized abelian surface.

1. Introduction

Let E and E' be elliptic curves over a field k that are *n-congruent*, meaning that there is an isomorphism of k-group schemes $\sigma\colon E[n] \to E'[n]$. We suppose that the characteristic of k does not divide n. We may use σ to transfer certain interesting arithmetic information between E and E'. For instance let k be a number field. An n-torsion element of the *Tate-Shafarevich* group $Ш(E/k)$ may be represented by a class $\xi \in H^1(k, E[n])$. Let $\sigma_* : H^1(k, E[n]) \to H^1(k, E'[n])$ be the isomorphism induced by σ. It might happen that while ξ maps to a non-trivial element in $Ш(E/k)[n]$, represented say by a curve C, the image of $\sigma_*(\xi)$ in $H^1(k, E')$, represented say by a curve C', could be trivial. This is an example of Mazur's concept of *visibility* (see [10, 16]): the graph $\Delta \subset E[n] \times E'[n]$ of the n-congruence σ provides an isogeny $E \times E' \to (E \times E')/\Delta$ and a model for C arises as the fibre of $(E \times E')/\Delta$ over a point in $E'(k)$ that bears witness to the triviality of C'.

The case $n = 2$ is relatively special, because quadratic twists have isomorphic 2-torsion. It is true, however, that given any $\xi \in H^1(k, E[2])$, one can find another elliptic curve E' with isomorphic 2-torsion such that $\sigma_*(\xi) \in H^1(k, E'[2])$ represents a trivial homogeneous space under E'; see [4, 15].

Date: 23rd January 2018.

2010 *Mathematics Subject Classification.* 11G05, 11G35, 14H10.

Key words and phrases. elliptic curves, Tate-Shafarevich groups, Mazur visibility, descent, K3 surfaces, local-global obstructions.

In order to determine if a given class $\xi \in H^1(k, E[n])$ can be made visible using an n-congruence, one can proceed in three steps. We assume $n > 2$.

(i) One parametrizes the elliptic curves n-congruent to E. This amounts to determining an appropriate twist $X_E(n)$ of the modular curve of full level n. (We make no reference to the Weil pairing in the definition of $X_E(n)$, so geometrically this curve has $\phi(n)$ components, where ϕ is Euler's totient function.)
(ii) If $n > 2$ then $X_E(n)$ is a fine moduli space and there is a universal elliptic curve E_t over $X_E(n)$. One constructs a fibred surface $S_{E,\xi}(n) \to X_E(n)$ whose fibres are the n-covers of E_t corresponding to $\xi \in H^1(k, E_t[n])$.
(iii) If one can find a rational point P on $S_{E,\xi}(n)$, and none of the cusps of $X_E(n)$ are rational points, then ξ can be made visible by taking E' to be the elliptic curve corresponding to the moduli point on $X_E(n)$ below P. On the other hand, if $S_{E,\xi}(n)$ has no rational points then ξ cannot be made visible using an elliptic curve n-congruent to E.

One can classify the n-congruence σ by the effect it has on the Weil pairing. If $n = 3, 4$, it can either preserve or invert it. Correspondingly, the modular curve $X_E(n)$ has two components $X_E^+(n)$ and $X_E^-(n)$. Note that there is a tautological point on $X_E^+(n)$ corresponding to E itself, and the fibre of $S_{E,\xi}^+(n) \to X_E^+(n)$ above this point represents the image of ξ in $H^1(k, E)$. If this image lies in $Ш(E/k)$ then the fibre, and hence also $S_{E,\xi}^+(n)$ itself, has points everywhere locally. Mazur uses this in [16] to show that any element of $Ш(E/k)$ of order 3 can be made visible using an elliptic curve 3-congruent to E. Indeed he shows that $S_{E,\xi}^+(3)$ is a blow-up of a twist of $\mathbb{P}^2$, and hence satisfies the local-to-global principle.

From a computational point of view, it is attractive if $(E \times E')/\Delta$ can be realized as a Jacobian, or more generally, admits a principal polarization. It naturally does so if we start with σ inverting the Weil pairing. Again taking $n = 3$, one can show that $S_{E,\xi}^+(3)$ is birational to $\mathbb{P}^2$ over k if and only if the same is true for $S_{E,\xi}^-(3)$. It follows (see [5]) that any element of $Ш(E/k)$ of order 3 is visible in the Jacobian of a genus 2 curve.

For larger n there are major obstacles to this kind of visibility over number fields. Once $n \geq 6$ the components of $X_E(n)$ have positive genus, and so rational points are rare: the set of candidate elliptic curves E' is sparse for $n = 6$ and finite for $n \geq 7$. See [14] for explicit examples over $\mathbb{Q}$ of non-existence of such E' for $n = 6, 7$.

In this article we consider the case $n = 4$. This case is particularly interesting for several reasons:

(i) The curve $X_E^+(4)$ is of genus 0, but the surface $S_{E,\xi}^+(4)$ is a K3-surface. Much is conjectured, but little is known about the rational points on K3-surfaces.

(ii) Given $\xi \in H^1(k, E[n])$, representing a genus 1 curve of degree n, there is another fibred surface $T_{E,\xi}(n) \to X_E(n)$ whose fibres are n-covers of E_t, but now sharing the same action of $E[n]$ on a suitable linear system. For $n = 3, 4, 5$, explicit invariant-theoretic constructions of these surfaces are given in [12], [13]. When n is odd the surfaces $S^{\pm}_{E,\xi}(n)$ and $T^{\pm}_{E,\xi}(n)$ are the same, but when n is even a correction to this idea is needed.

Taking $n = 4$, we may identify $X^{\pm}_E(4) \cong \mathbb{P}^1$. We start with $D = \{Q_1 = Q_2 = 0\} \subset \mathbb{P}^3$ a quadric intersection representing $\xi \in H^1(k, E[4])$. The invariant theory in [12] allows us to write down $T^{\pm}_{E,\xi}(4) \to \mathbb{P}^1$ as a family of quadric intersections in $\mathbb{P}^3$. However the fibres of $S^{\pm}_{E,\xi}(4) \to \mathbb{P}^1$ cannot always be written as quadric intersections. In this article we show how to write down a singular model for $S^{\pm}_{E,\xi}(4)$ as a complete intersection of quadrics in $\mathbb{P}^5$. On this model, the non-singular fibres are genus 1 curves of degree 8.

In fact the surfaces $S^{\pm}_{E,\xi}(4)$ and $T^{\pm}_{E,\xi}(4)$ are twists of surfaces $S(4)$ and $T(4)$ that may be defined as follows. Let $X(n)$ be the modular curve whose non-cuspidal points parametrize elliptic curves E together with a symplectic isomorphism $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mu_n$. We write

$$E_t\colon \quad y^2 = x(x-1)(x - \frac{(1-t^2)^2}{(1+t^2)^2})$$

for the universal elliptic curve over $X(4) \cong \mathbb{P}^1$. The *Shioda modular surface* of level 4 is the minimal fibred surface $S(4) \to X(4)$ with generic fibre E_t. The *theta modular surface* of level 4 is the minimal fibred surface $T(4) \to X(4)$ with generic fibre

$$D_t\colon \quad \left\{ \begin{array}{l} t(x_0^2 + x_2^2) + 2x_1x_3 = 0 \\ t(x_1^2 + x_3^2) + 2x_0x_2 = 0 \end{array} \right\} \subset \mathbb{P}^3.$$

The relation between the fibres is that D_t has Jacobian E_t.

We refer to [1] for many interesting facts about the geometry of the surfaces $S(4)$ and $T(4)$. For example, they are both K3-surfaces (in fact Kummer surfaces) with Picard number 20. Working over $\mathbb{C}$, the surface $T(4)$ is isomorphic to the diagonal quartic surface in $\mathbb{P}^3$. Moreover the surfaces $S(4)$ and $T(4)$ are related by generically 2-to-1 rational maps (in either direction) but are not birational.

1.1. **Outline of the article.** In Section 2 we review some of the interpretations of $H^1(k, E[n])$, most notably in terms of n-covers and theta groups. We also define the (twisted) Shioda and theta modular surfaces.

In Section 3 we look at methods for computing 4-covers of elliptic curves. A central notion is that of a *second 2-cover*: any 4-cover $D \to E$ factors through a 2-cover $C \to E$. The cover $D \to C$ is referred to as a *second 2-cover*. In terms of Galois cohomology this corresponds to the sequence

$$H^1(k, E[2]) \to H^1(k, E[4]) \to H^1(k, E[2]),$$

where the first $H^1(k, E[2])$ classifies the cover $D \to C$ and the second $H^1(k, E[2])$ classifies $C \to E$.

In Section 3.1 we review classical 4-descent. It has the drawback for us that it only gives those 4-covers with a degree 4 model in $\mathbb{P}^3$. In Section 3.2 we describe a variant of this method. In particular, given $D \to C \to E$ where D has a degree 4 model in $\mathbb{P}^3$, we show how to twist the second 2-cover $D \to C$ by an arbitrary element of $H^1(k, E[2])$. The new 4-cover has a degree 8 model in $\mathbb{P}^7$. However, for our purposes, it is convenient to project this to a curve in $\mathbb{P}^5$, still of degree 8.

In Section 4 we quantify the difference between $S^{\pm}_{E,\xi}(n)$ and $T^{\pm}_{E,\xi}(n)$ for arbitrary n. Indeed the fibres differ by a cohomology class $\nu = \nu(t)$, which we call the *shift*. It was already shown in [8, Lemma 3.11] that the shift is trivial when n is odd. We show that when n is even the shift takes values in $H^1(k, E[2])$.

Section 5 reviews the geometry of the surfaces $S(4)$ and $T(4)$. In Section 6 we describe how to compute the twists of these surfaces so that a prescribed 4-cover $D \to E$ appears as a fibre. We assume that D is given as a quadric intersection in $\mathbb{P}^3$. We use the invariant theory in [12] to write down the required twist of $T(4)$. By finding an explicit formula for the shift, and then using the method in Section 3.2, we are then able to compute the required twist of $S(4)$.

The methods in Section 6 for computing $S^{+}_{E,\xi}(4)$ and $T^{+}_{E,\xi}(4)$ are modified in Section 7 to compute $S^{-}_{E,\xi}(4)$ and $T^{-}_{E,\xi}(4)$. The arguments here are somewhat simplified by the observation that an elliptic curve and its quadratic twist by its discriminant are reverse 4-congruent.

In Section 9 we give several examples. We exhibit some elliptic curves $E/\mathbb{Q}$ such that for the elements $\xi \in H^1(\mathbb{Q}, E[4])$ representing elements of order 4 in $Ш(E/\mathbb{Q})$, the surface $S^{-}_{E,\xi}(4)$ has no rational points. We show this by computing an explicit model of the surface and checking that the surface has no p-adic points for some prime p. If $E(\mathbb{Q})/2E(\mathbb{Q})$ is trivial, it follows that visibility in a surface can only happen via a rational point on $S^{+}_{E,\xi}(4)$. We prove in Proposition 8.2 that if the Galois action on $E[4]$ is large enough, then the resulting abelian surface does not admit a principal polarization.

We note that if $\xi \in H^1(k, E[4])$ represents an element in $Ш(E/k)$ then $S^{+}_{E,\xi}(4)$ has points everywhere locally. Thus, any failure for $S^{+}_{E,\xi}(4)$ to have rational points constitutes a failure of the Hasse Principle. We plan to investigate this possibility further in future work.

2. Preliminaries

2.1. **Notation.** For a field k, we write k^{sep} for its separable closure. We write t for the generic point on various modular curves we consider. When these curves are isomorphic to $\mathbb{P}^1$, then t will instead denote a co-ordinate on $\mathbb{P}^1$. The identity element on an elliptic curve E will be written as either 0 or 0_E.

2.2. **Geometric interpretations of $H^1(k, E[n])$.** Let k be a field of characteristic not dividing n and let E be an elliptic curve over k.

Definition 2.1. An *n-cover* of E over k is a pair (C, π), where C is a nonsingular complete irreducible curve over k and $\pi\colon C \to E$ is a morphism such that there exists an isomorphism $\psi\colon (C \times_k k^{\mathrm{sep}}) \to (E \times_k k^{\mathrm{sep}})$ satisfying $\pi = [n] \circ \psi$. Two n-covers (C_1, π_1) and (C_2, π_2) are *isomorphic over k* if there is an isomorphism $\alpha : C_1 \to C_2$ over k such that $\pi_1 = \pi_2 \circ \alpha$.

The isomorphism classes of n-covers are naturally parametrized by $H^1(k, E[n])$. This means that given $\xi \in H^1(k, E[n])$ there is an n-cover $C_{E,\xi} \to E$, any n-cover is isomorphic to one of this form, and two n-covers are isomorphic if and only if they arise from the same class ξ. Restriction of cocycle classes corresponds to base extending the cover.

If (C, π) is an n-cover of E then C itself is a twist of E (as a curve, not as an elliptic curve). In fact C has the structure of homogeneous space under E, and so represents an element in $H^1(k, E)$. The map $H^1(k, E[n]) \to H^1(k, E)$ may be interpreted as forgetting the covering map π. In particular its kernel consists of those n-covers (C, π) for which $C(k)$ is non-empty.

Definition 2.2. A *theta group for $E[n]$* is a central extension $0 \to \mathbb{G}_{\mathrm{m}} \to \Theta \to E[n] \to 0$ of k-group schemes such that the commutator pairing on Θ agrees with the Weil-pairing on $E[n]$. An isomorphism of theta groups is an isomorphism of central extensions as k-group schemes.

The lift of the (translation) action of $E[n]$ on the linear system $|n.0_E|$ to the Riemann-Roch space $L(n.0_E)$ gives a theta group Θ_E. If $n \geq 3$ then $L(n.0_E)$ is the space of global sections of a very ample line bundle $\mathcal{L}_{E,n}$. Choosing a basis for this space provides a map $E \to \mathbb{P}^{n-1}$ that gives a model for E as an elliptic normal curve of degree n. The theta group Θ_E is then the full inverse image in GL_n of the group of projective linear transformations describing the action of $E[n]$ on E by translation.

As observed in [8, Sections 1.5 and 1.6], there is an action of $E[n]$ on Θ_E by conjugation, and every automorphism of Θ_E arises in this way. Therefore the isomorphism classes of theta groups for $E[n]$, viewed as twists of Θ_E, are parametrized by $H^1(k, E[n])$.

Since an n-cover $C_{E,\xi}$ (as a curve) is a twist of E by a cocycle taking values in $E[n]$, we see that $C_{E,\xi}$ comes equipped with a degree n line bundle $\mathcal{L}_{E,\xi}$ with a theta group $\Theta_{E,\xi}$ acting on it. It may be checked that $\Theta_{E,\xi}$ is indeed the twist of Θ_E by ξ (in the sense of the last paragraph). The line bundle $\mathcal{L}_{E,\xi}$ provides a model of $C_{E,\xi}$, but now only in an $(n-1)$-dimensional Brauer-Severi variety, i.e. a possibly non-trivial twist of $\mathbb{P}^{n-1}$. The k-isomorphism class of the Brauer-Severi variety gives a class in $\mathrm{Br}(k)[n]$.

Definition 2.3. We write $\mathrm{Ob}_{E,n}\colon H^1(k,E[n]) \to \mathrm{Br}(k)$ for the map that sends $\xi \in H^1(k,E[n])$ to the class of the Brauer-Severi variety corresponding to the global sections of $\mathcal{L}_{E,\xi}$. In particular $\mathrm{Ob}_{E,n}(\xi)$ is trivial if and only if $C_{E,\xi}$ admits a degree n model in $\mathbb{P}^{n-1}$ with $\mathcal{L}_{E,\xi}$ the pull back of $\mathcal{O}(1)$. In later sections we write $\mathrm{Ob}_n(C_{E,\xi}) = \mathrm{Ob}_{E,n}(\xi)$.

It is shown in [8] that $\mathrm{Ob}_{E,n}(\xi)$ is determined by the isomorphism class of $\Theta_{E,\xi}$ (as a theta group for $E[n]$) without reference to E itself.

2.3. **Twists of full level modular curves.** An *n-congruence* between two elliptic curves E, E' over k is an isomorphism of k-group schemes $\sigma\colon E[n] \to E'[n]$. We only concern ourselves with the case that the characteristic of k does not divide n. The torsion subgroup scheme $E[n]$ of an elliptic curve comes equipped with a Weil pairing

$$e_n\colon E[n] \times E[n] \to \mu_n.$$

When classifying n-congruences one should take into account what happens to the Weil pairing. The following proposition is trivial to prove and shows that $\mathrm{Aut}(\mu_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ classifies the possible types of n-congruences.

Proposition 2.4. *Let $\sigma\colon E[n] \to E'[n]$ be an n-congruence. Then there exists $\tau_\sigma \in \mathrm{Aut}(\mu_n)$ such that*

$$e_n \circ (\sigma \times \sigma) = \tau_\sigma \circ e_n.$$

We say that σ is a direct *n-congruence if τ_σ is the identity and that σ is a* reverse *n-congruence if τ_σ is inversion.*

In our case, for $n = 4$, any n-congruence is either direct or reverse.

Fixing an elliptic curve E, we consider the moduli space $Y_E^+(n)(k)$ of pairs (E', σ), where $\sigma\colon E[n] \to E'[n]$ is a direct n-congruence. This moduli space is represented by a curve $Y_E^+(n)$ over k, whose non-singular completion $X_E^+(n)$ is a twist of the modular curve $X(n)$ of full level n. Similarly, we write $X_E^-(n)$ for the twist of $X(n)$ corresponding to the moduli space of pairs (E', σ) where $\sigma\colon E[n] \to E'[n]$ is a reverse n-congruence.

If σ is a direct or reverse n-congruence, then the automorphism τ_σ from Proposition 2.4 can be extended to an automorphism $\mathbb{G}_\mathrm{m} \to \mathbb{G}_\mathrm{m}$. In this case, we see that σ provides a way of comparing theta groups.

Definition 2.5. Let $\sigma\colon E[n] \to E'[n]$ be a direct or reverse n-congruence. Given theta groups Θ, Θ' for $E[n]$ and $E'[n]$, we say a morphism $\psi\colon \Theta \to \Theta'$ (as k-group schemes) is a σ-isomorphism if it makes the diagram below commutative.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{G}_\mathrm{m} & \longrightarrow & \Theta & \longrightarrow & E[n] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tau_\sigma} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \sigma} & & \\
0 & \longrightarrow & \mathbb{G}_\mathrm{m} & \longrightarrow & \Theta' & \longrightarrow & E'[n] & \longrightarrow & 0
\end{array}$$

If σ is a direct n-congruence, this is the normal notion of isomorphism for theta groups upon identifying $E[n]$ and $E'[n]$ via σ.

2.4. **Shioda modular surfaces.** For $n \geq 3$, the moduli space $Y_E^+(n)$ is *fine*, so there is a universal elliptic curve E_t with a direct n-congruence $\sigma_t \colon E[n] \to E_t[n]$ over $Y_E^+(n)$. The relevant property for us is that any direct n-congruence between E and another elliptic curve can be obtained by specializing t at the relevant moduli point on $Y_E^+(n)$. We write $S_E^+(n) \to X_E^+(n)$ for the minimal fibred surface with generic fibre E_t. This is a twist of Shioda's modular surface of full level n.

Given $\xi \in H^1(k, E[n])$, we can twist this surface further. Writing k_t for the function field of $X_E^+(n)$, we view ξ as an element of $H^1(k_t, E_t[n])$ and take the n-cover $C_{t,\xi} \to E_t$ representing it. Let $S_{E,\xi}^+(n) \to X_E^+(n)$ be the minimal fibred surface with generic fibre $C_{t,\xi}$. This is again a twist of Shioda's modular surface, and is isomorphic to $S_E^+(n)$ over the splitting field of ξ. In [16], the surfaces $S_E^+(n)$ and $S_{E,\xi}^+(n)$ are called *first* and *second* twists.

We define $S_{E,\xi}^-(n)$ similarly, by using a universal reverse n-congruence σ_t.

2.5. **Theta modular surfaces.** Alternatively, given an elliptic curve E over k and $\xi \in H^1(k, E[n])$, we base extend $\Theta_{E,\xi}$ to a theta group over k_t, the function field of $X_E^+(n)$. Then $\Theta_{E,\xi} \times_k k_t = \Theta_{E_t,\xi_t}$ for some $\xi_t \in H^1(k_t, E_t[n])$. Just as in Section 2.4, we take the n-cover $C_{t,\xi_t} \to E_t$ representing ξ_t. Then we define the *theta modular surface* to be the minimal fibred surface $T_{E,\xi}^+(n) \to X_E^+(n)$ with generic fibre C_{t,ξ_t}.

By construction, the fibers of $T_{E,\xi}^+(n) \to X_E^+(n)$ are n-covers with a prescribed theta group. Since $\mathrm{Ob}_{E,n}(\xi)$ is a function of $\Theta_{E,\xi}$, we see that $\mathrm{Ob}_{E_t,n}(\xi_t)$ is the base change of $\mathrm{Ob}_{E,n}(\xi)$ to k_t. In particular, if $\mathrm{Ob}_{E,n}(\xi) = 0$ then C_{t,ξ_t} admits a degree n model in $\mathbb{P}^{n-1}$, with a linear action of $E_t[n]$. In that case, it follows that $T_{E,\xi}^+(n)$ is birational to a surface in $\mathbb{P}^{n-1}$, with an action of $E[n]$ through $\Theta_{E,\xi}$. This allows us to use invariant theory to write down models of $T_{E,\xi}^+(n)$.

Interestingly enough, $\nu(t) = \xi_t - \xi$ is not necessarily trivial. In fact, Theorem 4.1 proves that $\nu(t)$ is 2-torsion (as is seen by applying the result to the elliptic curves $E \times_k k_t$ and E_t). In particular, if n is odd then $\nu(t) = 0$ and the surfaces $S_{E,\xi}^+(n)$ and $T_{E,\xi}^+(n)$ are isomorphic.

We define $T_{E,\xi}^-(n)$ similarly, by reversing the order of multiplication on $\Theta_{E,\xi}$. Since $(\mathbb{Z}/4\mathbb{Z})^\times = \{\pm 1\}$, this is sufficient to define $T_{E,\xi}(4)$.

3. Computing 4-covers

Let E be an elliptic curve and let $\xi \in H^1(k, E[4])$. In this section, we write $D_{E,\xi}$ for the corresponding 4-cover of E. We have $2\xi \in H^1(k, E[2])$ and write $C_{E,2\xi}$ for the corresponding 2-cover of E. Note that the 4-cover $D_{E,\xi} \to E$ naturally factors as $D_{E,\xi} \to C_{E,2\xi} \to E$. It turns out to be advantageous to study 4-covers via this intermediate structure.

Definition 3.1. Let $C \to E$ be a 2-cover. A 2-cover of C is a cover $D \to C$ such that the composition of covers $D \to C \to E$ is a 4-cover. If we want to emphasize that D is a 2-cover of a 2-cover, and not of an elliptic curve directly, we say that $D \to C$ is a *second* 2-cover.

In this section we are concerned with finding models of second 2-covers. We fix a 2-cover $C \to E$ over a field k with $\operatorname{char} k \neq 2, 3$. We assume $\mathrm{Ob}_{E,2}(C) = 0$, so that C has a model

$$C\colon \quad Y^2 = G(X, Z), \tag{1}$$

where G is a binary quartic form, say

$$G(X, Z) = aX^4 + bX^3Z + cX^2Z^2 + dXZ^3 + eZ^4.$$

The classical invariants of G are

$$\begin{aligned} I &= 12ae - 3bd + c^2, \\ J &= 72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3. \end{aligned} \tag{2}$$

As observed by Weil, a model for E is given by

$$E\colon \quad y^2 = x^3 + Ax + B \text{ where } A = -I/48 \text{ and } B = -J/1728. \tag{3}$$

In the next two sections we assume for simplicity that $ae \neq 0$.

3.1. **Models of 2- and 4-covers with trivial obstruction.** In this section we review classical 4-descent, as described in [11, 17, 20, 21] and implemented in Magma [2].

If $D \to C$ is a second 2-cover such that $\mathrm{Ob}_4(D) = 0$ then D admits a degree 4 model in $\mathbb{P}^3$, say

$$D\colon \quad Q_1 = Q_2 = 0,$$

where $Q_1, Q_2 \in k[\mathbf{x}] = k[x_1, x_2, x_3, x_4]$ are quadratic forms. Conversely, any such smooth quadric intersection is a 4-cover of an elliptic curve.

Let A_i be the symmetric matrix such that $Q_i(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T A_i \mathbf{x}$. Then the intermediate 2-cover has a model (1) in weighted projective space, with $G(X, Z) = \det(XA_1 + ZA_2)$. In particular $\mathrm{Ob}_2(C) = 0$. Let $T_1, T_2 \in k[\mathbf{x}]$ be the quadratic forms given by $T_i(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T B_i \mathbf{x}$ where

$$\operatorname{adj}((\operatorname{adj} A_1)X + (\operatorname{adj} A_2)Z) = a^2A_1X^3 + aB_1X^2Z - eB_2XZ^2 + e^2A_2Z^3.$$

Then the covering map $D \to C$ is given by $(X : Z : Y) = (T_1 : T_2 : J)$ where

$$J = (1/4)\frac{\partial(Q_1, Q_2, T_1, T_2)}{\partial(x_1, x_2, x_3, x_4)}.$$

Let $F = k[\theta]$ be the étale algebra over k generated by a root θ of $g(x) = G(x, 1)$. A generic calculation shows that the quadratic form

$$\Xi = \theta^{-1}eQ_1 + T_1 - \theta T_2 + \theta^2 aQ_2 \tag{4}$$

in $F[\mathbf{x}]$ has rank 1 and satisfies $aN_{F/k}(\Xi) = J^2$. Specialising at any sufficiently general $\mathbf{x} \in k^4$ shows that there exist $\alpha \in F^\times$ and $r \in k^\times$ with $N_{F/k}(\alpha) = ar^2$. Moreover the class of α in $F^\times/F^{\times 2}k^\times$ only depends on the isomorphism class of the 2-cover $D \to C$.

Conversely, given a 2-cover C of the form (1), we can construct its 2-covers D with $\mathrm{Ob}_4(D) = 0$ in the following way. Let $F = k[\theta]$ as above, and suppose that $\alpha \in F^\times$ and $r \in k^\times$ satisfy $N_{F/k}(\alpha) = ar^2$. We consider the equation

$$\alpha(X - \theta Z) = (x_1 + x_2\theta + x_3\theta^2 + x_4\theta^3)^2. \tag{5}$$

Expanding in powers of θ gives 4 equations of the form

$$(\text{linear form in } X \text{ and } Z) = (\text{quadratic form in } x_1, \dots, x_4).$$

Taking the norm $N_{F/k}$ and then extracting a square root gives, upon choosing the sign of r, a further equation

$$rY = N_{F/k}(x_1 + x_2\theta + x_3\theta^2 + x_4\theta^3).$$

Taking linear combinations of these equations gives expressions for X, Y, Z in terms of $x_1, \dots, x_4$, and two further quadratic equations in $x_1, \dots, x_4$ only. These define a 2-cover $D_\alpha \to C$. Moreover the isomorphism class of this 2-cover only depends on the class of α in $F^\times/F^{\times 2}k^\times$.

The two constructions just presented are inverse to one another. We thus obtain the following proposition. In stating it we use our freedom to multiply $G(X, Z)$ by a square to reduce to the case $r = 1$.

Proposition 3.2. *Let $C \to E$ be a 2-cover. If there is a second 2-cover $D \to C$ with $\mathrm{Ob}_4(D) = 0$ then C has a model of the form $Y^2 = N_{F/k}(\alpha(X - \theta Z))$. Moreover if C takes this form then the collection of all 2-covers D of C with $\mathrm{Ob}_4(D) = 0$ is given by*

$$\ker(N_{F/k} \colon F^\times/F^{\times 2}k^\times \to k^\times/k^{\times 2}) \tag{6}$$

via the map $\delta \mapsto D_{\alpha\delta}$.

Remark 3.3. (i) Strictly speaking we should specify a choice of square root of $N_{F/k}(\delta)$, otherwise the 2-covers $D_{E,\xi}$ and $D_{E,-\xi}$ of $C_{E,2\xi}$, differing by the automorphism $Y \mapsto -Y$ of $C_{E,2\xi}$, cannot be distinguished.
(ii) Let $g'(x)$ be the derivative of $g(x) = G(x, 1)$. It is sometimes convenient to write the equations for D_α as

$$\mathrm{tr}_{F/k}\left(\frac{x^2}{\alpha g'(\theta)}\right) = \mathrm{tr}_{F/k}\left(\frac{\theta x^2}{\alpha g'(\theta)}\right) = 0, \tag{7}$$

where $x = x_1 + x_2\theta + x_3\theta^2 + x_4\theta^3$.
(iii) The group (6) may be identified with a certain subgroup of $H^1(k, E[2])/\langle 2\xi \rangle$ where 2ξ is the class of the 2-cover $C \to E$. See [11] for further details.

3.2. **Models for twists of second 2-covers.** Let $D \to C$ be a second 2-cover with $\mathrm{Ob}_4(D) = 0$. By Proposition 3.2 we may assume that C has a model

$$C: \quad Y^2 = G(X,Z) = N_{F/k}(\alpha(X - \theta Z)), \tag{8}$$

and that $D = D_\alpha$. In this section we are interested in models for *any* 2-cover of C; not just the ones with trivial obstruction (as a 4-cover). These covers are parametrized by $H^1(k, E[2])$.

We recall that C is a 2-cover of the elliptic curve $E\colon y^2 = f(x) = x^3 + Ax + B$ given by (3). Let $L = k[\varphi]$ be the étale algebra over k generated by a root φ of $f(x)$. It is well known that

$$H^1(k, E[2]) \cong \ker(N_{L/k}\colon L^\times/L^{\times 2} \to k^\times/k^{\times 2}). \tag{9}$$

In fact this is the special case of Remark 3.3(iii) with $C = E$.

The algebra L is related to F in the following way. We have that $g(x) = (x - \theta)h(x)$, for some cubic $h(x) \in F[x]$. Then $F[x]/(h(x)) = L \otimes_k F$, which we denote by LF. As an algebra over k, it is obtained by formally adjoining two roots, say θ and $\tilde\theta$, of $g(x)$. Let $\sigma \in \mathrm{Aut}_k(LF)$ be the involution that swaps θ and $\tilde\theta$. We write M for the subalgebra of LF fixed by σ. This is the étale algebra of unordered pairs of roots of $g(x)$ and it has degree $[M : k] = 6$. We may identify L as a subalgebra of M via

$$\varphi = -(a\theta\tilde\theta - c/3 + e/(\theta\tilde\theta))/4. \tag{10}$$

We fix a basis $m_1, \ldots, m_6$ for M over k, and put $\tilde\alpha = \sigma(\alpha)$. Let $\nu \in L^\times$ with $N_{L/k}(\nu) = s^2$ for some $s \in k^\times$. We show how to construct a twist $\mathcal{D}_\nu \to C$ of $D \to C$. This will turn out to be the twist by the element of $H^1(k, E[2])$ corresponding to ν under the isomorphism (9).

We consider the equation

$$N_{LF/M}(\alpha(X - \theta Z)) = \alpha\tilde\alpha(X - \theta Z)(X - \tilde\theta Z) = \nu(y_1 m_1 + \ldots + y_6 m_6)^2. \tag{11}$$

Expanding and taking coefficients of $m_1, \ldots, m_6$ gives 6 equations of the form

$$(\text{quadratic form in } X \text{ and } Z) = (\text{quadratic form in } y_1, \ldots, y_6).$$

Taking the norm $N_{M/L}$ and then extracting a square root gives

$$Y = \nu\, N_{M/L}(y_1 m_1 + \ldots + y_6 m_6) \tag{12}$$

and hence 3 equations of the form

$$(\text{linear form in } Y) = (\text{quadratic form in } y_1, \ldots, y_6).$$

Taking linear combinations to eliminate X^2, XZ, Z^2 and Y leaves 5 quadratic forms in $y_1, \ldots, y_6$. These define $\mathcal{D}_\nu \subset \mathbb{P}^5$, a genus 1 curve of degree 8. In fact $\mathcal{D}_\nu$ is a 2-cover of C. Equations for the covering map $\mathcal{D}_\nu \to C$ may be computed

as follows. Again starting from (11), we take the norm $N_{LF/F}$ and then extract a square root to give

$$\pm\alpha(X-\theta Z)Y = s\, N_{LF/F}(y_1m_1+\ldots+y_6m_6).$$

The sign choice here may be absorbed into the cubic norm. Using (12) to eliminate Y and then cancelling the common factor $y_1m_1+\ldots+y_6m_6$ gives 12 equations of the form

$$(\text{bilinear form in } X, Z \text{ and } y_1,\ldots,y_6) = (\text{quadratic form in } y_1,\ldots,y_6).$$

These equations together with (12) define the covering map $\mathcal{D}_\nu \to C$.

Remark 3.4. (i) If we just eliminate Y from the $6+3+12$ equations listed above, then we get 20 quadrics in $X, Z, y_1, \ldots, y_6$. These define a genus 1 curve embedded in $\mathbb{P}^7$ via a complete linear system of degree 8. However we will see that working with $\mathcal{D}_\nu \subset \mathbb{P}^5$ has some advantages.
(ii) Taking $\nu = 1$ gives a 2-cover $\mathcal{D}_1 \to E$ that is isomorphic to $D \to C$. Indeed on comparing (5) and (11) we see that an isomorphism is given by

$$y_1m_1+\cdots+y_6m_6 = (x_1+x_2\theta+x_3\theta^2+x_4\theta^3)(x_1+x_2\tilde{\theta}+x_3\tilde{\theta}^2+x_4\tilde{\theta}^3).$$

In fact the y_i span the same space as the 2×2 minors of the 2×4 matrix of partial derivatives of the quadratic forms defining D.
(iii) A generic calculation shows that $\mathcal{D}_\nu \subset \mathbb{P}^5$ has degree 8 and its homogeneous ideal is (minimally) generated by 5 quadrics and 2 cubics. However the 5 quadrics are sufficient to define the curve set-theoretically.
(iv) Let $z \in L^\times$ correspond under the isomorphism (9) to the class of $C \to E$. By [7, Equation (3.1)] we have $z \in M^{\times 2}$, and so z is a Kummer generator for the quadratic extension M/L. Absorbing z into the squared factor on the right of (11) we see that $\mathcal{D}_\nu$ and $\mathcal{D}_{\nu z}$ are isomorphic as curves. However as 2-covers of C they differ by the automorphism $Y \mapsto -Y$.

We prove an analogue of Proposition 3.2.

Proposition 3.5. *Let C be the 2-cover (8). Then the collection of all 2-covers of C is given by $\ker(N_{L/k}\colon L^\times/L^{\times 2} \to k^\times/k^{\times 2})$ via the map $\nu \mapsto \mathcal{D}_\nu$.*

Proof: Let $\eta \in H^1(k, E[2])$ map to the class of $\nu \in L^\times$ under the isomorphism (9). To prove the proposition, we show that $\mathcal{D}_\nu \to C$ is the twist of $\mathcal{D}_1 \to C$ by η.

Let $\overline{L} = L \otimes_k k^{\text{sep}}$. Note that L is the co-ordinate ring of $E[2]\setminus\{0_E\}$, so $\overline{L} = \text{Map}(E[2](k^{\text{sep}})\setminus\{0_E\}, k^{\text{sep}})$. There is a homomorphism of Galois modules

$$\begin{aligned} w : E[2] &\to \mu_2(\overline{L}) \\ S &\mapsto (T \mapsto e_2(S,T)). \end{aligned}$$

Noting that M is an L-algebra and a 6-dimensional k-vector space, we see that $L^\times$ acts linearly on $\mathbb{P}(M) = \mathbb{P}^5$. In particular $S \in E[2]$ acts on $\mathbb{P}^5$ via $w(S)$ and this action restricts to $\mathcal{D}_1$.

If $g(x)$ has roots $\theta_1, \ldots, \theta_4$ then $k^{\mathrm{sep}}(\mathcal{D}_1) = k^{\mathrm{sep}}(C)(\sqrt{f_{12}}, \sqrt{f_{13}})$ where $f_{ij} = (X - \theta_i Z)(X - \theta_j Z)/Z^2$. Since $\mathcal{D}_1$ is a homogeneous space under E, there is an action of $E[2]$ on $\mathcal{D}_1$. This is given by $\sqrt{f_{12}} \to \pm\sqrt{f_{12}}$ and $\sqrt{f_{13}} \to \pm\sqrt{f_{13}}$. It follows from the definition of the Weil pairing that this action agrees with the one defined in the last paragraph.

Let η be represented by the cocycle $\sigma \mapsto \eta_\sigma$. Then we have $w(\eta_\sigma) = \sigma(\gamma)\gamma^{-1}$ and $\nu = \gamma^2$ for some $\gamma \in \overline{L}$. There is a commutative diagram

$$\begin{array}{ccc} \mathcal{D}_\nu & \xrightarrow{\cdot\gamma} & \mathcal{D}_1 \\ \downarrow & & \downarrow \\ C & = & C \end{array}$$

Therefore $\mathcal{D}_\nu \to C$ is the twist of $\mathcal{D}_1 \to C$ via the cocycle $\sigma \mapsto \sigma(\gamma)\gamma^{-1}$, and this completes the proof. □

4. Theta groups and the shift

In this section we prove the following theorem. We work over a field k of characteristic not dividing n.

Theorem 4.1. *Let E, E' be elliptic curves over k with a direct or a reverse n-congruence $\sigma\colon E'[n] \to E[n]$. Then there exists $\nu \in H^1(k, E[n])$, depending only on E, E', σ, such that for any $\xi \in H^1(k, E[n])$ and $\xi' \in H^1(k, E'[n])$ we have*

(i) $2\nu = 0$ *(in particular, if n is odd then $\nu = 0$).*
(ii) $\xi = \sigma_*(\xi') + \nu$ *if and only if $\Theta_{E,\xi}$ and $\Theta_{E',\xi'}$ are σ-isomorphic.*

Proof: We start by comparing the trivial theta groups $\Theta_E, \Theta_{E'} \subset \mathrm{GL}_n$. There is an isomorphism ψ defined over k^{sep} making the following diagram commute

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_{\mathrm{m}} & \longrightarrow & \Theta_{E'} & \longrightarrow & E'[n] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tau_\sigma} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \sigma} & & \\ 0 & \longrightarrow & \mathbb{G}_{\mathrm{m}} & \longrightarrow & \Theta_E & \longrightarrow & E[n] & \longrightarrow & 0. \end{array} \tag{13}$$

Then $\Theta_{E'}$ is the twist of Θ_E by the cocycle $\rho \mapsto \rho(\psi)\psi^{-1}$. This cocycle takes values in $\mathrm{Aut}(\Theta_E) \cong \mathrm{Hom}(E[n], \mathbb{G}_{\mathrm{m}}) \cong E[n]$, and so gives a class $\nu \in H^1(k, E[n])$. If n is odd then $\nu = 0$ by [8, Lemma 3.11]. We now adapt the argument to the case where n is even.

The automorphism $[-1]$ of E lifts to $\iota \in \mathrm{GL}_n(k)$. For each $T \in E[n](k^{\mathrm{sep}})$ we pick a matrix $M_T \in \Theta_E(k^{\mathrm{sep}})$, representing translation by T, such that

$$\iota M_T \iota^{-1} = M_T^{-1}. \tag{14}$$

This condition determines the scaling of M_T up to a choice of sign. If $M_{S+T} = \lambda M_S M_T$ then conjugating by ι shows that $\lambda^2 = e_n(S,T)$ and so

$$M_{S+T} = \pm e_n(S,T)^{1/2} M_S M_T \quad \text{for all } S,T \in E[n](k^{\mathrm{sep}}). \tag{15}$$

We claim that $M_T^n = 1$. Indeed for a suitable choice of co-ordinates $x_0, \dots, x_{n-1}$, defined over k^{sep}, we have $M_T : x_i \mapsto \alpha\zeta^i x_i$ and $\iota : x_i \mapsto \beta x_{n-i}$ for some $\alpha, \beta \in k^{\mathrm{sep}}$ and $\zeta \in \mu_n$. By (14) we have $\alpha^2 = 1$. Since n is even it follows that $M_T^n = 1$. This proves the claim.

In exactly the same manner we pick $M'_T \in \Theta_{E'}(k^{\mathrm{sep}})$ for all $T \in E'[n](k^{\mathrm{sep}})$. We can then choose ψ so that $\psi(M'_T) = \pm M_{\sigma(T)}$ for all $T \in E'[n](k^{\mathrm{sep}})$. Indeed if we make this true on a basis for $E'[n]$, then the rest follows by (15) and its analogue for E'.

Let $\rho \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Since ι is defined over k, it follows from (14) that

$$\rho(M_T) = \pm M_{\rho(T)} \quad \text{for all } T \in E[n](k^{\mathrm{sep}}).$$

Likewise

$$\rho(M'_T) = \pm M'_{\rho(T)} \quad \text{for all } T \in E'[n](k^{\mathrm{sep}}).$$

The cocycle $\rho \mapsto \rho(\psi)\psi^{-1}$ now takes values in $\mathrm{Hom}(E[n], \mu_2) = E[2]$. Therefore ν is in the image of the natural map $H^1(k, E[2]) \to H^1(k, E[n])$, and this proves (i).

It also follows that $\Theta_{E'}$ is σ-isomorphic to $\Theta_{E,\nu}$. For the general statement, we choose a k^{sep}-isomorphism $\psi' \colon \Theta_{E',\xi'} \to \Theta_{E'}$. Then the cocycle $\rho \mapsto \rho(\psi\psi')(\psi\psi')^{-1}$ represents the class $\sigma_*(\xi') + \nu$. It follows that $\Theta_{E',\xi'}$ is σ-isomorphic to $\Theta_{E,\sigma_*(\xi')+\nu}$. Since, as we noted in Section 2.2, the twists of Θ_E are parametrized by $H^1(k, E[n])$, this proves (ii). □

5. Geometry of the Shioda and theta modular surfaces

In this section we give two particular models of the Shioda and theta modular surfaces of level 4. Any other Shioda or theta modular surface of level 4 will be a twist of one of these, so these particular models are convenient for studying the geometry of these surfaces. For the remainder of the paper, we revert to our assumption that $\mathrm{char}\, k \neq 2, 3$.

5.1. The universal elliptic curve of level 4.

The Legendre form

$$y^2 = x(x-1)(x-\lambda)$$

provides a family of elliptic curves E_λ with a prescribed isomorphism $(\mathbb{Z}/2\mathbb{Z} \times \mu_2) \to E_\lambda[2]$. The parameter λ gives an isomorphism $Y(2) \simeq \mathbb{P}^1 \setminus \{0, 1, \infty\}$. Setting $\lambda = (1-t^2)^2/(1+t^2)^2$ we obtain a family of elliptic curves E_t with a prescribed isomorphism $(\mathbb{Z}/4\mathbb{Z} \times \mu_4) \to E_t[4]$. The parameter t gives an isomorphism $Y(4) \simeq \mathbb{P}^1 \setminus \{0, \infty, \pm 1, \pm i\}$ and the expression for λ in terms of t is an explicit realisation of the map $Y(4) \to Y(2)$.

5.2. **The theta modular surface of level** 4. The quadric intersection

$$D_t\colon \quad \left\{\begin{array}{l} t(x_0^2+x_2^2)+2x_1x_3=0 \\ t(x_1^2+x_3^2)+2x_0x_2=0 \end{array}\right\} \subset \mathbb{P}^3 \tag{16}$$

is a 4-cover of E_t. By varying t these curves give a genus 1 fibration on the surface

$$x_0x_2(x_0^2+x_2^2)-x_1x_3(x_1^2+x_3^2)=0. \tag{17}$$

The action of $E_t[4]$ on D_t is generated by the transformations $x_\nu \mapsto x_{\nu+1}$ and $x_\nu \mapsto i^\nu x_\nu$, where we read the subscripts mod 4. (One convenient way to check an automorphism of a genus 1 curve is geometrically a translation map, is to check it has no fixed points.) The quadric intersections D_t therefore all have the same theta group, and so (17) is a model for the theta modular surface $T(4)$.

The surface $T(4)$ is isomorphic to the Fermat quartic $\{u_0^4-u_1^4+u_2^4-u_3^4=0\} \subset \mathbb{P}^3$ via the change of co-ordinates

$$(u_0:u_1:u_2:u_3)=(x_0+x_2:x_0-x_2:x_1-x_3:x_1+x_3).$$

5.3. **Shioda's modular surface of level** 4. The relative elliptic curve $E_t/Y(4)$ provides us with an open part of the Shioda modular surface. In order to find a suitable completion, we construct E_t as a (trivial) 4-cover of itself. The intermediate 2-cover is

$$C_t\colon \quad Y^2=XZ(X-Z)(X-\lambda Z) \quad \text{with } \lambda=\frac{(1-t^2)^2}{(1+t^2)^2}. \tag{18}$$

A small adaptation (needed since here $a=e=0$) of the construction in Section 3.2 leads to the second 2-cover given by

$$\begin{array}{rr} (X-Z)(X-\lambda Z)=y_1^2 & (1-\lambda)XZ=y_2^2 \\ X(X-\lambda Z)=y_3^2 & \lambda(X-Z)Z=y_4^2 \\ (X-\lambda Z)Z=y_5^2 & X(X-Z)=y_6^2 \end{array} \tag{19}$$

and

$$Y=\frac{1+t^2}{2t}y_1y_2=\frac{1+t^2}{1-t^2}y_3y_4=y_5y_6.$$

Taking linear combinations to eliminate X^2, XZ, Z^2 and Y gives 5 quadrics that define a smooth curve of degree 8 in $\mathbb{P}^5$:

$$\mathcal{D}_t\colon \quad \left\{\begin{array}{r} y_1^2+y_4^2-y_6^2=0 \\ y_2^2-y_3^2+y_6^2=0 \\ y_2^2+y_4^2-y_5^2=0 \\ (1-t^2)y_1y_2-2ty_3y_4=0 \\ (1+t^2)y_1y_2-2ty_5y_6=0 \end{array}\right\} \subset \mathbb{P}^5 \tag{20}$$

The first 3 quadrics in (20) define a surface $S_0 \subset \mathbb{P}^5$ of degree 8 with exactly 16 ordinary double points as singularities (8 defined over $\mathbb{Q}$ and the remaining 8 over $\mathbb{Q}(i)$). Each curve $\mathcal{D}_t$ passes through all 16 singular points. Furthermore, these are the points with $Y = 0$, and so make up the fibre of $\mathcal{D}_t \to E_t$ above 0_{E_t}. In particular, $\mathcal{D}_t$ has a rational point over 0_{E_t}, so $\mathcal{D}_t \to E_t$ is indeed the trivial 4-cover. Blowing up the singular points gives Shioda's modular surface $S(4)$.

The action of $E_t[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mu_2$ on C_t is generated by

$$(X : Z : Y) \mapsto (X - \lambda Z : X - Z : (\lambda - 1)Y),$$
$$(X : Z : Y) \mapsto (\lambda Z : X : -\lambda Y),$$

and the action of $E_t[4] \cong \mathbb{Z}/4\mathbb{Z} \times \mu_4$ on $\mathcal{D}_t$ is generated by

$$\begin{aligned}(y_1 : y_2 : y_3 : y_4 : y_5 : y_6) &\mapsto (-y_2 : y_1 : -y_3 : y_4 : -y_6 : y_5),\\ (y_1 : y_2 : y_3 : y_4 : y_5 : y_6) &\mapsto (iy_1 : -iy_2 : y_4 : y_3 : y_6 : y_5).\end{aligned} \tag{21}$$

The subgroup of $\operatorname{Pic} S(4)$ invariant under the action (21) was computed in [1], and shown to be free of rank 2 generated by divisor classes I and F, where F is the class of a fibre, and $2I$ is linearly equivalent to the sum of the 16 sections (i.e. the blow-ups of the 16 singular points on S_0). Our surface S_0 is the image of $S(4)$ under the morphism to $\mathbb{P}^5$ given by the complete linear system $|I + F|$.

More generally there is a natural action of the affine special linear group $\mathcal{G} = \mathrm{ASL}_2(\mathbb{Z}/4\mathbb{Z})$ on $S(4)$. The corresponding automorphisms of S_0 are again given by changes of co-ordinates on $\mathbb{P}^5$. The surfaces $S^{\pm}_{E,\xi}(4)$ are twists of $S(4)$ by cocycles taking values in $\mathcal{G}$, and so each must admit a model in a 5-dimensional Brauer-Severi variety. Our calculations in Sections 6 and 7 show that if $\mathrm{Ob}_{E,4}(\xi) = 0$ then this Brauer-Severi variety is trivial. Indeed we show how to write down a model for $S^{\pm}_{E,\xi}(4)$ as a complete intersection of quadrics in $\mathbb{P}^5$.

Remark 5.1. Our calculations also give the genus 1 fibration, but in fact this may be recovered directly from the equations for the surface. Indeed, if we take a complement to the 3-dimensional space of quadrics vanishing on the surface, inside the 6-dimensional space of quadrics vanishing at the singular points, then this defines a map to $\mathbb{P}^2$ with image a conic. For example, with S_0 as above, the map is given by $(X_1 : X_2 : X_3) = (y_1y_2 : y_3y_4 : y_5y_6)$ and the conic is $X_1^2 + X_2^2 = X_3^2$. Parametrising this conic gives the required map to $\mathbb{P}^1$.

6. Computing twists of $S(4)$ and $T(4)$ in the direct case

In this section we take $\xi \in H^1(k, E[4])$ with $\mathrm{Ob}_{E,4}(\xi) = 0$ and compute models for $S^{+}_{E,\xi}(4)$ and $T^{+}_{E,\xi}(4)$.

6.1. **The twisted universal elliptic curve of level 4.** Let E/k be the elliptic curve $y^2 = f(x) = x^3 + Ax + B$. If $P = (x_P, y_P)$ is a point on E then the

x-co-ordinate of $2P$ is $\gamma(x_P)$ where

$$\gamma(x) = (x^4 - 2Ax^2 - 8Bx + A^2)/(4(x^3 + Ax + B)).$$

The elliptic curves directly n-congruent to E are parametrized by the non-cuspidal points of $X_E^+(n)$. This is a twist of the usual modular curve $X(n)$.

Lemma 6.1. *The elliptic curves directly 4-congruent to E are*

$$E_t: \quad y^2 = -f(t)(x - \gamma(t))(x^3 + Ax + B)$$

with base point $(x, y) = (\gamma(t), 0)$, where t is a co-ordinate on $X_E^+(4) \cong \mathbb{P}^1$, and the original curve E corresponds to $t = \infty$. Moreover the cusps of $X_E^+(4)$ are the roots of $d(t) = 0$ where

$$d(x) = x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2$$

is the 4-division polynomial of E (divided by 2).

Proof: Putting E_t in Weierstrass form, and making a change of co-ordinates on $X_E^+(4)$, gives the family of curves computed by Silverberg. Indeed our parameter t on $X_E^+(4)$ and the parameter t, here denoted by $t_{\text{Silverberg}}$, in [19, Theorem 4.1] are related by

$$t = \frac{-(4A^3 + 27B^2)}{18ABt_{\text{Silverberg}}} - \frac{3B}{2A}.$$

An alternative proof, also treating the cases $j(E) = 0, 1728$, and leading to the lemma as stated here, is given in [3, Proposition 7.2]. See also Remark 6.4(i). □

6.2. **The twisted theta modular surface of level 4.** Let $D = \{Q_1 = Q_2 = 0\} \subset \mathbb{P}^3$ be a quadric intersection with Jacobian E. Then $D = D_{E,\xi}$ for some $\xi \in H^1(k, E[4])$ with $\mathrm{Ob}_{E,4}(\xi) = 0$. We use invariant theory to compute a model for $T_{E,\xi}^+(4)$ as a quartic surface in $\mathbb{P}^3$, together with its genus 1 fibration over $X_E^+(4)$.

We identify the quadratic forms Q_1 and Q_2 with 4×4 symmetric matrices A_1 and A_2 via $Q_i(x_1, \ldots, x_4) = \frac{1}{2}\mathbf{x}^T A_i \mathbf{x}$. We then define $G(X, Z)$ by

$$G(X, Z) = \det(XA_1 + ZA_2) = aX^4 + bX^3Z + cX^2Z^2 + dXZ^3 + eZ^4, \tag{22}$$

so that D is a 2-cover of $C : Y^2 = G(X, Z)$. As in Section 3, we assume $ae \neq 0$ and let $F = k[\theta]$ where θ is a root of $g(x) = G(x, 1)$.

Let $T_1, T_2 \in k[\mathbf{x}]$ be the quadratic forms defined in Section 3.1. The Hessian, as defined in [12], is an $\mathrm{SL}_2 \times \mathrm{SL}_4$-equivariant map from the space of quadric intersections to itself. It is given by

$$(Q_1, Q_2) \mapsto (Q_1', Q_2') = (6T_2 - cQ_1 - 3bQ_2, 6T_1 - cQ_2 - 3dQ_1).$$

Lemma 6.2. *The quadric intersection*

$$D_t\colon \quad \{12tQ_1+Q_1'=12tQ_2+Q_2'=0\}\subset\mathbb{P}^3 \tag{23}$$

has intermediate 2-cover (after cancelling a factor 12^4)

$$C_t\colon \quad Y^2=G_t(X,Z)=aN_{F/k}\big((t+\mu)X-(\theta t+\lambda)Z\big),$$

where

$$\begin{aligned}\lambda&=(6g'(\theta)-\theta g''(\theta))/24=-(c\theta^2+3d\theta+6e)/(12\theta),\\ \mu&=-g''(\theta)/24=-(6a\theta^2+3b\theta+c)/12.\end{aligned} \tag{24}$$

Proof: In principle this may be checked by a generic calculation. To make the calculation practical we consider the case $Q_1=\sum_{i=1}^4\xi_ix_i^2$ and $Q_2=-\sum_{i=1}^4\xi_i\theta_ix_i^2$. Then $g(X)=2^4(\prod_{i=1}^4\xi_i)\prod_{i=1}^4(X-\theta_i)$, and (Q_1,Q_2) has Hessian (Q_1',Q_2') where $Q_1'=12\sum_{i=1}^4\xi_i\mu_ix_i^2$ and $Q_2'=-12\sum_{i=1}^4\xi_i\lambda_ix_i^2$. Computing the intermediate 2-cover, by the method used in (22), gives the equation for C_t as stated. □

Corollary 6.3. *Let $\xi\in H^1(k,E[4])$ with $D_{E,\xi}=\{Q_1=Q_2=0\}\subset\mathbb{P}^3$. Then the surface $T^+_{E,\xi}(4)$ has a model*

$$\{Q_1Q_2'-Q_2Q_1'=0\}\subset\mathbb{P}^3$$

with genus 1 fibration D_t as given in Lemma 6.2.

Let I and J be the invariants (2) of the binary quartic $G(X,Z)$. Then E has Weierstrass equation $y^2=x^3+Ax+B$ where $A=-I/48$ and $B=-J/1728$. Let E_t be the family of elliptic curves directly 4-congruent to E, as given in Lemma 6.1.

Remark 6.4. (i) The genus 1 curves C_t and D_t have Jacobian E_t. As observed in [12], this gives an alternative proof of Lemma 6.1.
(ii) The family of quartics $G_t(X,Z)$ has constant (meaning independent of t) level 2 theta group. It should therefore be possible to write $G_t(X,Z)$ as a linear combination of the binary quartic $G(X,Z)$ and its Hessian

$$\begin{aligned}H(X,Z)=(8ac-3b^2)X^4+(24ad-4bc)X^3Z+(48ae+6bd-4c^2)X^2Z^2\\ +(24be-4cd)XZ^3+(8ce-3d^2)Z^4.\end{aligned}$$

We find that $G_t(X,Z)=(t^3+At+B)\big(4\gamma(t)G(X,Z)+\frac{1}{12}H(X,Z)\big)$.

We can also use Proposition 3.2 to describe the family of 4-covers D_t. Let $\alpha\in F^\times/F^{\times2}k^\times$ such that $D=D_\alpha$. We may compute α from D by evaluating the rank 1 quadratic form (4) at any point $\mathbf{x}\in k^4$ where it is non-zero (in each constituent field of F).

Theorem 6.5. *The family of 2-covers $D_t\to C_t$ such that each 4-cover $D_t\to E_t$ has the same theta group as our original 4-cover $D\to E$, is obtained by the procedure in Section 3.1, starting in place of (5) with*

$$\alpha\big((t+\mu)X-(\theta t+\lambda)Z\big)=(x_1+x_2\theta+x_3\theta^2+x_4\theta^3)^2. \tag{25}$$

PROOF: We show that the family of curves D_t is identical to that considered in Lemma 6.2. In particular, the theta groups are not just constant up to isomorphism, but constant as subschemes of GL_4. The quartic $g_t(x) = G_t(x,1)$ has root $\theta_t = (\theta t + \lambda)/(t+\mu)$. Following (7), the quadric intersection obtained from (25) is

$$\mathrm{tr}_{F/k}\left(\frac{x^2}{\alpha(t+\mu)g_t'(\theta_t)}\right) = \mathrm{tr}_{F/k}\left(\frac{\theta_t x^2}{\alpha(t+\mu)g_t'(\theta_t)}\right) = 0,$$

where $x = x_1 + x_2\theta + x_3\theta^2 + x_4\theta^3$. Since

$$g_t'(\theta_t) = g'(\theta)d(t)/(t+\mu)^2 \tag{26}$$

this may be re-written as

$$\mathrm{tr}_{F/k}\left(\frac{(t+\mu)x^2}{\alpha g'(\theta)}\right) = \mathrm{tr}_{F/k}\left(\frac{(\theta t+\lambda)x^2}{\alpha g'(\theta)}\right) = 0.$$

The formula for the Hessian used in the proof of Lemma 6.2 now shows that the fibre with $t = \infty$ has Hessian the fibre with $t = 0$. The proof is completed by noting that the fibre with $t = \infty$ is our original 4-cover $D = D_\alpha$. □

Remark 6.6. Expanding (25) in powers of θ gives 4 equations of the form

$$(\text{linear form in } X,\ Z,\ tX,\ tZ) = (\text{quadratic form in } x_1, \ldots, x_4).$$

Eliminating X, Z, t, we obtain a single quartic equation in $x_1, \ldots, x_4$, describing the twist of (17) that has D_t as fibres. This provides an alternative way of arriving at the equation for $T^+_{E,\xi}(4)$ in Corollary 6.3.

6.3. **The twisted Shioda modular surface of level 4.** As in Section 3.2, let $L = k[\varphi]$ where φ is a root of $x^3 + Ax + B = 0$, and write σ for the involution of LF swapping θ and $\tilde{\theta}$. We write $\tilde{\lambda} = \sigma(\lambda)$ and $\tilde{\mu} = \sigma(\mu)$. By the construction in Section 3.2, alternative equations for the curves D_t in Theorem 6.5 are given by

$$\alpha\tilde{\alpha}\big((t+\mu)X - (\theta t+\lambda)Z\big)\big((t+\tilde{\mu})X - (\tilde{\theta}t+\tilde{\lambda})Z\big) = (y_1m_1 + \ldots + y_6m_6)^2.$$

We now modify this by introducing a factor $\nu(t)$ representing the shift from Theorem 4.1.

Theorem 6.7. *The family of 2-covers $\mathcal{D}_t \to C_t$ such that each 4-cover $\mathcal{D}_t \to E_t$ has the same fibre above 0 (as an $E[4]$-torsor) as our original 4-cover $D \to E$, is obtained by the procedure in Section 3.2, starting in place of (11) with*

$$\alpha\tilde{\alpha}\big((t+\mu)X - (\theta t+\lambda)Z\big)\big((t+\tilde{\mu})X - (\tilde{\theta}t+\tilde{\lambda})Z\big) = \nu(t)(y_1m_1 + \ldots + y_6m_6)^2 \tag{27}$$

where

$$\nu(t) = \frac{d(t)}{t^2 - 2t\varphi - 2\varphi^2 - A}. \tag{28}$$

PROOF: We first note that

$$N_{L/k}(t^2 - 2t\varphi - 2\varphi^2 - A) = d(t), \tag{29}$$

and so $\nu(t)$ does indeed correspond to an element of $H^1(k, E[2])$ via the isomorphism (9).

In Section 5.3 we exhibited another family of 4-covers $\mathcal{D}_t \to E_t$. This had constant fibre above 0, as could be checked by substituting $(X : Z) = (0 : 1)$, $(1 : 0)$, $(1 : 1)$ or $(\lambda : 1)$ into the equations (19), and observing that in each case the 4 solutions for $(y_1 : \ldots : y_6) \in \mathbb{P}^5(k^{\mathrm{sep}})$ do not depend on λ. The argument here is similar.

A calculation using (2), (3), (10) and (24) shows that

$$(t + \tilde{\mu})(\theta t + \lambda) - (t + \mu)(\tilde{\theta} t + \tilde{\lambda}) = (\theta - \tilde{\theta})(t^2 - 2\varphi t - 2\varphi^2 - A). \tag{30}$$

Let $\tilde{\tilde{\theta}}$ be another root of g. Substituting $X = \tilde{\tilde{\theta}} t + \tilde{\tilde{\lambda}}$ and $Z = t + \tilde{\tilde{\mu}}$ into the left hand side of (27), gives a quartic polynomial in t, which by (29) and (30) is a constant times $\nu(t)$, as defined in (28). Therefore the 16 points on $\mathcal{D}_t$ mapping to the points on C_t with $Y = 0$, are independent of t. This shows that the fibre above 0 is constant (with respect to t) as a k-scheme. In Section 5.3 we saw that the action of $E_t[4]$ on $\mathcal{D}_t$ is given by formulae independent of t. Therefore the fibre above 0 is also constant as an $E[4]$-torsor.

Finally we note that taking $t = \infty$ gives the cover (11) with $\nu = 1$, which by Remark 3.4(ii) is isomorphic to D. Of course, setting $t = \infty$ in (28) does not literally make sense. However after homogenising, and rescaling by a square, we do indeed have $\nu(\infty) = 1$. □

Corollary 6.8. *Suppose that $\xi \in H^1(k, E[4])$ and $D_{E,\xi}$ is given by (5). Then the surface $S^+_{E,\xi}(4)$ has a singular model in $\mathbb{P}^5$ defined by 3 quadrics. These quadrics are obtained from the $[M : k] = 6$ equations in $k(t)[X, Z, y_1, \ldots, y_6]$ coming from (27), by taking linear combinations to eliminate X^2, XZ and Z^2.*

PROOF: The key point is that the 3 quadrics are independent of t. Again the argument is best understood by comparing with the situation in Section 5.3. The same calculation as mentioned in the proof of Theorem 6.7 shows that the linear combinations of the left hand sides in (19) that vanish at $(X : Z) = (0 : 1)$, $(1 : 0)$, $(1 : 1)$ and $(\lambda : 1)$, and therefore vanish identically, do not depend on t. This explains why the first 3 quadrics in (20) do not depend on t. The same idea works here. □

Remark 6.9. In Theorem 6.7 we not only made the fibre above 0 constant as a k-scheme, we made it constant as a subscheme of $\mathbb{P}^5$. For this, and the application to Corollary 6.8, we needed to know $\nu(t)$ mod $L^{\times 2}$, not just mod $L(t)^{\times 2}$.

The genus 1 fibration is given either by using (12) (which gives two further quadratic forms in $y_1, \ldots, y_6$, now depending on t) or by using Remark 5.1.

7. Computing twists of $S(4)$ and $T(4)$ in the reverse case

In this section we take $\xi \in H^1(k, E[4])$ with $\mathrm{Ob}_{E,4}(\xi) = 0$ and compute models for $S^-_{E,\xi}(4)$ and $T^-_{E,\xi}(4)$.

Let E/k be an elliptic curve $y^2 = f(x) = x^3+Ax+B$, and $\Delta = -16(4A^3+27B^2)$ its discriminant. We write E^Δ for the quadratic twist of E by Δ. Likewise if $C \to \mathbb{P}^1$ is a double cover, then we write C^Δ for its quadratic twist (over $\mathbb{P}^1$) by Δ. We may summarise the results of this section by saying that everything carries over from Section 6 with the following changes.

- We replace E_t by E_t^Δ and C_t by C_t^Δ.
- The family D_t is computed using the contravariants instead of the covariants (these were the identity map and the Hessian).
- In Theorem 6.5 we multiply one side of the equation by $g'(\theta)$. This is an element of F whose norm is Δ (up to squares).
- In Theorem 6.7 we multiply one side of the equation by $(\theta - \tilde{\theta})^2\Delta$.

We now go through the changes in detail.

7.1. Reverse twists of the universal elliptic curve.

Let

$$E^\Delta\colon y^2 = \Delta\, f(x)$$

be the quadratic twist of E by Δ. Then by [3, Corollary 7.4], or Remark 7.3 below, there is a reverse 4-congruence $\sigma\colon E[4] \to E^\Delta[4]$. We may thus identify $X^-_E(4) = X^+_{E^\Delta}(4)$. It is immediate from Lemma 6.1 that

$$E_t^\Delta : \quad y^2 = -\Delta\, f(t)\,(x - \gamma(t))(x^3 + Ax + B),$$

with base point $(x, y) = (\gamma(t), 0)$, is the universal elliptic curve over $X^-_E(4)$.

7.2. Reverse twists of the theta modular surface.

Let $\xi \in H^1(k, E[4])$ with $\mathrm{Ob}_{E,4}(\xi) = 0$. Then the 4-cover $D_{E,\xi}$ has a model as a quadric intersection $D \subset \mathbb{P}^3$ with theta group $\Theta = \Theta_{E,\xi} \subset \mathrm{GL}_4$. Let $\Theta^\vee \subset \mathrm{GL}_4$ be the subgroup of matrices inverse transpose to those in Θ. Let $\pi : \Theta^\vee \to E^\Delta[4]$ be the map that makes the following diagram commute (where the superscript $-T$ denotes inverse transpose)

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{G}_{\mathrm{m}} & \longrightarrow & \Theta & \longrightarrow & E[4] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle .^{-1}} & & \downarrow{\scriptstyle .^{-T}} & & \downarrow{\scriptstyle \sigma} & & \\
0 & \longrightarrow & \mathbb{G}_{\mathrm{m}} & \longrightarrow & \Theta^\vee & \xrightarrow{\pi} & E^\Delta[4] & \longrightarrow & 0
\end{array}$$

Since σ reverses the Weil pairing, the second row gives $\Theta^\vee$ the structure of theta group for $E^\Delta[4]$. The diagram then shows that Θ and $\Theta^\vee$ are σ-isomorphic (see Definition 2.5).

We have $\Theta^\vee = \Theta_{E^\Delta,\xi'}$ for some $\xi' \in H^1(k, E^\Delta[4])$. By [8, Theorem 5.2] there is a unique model for the 4-cover $D_{E^\Delta,\xi'}$ as a quadric intersection $D^\vee \subset \mathbb{P}^3$ with

theta group $\Theta^\vee$. The contravariants, introduced in [12], give a way of computing equations for $D^\vee$. The details are as follows.

Let $D = \{Q_1 = Q_2 = 0\} \subset \mathbb{P}^3$, and let A_1 and A_2 be the corresponding symmetric matrices. Let a, b, c, d, e and I, J and A, B be as defined in Section 3. Let $S_0, \dots, S_3$ be the quadratic forms corresponding to the matrices $C_0, \dots, C_3$ defined by

$$\operatorname{adj}(XA_1 + ZA_2) = C_0X^3 + C_1X^2Z + C_2XZ^2 + C_3Z^3.$$

The contravariants are defined by

$$\begin{aligned}
R_1 &= \frac{1}{12}\left(\frac{\partial I}{\partial a}S_0 + \frac{\partial I}{\partial b}S_1 + \frac{\partial I}{\partial c}S_2 + \frac{\partial I}{\partial d}S_3\right),\\
R_2 &= \frac{1}{12}\left(\frac{\partial I}{\partial b}S_0 + \frac{\partial I}{\partial c}S_1 + \frac{\partial I}{\partial d}S_2 + \frac{\partial I}{\partial e}S_3\right),\\
R_1' &= \frac{1}{12^2}\left(\frac{\partial J}{\partial a}S_0 + \frac{\partial J}{\partial b}S_1 + \frac{\partial J}{\partial c}S_2 + \frac{\partial J}{\partial d}S_3\right),\\
R_2' &= \frac{1}{12^2}\left(\frac{\partial J}{\partial b}S_0 + \frac{\partial J}{\partial c}S_1 + \frac{\partial J}{\partial d}S_2 + \frac{\partial J}{\partial e}S_3\right).
\end{aligned}$$

The quadric intersection $D^\vee$ then has equations

$$D^\vee\colon \quad \{-9BR_2 + 2AR_2' = 9BR_1 - 2AR_1' = 0\} \subset \mathbb{P}^3. \tag{31}$$

Indeed the invariant theory shows that $\Theta^\vee$ acts on $D^\vee$, and that $D^\vee$ has Jacobian E^Δ. Strictly speaking, to show that $D^\vee$ has theta group $\Theta^\vee$, we need that the two actions of $E^\Delta[4]$ on $D^\vee$ (one arising from the identification $\Theta^\vee/\mathbb{G}_{\mathrm{m}} = E^\Delta[4]$ and the other from the structure of $D^\vee$ as a homogeneous space) agree. Since they agree up to an automorphism of $E^\Delta[4]$ that respects the Weil pairing, the desired agreement may be achieved by adjusting our choice of σ.

Remark 7.1. It is convenient to fix our choice of σ once and for all. Following the proof of [3, Corollary 7.4] we let σ correspond to the non-trivial element in the centre of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})/\{\pm 1\}$, represented by the matrices

$$\pm\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}.$$

One way of seeing that this σ and the one from the previous paragraph agree (up to sign) is by observing that both are defined for the elliptic curve $E\colon x^3 + a_2x^2 + a_4x + a_6$ over $k(a_2, a_4, a_6)$, which is a sufficiently general elliptic curve not to admit other σ. But then any elliptic curve over k can be obtained by specializing this E, and σ specializes with it.

The following lemma follows from (31) by direct calculation.

Lemma 7.2. *If $D \subset \mathbb{P}^3$ has intermediate 2-cover $C\colon Y^2 = G(X,Z)$ then $D^\vee \subset \mathbb{P}^3$ has intermediate 2-cover $C^\Delta\colon Y^2 = \Delta G(X,Z)$.*

Remark 7.3. Since C^Δ is a 2-cover of E^Δ, it follows that $D^\vee$ has Jacobian E^Δ. As observed in [12], this gives an alternative proof that E and E^Δ are reverse 4-congruent.

Let $u_1, \ldots, u_4$ and $v_1, \ldots, v_4$ be a pair of bases for F as a k-vector space, that are dual with respect to the trace form, i.e. $\mathrm{tr}_{F/k}(u_i v_j) = \delta_{ij}$. For example we could take $u_i = \theta^{i-1}$ and $v_j = \beta_{j-1}/g'(\theta)$ where

$$\frac{g(X)}{X-\theta} = \beta_3 X^3 + \beta_2 X^2 + \beta_1 X + \beta_0.$$

Lemma 7.4. *The theta groups for the quadric intersections obtained from*

$$\alpha(X - \theta Z) = (x_1 u_1 + \ldots + x_4 u_4)^2 \tag{32}$$

and

$$\frac{1}{\alpha g'(\theta)}(X - \theta Z) = (x_1 v_1 + \ldots + x_4 v_4)^2, \tag{33}$$

are the inverse transpose of each other.

Proof: Extending our field we may assume $F = k^4$. It then suffices to prove the lemma in the case where $u_1, \ldots, u_4$ and $v_1, \ldots, v_4$ are the standard bases.

Following (7), the quadric intersections obtained from (32) and (33) are

$$\mathrm{tr}_{F/k}\left(\frac{x^2}{\alpha g'(\theta)}\right) = \mathrm{tr}_{F/k}\left(\frac{\theta x^2}{\alpha g'(\theta)}\right) = 0,$$

and

$$\mathrm{tr}_{F/k}\left(\alpha x^2\right) = \mathrm{tr}_{F/k}\left(\alpha\theta x^2\right) = 0.$$

The lemma reduces to showing that if $D \subset \mathbb{P}^3$ is defined by

$$\sum_{i=1}^4 \xi_i x_i^2 = \sum_{i=1}^4 \xi_i \theta_i x_i^2 = 0,$$

then $D^\vee \subset \mathbb{P}^3$ is defined by

$$\sum_{i=1}^4 \frac{x_i^2}{\xi_i g'(\theta_i)} = \sum_{i=1}^4 \frac{\theta_i x_i^2}{\xi_i g'(\theta_i)} = 0.$$

where $g(\theta) = \prod_{i=1}^4 (X - \theta_i)$. This follows by direct calculation using the contravariants. □

We obtain the following analogue of Theorem 6.5. Let λ and μ be as defined in Lemma 6.2. We identify $E[4] = E^\Delta[4]$ via σ as specified in Remark 7.1.

Theorem 7.5. *The family of 2-covers $D_t^\vee \to C_t^\Delta$ such that each 4-cover $D_t^\vee \to E_t^\Delta$ has theta group the inverse transpose of that for our original 4-cover $D \to E$, is obtained by the procedure in Section 3.1, starting in place of (5) with*

$$\alpha g'(\theta)\big((t+\mu)X - (\theta t + \lambda)Z\big) = (x_1 + x_2\theta + x_3\theta^2 + x_4\theta^3)^2. \tag{34}$$

Proof: According to Lemma 7.4 we need to add a factor $g'_t(\theta_t)$ to the formula in Theorem 6.5. However, since we only care about the image of this element in $F^\times/F^{\times 2}k^\times$ we see by (26) that we can use $g'(\theta)$ instead. □

The analogue of Corollary 6.3 is that the surface $T^-_{E,\xi}(4)$ fibered by $D_t^\vee$ is given by

$$\{R_1R_2' - R_2R_1' = 0\} \subset \mathbb{P}^3.$$

Alternatively, an equation for this surface may be obtained from (34), exactly as in Remark 6.6.

7.3. **Reverse twists of Shioda's modular surface.** Let $\sigma\colon E[4] \to E^\Delta[4]$ be the reverse 4-congruence specified in Remark 7.1. Given $\xi \in H^1(k, E[4])$ with $\mathrm{Ob}_{E,4}(\xi) = 0$ we would like to write down a model for $S^-_{E,\xi}(4) = S^+_{E^\Delta,\sigma_*(\xi)}(4)$. If $\mathrm{Ob}_{E^\Delta,4}(\sigma_*(\xi)) = 0$, i.e. $\sigma_*(\xi)$ is represented by a quadric intersection (and we have these equations explicitly) then Theorem 6.7 gives equations for $S^-_{E,\xi}(4)$. Unfortunately this condition is not always satisfied.

Since $\mathrm{Ob}_{E,4}(\xi) = 0$ we have a model $D = D_{E,\xi} \subset \mathbb{P}^3$. The work in Section 7.2 gives us $D^\vee = D_{E^\Delta,\xi'} \subset \mathbb{P}^3$. It remains to determine $\kappa = \sigma_*(\xi) - \xi'$. If D is a 2-cover of C then Lemma 7.2 shows that $D^\vee$ is a 2-cover of C^Δ. Since the matrix in Remark 7.1 is congruent to the identity mod 2, we see that $D_{E^\Delta,\sigma_*(\xi)}$ is also a 2-cover of C^Δ. Therefore $2\xi' = 2\sigma_*(\xi)$, and so κ is 2-torsion.

Lemma 7.6. *Suppose we have a 4-cover $D = D_{E,\xi}$ with $\mathrm{Ob}_{E,4}(\xi) = 0$ and let $D^\vee = D_{E^\Delta,\xi'}$. Then $\sigma_*(\xi) = \xi' + \kappa$, where*

$$\kappa = (3\varphi^2 + A)/(4A^3 + 27B^2)$$

under the isomorphism (9).

Proof: By the same argument as in the proof of Theorem 4.1, we see that κ only depends on $\sigma\colon E[4] \to E^\Delta[4]$, and not on ξ itself. Thus it suffices to show that the inverse transpose of Θ_E is the twist of Θ_{E^Δ} by κ.

Let E have Weierstrass equation $y^2 = x^3 + Ax + B$. We embed $E \to \mathbb{P}^3$ via $(x_1 : \ldots : x_4) = (1 : x : y : 3x^2 + A)$. The image is $D \subset \mathbb{P}^3$ defined by

$$\begin{aligned} Ax_1^2 - x_1x_4 + 3x_2^2 &= 0, \\ 3Bx_1^2 + 2Ax_1x_2 + x_2x_4 - 3x_3^2 &= 0. \end{aligned}$$

Then by (31), $D^\vee \subset \mathbb{P}^3$ has equations

$$\begin{aligned} 3Ax_1^2 - 9Bx_1x_2 - A^2x_2^2 + 6(4A^3 + 27B^2)x_4^2 = 0, \\ 9Bx_1^2 + 4A^2x_1x_2 - 3ABx_2^2 + (4A^3 + 27B^2)(x_3^2 + 4x_2x_4) = 0. \end{aligned} \tag{35}$$

On the other hand the 2-cover of E^Δ corresponding to κ is given by

$$x + (4A^3 + 27B^2)\varphi = \kappa(u + v\varphi + w\varphi^2)^2.$$

Expanding and taking the coefficients of φ and φ^2 gives equations

$$\begin{aligned} 3u^2 - 2Av^2 - 4Auw - 6Bvw + 2A^2w^2 = 0, \\ -4Auv - 3Bv^2 - 6Buw + 4A^2vw + 5ABw^2 = s^2. \end{aligned} \tag{36}$$

The curves (35) and (36) are isomorphic via

$$(x_1 : x_2 : x_3 : x_4) = (18Bv - 4A^2w : 12Av + 18Bw : 6s : 3u - 2Aw). \qquad \square$$

Using the construction in Section 3.2, alternative equations for the curves $D_t^\vee$ in Theorem 7.5 are given by

$$N_{LF/M}\big(\alpha g'(\theta)\big((t+\mu)X - (\theta t + \lambda)Z\big)\big) = (y_1m_1 + \ldots + y_6m_6)^2. \tag{37}$$

We now modify this by introducing a factor $\nu(t)\kappa$ representing the shift from Theorem 4.1. We identify $E[4] = E^\Delta[4]$ via σ as specified in Remark 7.1.

Theorem 7.7. *The family of 2-covers $\mathcal{D}_t^\vee \to C_t^\Delta$ such that each 4-cover $\mathcal{D}_t^\vee \to E_t^\Delta$ has the same fibre above 0 (as an $E[4]$-torsor) as our original 4-cover $D \to E$, is obtained by the procedure in Section 3.2, starting in place of (11) with*

$$N_{LF/M}(\alpha\big((t+\mu)X - (\theta t + \lambda)Z\big)) = \nu(t)(\theta - \tilde\theta)^2\Delta(y_1m_1 + \ldots + y_6m_6)^2 \tag{38}$$

where $\nu(t)$ is given by (28).

Proof: We introduce an extra factor $\nu(t)\kappa$ to the right hand side of (37). Since the factors $g'(\theta)$ and κ do not depend on t, the proof that we obtain a family of curves with constant fibre above 0 is exactly the same as for Theorem 6.7.

If $D = D_{E,\xi}$ then by Lemmas 7.4 and 7.6 the fibre above $t = \infty$ is $D_{E^\Delta,\sigma_*(\xi)}$.

Finally we simplify our modified version of (37). A calculation along the same lines as the proof of (30) shows that

$$g'(\theta)g'(\tilde\theta) = -16(\theta - \tilde\theta)^2(3\varphi^2 + A).$$

Therefore

$$g'(\theta)g'(\tilde\theta)\kappa \equiv (\theta - \tilde\theta)^2\Delta \mod L^{\times 2},$$

and this gives the equation (38) as required. $\square$

Exactly as in Section 6.3, we obtain the following.

Corollary 7.8. *Suppose that $\xi \in H^1(k, E[4])$ and $D_{E,\xi}$ is given by (5). Then the surface $S^-_{E,\xi}(4)$ has a singular model in $\mathbb{P}^5$ defined by 3 quadrics. These quadrics are obtained from the $[M : k] = 6$ equations in $k(t)[X, Z, y_1, \ldots, y_6]$ coming from (38), by taking linear combinations to eliminate X^2, XZ and Z^2.*

For the purposes of Corollary 7.8 we may ignore the factor $\Delta \in k$ in (38). So compared to the direct case, we only need to multiply $\nu(t)$ by a factor $(\theta - \tilde{\theta})^2$. This is a Kummer generator for the quadratic extension LF/M.

8. Polarizations

Let A be an abelian surface over a field k of characteristic 0. We write $A^\vee$ for the dual abelian surface. As is described in, for instance, [18, Section 13], there is an injective group homomorphism $\mathrm{NS}(A) \to \mathrm{Hom}(A, A^\vee)$. A *polarization* is a homomorphism that lies in the image of the ample cone. These are isogenies. A *principal polarization* is a polarization that is an isomorphism.

If an abelian variety A has a principal polarization λ_A, then the map $\lambda \mapsto \psi_\lambda = \lambda_A^{-1}\lambda$ identifies the set of polarizations with a special semigroup in $\mathrm{End}(A)$.

Elliptic curves E have a natural principal polarization $\lambda_E \colon E \to E^\vee$ and on a product of elliptic curves $E \times E'$, the product of these gives a principal product polarization.

If E, E' are two non-isogenous elliptic curves without complex multiplication (CM) then $\mathrm{End}(E \times E') = \mathrm{End}(E) \times \mathrm{End}(E') = \mathbb{Z} \times \mathbb{Z}$. For such a surface one has $\mathrm{NS}(E \times E') \simeq \mathbb{Z} \times \mathbb{Z}$, the semigroup of ample classes is $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$, and polarizations correspond to the endomorphisms $[n]_E \times [n']_{E'}$, with $n, n' \in \mathbb{Z}_{>0}$.

An abelian surface A is called *decomposable* if it admits a non-constant map to an elliptic curve. In that case the Poincaré reducibility theorem [18, Proposition 12.1] gives us that there are two elliptic curves $E, E' \subset A$, such that the natural map $\phi \colon E \times E' \to A$ is an isogeny. We call such an isogeny an *optimal* decomposition.

In this section we are interested in determining when such a surface A may admit a principal polarization λ_A. If it does, we have a polarization $\phi^*(\lambda_A) = \phi^\vee \lambda_A \phi$ on $E \times E'$ of degree $\deg(\phi)^2$.

On a principally polarized abelian variety A we write e_n for the Weil pairing on $A[n]$ and $e_{A[n]}$ if we want to emphasize the abelian variety. We paraphrase [18, Proposition 16.8].

Proposition 8.1. *Let $\phi \colon E \times E' \to A$ be an isogeny and $\Delta = \ker \phi$. Let λ be a polarization on $E \times E'$. Suppose that $\Delta \subset \ker \lambda \subset (E \times E')[n]$. Then $\lambda = \phi^*(\lambda')$ for some polarization λ' on A if and only if the Weil pairing e_n on $(E \times E')[n]$ restricts to the trivial pairing on $\Delta \times \psi_\lambda(\frac{1}{n}\Delta)$.*

Proposition 8.2. *Let A be a principally polarized decomposable abelian surface, with optimal decomposition $\phi \colon E \times E' \to A$. Suppose that E, E' are non-isogenous*

and have no CM. Then the kernel of ϕ is the graph of a reverse n-congruence, where $\deg(\phi) = n^2$.

PROOF: Since $\ker\phi$ intersects trivially with $E \times \{0\}$ and $\{0\} \times E'$, we have that $\ker\phi \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ for some positive integers d_1 and d_2. The principal polarization on A pulls back to a polarization λ of degree $d_1^2 d_2^2$. It follows that ψ_λ must be an endomorphism of the same degree. Therefore $\psi_\lambda = [n]_E \times [n']_{E'}$ for some positive integers n and n' with $nn' = d_1 d_2$. Let $\mathrm{pr}_1 : E \times E' \to E$ be the first projection. Since $\ker\phi \subset \ker\lambda$ we have $\ker\phi \cong \mathrm{pr}_1(\ker\phi) \subset E[n]$. Therefore $d_1 \mid n$ and $d_2 \mid n$. The same argument shows that $d_1 \mid n'$ and $d_2 \mid n'$. Since $nn' = d_1 d_2$ it follows that $d_1 = d_2 = n = n'$. Hence we have that $\Delta = \ker\phi$ is the graph of an isomorphism $\sigma\colon E[n] \to E'[n]$.

We see that $\Delta \subset \psi_\lambda(\frac{1}{n}\Delta)$, so Proposition 8.1 implies that $e_n(\Delta, \Delta) = 1$. In particular, if we have points $T_1 = (t_1, \sigma(t_1))$ and $T_2 = (t_2, \sigma(t_2))$ belonging to Δ then by Proposition 2.4 we have that

$$1 = e_n(T_1, T_2) = e_{E[n]}(t_1, t_2)\tau_\sigma(e_{E[n]}(t_1, t_2)).$$

Therefore $\tau_\sigma(\zeta) = \zeta^{-1}$, i.e. the n-congruence σ is indeed a reverse n-congruence. □

Lemma 8.3. *If $\sigma\colon E[n] \to E'[n]$ is a reverse n-congruence, then the restriction $\sigma'\colon E[d] \to E'[d]$ for any $d \mid n$ is also a reverse congruence.*

PROOF: Let $n = dm$. If t_1, t_2 are generators of $E[n]$, then mt_1, mt_2 are generators of $E[d]$. The result follows from the basic property of Weil pairings that

$$e_{dm}(t_1, t_2)^m = e_d(mt_1, mt_2).$$ □

9. Examples

We first give an example showing how our methods improve on [12]. We then give an example where $Ш(E/\mathbb{Q})[4]$ is made visible by a second elliptic curve E', but our methods are needed to find E'. Finally we give some examples of 4-torsion in $Ш(E/\mathbb{Q})$ that cannot be made visible in a principally polarized abelian surface. We do this by exhibiting some twists of $S(4)$ that are not everywhere locally soluble.

We refer to elliptic curves by their labels in Cremona's tables [6].

Example 9.1. Let E and E' be the elliptic curves 96266a1 and 96266b1. We have $E(\mathbb{Q}) = 0$ and $E'(\mathbb{Q}) \cong \mathbb{Z}^2$. In this case there is a direct 4-congruence, and the Mordell-Weil group of E' explains a subgroup $(\mathbb{Z}/4\mathbb{Z})^2 \subset Ш(E/\mathbb{Q})$. We verify this for one element of $Ш(E/\mathbb{Q})$ of order 4, the other cases being similar. The element we consider is represented by $C = \{Q_1 = Q_2 = 0\} \subset \mathbb{P}^3$ where

$$Q_1 = x_1^2 + 3x_1x_2 + x_1x_3 + x_1x_4 - x_2^2 + 2x_2x_3 + 2x_2x_4 - 2x_3^2 - x_3x_4 - 3x_4^2,$$
$$Q_2 = x_1^2 - 3x_1x_2 + 2x_1x_3 - 6x_1x_4 + 3x_2^2 - 4x_2x_3 + 2x_2x_4 - 4x_3^2 - 2x_3x_4 - 2x_4^2.$$

One of the elements of $E'(\mathbb{Q})/4E'(\mathbb{Q})$ of order 4 maps to the 4-covering $C' = \{Q'_1 = Q'_2 = 0\} \subset \mathbb{P}^3$ where

$$\begin{aligned} Q'_1 &= x_1x_2 + 2x_1x_3 + x_2x_3 - x_2x_4 + 2x_3x_4 + 6x_4^2, \\ Q'_2 &= x_1x_2 + x_1x_3 + 3x_1x_4 + 2x_2^2 - 2x_2x_3 - x_2x_4 + 2x_3^2 - 3x_3x_4 + 4x_4^2. \end{aligned}$$

Starting from either C or C', and computing a twist of Shioda's modular surface using the method described in Corollary 6.8, we obtain

$$S: \quad \left\{ \begin{array}{r} 2y_1y_4 - 2y_1y_5 - 2y_2y_6 + y_3^2 - y_5^2 + y_6^2 = 0 \\ 2y_1^2 - 2y_1y_3 - y_1y_5 + y_1y_6 - 2y_2y_3 \\ +2y_2y_4 - y_2y_5 + y_2y_6 - y_3^2 + y_3y_5 + y_4y_6 + y_5y_6 - y_6^2 = 0 \\ y_1^2 + 4y_1y_3 - 2y_1y_4 - 2y_1y_5 + 2y_1y_6 + 2y_2^2 + 2y_2y_3 + 2y_2y_4 \\ -2y_2y_5 + y_3^2 + 2y_3y_4 - 2y_3y_6 + 2y_4y_5 - 2y_5^2 + 2y_5y_6 + y_6^2 = 0 \end{array} \right\} \subset \mathbb{P}^5.$$

The embeddings $C \to S$ and $C' \to S$ are given by

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \end{pmatrix} = \begin{pmatrix} 30 & 16 & 12 & 22 & 10 & 8 \\ -3 & -12 & 2 & -23 & -33 & -14 \\ -7 & -4 & -6 & 37 & -13 & 6 \\ 41 & -4 & -38 & 21 & 3 & 6 \\ 22 & 40 & -36 & 30 & -14 & 4 \\ 10 & 24 & -28 & 2 & -18 & 28 \end{pmatrix} \begin{pmatrix} f_{12} \\ f_{13} \\ f_{14} \\ f_{23} \\ f_{24} \\ f_{34} \end{pmatrix}$$

and

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \end{pmatrix} = \begin{pmatrix} -2 & -10 & -4 & 6 & 2 & 0 \\ 10 & 3 & 3 & -2 & 0 & -5 \\ -20 & 1 & -1 & 4 & 2 & 1 \\ -16 & -11 & 7 & 8 & -6 & 1 \\ -20 & -16 & -4 & 0 & -4 & -2 \\ -8 & -16 & 4 & -2 & 2 & 0 \end{pmatrix} \begin{pmatrix} f'_{12} \\ f'_{13} \\ f'_{14} \\ f'_{23} \\ f'_{24} \\ f'_{34} \end{pmatrix}$$

where

$$f_{ij} = \frac{\partial(Q_1, Q_2)}{\partial(x_i, x_j)} \quad \text{and} \quad f'_{ij} = \frac{\partial(Q'_1, Q'_2)}{\partial(x_i, x_j)}.$$

It may be checked that these maps send the flex points on C and C' to the singular points of S. In particular C and C' correspond to the same element of $H^1(\mathbb{Q}, E[4]) = H^1(\mathbb{Q}, E'[4])$.

Suppose instead that we use invariant theory. Let (Q'_1, Q'_2) have Hessian (Q''_1, Q''_2). Then the quadric intersection $\{-281Q'_1 + Q''_1 = -281Q'_2 + Q''_2 = 0\} \subset \mathbb{P}^3$ is a 4-covering of E. However this 4-covering is not locally soluble at 2. Therefore the method in [12] for computing visible elements of $Ш(E/\mathbb{Q})$ of order 4 does not apply. This is because the shift is not locally soluble at 2.

The equations for C, C' and S in Example 9.1 were simplified by making careful choices of co-ordinates. This was achieved by a combination of *minimisation* and *reduction*. For quadric intersections (such as C and C') these processes are described in [9]. We make some brief comments on how this works for S.

The minimisation step relies on defining a suitable invariant. The discriminant of a binary cubic form $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ is

$$\Delta(f) = -27a^2d^2 + 18abcd - 4ac^3 - 4b^3d + b^2c^2.$$

Let $q_1, q_2 \in k[z_1, z_2, z_3]$ be a pair of quadratic forms with corresponding 3×3 symmetric matrices B_1, B_2. Then $f(x,y) = \det(B_1x + B_2y)$ is a binary cubic form. We define $\Delta(q_1, q_2) = \Delta(f)$. Now let Q_1, Q_2, Q_3 be quadratic forms defining a twist of the surface S_0 in Section 5.3. Writing A_1, A_2, A_3 for the corresponding 6×6 symmetric matrices we find that

$$\det(A_1z_1 + A_2z_2 + A_3z_3) = f(q_1, q_2) \tag{39}$$

where f is a binary cubic and $q_1, q_2 \in k[z_1, z_2, z_3]$ are quadratic forms. We define $\Delta(Q_1, Q_2, Q_3) = \Delta(f)\Delta(q_1, q_2)$. This definition is independent of the choices of f, q_1, q_2, provided that they satisfy (39).

Now let $S \subset \mathbb{P}^5$ be a twist of S_0 defined over $\mathbb{Q}$. Clearing denominators we may assume that S is defined by $Q_1, Q_2, Q_3 \in \mathbb{Z}[y_1, \ldots, y_6]$. Then the discriminant $\Delta = \Delta(Q_1, Q_2, Q_3)$ is a non-zero integer. Using the natural action of $\mathrm{GL}_3(\mathbb{Q}) \times \mathrm{GL}_6(\mathbb{Q})$ we seek to minimise $|\Delta|$, while preserving that the coefficients of the Q_i are integers. This process is carried out one prime at a time, the idea being that for each prime p dividing Δ we consider the scheme defined by the reductions of the Q_i mod p. We did not work out algorithms guaranteed to minimise $|\Delta|$, but rather implemented some methods that seem to work reasonably well in practice.

The reduction step relies on defining a suitable inner product. Specifically we take the inner product (unique up to scalars) that is invariant under the action of $\mathrm{ASL}_2(\mathbb{Z}/4\mathbb{Z})$. For the surface S_0 in Section 5.3 this is the standard inner product. For general S we reduce to this case by finding a change of co-ordinates over $\mathbb{C}$ relating S and S_0. Performing lattice reduction on the Gram matrix of the inner product then gives a change of co-ordinates in $\mathrm{GL}_6(\mathbb{Z})$ that may be used to simplify our equations for S.

In preparing Example 9.1 we also had to find the change of co-ordinates relating the surfaces constructed from C and C'. However it was easy to solve for this as the unique change of co-ordinates defined over $\mathbb{Q}$ taking the singular points to the singular points.

Example 9.2. Let E be the elliptic curve 31252a1. We have $E(\mathbb{Q}) = 0$ and $Ш(E/\mathbb{Q})[4] \cong (\mathbb{Z}/4\mathbb{Z})^2$. One of the elements of order 4 in $Ш(E/\mathbb{Q})$ is represented

by the 4-covering $\{Q_1 = Q_2 = 0\} \subset \mathbb{P}^3$ where

$$Q_1 = 2x_1x_2 + 2x_1x_3 + x_3^2 + 2x_4^2,$$
$$Q_2 = 6x_1^2 + 6x_1x_2 - 14x_1x_3 + 9x_1x_4 + 11x_2^2 + 10x_2x_3 - 31x_2x_4 + 3x_3^2 + 22x_3x_4 + 7x_4^2.$$

Corollary 7.8 gives the following reverse twist of Shioda's modular surface.

$$S: \quad \left\{ \begin{array}{l} 2y_1y_3 + 2y_1y_5 + 2y_1y_6 + 2y_2^2 - 2y_2y_4 - 2y_3y_4 + y_5^2 = 0 \\ y_1^2 - 2y_1y_2 - y_1y_4 + 2y_1y_5 + y_2^2 + y_2y_3 \\ \quad -y_2y_4 + y_2y_5 + y_2y_6 - y_3y_5 + y_3y_6 - y_4^2 - y_4y_6 = 0 \\ y_1^2 - y_1y_3 + 2y_1y_4 - y_1y_5 - y_1y_6 + 2y_2y_3 \\ \quad +3y_2y_4 + y_3^2 + y_3y_5 + y_4y_5 + y_4y_6 - y_5^2 - y_5y_6 = 0 \end{array} \right\} \subset \mathbb{P}^5.$$

A useful check on our calculations is that the flex points on C and the singular points of S have the same field of definition. The genus 1 fibration on S may be computed as described in Remark 5.1. We searched for rational points on S of small height. Among the points we found were

$$(3:0:-1:-2:-2:3), \quad (1:-8:3:-22:-6:31),$$
$$(-33:13:-25:23:34:22), \quad (21:-10:-17:-26:-14:55),$$

all lying on a fibre isomorphic to $E' : y^2 = x^3 + 10609x + 58646$ with $E'(\mathbb{Q}) \cong \mathbb{Z}^3$. The elliptic curves E and E' are reverse 4-congruent. It turns out that all of $Ш(E/\mathbb{Q})[4]$ is explained by $E'(\mathbb{Q})$. The conductors of E and E' are $31252 = 2^2 \cdot 13 \cdot 601$ and $2468908 = 2^2 \cdot 13 \cdot 79 \cdot 601$. In particular E' is beyond the range of any current tables of elliptic curves. (In fact E is 2-congruent to a rank 2 elliptic curve of the same conductor, but these curves are not 4-congruent.)

Finally we give some examples where our twists of $S(4)$ are not locally soluble. As explained in the introduction, this can only happen in the reverse case. In Table 1 we list some elliptic curves $E/\mathbb{Q}$ with $E(\mathbb{Q}) = 0$ and $Ш(E/\mathbb{Q})[4] \cong (\mathbb{Z}/4\mathbb{Z})^2$. In each case, for *some* of the elements $\xi \in H^1(\mathbb{Q}, E[4])$, representing an element of $Ш(E/\mathbb{Q})$ of order 4, the surface $S^-_{E,\xi}(4)$ has no points locally at p, where p is the prime indicated.

Proposition 9.3. *Each of the elliptic curves $E/\mathbb{Q}$ in Table 1 has an element of order 4 in $Ш(E/\mathbb{Q})$ that cannot be made visible in a principally polarized abelian surface over $\mathbb{Q}$.*

Proof: By construction, there exists $\xi \in H^1(\mathbb{Q}, E[4])$ such that $[C_{E,\xi}] \in Ш(E/\mathbb{Q})$ has order 4, yet $S^-_{E,\xi}(4)(\mathbb{Q}_p) = \emptyset$. Let us now assume that $[C_{E,\xi}]$ is visible in an abelian surface A, i.e., that there is an injection $E \to A$ such that $[C_{E,\xi}]$ lies in the kernel of the induced map on Galois cohomology $H^1(\mathbb{Q}, E) \to H^1(\mathbb{Q}, A)$.

TABLE 1. Some elliptic curves E for which there exists $\xi \in H^1(\mathbb{Q}, E[4])$ with $[C_{E,\xi}] \in Ш(E/\mathbb{Q})$, yet $S^-_{E,\xi}(4)(\mathbb{Q}_p) = \emptyset$. Proposition 9.3 establishes that $[C_{E,\xi}]$ is not visible in a principally polarized abelian surface.

$p = 2$	$21720c1, 26712e1, 32784c1, 32816j1, 33536e1, 34560o1, 37984e1,$ $40328b1, 47664p1, 49176b1, 59248g1, 62328bj1, 69192f1, 69312ch1,$ $69312dp1, 73600bn1, 73840a1, 74368b1, 77440cl1, 77440cr1, 77600p1$
$p = 5$	$23950g1, 60725j1, 63825g1, 64975e1, 72600df1, 76175e1, 90450bs1,$ $105350z1, 120300n1, 121950ca1, 129850r1, 133950cy1, 137025s1,$ $141200bf1, 146700p1, 153425u1, 153425bd1, 154850m1, 154850m2$
$p = 13$	$56446n1, 62192t1, 70135c1, 100386g1, 104442w1, 124384g1,$ $132496df1, 172042o1, 200772u1, 216151f1, 226629g1, 256880dn1,$ $294060j1, 306735z1, 321945v1, 331240cy1, 335296dj1, 337155x1$
$p = 29$	$220342v1, 277530bc1, 277530bs1, 323785n1, 364994k1$
$p = 37$	$370999a1$
$p = 61$	$301401k1, 260470l1, 260470l2$
$p = 101$	$306030bg1, 306030bg2$

As described in Section 8, there is an elliptic curve $E' \subset A$ and an optimal decomposition $\phi : E \times E' \to A$. In particular, the kernel of ϕ is the graph of an isomorphism between finite subgroups of E and E'.

For each of the elliptic curves on our list we have $E(\mathbb{Q})/2E(\mathbb{Q}) = 0$, equivalently $\operatorname{rank} E(\mathbb{Q}) = 0$ and $E[2]$ is irreducible as a Galois module. By [14, Theorem 3.1], there exists, for some $l \geq 2$, a congruence $\sigma\colon E[2^l] \to E'[2^l]$ such that the graph of σ is contained in $\ker \phi$, and $[C_{E,\xi}] = \pi(P')$ for some $P' \in E'(\mathbb{Q})$, where π is the diagonal map in the following commutative diagram

$$\begin{array}{ccccccc} E(\mathbb{Q})/2^lE(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, E[2^l]) & \longrightarrow & H^1(\mathbb{Q}, E)[2^l] & \longrightarrow & 0 \\ & & \| & \nearrow_{\pi} & & & \\ E'(\mathbb{Q})/2^lE'(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, E'[2^l]) & \longrightarrow & H^1(\mathbb{Q}, E')[2^l] & \longrightarrow & 0 \end{array}$$

Since $E(\mathbb{Q})/2^lE(\mathbb{Q}) = 0$, we see that $P' \in E'(\mathbb{Q})/2^lE'(\mathbb{Q})$ has order 4. Since $E'(\mathbb{Q})[2] = 0$ it follows that $\operatorname{rank} E'(\mathbb{Q}) > 0$ and $P' \in 2^{l-2}E'(\mathbb{Q})$. Therefore ξ is explained (via a 4-congruence) by an element of $E'(\mathbb{Q})/4E'(\mathbb{Q})$.

Since $\operatorname{rank} E(\mathbb{Q}) = 0$ and $\operatorname{rank} E'(\mathbb{Q}) > 0$, it is clear that E and E' are not isogenous. Computation shows that the 4-division polynomial of E is irreducible with Galois group of order 48. Since the largest abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ has order 16, it follows that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{sep}}/\mathbb{Q})$ acts on $E[4]$ via a large enough group to ensure that E has no CM. It follows that any elliptic curve 4-congruent to E, in particular E', has no CM.

Proposition 8.2 and Lemma 8.3 show that for A to be principally polarized, the congruence σ must be reverse.

However, as noted at the start of the proof, $S^-_{E,\xi}(4)$ does not have any rational points. Therefore the 4-congruence induced by σ is not reverse, and hence neither is σ itself. This is the required contradiction. □

Remark 9.4. A curious fact about the examples in Table 1 is that the odd primes p at which we find local obstructions satisfy $p \equiv 5 \pmod 8$. Indeed, for any one p, there are only finitely many $\mathbb{Q}_p$-isomorphism classes for the surface $S^-_{E,\xi}(4)$, so determining which ones have local obstructions is in principle a finite amount of work. Proposition 9.5 provides one description of an insolvability criterion, that appears to explain all the examples in Table 1 with p odd. Specifically, we have checked in each of these cases that the elliptic curve E is directly 4-congruent over $\mathbb{Q}_p$ to an elliptic curve of the form considered in the proposition.

Proposition 9.5. *Let p be a prime with $p \equiv 5 \pmod 8$. Let E be the elliptic curve $y^2 = x^3 + Ax$ for some $A \in \mathbb{Q}_p^\times$ with $v_p(A)$ odd. Let ξ be the image of $P = (0,0)$ under the connecting map*

$$E(\mathbb{Q}_p)/4E(\mathbb{Q}_p) \longrightarrow H^1(\mathbb{Q}_p, E[4]).$$

Then the surface $S^-_{E,\xi}(4)$, which is defined over $\mathbb{Q}_p$, has no $\mathbb{Q}_p$-points.

Proof: We use Corollary 7.8 to show that $S^-_{E,\xi}(4)$ has equations

$$\begin{aligned} 0 &= y_2y_3 - Ay_5y_6 \\ 0 &= y_1y_4 + 2y_2y_5 + y_3^2 - Ay_6^2 \\ 0 &= (y_1^2 - 2y_2^2) + A(y_4^2 + 2y_5^2) + 4Ay_3y_6 \end{aligned}$$

Since multiplying A by a 4th power gives the same elliptic curve we may suppose $v_p(A) = \pm 1$. We consider the case $v_p(A) = 1$. Suppose $(y_1 : \ldots : y_6)$ is a $\mathbb{Q}_p$-point, with $y_1, \ldots, y_6 \in \mathbb{Z}_p$, not all in $p\mathbb{Z}_p$. Since $(2/p) = -1$ we have $y_1 \equiv y_2 \equiv y_3 \equiv 0 \pmod p$. Then since $(-2/p) = -1$ we have $y_4 \equiv y_5 \equiv y_6 \equiv 0 \pmod p$. This is the required contradiction. The case $v_p(A) = -1$ is similar. □

Remark 9.6. We also found 4 examples (225336k1, 271800bt1, 329536y1, 368928bj1) where for *every* $\xi \in H^1(\mathbb{Q}, E[4])$, representing an element of $Ш(E/\mathbb{Q})$ of order 4, the surface $S^-_{E,\xi}$ has no points locally at 2, and a further 4 examples (271800bj1, 352800md1, 378400bv1, 378400by1) where each $S^-_{E,\xi}(4)$ is locally insoluble either at 2 or 5.

Example 9.7. Let $E/\mathbb{Q}$ be the elliptic curve 225336k1 with Weierstrass equation

$$y^2 = x^3 - x^2 - 453476x - 197032572.$$

One of the elements of $Ш(E/\mathbb{Q})$ of order 4 is represented by $D = D_{E,\xi} \subset \mathbb{P}^3$ with equations

$$3x_1x_2 + 2x_1x_3 + 4x_1x_4 - 3x_2x_3 - 3x_2x_4 + 2x_3^2 + x_3x_4 + 3x_4^2 = 0$$
$$4x_1^2 + 2x_1x_2 + x_1x_3 + x_1x_4 + 4x_2^2 + 2x_2x_3 + 4x_3^2 - 2x_4^2 = 0$$

In the reverse case we get a surface $S = S^-_{E,\xi}(4) \subset \mathbb{P}^5$ with equations

$$\begin{aligned}
&7y_1y_2 - 7y_1y_3 - y_1y_4 + 19y_1y_5 + y_1y_6 - 4y_2^2 + y_2y_3 + 5y_2y_4 - 11y_2y_5 \\
&-9y_2y_6 + 2y_3^2 + 4y_3y_5 + 10y_3y_6 + 13y_4^2 - 10y_4y_5 + 2y_4y_6 - 4y_5^2 - 22y_5y_6 + 8y_6^2 = 0, \\
&4y_1^2 - 8y_1y_3 - 6y_1y_4 + 11y_1y_5 - 18y_1y_6 - y_2^2 + 17y_2y_3 - 8y_2y_4 - 11y_2y_5 - y_2y_6 \\
&-5y_3^2 + 17y_3y_4 + 3y_3y_5 + 18y_3y_6 - 15y_4^2 + 4y_4y_5 - 21y_4y_6 - 12y_5^2 - 13y_5y_6 + 3y_6^2 = 0, \\
&3y_1^2 + 4y_1y_2 + 16y_1y_3 + 4y_1y_4 - 11y_1y_5 + 6y_1y_6 - 11y_2^2 + 3y_2y_3 - 4y_2y_4 + 15y_2y_5 \\
&+y_2y_6 + 10y_3^2 + 19y_3y_4 + 7y_3y_5 + 28y_3y_6 + 2y_4^2 - 23y_4y_6 - y_5^2 + 31y_5y_6 + 20y_6^2 = 0.
\end{aligned}$$

As a check on our calculations we verified that the flex points on D and the singular points on S are defined over the same degree 16 number field.

We find that $S(\mathbb{Q}_2) = \emptyset$. As indicated in Remark 9.6, exactly the same happens for the other elements of order 4 in $Ш(E/\mathbb{Q})$. The argument in Proposition 9.3 now shows that none of the elements of $Ш(E/\mathbb{Q})$ of order 4 are visible in a principally polarized abelian surface.

References

[1] Wolf Barth and Klaus Hulek, *Projective models of Shioda modular surfaces*, Manuscripta Math. **50** (1985), 73–132.

[2] The MAGMA computer algebra system is described in Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

[3] Nils Bruin and Kevin Doerksen, *The arithmetic of genus two curves with* $(4,4)$*-split Jacobians*, Canad. J. Math. **63** (2011), no. 5, 992–1024.

[4] Nils Bruin, *Visualising Sha[2] in abelian surfaces*, Math. Comp. **73** (2004), no. 247, 1459–1476 (electronic).

[5] Nils Bruin and Sander R. Dahmen, *Visualizing elements of Sha[3] in genus 2 Jacobians*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 110–125.

[6] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997. See also http://www.warwick.ac.uk/~masgaj/ftp/data/.

[7] ———, *Classical invariants and 2-descent on elliptic curves*, J. Symbolic Comput. **31** (2001), no. 1–2, 71–87.

[8] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155.

[9] John E. Cremona, Tom A. Fisher, and Michael Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra Number Theory **4** (2010), no. 6, 763–820.

[10] John E. Cremona and Barry Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28.

[11] Tom Fisher, *Some improvements to 4-descent on an elliptic curve*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 125–138.
[12] ———, *The Hessian of a genus one curve*, Proc. Lond. Math. Soc. (3) **104** (2012), no. 3, 613–648.
[13] ———, *Invariant theory for the elliptic normal quintic, I. Twists of X(5)*, Math. Ann. **356** (2013), no. 2, 589–616.
[14] ———, *Invisibility of Tate-Shafarevich groups in abelian surfaces*, Int. Math. Res. Not. IMRN **15** (2014), 4085–4099.
[15] Tomas Antonius Klenke, *Visualizing elements of order two in the Weil-Châtelet group*, J. Number Theory **110** (2005), no. 2, 387–395.
[16] B. Mazur, *Visualizing elements of order three in the Shafarevich-Tate group*, Asian J. Math. **3** (1999), no. 1, 221–232. Sir Michael Atiyah: a great mathematician of the twentieth century.
[17] J. R. Merriman, S. Siksek, and N. P. Smart, *Explicit 4-descents on an elliptic curve*, Acta Arith. **77** (1996), no. 4, 385–404.
[18] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.
[19] Alice Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 447–461.
[20] Sebastian Karl Michael Stamminger, *Explicit 8-descent on elliptic curves*, International University Bremen, 2005, http://nbn-resolving.de/urn:nbn:de:101:1-201305171186. (PhD thesis).
[21] T. Womack, *Explicit descent on elliptic curves* (2003). (PhD thesis).

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

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK
E-mail address: T.A.Fisher@dpmms.cam.ac.uk