VISUALISING ELEMENTS OF ORDER 7 IN THE TATE-SHAFAREVICH GROUP OF AN ELLIPTIC CURVE

TOM FISHER

Abstract. We study the elliptic curves in Cremona's tables that are predicted by the Birch–Swinnerton-Dyer conjecture to have elements of order 7 in their Tate-Shafarevich group. We show that in many cases these elements are visible in an abelian surface or abelian threefold.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. Two groups of particular arithmetic interest associated to E are the Mordell-Weil group $E(\mathbb{Q})$ and the Tate-Shafarevich group $Ш(E/\mathbb{Q})$. Whilst the study of these groups is intimately related, it seems much easier to write down elements of the first group than the second. In an attempt to remedy this, Mazur [M] suggested visualizing elements of $Ш(E/\mathbb{Q})$ as cosets of E inside some larger abelian variety.

We recall some basic definitions. A *torsor* (or *principal homogeneous space*) under E is a pair (C, μ) where C is a genus one curve, and $\mu : E \times C \to C$ is a morphism inducing a simply transitive action on $\overline{\mathbb{Q}}$-points. We may view C as a twist of E by a cocycle taking values in E (acting on itself by translations) and so as an element of the *Weil-Châtelet group* $H^1(\mathbb{Q}, E)$. The identity in this group corresponds to the torsors with a $\mathbb{Q}$-point, equivalently those that are isomorphic to E. The *Tate-Shafarevich group* $Ш(E/\mathbb{Q})$ is the subgroup consisting of torsors that are everywhere locally soluble, i.e. have a $\mathbb{Q}_v$-point for all places v.

Let $\iota : E \to A$ be an inclusion of abelian varieties. If C is the twist of E by $\xi \in H^1(\mathbb{Q}, E)$, and V is the twist of A by $\iota_*(\xi) \in H^1(\mathbb{Q}, A)$, then there is a natural inclusion $C \to V$. One might say that C is visible in V. Accordingly, the subgroup of $H^1(\mathbb{Q}, E)$ *visible* in A is

$$\operatorname{Vis}_A H^1(\mathbb{Q}, E) = \ker \Big(H^1(\mathbb{Q}, E) \xrightarrow{\iota_*} H^1(\mathbb{Q}, A) \Big).$$

The *visibility dimension* of $\xi \in H^1(\mathbb{Q}, E)$ is the least dimension of an abelian variety A such that $\xi \in \operatorname{Vis}_A H^1(\mathbb{Q}, E)$.

To construct a suitable abelian variety A, we usually start with an abelian variety $F/\mathbb{Q}$ chosen so that E and F have a common finite Galois submodule Δ.

Date: 23rd May 2016.

We then take $A = (E \times F)/\Delta$ where the quotient is by the diagonal embedding of Δ.

Cremona and Mazur [CM], [AS2] gave some examples of elliptic curves $E/\mathbb{Q}$ and elements of order $n \in \{2, 3, 4, 5\}$ in $Ш(E/\mathbb{Q})$ that are visible in an abelian surface. For this they take F to be a second elliptic curve (often of the same conductor as E) with $E[n] \cong F[n]$ as Galois modules. An argument using restriction of scalars (see [AS1, Proposition 2.4]) shows that if $\xi \in Ш(E/\mathbb{Q})$ has order n then it has visibility dimension at most n. Mazur [M] showed that elements of order 3 in $Ш(E/\mathbb{Q})$ are always visible in an abelian surface. In [F3] we gave some examples of elements of orders 6 and 7 that are not visible in an abelian surface.

In this paper we give examples of elements of $Ш(E/\mathbb{Q})$ of order 7 that are visible in an abelian surface or abelian threefold. Continuing the work of Cremona and Mazur, our data shows that, at least for curves of small conductor, the visibility dimension is often much smaller than the bound coming from restriction of scalars.

Theorem 1.1. (i) *There are 222 isogeny classes of elliptic curves $E/\mathbb{Q}$ with conductor $N_E < 10^5$, that do not admit a rational 7-isogeny, but are predicted by the Birch–Swinnerton-Dyer conjecture to have $Ш(E/\mathbb{Q})[7] \neq 0$.*

(ii) *Of these examples, at least 79 are explained by visibility in an abelian surface, and at least a further 14 are explained by visibility in an abelian threefold.*

The list in Theorem 1.1(i) is taken from Cremona's tables [C]. In each case $\operatorname{rank} E(\mathbb{Q}) = 0$ and the Birch–Swinnerton-Dyer conjecture predicts that $Ш(E/\mathbb{Q})$ has order $(7m)^2$ for some integer m coprime to 7. We chose to investigate the following example in greater detail.

Theorem 1.2. *Let $E/\mathbb{Q}$ be the elliptic curve*

$$67080r \qquad y^2 = x^3 - x^2 + 782367544x + 10114340277756.$$

Then $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ and $Ш(E/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^2$. Moreover

(i) *Every element of $Ш(E/\mathbb{Q})$ is visible in an abelian threefold isogenous to $E \times \operatorname{Jac}(C)$ where $C/\mathbb{Q}$ is the genus 2 curve $y^2 = x(x+4)(x^4+2x^3-x-3)$.*

(ii) *Conditional on the Generalised Riemann Hypothesis, none of the non-zero elements of $Ш(E/\mathbb{Q})$ are visible in an abelian surface.*

The computer calculations in support of this work were carried out using Magma [BCP], Pari/GP [P] and Sage [S+].

2. Background on visibility

In this section we review some basic facts about visibility. References for this include [CM], [AS1], [AS2].

Let E and F be abelian varieties over a number field K, with common finite Galois submodule Δ. Let $A = (E \times F)/\Delta$, where the quotient is by the diagonal embedding of Δ. Let $F' = A/E$ and $E' = A/F$. There is then a commutative diagram

$$\begin{tikzcd} & & 0 \arrow[d] & & \\ & & F \arrow[d] \arrow[dr, "\psi"] & & \\ 0 \arrow[r] & E \arrow[r] \arrow[dr, "\phi"'] & A \arrow[r] \arrow[d] & F' \arrow[r] & 0 \\ & & E' \arrow[d] & & \\ & & 0 & & \end{tikzcd}$$

where the row and column are exact sequences of abelian varieties, and the diagonal maps ϕ and ψ are isogenies with kernel Δ.

There is a commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & \Delta \arrow[r] \arrow[d] & F \arrow[r, "\psi"] \arrow[d] & F' \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & E \arrow[r] & A \arrow[r] & F' \arrow[r] & 0. \end{tikzcd}$$

Taking the long exact sequence of Galois cohomology gives

$$\begin{tikzcd} & F(K) \arrow[r, "\psi"] \arrow[d] & F'(K) \arrow[r] \arrow[d, equal] & H^1(K,\Delta) \arrow[d] & \\ E(K) \arrow[r] & A(K) \arrow[r] & F'(K) \arrow[r, "\pi"] & H^1(K,E) \arrow[r] & H^1(K,A). \end{tikzcd} \tag{2.1}$$

It follows by a diagram chase that there are short exact sequences

$$0 \to \frac{A(K)}{E(K)+F(K)} \to \frac{F'(K)}{\psi F(K)} \to \operatorname{Vis}_A H^1(K,E) \to 0$$

and (swapping the roles of E and F)

$$0 \to \frac{A(K)}{E(K)+F(K)} \to \frac{E'(K)}{\phi E(K)} \to \operatorname{Vis}_A H^1(K,F) \to 0.$$

These two exact sequences immediately give the following lemma.

Lemma 2.1. *If $E'(K)/\phi E(K) = 0$ then $F'(K)/\psi F(K) \cong \operatorname{Vis}_A H^1(K,E)$.*

Next we give some local conditions under which the visible subgroup of $H^1(K,E)$ is actually a subgroup of $\text{Ш}(E/K)$. Let $d = |\Delta|$ be the degree of ϕ and ψ.

Theorem 2.2. *If $E'(K)/\phi E(K) = 0$ and*

(i) *all the Tamagawa numbers of E and F are coprime to d, and*
(ii) *A has good reduction at all places $v \mid d$, and*
(iii) *writing p for the rational prime below v, $e(K_v/\mathbb{Q}_p) < p-1$ for all places $v \mid d$,*

then $F'(K)/\psi F(K) \cong \mathrm{Vis}_A \text{Ш}(E/K)$.

Proof. We write $A^0(K_v)$ for the subgroup of $A(K_v)$ consisting of points whose reduction mod v belong to the identity component of the special fibre of the Néron model. The following three facts are established in [AS1].

(1) The unramified subgroup of $H^1(K_v,E)$ has order equal to the Tamagawa number $c_v(E) = [E(K_v) : E^0(K_v)]$.
(2) If $v \nmid d$ then $\psi : F^0(K_v^{\mathrm{nr}}) \to F'^0(K_v^{\mathrm{nr}})$ is surjective.
(3) If A has good reduction at v and $e(K_v/\mathbb{Q}_p) < p-1$ then $A(K_v^{\mathrm{nr}}) \to F'(K_v^{\mathrm{nr}})$ is surjective.

We consider the diagram (2.1) with K replaced by K_v. To prove the theorem it suffices to show that $\pi_v : F'(K_v) \to H^1(K_v,E)$ is the zero map for all places v of the number field K. It is clear that the image of π_v is killed by multiplication by d. So by fact (1) and our hypothesis on the Tamagawa numbers of E, it suffices to show that every element in the image of π_v is unramified. This follows by fact (2) if $v \nmid d$ and by fact (3) if $v \mid d$.

Finally we note that by hypothesis (iii), d is odd, and so there are no local conditions to check at the infinite places. □

3. Visibility in abelian surfaces

In this section we give some examples of elements of order 7 in $\text{Ш}(E/\mathbb{Q})$ that are visible in an abelian surface.

Elliptic curves E and F are said to be *n-congruent* if $E[n] \cong F[n]$ as Galois modules. We write $X_E(n)$, respectively $X_E^-(n)$, for the twist of the modular curve $X(n)$ whose non-cuspidal points parametrise the elliptic curves n-congruent to E via an isomorphism of n-torsion subgroups that preserves, respectively reverses, the Weil pairing. In the case $n = 7$ these curves are twists of the Klein quartic $X(7) = \{x^3y + y^3z + z^3x = 0\} \subset \mathbb{P}^2$. Since each element of $(\mathbb{Z}/7\mathbb{Z})^\times$ is plus or minus a square, each elliptic curve 7-congruent to E corresponds to a rational point on either $X_E(7)$ or $X_E^-(7)$.

Theorem 3.1. [HK, Théorème 2.1] *Let E be an elliptic curve with Weierstrass equation $y^2 = x^3 + ax + b$. Then $X_E(7) \subset \mathbb{P}^2$ has equation*

$$ax^4+7bx^3z+3x^2y^2-3a^2x^2z^2-6bxyz^2-5abxz^3+2y^3z+3ay^2z^2+2a^2yz^3-4b^2z^4 = 0.$$

In [PSS, Section 7.2] an equation for $X_E^-(7)$ is derived from that for $X_E(7)$. Formulae for the families of elliptic curves parametrised by $X_E(7)$ and $X_E^-(7)$ are given in [HK] and [F2].

Example 3.2. Let E be the elliptic curve $3364c$ in [C]. (By convention a Cremona label without a final number refers to the first curve in the isogeny class.) We take $a = -4062871$ and $b = -3152083138$ in Theorem 3.1. We then make the change of co-ordinates

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \leftarrow \begin{pmatrix} 2320 & 0 & -3509 \\ -2716430 & 1682 & 4042687 \\ -2 & 0 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

so that $X_E(7) \subset \mathbb{P}^2$ has equation

$$\begin{aligned} x^4 + 2x^3y + x^3z + 3x^2y^2 + 3x^2yz + 3x^2z^2 + 2xy^3 \\ - 3xy^2z + 6xyz^2 + 12xz^3 - 3y^3z - 3y^2z^2 + 6yz^3 - 2z^4 = 0. \end{aligned}$$

The MAGMA function `PointSearch` (with height bound 10^6) finds only two rational points $(0 : 1 : 0)$ and $(1 : -1 : 0)$ on $X_E(7)$, and no rational points on $X_E^-(7)$. These rational points correspond to the elliptic curves $E = 3364c$ and $F = 10092c$. In particular this proves that E and F are 7-congruent.

We performed a similar search for rational points on $X_E(7)$ and $X_E^-(7)$ for each of the elliptic curves $E/\mathbb{Q}$ in Theorem 1.1(i). Many of the 7-congruent elliptic curves we found had rank 0 or 1, but in the 79 cases listed in Table 3.1 we found an elliptic curve $F/\mathbb{Q}$ of rank 2. In the small number of cases where we found more than one such F, we just kept the one with smallest conductor. The elliptic curves F beyond the range of Cremona's tables were as follows. (In these cases we label the curve by its conductor followed by a $*$.)

$561090*$	$y^2 + xy = x^3 + x^2 + 95243x - 147561011$
$3140928*$	$y^2 = x^3 - 8580204x + 8146637424$
$2967232150*$	$y^2 + xy + y = x^3 - 3223101295946x + 3747757318724534268$
$6659445*$	$y^2 + y = x^3 - x^2 - 67728609901x + 7329794977161867$
$25859475*$	$y^2 + y = x^3 - 31493068950x - 6675516099954594$

Theorem 3.3. *Let (E, F) be any one of the 79 pairs of elliptic curves listed in Table 3.1. Then $F(\mathbb{Q})$ explains a subgroup of $\text{Ш}(E/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$.*

Table 3.1. Pairs of 7-congruent elliptic curves

E	F	E	F	E	F	E	F
$3364c$	$10092c$	$31311h$	$31311k$	$60885r$	$60885q$	$84150gk$	$84150gl$
$6552y$	$6552ba$	$31800e$	$31800f$	$61200gv$	$61200gu$	$84474w$	$84474u$
$9450p$	$9450t$	$34974h$	$174870bi$	$61950q$	$61950o$	$84672kg$	$84672kd$
$9510e$	$561090*$	$35682k$	$35682j$	$65088be$	$65088bc$	$84681e$	$84681h$
$10800y$	$10800u$	$36270l$	$36270j$	$68805d$	$68805c$	$84966ea$	$84966dx$
$11970o$	$11970s$	$36300br$	$36300by$	$69440z$	$69440ba$	$85050s$	$85050x$
$12927e$	$12927d$	$36414u$	$36414y$	$71148bh$	$71148bg$	$88305h$	$88305g$
$18832a$	$1712d$	$40362s$	$40362t$	$72384o$	$72384n$	$88450f$	$2967232150*$
$19350q$	$19350s$	$41616cw$	$41616cx$	$73416g$	$10488b$	$89211c$	$681c$
$20544v$	$20544u$	$43296g$	$43296f$	$74400h$	$74400j$	$91035c$	$18207a$
$21312ce$	$21312cd$	$43350q$	$43350p$	$75075f$	$75075d$	$91800be$	$91800bd$
$21696l$	$21696k$	$45494e$	$45494d$	$75712bz$	$10816bf$	$92778r$	$92778t$
$23232dv$	$23232dt$	$45738ca$	$45738bz$	$76176cd$	$76176cg$	$92862j$	$13266e$
$26600m$	$26600l$	$46704k$	$6672i$	$76362r$	$76362q$	$92950be$	$92950bd$
$26640bu$	$26640bt$	$46800ew$	$46800fa$	$76608bl$	$3140928*$	$93795e$	$6659445*$
$27930bj$	$27930bh$	$47232bu$	$47232bp$	$78210k$	$7110h$	$95040cd$	$95040ci$
$28314bn$	$28314bp$	$49938i$	$49938h$	$78400dg$	$235200eb$	$96558i$	$5082d$
$29400di$	$29400do$	$51600m$	$51600l$	$79350cy$	$79350cx$	$97470bp$	$97470br$
$30276r$	$30276q$	$54450gm$	$54450go$	$79530a$	$15906c$	$98325x$	$25859475*$
$30996b$	$30996a$	$57150g$	$57150e$	$81600ho$	$81600hn$		

Proof. By construction these elliptic curves are 7-congruent, and do not admit any rational 7-isogenies. They also have ranks 0 and 2. So by Lemma 2.1 we have

$$(\mathbb{Z}/7\mathbb{Z})^2 \;\cong\; F(\mathbb{Q})/7F(\mathbb{Q}) \;\cong\; \mathrm{Vis}_A\, H^1(\mathbb{Q}, E).$$

The Tamagawa numbers of E and F (at all bad primes) are coprime to 7. So in the 50 cases where E and F have good reduction at 7, it follows by Theorem 2.2 that $\mathrm{Vis}_A\, H^1(\mathbb{Q}, E)$ is a subgroup of $\text{Ш}(E/\mathbb{Q})$. In a further 4 cases ($27930bj$, $31311h$, $71148bh$, $84966ea$) the elliptic curves E and F attain good reduction over $K = \mathbb{Q}_7(\sqrt[4]{7})$. Since $[K : \mathbb{Q}_7]$ is coprime to 7 and $e(K/\mathbb{Q}_7) < 6$ this again suffices to check local solubility.

The right hand square in (2.1) gives a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & E(\mathbb{Q}_7)/7E(\mathbb{Q}_7) \arrow[r] & H^1(\mathbb{Q}_7, E[7]) \arrow[r] \arrow[d, equal] & H^1(\mathbb{Q}_7, E)[7] \arrow[r] & 0 \\
0 \arrow[r] & F(\mathbb{Q}_7)/7F(\mathbb{Q}_7) \arrow[r] \arrow[urr, "\pi_7"'] & H^1(\mathbb{Q}_7, F[7]) \arrow[r] & H^1(\mathbb{Q}_7, F)[7] \arrow[r] & 0
\end{tikzcd}$$

where the rows are the Kummer exact sequences for E and F. To complete the proof it suffices to show that π_7 is the zero map. This follows by Theorem 3.4(i) in 20 examples, and by Theorem 3.4(ii) in 4 examples ($46704k$, $73416g$, $75712bz$, $92862j$). In the remaining example with $E = 84672kg$ we found that $E[7] \cong F[7]$ has a unique cyclic $\mathrm{Gal}(\overline{\mathbb{Q}}_7/\mathbb{Q}_7)$-submodule, and were able to prove that π_7 is the zero map by a brute force calculation using Lemma 4.1, Lemma 4.3(i) and Velu's formulae [V]. □

Theorem 3.4. *Let E and F be 7-congruent elliptic curves over $\mathbb{Q}_7$. Suppose that either*

(i) *E and F have potentially multiplicative reduction, or*
(ii) *E has non-split multiplicative reduction and F has good reduction.*

Then $E(\mathbb{Q}_7)/7E(\mathbb{Q}_7)$ and $F(\mathbb{Q}_7)/7F(\mathbb{Q}_7)$ have the same images (via the Kummer exact sequence) in $H^1(\mathbb{Q}_7, E[7]) \cong H^1(\mathbb{Q}_7, F[7])$.

Proof. These are special cases of Theorems 4.2 and 4.4 below, applied over either $\mathbb{Q}_7$ or a quadratic extension. □

4. Conditions for local solubility

In this section K will be a p-adic field, i.e. a finite extension of $\mathbb{Q}_p$, with discrete valuation v_K (normalised to take integer values) and valuation ring $\mathcal{O}_K$. Let ℓ be an odd prime. We write $\zeta_\ell \in \overline{K}$ for a primitive ℓth root of unity, and j_E for the j-invariant of an elliptic curve E.

Lemma 4.1. *Let $\phi : E \to E'$ be an ℓ-isogeny of elliptic curves over K, with dual isogeny $\widehat{\phi} : E' \to E$. Then the following are equivalent.*

(i) *$E'(K)/\phi E(K) \cong H^1(K, E[\phi])$,*
(ii) *$E(K)/\widehat{\phi} E'(K) = 0$,*
(iii) *the images of $E(K)/\ell E(K)$ and $H^1(K, E[\phi])$ in $H^1(K, E[\ell])$ are the same.*

Proof. There is a commutative diagram with exact rows and exact right hand column

$$
\begin{tikzcd}
E(K) \arrow[r, "\phi"] \arrow[d, equal] & E'(K) \arrow[r, "\delta_\phi"] \arrow[d, "\widehat{\phi}"'] & H^1(K, E[\phi]) \arrow[d] \\
E(K) \arrow[r, "\ell"] \arrow[d, "\phi"'] & E(K) \arrow[r, "\delta_\ell"] \arrow[d, equal] & H^1(K, E[\ell]) \arrow[d] \\
E'(K) \arrow[r, "\widehat{\phi}"] & E(K) \arrow[r, "\delta_{\widehat{\phi}}"] & H^1(K, E'[\widehat{\phi}]).
\end{tikzcd}
\tag{4.1}
$$

By Tate local duality, δ_ϕ is surjective if and only if $\delta_{\widehat{\phi}}$ has trivial image. The remaining statements follow by a diagram chase. □

Theorem 4.2. *Let E and F be ℓ-congruent elliptic curves over K, both with split multiplicative reduction. Suppose that either $\zeta_\ell \notin K$ or $v_K(j_E) \not\equiv 0 \pmod{\ell}$. Then $E(K)/\ell E(K)$ and $F(K)/\ell F(K)$ have the same images (via the Kummer exact sequence) in $H^1(K, E[\ell]) \cong H^1(K, F[\ell])$.*

Proof. By the Tate parametrisation there is an isomorphism of $\mathrm{Gal}(\overline{K}/K)$-modules $E(\overline{K}) \cong \overline{K}^\times/q^{\mathbb{Z}}$ for some $q \in K^\times$ with $v_K(q) = -v_K(j_E)$. We consider the ℓ-isogenies $\phi : E \to E'$ and $\widehat{\phi} : E' \to E$ given on K-points by

$$
\begin{aligned} K^\times/q^{\mathbb{Z}} &\to K^\times/q^{\ell\mathbb{Z}} \\ x &\mapsto x^\ell, \end{aligned}
\qquad \text{and} \qquad
\begin{aligned} K^\times/q^{\ell\mathbb{Z}} &\to K^\times/q^{\mathbb{Z}} \\ x &\mapsto x. \end{aligned}
$$

Since the second of these maps is surjective, the conditions in Lemma 4.1 are satisfied. As Galois modules we have $E[\phi] \cong \mu_\ell$ and $E'[\widehat{\phi}] \cong \mathbb{Z}/\ell\mathbb{Z}$, and so an exact sequence

$$
0 \longrightarrow \mu_\ell \longrightarrow E[\ell] \longrightarrow \mathbb{Z}/\ell\mathbb{Z} \longrightarrow 0. \tag{4.2}
$$

If the isomorphism $E[\ell] \cong F[\ell]$ identifies the submodules μ_ℓ, then applying Lemma 4.1 to both E and F proves the theorem. If the submodules μ_ℓ are not identified then $\mu_\ell \cong \mathbb{Z}/\ell\mathbb{Z}$ and (4.2) splits, in which case $\zeta_\ell \in K$ and $v_K(j_E) \equiv 0 \pmod{\ell}$, contradicting our hypotheses. □

Another way to check the conditions in Lemma 4.1 is provided by the following lemma. We write $c_K(E)$ for the Tamagawa number of E/K.

Lemma 4.3. *Let $\phi : E \to E'$ be an ℓ-isogeny of elliptic curves over K, with dual isogeny $\widehat{\phi} : E' \to E$. Let ω and ω' be Néron differentials on E and E'.*

(i) We have $\phi^*\omega' = \alpha\omega$ *and* $\widehat{\phi}^*\omega = \beta\omega'$ *for some* $\alpha, \beta \in \mathcal{O}_K$ *satisfying* $\alpha\beta = \ell$, *and*

$$\frac{\#(E'(K)/\phi E(K))}{\#E(K)[\phi]} = |\alpha|_K^{-1} \frac{c_K(E')}{c_K(E)}$$

(ii) If E *and* E' *have good reduction,* $E(K)[\phi] \neq 0$ *and* $e(K/\mathbb{Q}_p) < p-1$ *then* α *is a unit.*

Proof. (i) See [Sc, Lemma 3.8].
(ii) We suppose $p = \ell$ as otherwise α is a unit by (i). Since $e(K/\mathbb{Q}_p) < p-1$ the theory of formal groups shows that $E(K)[\phi] \cong \mathbb{Z}/p\mathbb{Z}$ cannot belong to the kernel of reduction. Therefore, arguing exactly as in the proof of [S2, Chapter X, Theorem 4.2], the image of δ_ϕ in (4.1) lies in the unramified subgroup. Since K has a unique unramified extension of degree p it follows that $\#(E'(K)/\phi E(K))$ divides p, and so α is a unit by (i). □

Theorem 4.4. *Let* E *and* F *be* ℓ*-congruent elliptic curves over* K*. Suppose that* E *has non-split multiplicative reduction and* F *has good reduction. If* $p = \ell$ *then further suppose that* $e(K/\mathbb{Q}_p) < p-1$*. Then* $E(K)/\ell E(K)$ *and* $F(K)/\ell F(K)$ *have the same images (via the Kummer exact sequence) in* $H^1(K, E[\ell]) \cong H^1(K, F[\ell])$*.*

Proof. Let L be the unramified quadratic extension of K. By the Tate parametrisation there is an exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \to M_1 \to E[\ell] \to M_2 \to 0$$

with $M_1 \cong \mu_\ell$ and $M_2 \cong \mathbb{Z}/\ell\mathbb{Z}$ over L. Since $[L : K]$ is coprime to ℓ, the proof of Theorem 4.2 shows that $E(K)/\ell E(K)$ and $H^1(K, M_1)$ have the same image in $H^1(K, E[\ell])$. Since $E[\ell] \cong F[\ell]$, there are ℓ-isogenies $\phi : F \to F'$ and $\widehat{\phi} : F' \to F$ with kernels M_1 and M_2. By our assumption that E has *non-split* reduction, the action of $\mathrm{Gal}(L/K)$ on M_2 is non-trivial. Applying Lemma 4.3(ii) to the isogeny $\widehat{\phi} : F' \to F$ over L, and then Lemma 4.3(i) to the same isogeny over K, shows that $F(K)/\widehat{\phi}F'(K) = 0$. We are again done by Lemma 4.1. □

5. Visibility in abelian threefolds

In this section we give some examples of elements of order 7 in Ш$(E/\mathbb{Q})$ that are visible in an abelian threefold.

Let $E/\mathbb{Q}$ be one of the elliptic curves in Theorem 1.1(i). We may use the modular symbols algorithms in Magma or Sage to look for modular forms $f \in S_2(\Gamma_0(N_E))$ satisfying a $\mathfrak{p}$-congruence with E for some prime $\mathfrak{p}|7$. Table 5.1 lists the first few examples we found with $\mathbb{Q}(f) \neq \mathbb{Q}$. Each f is a normalised Hecke eigenform with $\mathbb{Q}(f) = \mathbb{Q}(\sqrt{2})$ and satisfies $a_p(f) \equiv a_p(E) \bmod (3 + \sqrt{2})$ for all primes p with $p < 1000$. By work of Shimura [Sh] we may associate to each f

Table 5.1. Hecke eigenvalues $a_p(f)$

E	a_2	a_3	a_5	a_7	a_{11}	a_{13}
$6622b$	-1	$-\sqrt{2}-1$	$\sqrt{2}-2$	-1	1	$2\sqrt{2}-2$
$9510e$	-1	-1	1	$\sqrt{2}-3$	$-2\sqrt{2}-2$	-5
$14938n$	1	-2	$\sqrt{2}-2$	-1	-1	-2
$15219c$	$-\sqrt{2}-1$	0	-1	$2\sqrt{2}-2$	-5	$-2\sqrt{2}+3$
$20502ba$	1	0	$-\sqrt{2}-3$	$-\sqrt{2}-3$	$3\sqrt{2}-2$	$\sqrt{2}-2$

a modular abelian surface A_f with real multiplication by $\sqrt{2}$. Our data suggests that $A_f[3+\sqrt{2}] \cong E[7]$ as Galois modules. If A_f is isogenous over $\mathbb{Q}$ to the Jacobian of a genus 2 curve $C/\mathbb{Q}$ then for each prime p of good reduction for C we have (see [FLS+, Section 2.1] or [MS, Lemma 3])

$$\begin{aligned} \mathrm{Trace}(a_p) &= p+1-n_1, \\ \mathrm{Norm}(a_p) &= (n_1^2+n_2)/2-(p+1)n_1-p, \end{aligned} \tag{5.1}$$

where $n_1 = \#C(\mathbb{F}_p)$ and $n_2 = \#C(\mathbb{F}_{p^2})$. We used the following result to help find the corresponding genus 2 curves. (An alternative approach is described in [GGG], [Wa].)

Theorem 5.1. [B, Theorem 4.1] *Let $g(x) = \prod_{i=1}^{3}(x^2-\alpha_i x + P\alpha_i^2 + Q\alpha_i + R)$ where $\alpha_1, \alpha_2, \alpha_3$ are the roots of $x^3+Ax^2+Bx+C=0$ and $A,B,C,P,Q,R \in \mathbb{Q}$ with $P \neq 0$ and*

$$R = 4P, \quad B = (Q(PA-Q)+4P^2+1)/P^2, \quad C = 4(PA-Q)/P.$$

If $g(x)$ has distinct roots in $\overline{\mathbb{Q}}$ then $y^2 = g(x)$ defines a smooth curve of genus 2 whose Jacobian admits real multiplication by $\sqrt{2}$, defined over $\mathbb{Q}$, and fixed by the Rosati involution. Moreover every such genus 2 curve arises in this way, up to quadratic twist.

By searching over $A,P,Q \in \mathbb{Q}$ of small height, we found for each of the modular forms in Table 5.1, a genus 2 curve satisfying (5.1) for all good primes $p < 1000$. We record the genus 2 curves (and Cremona labels for E) in Table 5.2 and the values of A,P,Q in Table 5.3.

At this point we abandoned the computation of modular forms (which is increasingly time consuming as the level increases) and took the following more

Table 5.2. Genus 2 curves

$6622b$	$y^2 = 20x^6 + 44x^5 - 23x^4 - 10x^3 + 81x^2 - 52x + 4$
$9510e$	$y^2 = 9x^6 - 12x^5 + 2x^4 - 84x^3 + 437x^2 + 528x + 144$
$14938n$	$y^2 = 4x^6 + 36x^5 + 37x^4 - 150x^3 - 47x^2 - 72x + 16$
$15219c$	$y^2 = -7x^6 + 18x^5 - 93x^4 + 18x^3 + 117x^2 - 36x + 64$
$20502ba$	$y^2 = 36x^6 + 108x^5 + 381x^4 + 474x^3 + 849x^2 + 504x + 144$

naive approach. We used Theorem 5.1 to draw up a list of genus 2 curves by looping over $A, P, Q \in \mathbb{Q}$ of small height and keeping only those curves whose primes of bad reduction are smaller than some threshold. For each curve C on our list, we computed the right hand sides t_p and n_p in (5.1) for all $p < 100$. Then for each elliptic curve E in Theorem 1.1(i) we tested to see whether

$$a_p(E)^2 \pm t_p a_p(E) + n_p \equiv 0 \pmod 7 \tag{5.2}$$

for some choice of sign $\pm$. If this test is passed for many primes p then it seems likely that E and the Jacobian of C satisfy a congruence up to quadratic twist. Indeed in all such cases we were able to replace C by a quadratic twist so that (5.2) holds with a minus sign for all good primes $p < 1000$.

The examples we found are recorded in Table 5.3, except that we list just one genus 2 curve C for each elliptic curve E. In cases where we found more than one C, it appears that the Jacobians of these curves are isogenous. The data recorded is as follows.

The elliptic curve $E/\mathbb{Q}$: This is specified by its reference in Cremona's tables [C]. An entry in brackets indicates that this curve already appeared in Table 3.1.

The ratio of levels: The odd part of the conductor of $F = \mathrm{Jac}(C)$, computed using Liu's program `genus2reduction` in Sage, is $(\kappa N_{\mathrm{odd}})^2$ where N_{odd} is the odd part of the conductor of E, and κ is recorded in the second column of the table. In most cases $\kappa = 1$, as we would expect if E and F correspond to newforms of the same level.

The genus 2 curve $C/\mathbb{Q}$: This is specified as the quadratic twist by δ of the curve in Theorem 5.1 with parameters A, P, Q.

The Mordell-Weil group of $F = \mathrm{Jac}(C)$: We used Magma to compute the order of the torsion subgroup and the rank of $F(\mathbb{Q})$. For the latter, we used Stoll's implementation of 2-descent to bound the rank, and then the functions `Points` and `ReducedBasis` to find sufficiently many independent

Table 5.3. Pairs of elliptic curves and genus 2 curves

E	κ	A	P	Q	δ	#tors	rank	$7 \mid c_p$	$p=7$
6622b	1	41/4	1/5	0	1	1	4	$\{11\}$	m
(**9510e**)	1	29/5	18	53	2	1	4		g
14938n	1	9	1/4	3	1	2	4		m
15219c	1	9/8	−4/7	−6/7	1	1	4		g
20502ba	1	6	9/16	7/4	1	1	4		g
21771b	1	81/8	2	12	2	1	4		g
23025c	19	−52/3	−3/4	3	5	2	2	$\{19\}$	g
23085h	1	6	3/5	22/5	1	1	4		g
23744v	1	−7	−2	9	1	1	4		m
24432j	1	−8	−3/4	7	15	1	4		g
25296a	37	9	2/5	5/2	1	1	6	$\{31, 37\}$	g
26166h	1	83/12	4	95/6	1	1	4	$\{3\}$	$g^{(3)}$
29445c	1	−14/3	−1/2	5/2	1	1	4		g
39984bf	1	3	4	11	1	1	4		$g^{(3)}$
40764a	1/3	8	2	7	1	1	4		g
40950u	1	9	4/5	29/5	5	4	4		m
41616l	1	23/3	9	40	1	1	4		g
45770c	1	4	1	−1	1	1	4	$\{5\}$	g
54327c	1	47/7	7/6	4	42	2	4		m
54663a	1	−6	−1/8	13/8	1	2	4		m
61320v	1	53/6	1	14/3	1	1	4		m
67032cf	1	2	3/16	5/4	7	2	4		m^*
67080r	1/5	7	9	37	1	2	4		g
67179c	1	6	7/4	31/4	1	2	4		m^*
70950bc	1	27/5	1	29/10	1	1	4	$\{2\}$	g
72128j	1	8	8/7	31/7	14	2	4		m^*
(75712bz)	17/7	5	4	17	−26	2	2	$\{17\}$	
(**76176cd**)	1	12	−1/4	1	1	1	4		g
(76608bl)	11	2/7	7/6	−1/3	−14	1	4		m
78400le	1	8	−4/7	−29/7	1	2	4		$g^{(4)}$

E	κ	A	P	Q	δ	#tors	rank	$7 \mid c_p$	$p=7$
$(84474w)$	49	17	3/4	7	7	1	4		
$90650i$	1	−8	−1	3	−35	1	4		m^*
90950i	1	7	8	27	1	1	4		g
90950m	1	1	4/5	1	5	1	4		g
96300bd	1	8	10/3	43/3	1	1	4		g

points of infinite order. Since $F(\mathbb{Q})$ is a $\mathbb{Z}[\sqrt{2}]$-module, the rank is necessarily even. It is striking that in nearly all cases we have rank $F(\mathbb{Q}) = 4$.

The primes with Tamagawa number divisible by 7: The Tamagawa numbers $c_p(E)$ are coprime to 7 in all cases. We list the primes p for which the Tamagawa number $c_p(F)$ is divisible by 7. These entries were computed using Liu's program `genus2reduction` in Sage, Donnelly's programs `RegularModel` and `ComponentGroup` in Magma, and our own calculations for curves with multiplicative reduction, following [FLS+, Section 3.4] and [BLR, Theorem 9.6.1]. There was one case ($E = 76608bl$ and $p = 2$) not covered by these methods. Liu's program nonetheless reports that the potential stable reduction is the union of two elliptic curves. The Jacobian F therefore has potential good reduction, and so by a result of Silverman [S1] the Tamagawa number is coprime to 7.

The reduction behaviour at $p = 7$: We write g in cases where E and F both have good reduction, and m in cases where they both have multiplicative reduction. We write m^* if the $\sqrt{7}$-twists of E and F both have multiplicative reduction. The label $g^{(n)}$ indicates that E and F attain good reduction over $\mathbb{Q}_7(\sqrt[n]{7})$.

Theorem 5.2. *Let (E, F) be any one of the 16 pairs of elliptic curves and genus 2 Jacobians listed in Table 5.3, for which the Cremona reference for E appears in bold. Then $F(\mathbb{Q})$ explains a subgroup of $Ш(E/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$.*

Proof. In Theorem 6.3 we show that (making an appropriate choice of sign for $\sqrt{2}$) we have $E[7] \cong F[3+\sqrt{2}]$ as Galois modules. The ranks of E and F are 0 and 4, and they have torsion subgroups of order coprime to 7. Since $F(\mathbb{Q})$ is a $\mathbb{Z}[\sqrt{2}]$-module, it follows by Lemma 2.1 that

$$(\mathbb{Z}/7\mathbb{Z})^2 \cong F(\mathbb{Q})/[3+\sqrt{2}]F(\mathbb{Q}) \cong \mathrm{Vis}_A\, H^1(\mathbb{Q}, E).$$

For the examples highlighted in bold:

(i) all Tamagawa numbers of E and F are coprime to 7, and

(ii) E and F have potential good reduction at 7, and this good reduction is achieved over an extension of $\mathbb{Q}_7$ of degree less than 6.

It follows by Theorem 2.2 that $\mathrm{Vis}_A H^1(\mathbb{Q}, E)$ is a subgroup of $\text{Ш}(E/\mathbb{Q})$. $\square$

Remark 5.3. We expect that Theorem 5.2 is true for all the pairs (E, F) in Table 5.3 with $\operatorname{rank} F(\mathbb{Q}) \geq 4$. Moreover, in all cases except the one with $E = 84474w$, this would follow from an appropriate generalisation of Theorem 4.2.

Remark 5.4. We checked (using the method in [CF, p158], [St]) that the genus 2 Jacobian F is absolutely simple in all cases except the one with $E = 78400le$. In the exceptional case the formulae in [B, Section 5] show that F is isogenous to the restriction of scalars of the $\mathbb{Q}$-curve

$$y^2 = x\left(x^2 + 5(7 + \sqrt{-7})x + 70(1 + \sqrt{-7})\right).$$

In this case we were able to check the congruence $E[7] \cong F[3 + \sqrt{2}]$ using Theorem 3.1.

6. Checking the congruences

In Table 5.3 we gave a list of pairs (E, F) where $E/\mathbb{Q}$ is an elliptic curve and F is the Jacobian of a genus 2 curve $C/\mathbb{Q}$. The genus 2 curves C were constructed using Theorem 5.1, and so their Jacobians are known to have real multiplication by $\sqrt{2}$. We suspect (on the basis of comparing traces of Frobenius for all good primes $p < 1000$) that $E[7] \cong F[3 + \sqrt{2}]$ as Galois modules. In this section we prove that this is indeed the case.

It would of course be interesting to prove this using modularity, or by finding a result analogous to Theorem 3.1, but we take a more direct approach, based on that used in [KO, Section 5] to exhibit a pair of 7-congruent elliptic curves.

Proposition 6.1. *Let $E/\mathbb{Q}$ be an elliptic curve and $F/\mathbb{Q}$ a genus 2 Jacobian with real multiplication by $\sqrt{2}$, defined over $\mathbb{Q}$, and fixed by the Rosati involution. Suppose that*

(i) *The Galois representation $\overline{\rho}_{E,7} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[7])$ is surjective.*
(ii) *There are non-zero torsion points $P \in E[7]$ and $Q \in F[7]$ whose images in $E/\{\pm 1\}$ and $F/\{\pm 1\}$ have the same field of definition. (By (i) this is a degree 24 number field.)*

Then for some choice of sign $\pm$ the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules $E[7]$ and $F[3 \pm \sqrt{2}]$ are isomorphic up to quadratic twist.

Proof. We write $Q = Q_+ + Q_-$ where $Q_\pm = (-3 \pm \sqrt{2})Q \in F[3 \pm \sqrt{2}]$. Let $L, L_\pm$ be the fields of definition of the images of $Q, Q_\pm$ in $F/\{\pm 1\}$. It is clear that L_+

and L_- are subfields of L and that $[L : L_1L_2] \leq 2$. By our hypotheses on E, the subfields of L correspond to the subgroups H with $\{\left(\begin{smallmatrix} \pm 1 & * \\ 0 & * \end{smallmatrix}\right)\} \subset H \subset \mathrm{GL}_2(\mathbb{F}_7)$. In particular L has degree 24, and its only non-trivial subfield has degree 8. So either $L = L_+$ or $L = L_-$. Suppose it is the former. Then replacing Q by Q_+ we may assume that $Q \in F[3 + \sqrt{2}]$.

Since $\sqrt{2}$ is fixed by the Rosati involution, it is self-adjoint for the Weil pairing $e_7 : F[7] \times F[7] \to \mu_7$. In particular $F[7] = F[3+\sqrt{2}] \times F[3-\sqrt{2}]$ is an orthogonal decomposition with respect to e_7. Since the Weil pairing is alternating and non-degenerate we have

$$\wedge^2 E[7] \cong \wedge^2 F[3 \pm \sqrt{2}] \cong \mu_7.$$

The proposition is now a special case of the following lemma. □

Lemma 6.2. *Let $\ell \geq 5$ be a prime, and let M_1, M_2 be Galois modules each isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$ as an abelian group. Suppose that $\wedge^2 M_1 \cong \wedge^2 M_2$ and*

(i) *the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(M_1)$ is surjective, and*

(ii) *the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(M_2)) \to \mathrm{SL}(M_1)$ is not surjective.*

Then M_1 and M_2 are isomorphic up to quadratic twist.

Proof. This is a variant of [Se, Lemme 8], the difference being that we have removed the hypothesis that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(M_2)$ is surjective.

Let B_1 and B_2 be finite groups and H a subgroup of $B_1 \times B_2$ with $\mathrm{pr}_1(H) = B_1$ and $\mathrm{pr}_2(H) = B_2$. We identify B_1 with $B_1 \times \{1\}$ in $B_1 \times B_2$ and let $N_1 = B_1 \cap H$. Likewise we put $N_2 = B_2 \cap H$. Then N_1 is normal in B_1, and N_2 is normal in B_2. Moreover the image of H in $B_1/N_1 \times B_2/N_2$ is the graph of an isomorphism $\alpha : B_1/N_1 \to B_2/N_2$.

We apply the above with B_i the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(M_i)$ for $i = 1, 2$, and H the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(M_1) \times \mathrm{GL}(M_2)$. Hypothesis (ii) shows that N_1 is a proper subgroup of $\mathrm{SL}(M_1)$. Since N_1 is normal in $B_1 \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ it follows that $N_1 \subset \{\pm 1\}$. Hence $B_1/N_1 \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ or $\mathrm{GL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. The only index two subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is the subgroup of elements with determinant a square. By inspection of the centres we see that this subgroup is not isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/\{\pm 1\}$. Since $B_1/N_1 \cong B_2/N_2$ it follows that $B_2 \cong \mathrm{GL}_2(\mathbb{F}_\ell)$. In other words, we have shown that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(M_2)$ is surjective. The proof in [Se] (using the fact that every automorphism of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is inner) now applies. □

Theorem 6.3. *Let (E, F) be any one of the pairs in Table 5.3. Then for some choice of sign $\pm$ we have $E[7] \cong F[3 \pm \sqrt{2}]$ as Galois modules.*

Proof. In each case it is easy to find a good prime p for which $f_p(X) = X^2 - a_p(E)X + p$ is irreducible mod 7, and another good prime $p \neq 7$ for which $f_p(X)$

has distinct roots mod 7. It follows by [Se, Section 4] that $\overline{\rho}_{E,7} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[7])$ is surjective.

Let L be the number field of degree 24 defined by the x-coordinate of a 7-torsion point on E. As noted in [KO] the degree 8 subfield is $K = \mathbb{Q}(\theta)$ where θ is a root of

$$(X^2 + 5X + 1)^3(X^2 + 13X + 49) - j_E X = 0. \tag{6.1}$$

We specify points on $F = \mathrm{Jac}(C)$ by pairs of points $[P_1, P_2]$ on C corresponding to the divisor class $[P_1 + P_2 - \Omega]$, where Ω is a canonical divisor. We also write $P_i = (x_i, y_i)$ for $i = 1, 2$. Let β_0 be the rational function specified on p18 of [CF]. Then there is a morphism

$$F \to \mathbb{P}^3 ; \quad [P_1, P_2] \mapsto (1 : x_1 + x_2 : x_1x_2 : \beta_0)$$

whose image is the Kummer surface $\mathcal{K} \subset \mathbb{P}^3$. This is a quartic surface isomorphic to $F/\{\pm 1\}$.

We use the machinery for computing with analytic Jacobians in Magma [W] to compute (numerical approximations to) 24 points $[(x_1, y_1), (x_2, y_2)]$, representing the pairs of inverse elements in $F[3 + \sqrt{2}] - \{0\}$. In all cases except $E = 78400le$ (discussed in Remark 5.4) we have $\mathrm{End}_{\mathbb{C}}(F) = \mathbb{Z}[\sqrt{2}]$, and so the only ambiguity in choosing $\sqrt{2}$ is up to sign. We arrange the 24 points into 8 sets of 3 corresponding to the action of $(\mathbb{Z}/7\mathbb{Z})^\times/\{\pm 1\}$. We anticipate that each set of 3 points (or rather their images in $\mathcal{K}$) will be jointly defined over K.

Let $[(x_1, y_1), (x_2, y_2)]$ be one of the points. Let g and h be the minimal polynomials of $x_1 + x_2$ and x_1x_2 over K. Let c be one of the coefficients of g or h. We compute the minimal polynomial of c over $\mathbb{Q}$ by first computing the coefficients numerically and then recognising them as rational numbers. We then find a root of this polynomial in K. If we are unable to find a root then we either increase the precision, or go back and change the sign of $\sqrt{2}$. In this way we compute cubic polynomials $g, h \in K[X]$.

We then solve for a point $Q = (1 : \xi_2 : \xi_3 : \xi_4) \in \mathcal{K}(L)$ where ξ_2 and ξ_3 are roots of g and h. For this we try all pairs of roots of g and h and use the equation for $\mathcal{K}$ to solve for ξ_4. Since the multiplication-by-m maps on the Kummer surface are implemented in Magma it is then easy to check (now by an exact calculation) that $7Q = (0 : 0 : 0 : 1)$. Moreover in each case we found that $L = \mathbb{Q}(\xi_2)$.

Proposition 6.1 now shows that $E[7] \cong F[3 \pm \sqrt{2}]$ up to quadratic twist. But any quadratic twist would be supported on the bad primes. So our earlier comparison of traces of Frobenius for all good primes $p < 1000$ is more than sufficient to finish the proof. □

7. Proof of Theorem 1.2

Let E be the elliptic curve $67080r$. Theorem 5.2 shows that $Ш(E/\mathbb{Q})$ contains a subgroup $(\mathbb{Z}/7\mathbb{Z})^2$ visible in an abelian threefold. Moreover the abelian threefold is as described in Theorem 1.2, since taking $(A, P, Q) = (7, 9, 37)$ in Theorem 5.1 we have

$$9(x+1)^6 g\left(\frac{-x-2}{x+1}\right) = x(x+4)(x^4+2x^3-x-3).$$

Following the methods in [GJP+], we show that this is all of $Ш(E/\mathbb{Q})$. The bad primes of E split in $K = \mathbb{Q}(\sqrt{D})$ with $D = -191$. Computing L-values and using the Gross-Zagier formula shows there is a point $y_K \in E(K)$ with canonical height $\widehat{h}_K(y_K) \approx 217958.077$. Following [GJP+, Section 2.1] we find that $\overline{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$ is surjective for all odd primes p. Therefore by work of Kolyvagin

$$v_p(\#Ш(E/\mathbb{Q})) \leq 2\, v_p([E(K) : \mathbb{Z}y_K]).$$

We found a point of infinite order $P \in E^D(\mathbb{Q})$ using 12-descent [F1]. Since the point is rather large, we record it as follows. Let $C_4 \subset \mathbb{P}^3$ be the 4-covering of the elliptic curve 2-isogenous to E^D defined by

$$x_1^2 + 6x_1x_2 + 7x_1x_3 + 23x_1x_4 - 3x_2^2 + 12x_2x_3 + 8x_2x_4 - 30x_3^2 + 54x_3x_4 - 60x_4^2 = 0$$
$$6x_1^2 - x_1x_2 + 89x_1x_3 - 37x_1x_4 + 37x_2^2 - 86x_2x_3 + 22x_2x_4 - 166x_3^2 + 114x_3x_4 + 199x_4^2 = 0$$

The 4-covering map is given by formulae of classical invariant theory; see [AKM+]. Then $P \in E^D(\mathbb{Q})$ is the image, under the 4-covering map and the 2-isogeny, of the point

$$(847793227 : 2227947281 : 2665508726 : 1875455642) \in C_4(\mathbb{Q}).$$

We find $\widehat{h}_K(P) = 2\widehat{h}_{\mathbb{Q}}(P) \approx 1112.031$ and $\widehat{h}_K(y_K)/\widehat{h}_K(P) \approx 196.000$. We checked using the methods in [Si] (specifically the Magma functions `SiksekBound`, `Saturation` and `Points`) that P is a generator for $E^D(\mathbb{Q})$ modulo torsion. It was useful to exploit here that E has a rational 2-torsion point.

Since $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z}$ it follows that $[E(K) : \mathbb{Z}y_K] = 2^a \cdot 7$ for some integer a. A 2-descent shows that $Ш(E/\mathbb{Q})[2] = 0$, and we have already shown that $Ш(E/\mathbb{Q})$ contains a copy of $(\mathbb{Z}/7\mathbb{Z})^2$. Therefore $Ш(E/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^2$.

To prove Theorem 1.2(ii) it suffices to show (see [F3, Theorem 3.2]) that the only elliptic curves 7-congruent to E are those isogenous to E. We take $a = 1013948336592$ and $b = 471906827379024768$ in Theorem 3.1 and then make the change of co-ordinates

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \leftarrow \begin{pmatrix} 102188568 & -22341576 & -103840044 \\ 73939908228192 & 94676367452256 & 135756936508464 \\ -28 & 46 & -151 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

so that $C = X_E(7) \subset \mathbb{P}^2$ is defined by

$$\begin{aligned} \mathcal{F}(x,y,z) = 6x^4 &+ 25x^3y - 39x^3z - 3x^2y^2 - 15x^2yz + 27x^2z^2 - 42xy^2z \\ &- 141xyz^2 - 87xz^3 + 8y^4 - 6y^3z - 21y^2z^2 + 127yz^3 - 15z^4. \end{aligned}$$

This curve has rational points $P_1 = (4 : 9 : 2)$ and $P_2 = (5 : -10 : 3)$, corresponding to E and its 2-isogenous curve. To show that these are the only rational points on C, we closely follow the methods in [PSS]. In view of this, we give just a few of the details.

Since $C \subset \mathbb{P}^2$ is a twist of the Klein quartic it has automorphism group $G \cong \mathrm{PSL}_2(\mathbb{F}_7)$. By [AR, Theorem 24.1], the G-invariant divisor classes on C form a cyclic group, generated by Λ (say) of degree 2. Let K be the degree 8 number field, defined by (6.1), arising as the field of definition of a cyclic subgroup of $E[7]$. A 2-descent on $J = \mathrm{Jac}(C)$ proves the following.

Theorem 7.1. *If the class number of K is odd then $J(\mathbb{Q}) \cong \mathbb{Z}^2$, and $G_1 = [\Lambda - 2P_1]$ and $G_2 = [P_1 - P_2]$ generate a subgroup of finite index.*

Both Magma and Pari/GP report that, conditional on the Generalised Riemann Hypothesis, K has class number 1. We will now assume this is the case.

The reduction of C mod 7 has a unique singular point at $(4 : 3 : 1)$. Since $\mathcal{F}(4,3,1) \equiv 35 \pmod{49}$ this is a regular point. The smooth $\overline{\mathbb{F}}_7$-points are parametrised by

$$s \mapsto (4s^4 + 2s^2 + 2s + 4 : 3s^4 + 3s^2 + 5s + 5 : s^4 + 4s + 2).$$

Integrating these polynomials in s, and then summing over the points of a divisor, gives an isomorphism $\widetilde{J}(\mathbb{F}_7) \cong (\mathbb{Z}/7\mathbb{Z})^3$, where $\widetilde{J}$ is the special fibre of the Néron model of $J/\mathbb{Q}_7$. We find that the images of G_1 and G_2 are linearly independent. The image of $J(\mathbb{Q}) \cong \mathbb{Z}^2$ in $\widetilde{J}(\mathbb{F}_7)$ is therefore the subgroup generated by $\widetilde{G}_1$ and $\widetilde{G}_2$. The only smooth points $P \in \widetilde{C}(\mathbb{F}_7)$ with $[P - \widetilde{P}_1]$ belonging to this subgroup are $\widetilde{P}_1$, $\widetilde{P}_2$ and $(1 : -1 : 0)$. Moreover if $P \in C(\mathbb{Q})$ is a point reducing to $(1 : -1 : 0)$ then

$$[P - P_1] \in G_1 + 4G_2 + 7J(\mathbb{Q}). \tag{7.1}$$

We used Chabauty's method to show that P_1 and P_2 are the only points in $C(\mathbb{Q})$ reducing to $\widetilde{P}_1$ and $\widetilde{P}_2$ (for this we show there is a differential on $C/\mathbb{Q}_7$ killing $J(\mathbb{Q})$ whose reduction mod 7 corresponds to $x+y+3z$), and then the Mordell-Weil sieve with $p = 41$ to show there are no points $P \in C(\mathbb{Q})$ satisfying (7.1). Therefore $C(\mathbb{Q}) = \{P_1, P_2\}$.

Since $X_E^-(7)$ has no $\mathbb{Q}_2$-points, this completes the proof of Theorem 1.2.

References

[AR] A. Adler and S. Ramanan, *Moduli of abelian varieties*, Lecture Notes in Mathematics **1644**, Springer-Verlag, Berlin, 1996.

[AS1] A. Agashé and W.A. Stein, Visibility of Shafarevich-Tate groups of abelian varieties, *J. Number Theory* **97** (2002), no. 1, 171–185.

[AS2] A. Agashé and W.A. Stein, Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero, with an appendix by J.E. Cremona and B. Mazur, *Math. Comp.* **74** (2005), no. 249, 455–484.

[AKM+] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum and A.R. Perlis, Jacobians of genus one curves, *J. Number Theory* **90** (2001), no. 2, 304–315.

[B] P.R. Bending, *Curves of genus* 2 *with* $\sqrt{2}$ *multiplication*, 1999, `http://arxiv.org/abs/math/9911273`

[BLR] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **21**, Springer-Verlag, Berlin, 1990.

[BCP] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comb.* **24**, 235-265 (1997). See also `http://magma.maths.usyd.edu.au/magma/`

[CF] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, LMS Lecture Note Series **230**, Cambridge University Press, Cambridge, 1996.

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

[CM] J.E. Cremona and B. Mazur, Visualizing elements in the Shafarevich-Tate group, *Experimental Mathematics* **9**:1, (2000) 13-28.

[F1] T.A. Fisher, Finding rational points on elliptic curves using 6-descent and 12-descent, *J. Algebra* **320** (2008), no. 2, 853–884.

[F2] T.A. Fisher, On families of 7 and 11-congruent elliptic curves, *LMS J. Comput. Math.* **17** (2014), no. 1, 536–564.

[F3] T.A. Fisher, Invisibility of Tate-Shafarevich groups in abelian surfaces, *Int. Math. Res. Not.* (2014), no. 15, 4085–4099.

[FLS+] E.V. Flynn, F. Leprévost, E.F. Schaefer, W.A. Stein, M. Stoll and J.L. Wetherell, Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves, *Math. Comp.* **70** (2001), no. 236, 1675–1697.

[GGG] E. González-Jiménez, J. González and J. Guàrdia, Computations on modular Jacobian surfaces, *Algorithmic number theory (Sydney, 2002)*, 189–197, Lecture Notes in Comput. Sci., **2369**, Springer, Berlin, 2002.

[GJP+] G. Grigorov, A. Jorza, S. Patrikis, W.A. Stein and C. Tarnita, Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves, *Math. Comp.* **78** (2009), no. 268, 2397–2425.

[HK] E. Halberstadt and A. Kraus, Sur la courbe modulaire $X_E(7)$, *Experiment. Math.* **12** (2003), no. 1, 27–40.

[KO] A. Kraus and J. Oesterlé, Sur une question de B. Mazur, *Math. Ann.* **293** (1992), no. 2, 259–275.

[M] B. Mazur, Visualizing elements of order three in the Shafarevich-Tate group, *Asian J. Math.* **3** (1999), no. 1, 221–232.

[MS] J.R. Merriman and N.P. Smart, Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point, *Math. Proc. Cambridge Philos. Soc.* **114** (1993), no. 2, 203–214.

[P] PARI/GP, Version 2.5.5, Bordeaux, 2013, `http://pari.math.u-bordeaux.fr/`

[PSS] B. Poonen, E.F. Schaefer and M. Stoll, Twists of $X(7)$ and primitive solutions to $x^2+y^3=z^7$, *Duke Math. J.* **137** (2007), no. 1, 103–158.

[Sc] E.F. Schaefer, Class groups and Selmer groups, *J. Number Theory* **56** (1996), no. 1, 79–114.

[Se] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), no. 4, 259–331.

[Sh] G. Shimura, On the factors of the Jacobian variety of a modular function field, *J. Math. Soc. Japan* **25** (1973), 523–544.

[Si] S. Siksek, Infinite descent on elliptic curves, *Rocky Mountain J. Math.* **25** (1995), no. 4, 1501–1538.

[S1] J.H. Silverman, The Néron fiber of abelian varieties with potential good reduction, *Math. Ann.* **264** (1983), no. 1, 1–3.

[S2] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Text in Mathematics **106**, Springer-Verlag, New York, 1986.

[S+] W.A. Stein et al., *Sage Mathematics Software (Version 6.2)*, The Sage Development Team, 2014, `http://www.sagemath.org`

[St] M. Stoll, Two simple 2-dimensional abelian varieties defined over $\mathbb{Q}$ with Mordell-Weil group of rank at least 19, *C. R. Acad. Sci. Paris* **321**, Série I, 1341-1345 (1995).

[V] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), A238–A241.

[W] P.B. van Wamelen, Computing with the analytic Jacobian of a genus 2 curve, in *Discovering mathematics with Magma*, W. Bosma and J. Cannon (eds.), Algorithms and Computation in Mathematics **19**, Springer-Verlag, Berlin, 2006, 117–135.

[Wa] X.D. Wang, 2-dimensional simple factors of $J_0(N)$, *Manuscripta Math.* **87** (1995), no. 2, 179–197.

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK

E-mail address: `T.A.Fisher@dpmms.cam.ac.uk`