INVISIBILITY OF TATE-SHAFAREVICH GROUPS IN ABELIAN SURFACES

TOM FISHER

Abstract. We give some examples of elliptic curves over the rationals whose Tate-Shafarevich groups contain elements of order 6 or 7 that are not visible in an abelian surface. We then show that some of these elements are visible in an abelian threefold.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. The Tate-Shafarevich group $Ш(E/\mathbb{Q})$ is the subgroup of the Weil-Châtelet group $H^1(\mathbb{Q}, E)$ consisting of principal homogeneous spaces that are everywhere locally soluble. Mazur suggested trying to visualise elements of this group as cosets of E inside some larger abelian variety A. More precisely, let $\iota : E \to A$ be an inclusion of abelian varieties over $\mathbb{Q}$ (that is, both a morphism of group schemes and a closed immersion). Then the subgroup of $H^1(\mathbb{Q}, E)$ *visible* in A is

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

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

We usually construct A from an abelian variety $F/\mathbb{Q}$ chosen so that E and F have a common finite Galois submodule Δ. We then take $A = (E \times F)/\Delta$ where the quotient is by the diagonal embedding of Δ.

Cremona and Mazur [CM], [AS2, Appendix] gave some examples of elliptic curves $E/\mathbb{Q}$ and elements of $Ш(E/\mathbb{Q})$ of order $n \in \{2, 3, 4, 5\}$ 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) that is n-congruent to E, i.e. $E[n] \cong F[n]$ 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 [Ma] showed that elements of order $n = 3$ are always visible in an abelian surface. It seems likely (although much harder to prove) that this is still be true for $n = 4, 5$. Indeed for $n = 3, 4, 5$ the relevant twists of the modular curve $X(n)$ are isomorphic to $\mathbb{P}^1$. This means that there are

Date: 11th January 2013.

infinitely many candidates to try for the second elliptic curve F. The case $n = 3$ is special in that the total space is also rational, and this is the key ingredient in Mazur's proof.

It is conjectured (see [D, Conjecture 4.4]) that for n sufficiently large there are no non-trivial n-congruences, i.e. any two n-congruent elliptic curves are isogenous. So it was always unlikely that every element of $Ш(E/\mathbb{Q})$ would be visible in an abelian surface. In this article we give some examples to put this beyond doubt. In fact we show that $Ш(E/\mathbb{Q})$ can contain elements of orders 6 and 7 with visibility dimension 3. For this we use work of Rubin and Silverberg [RS] (case $n = 6$) and Poonen, Schaefer and Stoll [PSS] (case $n = 7$) on finding all elliptic curves n-congruent to a given elliptic curve.

2. Some twisted modular curves

Let E and F be n-congruent elliptic curves. The isomorphism of Galois modules $E[n] \cong F[n]$ takes the Weil pairing to its rth power for some $r \in (\mathbb{Z}/n\mathbb{Z})^\times$. Composing with multiplication by $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ changes r by a square. So for $n \in \{6, 7\}$ we may assume without loss of generality that $r \in \{\pm 1\}$. We say an n-congruence is *direct* if $r = 1$, and *reverse* if $r = -1$. We write $X_E(n)$, respectively $X_E^-(n)$, for the twist of $X(n)$ whose non-cuspidal points parametrise elliptic curves directly, respectively reverse, n-congruent to E.

Remark 2.1. (i) If $n \in \{6, 7\}$ then every elliptic curve n-congruent to E corresponds to a rational point on either $X_E(n)$ or $X_E^-(n)$.
(ii) If $\phi : E \to F$ is an isogeny of elliptic curves, with degree d coprime to n, then E and F are n-congruent. Moreover F corresponds to a rational point on $X_E(n)$ or $X_E^-(n)$ according as d or $-d$ is a square mod n.
(iii) If E and F are n-congruent elliptic curves then their quadratic twists (by the same quadratic character) are also n-congruent.

The modular curve $X(6)$ has genus one. In fact it is the elliptic curve $y^2 = x^3 + 1$. Rubin and Silverberg [RS] (and independently Papadopoulos [P]) show that $X_E(6)$ has Weierstrass equation $y^2 = x^3 + \Delta_E$ where Δ_E is the discriminant of E. They also show that if $j(E)$ is not 0, 1728, $4 \cdot 1728$ or $-8 \cdot 1728$ then $X_E(6)$ has infinitely many rational points, and so there are infinitely many elliptic curves 6-congruent to E. If $j(E) = 0, 1728$ or $4 \cdot 1728$ then E has reducible 2-torsion or reducible 3-torsion. We will therefore work with the elliptic curves

$$E_d : y^2 = x^3 - 6d^2x + 6d^3$$

with j-invariant $-8 \cdot 1728$.

Theorem 2.2. *For $d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ the only elliptic curves over $\mathbb{Q}$ that are 6-congruent to E_d are E_d and E_{-d}.*

The weaker statement that these are the only elliptic curves *directly* 6-congruent to E_d is proved in [RS, Theorem 4.1(c)]. In general we use the following lemma.

Lemma 2.3. *Let $K = \mathbb{Q}(\sqrt{3})$ and $d \in K^\times/(K^\times)^2$.*

(i) *The only elliptic curves over K that are directly 6-congruent to E_d are E_d and E_{-d}.*
(ii) *The elliptic curves E_d and $E_{(3-2\sqrt{3})d}$ are reverse 6-congruent.*

PROOF: (i) Let $E = E_d$. Then $X_E(6)$ has affine equation $y^2 = x^3 - 27$. As noted in the proof of [RS, Theorem 4.1(c)], there are exactly two $\mathbb{Q}$-rational points on this curve and these correspond to E_d and E_{-d}. We find there are no further rational points over K. Indeed the elliptic curves $y^2 = x^3 - 1$ and $y^2 = x^3 - 27$ both have rank 0 over $\mathbb{Q}$, and the torsion subgroup over K has order 2.
(ii) Since these curves are quadratic twists they are 2-congruent. So it suffices to show they are reverse 3-congruent. This follows from the formulae in [F3, Section 13] for the family of curves parametrised by $X_E^-(3)$. □

If $d \in K^\times/(K^\times)^2$ then by Lemma 2.3 there are exactly four elliptic curves over K that are 6-congruent to E_d. Theorem 2.2 follows on noting that if $d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ then only two of these curves are defined over $\mathbb{Q}$.

To find similar examples in the case $n = 7$ we work with twists of the Klein quartic $X(7) = \{x^3y + y^3z + z^3x = 0\} \subset \mathbb{P}^2$.

Proposition 2.4 (Halberstadt, Kraus)**.** *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*

$$\begin{aligned} ax^4 &+ 7bx^3z + 3x^2y^2 - 3a^2x^2z^2 - 6bxyz^2 \\ &- 5abxz^3 + 2y^3z + 3ay^2z^2 + 2a^2yz^3 - 4b^2z^4 = 0. \end{aligned}$$

PROOF: See [HK, Théorème 2.1]. □

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 [F4]. A version of these formulae for $X_E(7)$ (not quite covering all cases) is already given in [HK, Section 5].

We specify elliptic curves by their labels in Cremona's tables [C]. In cases beyond the range of his tables we label a curve as $N*$ (where N is the conductor) and also give a Weierstrass equation.

Theorem 2.5. *The elliptic curves in each row of the following table are a complete set of 7-congruent elliptic curves over $\mathbb{Q}$. (The labels $C_4, \ldots, C_9$ refer to* [PSS, Table 3]*.)*

C_4	$27a1,\ 27a2,\ 27a3,\ 27a4,\ 1323m1,\ 1323m2$
C_6	$288a1,\ 288a2,\ 32544b1,\ 32544c1$
C_7	$864a1,\ 14688d1,\ 56160h1$
C_8	$864b1,\ 844128{*} = (y^2 = x^3 + 975182301x - 6403527885798)$
C_9	$864c1,\ 477792{*} = (y^2 = x^3 - 347727411x - 2420740718874)$

Proof: For the first elliptic curve E in each row, it is shown in [PSS] (by a combination of 2-descent, Chabauty's method and the Mordell-Weil sieve) that the only rational points on $X_E(7)$ are those listed in [PSS, Table 3]. If E is taken from the first row then $X_E(7) \cong X_E^-(7)$, since $27a1$ and $27a3$ are both 3-isogenous and $\sqrt{-3}$-twists. If E is taken from any of the last 4 rows then $X_E^-(7)$ has no $\mathbb{Q}_2$-rational points. So in each case we know the complete set of $\mathbb{Q}$-rational points on both $X_E(7)$ and $X_E^-(7)$. The theorem follows by Remark 2.1(i). $\square$

Remark 2.6. In [PSS, Table 3] the authors in fact consider 10 curves $C_1, \ldots, C_{10}$, each of the form $X_E(7)$. In the first three cases E has reducible 7-torsion. In the fifth case the complete set of $\mathbb{Q}$-rational points has not been determined, since C_5 has Jacobian of rank 3 and so Chabauty's method does not apply. The same problem arises in the last case when we try to determine the complete set of $\mathbb{Q}$-rational points on $X_E^-(7)$.

3. Visibility in abelian surfaces

The following theorem will be used to show that certain elements of the Weil-Châtelet group $H^1(\mathbb{Q}, E)$ are not visible in an abelian surface.

Theorem 3.1. *Let $E/\mathbb{Q}$ be an elliptic curve and $\xi \in H^1(\mathbb{Q}, E)$ an element of order n that is visible in an abelian surface A. Suppose that E has irreducible ℓ-torsion for all primes ℓ dividing n. Then there is a multiple m of n, with the same prime factors as n, an elliptic curve $F/\mathbb{Q}$ with $E[m] \cong F[m]$, and a point $P \in F(\mathbb{Q})$ such that $\pi_m(P) = \xi$ where π_m is the diagonal map in the following commutative diagram (whose rows are the Kummer exact sequences* *for E and F).*

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

Proof: We have $E \subset A$ where A is an abelian surface. By the Poincaré reducibility theorem [Mi, Proposition 12.1] there is an elliptic curve $F \subset A$ complementary to E, i.e. $\Delta = E \cap F$ is finite and $E + F = A$. Let $F' = A/E$ and $E' = A/F$. Then the diagonal maps ϕ and ψ in the following commutative diagram are isogenies with kernel Δ.

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

There is a commutative diagram with exact rows

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

Taking the long exact sequence of Galois cohomology gives

$$\begin{tikzcd}
F(\mathbb{Q}) \arrow[r, "\psi"] & F'(\mathbb{Q}) \arrow[r] \arrow[d, equal] & H^1(\mathbb{Q}, \Delta) \arrow[d] & \\
 & F'(\mathbb{Q}) \arrow[r, "\pi"] & H^1(\mathbb{Q}, E) \arrow[r, "\iota_*"] & H^1(\mathbb{Q}, A)
\end{tikzcd}$$

and so a commutative diagram

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

where the image of π is $\mathrm{Vis}_A\, H^1(\mathbb{Q}, E)$. In particular there exists $P' \in F'(\mathbb{Q})$ with $\pi(P') = \xi$.

Since $\xi \in H^1(\mathbb{Q}, E)$ has order n, every prime factor ℓ of n must also divide $\deg \psi = |\Delta|$. We are assuming that E has irreducible ℓ-torsion for all primes ℓ dividing n. Therefore E and F are ℓ-congruent, and so in particular F has irreducible ℓ-torsion. We can now factor ψ as $\psi' \circ [m]$ where m is an integer with the same prime factors as n, and ψ' is an isogeny of degree coprime to n. Since ξ has order n we can replace P' by an integer multiple so that $P' = \psi'(P)$ for some $P \in F(\mathbb{Q})$. Then by the commutative diagram

$$\begin{tikzcd} F(\mathbb{Q}) \arrow[r, "m"] \arrow[d, equal] & F(\mathbb{Q}) \arrow[r] \arrow[d, "\psi'"] & H^1(\mathbb{Q}, F[m]) \arrow[d] \\ F(\mathbb{Q}) \arrow[r, "\psi"] & F'(\mathbb{Q}) \arrow[r] & H^1(\mathbb{Q}, \Delta) \end{tikzcd}$$

we have $\pi_m(P) = \pi(P') = \xi$. Again since ξ has order n it follows that m is a multiple of n. $\square$

Theorem 3.2. *Let $E/\mathbb{Q}$ be an elliptic curve and let $E, E_1, \dots, E_t$ be representatives for the isogeny classes of elliptic curves n-congruent to E. Suppose that*

(i) *$E[\ell]$ is irreducible for all primes ℓ dividing n, and*
(ii) $\operatorname{rank} E(\mathbb{Q}) = 0$.

If some of the E_i have positive rank then further assume that

(iii) *the only automorphisms of the Galois module $E[n]$ are scalar multiplications by integers coprime to n, and*
(iv) *for each prime ℓ dividing n, none of the E_i of positive rank is ℓ^{k+1}-congruent to E where ℓ^k is the exact power ℓ dividing n.*

Then the number of elements in $H^1(\mathbb{Q}, E)$ of order n that are visible in an abelian surface is at most $\sum_{i=1}^t \nu_i$ where ν_i is the number of elements of order n in $E_i(\mathbb{Q})/nE_i(\mathbb{Q})$.

Proof: Suppose $\xi \in H^1(\mathbb{Q}, E)$ has order n and is visible in an abelian surface. Then the elliptic curve $F/\mathbb{Q}$ constructed in Theorem 3.1 is isogenous to either E or one of the E_i. By (i) the torsion subgroup of $F(\mathbb{Q})$ has order coprime to m. So if F has rank 0 then $F(\mathbb{Q})/mF(\mathbb{Q}) = 0$ contradicting that ξ is non-zero. Therefore F has positive rank. By (ii) it is isogenous to one of the E_i. Then by (iv) we have $m = n$. Therefore ξ is in the image of

$$\pi_n : F(\mathbb{Q})/nF(\mathbb{Q}) \to H^1(\mathbb{Q}, E)[n].$$

To complete the proof we note that this image depends only on the isogeny class of F. Indeed by (i) all isogenies are of degree coprime to n, and by (iii) the isomorphism $E[n] \cong F[n]$ (used in the definition of π_n) is unique up to scalars. $\square$

We apply Theorem 3.2 with $E, E_1, \ldots, E_t$ the elliptic curves constructed in Theorem 2.2 (case $n = 6$) or Theorem 2.5 (case $n = 7$). Conditions (i) and (iv) are satisfied in all these cases as is seen by factoring division polynomials, respectively comparing a few traces of Frobenius. Condition (iii) is also satisfied since a non-trivial automorphism of $E[n]$ would have generated additional rational points on $X_E(n)$ and $X_E^-(n)$.

4. Examples

Let $n = 6$ or 7. In this section we construct some elements of order n in the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ that are not visible in an abelian surface. We first give an example in the case $n = 6$.

Example 4.1. Let $E = E_{-239}$ and $F = E_{239}$ where

$$E_d : y^2 = x^3 - 6d^2x + 6d^3.$$

We have $\operatorname{rank} E(\mathbb{Q}) = 0$ and $\operatorname{rank} F(\mathbb{Q}) = 1$. The Birch Swinnerton-Dyer conjecture predicts that $Ш(E/\mathbb{Q})$ has order 36, in which case (by properties of the Cassels pairing) it is isomorphic to $(\mathbb{Z}/6\mathbb{Z})^2$. We use 2-descent and 3-descent in Magma [BCP] to check that $Ш(E/\mathbb{Q})$ does indeed contain a subgroup $(\mathbb{Z}/6\mathbb{Z})^2$. Explicitly, we find a subgroup $(\mathbb{Z}/2\mathbb{Z})^2 \subset S^{(2)}(E/\mathbb{Q})$ whose non-trivial elements are represented by the double covers of $\mathbb{P}^1$

$$\begin{aligned} y^2 &= -66x^4 - 606x^3 - 180x^2 + 485x - 144, \\ y^2 &= -478x^4 - 1912x^3 + 1912x - 956, \\ y^2 &= -79x^4 + 1364x^3 - 1008x^2 - 3392x - 1640, \end{aligned} \tag{4.1}$$

and a subgroup $(\mathbb{Z}/3\mathbb{Z})^2 \subset S^{(3)}(E/\mathbb{Q})$ whose inverse pairs of non-trivial elements are represented by the plane cubics

$$\begin{aligned} -8x^3 + 9x^2y + 2x^2z - 6xy^2 + 28xyz + 8xz^2 + 18y^3 + 17y^2z - yz^2 + 15z^3 &= 0, \\ 3x^3 - 12x^2y - 4x^2z - 11xy^2 - 26xyz + 9xz^2 - 10y^3 + 8y^2z - 34yz^2 - 25z^3 &= 0, \\ 10x^3 + x^2y + 14x^2z - 8xy^2 - 2xyz + 38xz^2 + 10y^3 - 23y^2z + 36yz^2 + 11z^3 &= 0, \\ 2x^3 - 5x^2y + 12xy^2 + 6xyz + 52xz^2 + 9y^3 + 4y^2z + 33yz^2 + 25z^3 &= 0. \end{aligned}$$

The formulae in [CrFi] and [F2] may be used to check that these genus one curves do indeed represent distinct Selmer group elements. Since $E(\mathbb{Q}) = 0$ it follows that $Ш(E/\mathbb{Q})$ contains a subgroup $(\mathbb{Z}/6\mathbb{Z})^2$ as claimed.

By Theorem 2.2 the only elliptic curves 6-congruent to E are E and F. Theorem 3.2 then shows that there are at most 2 elements of order 6 in

$H^1(\mathbb{Q}, E)$ that are visible in an abelian surface. Therefore $Ш(E/\mathbb{Q})$ contains elements of order 6 that are not visible in an abelian surface.

Remark 4.2. The first of the double covers in (4.1) has rational point $(x, y) = (0, 12\sqrt{-1})$. It is therefore visible in an abelian surface isogenous to $E \times F$. Using the methods in [F3, Sections 14 and 15] we were able to check the same for the first of the plane cubics. Therefore there are exactly 2 elements of order 6 in $H^1(\mathbb{Q}, E)$ that are visible in an abelian surface. Moreover we have shown that these elements belong to $Ш(E/\mathbb{Q})$.

Remark 4.3. It would have simplified Example 4.1 had we chosen d so that E_d and E_{-d} both have rank 0. However a root number calculation shows (conditional on the Birch Swinnerton-Dyer conjecture) that the ranks of these curves always have opposite parity.

Next we give some examples in the case $n = 7$.

Example 4.4. Let E_d be the quadratic twist of E by d where $(E, d) = (288a, 843), (864a, -537)$ or $(864b, -554)$. In each of these cases $\operatorname{rank} E_d(\mathbb{Q}) = 0$ and the Birch Swinnerton-Dyer conjecture (together with the Cassels pairing) predicts that $Ш(E_d/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^2$. The complete list of elliptic curves 7-congruent to E is recorded in Theorem 2.5. Taking quadratic twists by d gives the complete list of elliptic curves 7-congruent to E_d. Each of these curves has rank 0. It follows by Theorem 3.2 that there are no elements of order 7 in $H^1(\mathbb{Q}, E)$ that are visible in an abelian surface. Therefore, conditional on the Birch Swinnerton-Dyer conjecture, $Ш(E_d/\mathbb{Q})$ contains elements of order 7 that are not visible in an abelian surface.

Example 4.5. Let E_d be the quadratic twist of E by d where $(E, d) = (27a, -373), (864a, 587), (864b, -163), (864c, -427), (1323m, 251), (14688d, 239), (56160h, -199), (477792*, 82)$ or $(844128*, -51)$. In each of these cases $\operatorname{rank} E_d(\mathbb{Q}) = 0$ and the Birch Swinnerton-Dyer conjecture (together with the Cassels pairing) predicts that $Ш(E_d/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^2$. The complete list of elliptic curves 7-congruent to E_d are the quadratic twists of those listed in Theorem 2.5. Each of these curves has rank 0 or 1. It follows by Theorem 3.2 that there are at most 12 elements of order 7 in $H^1(\mathbb{Q}, E)$ that are visible in an abelian surface. Therefore, conditional on the Birch Swinnerton-Dyer conjecture, $Ш(E_d/\mathbb{Q})$ contains elements of order 7 that are not visible in an abelian surface. The example with $(E, d) = (27a, -373)$ is made unconditional by the descent calculation in Section 6, and the example with $(E, d) = (864a, 587)$ is made unconditional in Example 5.4.

5. Visibility in abelian threefolds

In Section 4 we gave some examples of elements of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ that are not visible in an abelian surface. In this section we show that some of these examples are visible in an abelian threefold, and so have visibility dimension exactly 3.

Lemma 5.1. *Let $E/\mathbb{Q}$ be an elliptic curve, and let $\xi, \eta \in H^1(\mathbb{Q}, E)$. Then* $\operatorname{vis\,dim}(\xi + \eta) \leq \operatorname{vis\,dim}(\xi) + \operatorname{vis\,dim}(\eta) - 1$.

Proof: If ξ and η are visible in abelian varieties A and B then $\xi + \eta$ is visible in $(A \times B)/E$. □

By the results cited in the introduction we know that every element of $Ш(E/\mathbb{Q})$ or order 2 or 3 is visible in an abelian surface. It follows by Lemma 5.1 that every element of order 6 is visible in an abelian threefold. Therefore the elements constructed in Example 4.1 that are not visible in an abelian surface have visibility dimension exactly 3.

Proposition 5.2. *Let E and F be n-congruent elliptic curves over $\mathbb{Q}$. Suppose that n is odd and that E and F have good reduction at all primes dividing n. If $E(\mathbb{Q})/nE(\mathbb{Q}) = 0$ and all Tamagawa numbers of E are coprime to n then there is an injective group homomorphism*

$$(F^0(\mathbb{Q}) + nF(\mathbb{Q}))/nF(\mathbb{Q}) \to \operatorname{Vis}_A Ш(E/\mathbb{Q})$$

where A is an abelian surface isogenous to $E \times F$, and $F^0(\mathbb{Q}) \subset F(\mathbb{Q})$ is the subgroup of points with everywhere good reduction.

Proof: If all Tamagawa numbers of F are coprime to n then this is a special case of [AS1, Theorem 3.1]. The general case is proved in exactly the same way. □

Example 5.3. We computed the conjectural order of the Tate-Shafarevich group for all rank 0 quadratic twists E_d of $E = 32544b$ for square-free $d \in \mathbb{Z}$ with $|d| \leq 500$. The conjectural order of $Ш(E_d/\mathbb{Q})$ was divisible by 7 for $d = -26$, 61, 95, ± 129, 157, -195, -239, ± 311, ± 321, ± 335, ± 341, ± 365, -370 and -391. In each of these cases the quadratic twist F_d of $F = 288a$ has rank 2. Moreover E_d and F_d have good reduction at 7 and all Tamagawa numbers are coprime to 7. It follows by Proposition 5.2 that $Ш(E_d/\mathbb{Q})$ contains a subgroup $(\mathbb{Z}/7\mathbb{Z})^2$ that is visible in an abelian surface.

Example 5.4. The quadratic twists by d of $864a$, $14688d$ and $56160h$ are

$$\begin{aligned} E_d: &\quad y^2 = x^3 - 3d^2x + 6d^3, \\ F_d: &\quad y^2 = x^3 - 228813d^2x - 42127856d^3, \\ G_d: &\quad y^2 = x^3 + 16968d^2x + 35415344d^3. \end{aligned}$$

Taking $d = 587$ we have $\operatorname{rank} E_d(\mathbb{Q}) = 0$ and $\operatorname{rank} F_d(\mathbb{Q}) = \operatorname{rank} G_d(\mathbb{Q}) = 1$. The rank one curves F_d and G_d have generators

$$P_1 = (4571513149/87^2, 266824295540902/87^3)$$

and

$$P_2 = (-3374364792784191/145744^2, -146042290272854197531103/145744^3).$$

The elliptic curves E_d, F_d, G_d have good reduction at 7, and all Tamagawa numbers are coprime to 7, except for $c_{17}(F_d) = 7$ and $c_{13}(G_d) = 7$. We find that P_1 reduces to a smooth point mod 17, and P_2 reduces to a smooth point mod 13. It follows by Proposition 5.2 that $Ш(E_d/\mathbb{Q})$ contains two cyclic subgroups of order 7 consisting of elements that are visible in an abelian surface. We claim that the these two subgroups are different. Indeed if they were the same then the $E_d[7]$-torsors $[7]^{-1}P_1$ and $[7]^{-1}P_2$ would be isomorphic (as sets with Galois action). However reducing mod 71 we find that $\widetilde{P}_1 \in 7\widetilde{F}_d(\mathbb{F}_{71})$ yet $\widetilde{P}_2 \notin 7\widetilde{G}_d(\mathbb{F}_{71})$. It follows by Example 4.5 and Lemma 5.1 that there are elements of order 7 in $Ш(E_d/\mathbb{Q})$ with visibility dimension 3.

Remark 5.5. To make Example 4.5 unconditional in the case $(E, d) = (864a1, 587)$ it suffices to work with just one of the curves F_d and G_d in Example 5.4. Indeed E_d has analytic rank 0 and so $Ш(E_d/\mathbb{Q})$ is finite by Kolyvagin's theorem. The Cassels pairing is therefore nondegenerate. So once we show that $Ш(E_d/\mathbb{Q})$ contains a subgroup $\mathbb{Z}/7\mathbb{Z}$ it must in fact contain a subgroup $(\mathbb{Z}/7\mathbb{Z})^2$.

6. A descent calculation

In this section we carry out the descent calculation necessary to make Example 4.5 unconditional in the case $(E, d) = (27a, -373)$.

Let D_λ be the elliptic curve

$$y^2 + (1 + \lambda - \lambda^2)xy + (\lambda^2 - \lambda^3)y = x^3 + (\lambda^2 - \lambda^3)x^2$$

with 7-torsion point $P = (0, 0)$. Let $\widehat{\phi} : D_\lambda \to C_\lambda$ be the isogeny with kernel generated by P. By properties of the Weil pairing, the dual isogeny $\phi : C_\lambda \to D_\lambda$ has kernel isomorphic to μ_7 as a Galois module.

Let K be a number field and $\mathfrak{p}$ a prime of K. Taking Galois cohomology of the exact sequences $0 \to \mu_7 \to C_\lambda \to D_\lambda \to 0$ and $0 \to \mathbb{Z}/7\mathbb{Z} \to D_\lambda \to C_\lambda \to 0$ gives exact sequences

$$\ldots \longrightarrow C_\lambda(K_\mathfrak{p}) \longrightarrow D_\lambda(K_\mathfrak{p}) \xrightarrow{\delta_\mathfrak{p}} K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^7 \longrightarrow \ldots$$
$$\ldots \longrightarrow D_\lambda(K_\mathfrak{p}) \longrightarrow C_\lambda(K_\mathfrak{p}) \xrightarrow{\delta'_\mathfrak{p}} \mathrm{Hom}(G_\mathfrak{p}, \mathbb{Z}/7\mathbb{Z}) \longrightarrow \ldots$$

where $G_\mathfrak{p} = \mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p})$. Let $\mathcal{O}_\mathfrak{p} \subset K_\mathfrak{p}$ be the valuation ring and $I_\mathfrak{p} \subset G_\mathfrak{p}$ the inertia subgroup.

Lemma 6.1. *If* $\lambda \in \mathcal{O}_\mathfrak{p}$ *with* $\lambda(\lambda-1)(\lambda^3 - 8\lambda^2 + 5\lambda + 1) \not\equiv 0 \pmod{\mathfrak{p}}$ *then* $\mathrm{im}\,\delta_\mathfrak{p} = \mathcal{O}_\mathfrak{p}^\times/(\mathcal{O}_\mathfrak{p}^\times)^7$ *and* $\mathrm{im}\,\delta'_\mathfrak{p} = \mathrm{Hom}(G_\mathfrak{p}/I_\mathfrak{p}, \mathbb{Z}/7\mathbb{Z})$.

Proof: The first part is [F1, Proposition 3.12(b)]. The second part follows by Tate local duality, as described in [F1, Section 1.4]. □

We compute the 7-Selmer group $S^{(7)}(E_d/\mathbb{Q})$ where $E_d : y^2 = x^3 + 16d^3$ is the quadratic twist of $E = 27a3$ by d. Let $K = \mathbb{Q}(\zeta_3)$ and $L = K(\alpha, \beta)$ where $\alpha^2 = -d(5 + \zeta_3)$ and $\beta^3 = 1 + 3\zeta_3$. Then E_d has a 7-torsion point defined over L given by

$$T = \left(4(2 + 3\zeta_3)\beta^2 d/7, 4(1 + 5\zeta_3)\alpha d/7\right).$$

Let $\chi : \mathrm{Gal}(L/K) \cong (\mathbb{Z}/7\mathbb{Z})^\times$ be the character such that $\sigma(T) = \chi(\sigma)T$ for all $\sigma \in G_K$. Explicitly $\chi : \sigma_3 \mapsto 3$ where $\sigma_3(\alpha) = -\alpha$ and $\sigma_3(\beta) = \zeta_3\beta$. For A a $\mathbb{F}_7[G_K]$-module (written multiplicatively) we write

$$A^\chi = \{a \in A : \sigma(a) = a^{\chi(\sigma)} \text{ for all } \sigma \in G_K\}.$$

The prime 7 splits in K as $7\mathcal{O}_K = \mathfrak{q}\mathfrak{q}'$ where $\mathfrak{q} = (2 - \zeta_3)$ and $\mathfrak{q}' = (3 + \zeta_3)$. The first of these primes ramifies completely in L, say $\mathfrak{q}\mathcal{O}_L = \mathfrak{Q}^6$.

Theorem 6.2. *The* 7*-Selmer group of* $E_d : y^2 = x^3 + 16d^3$ *is*

$$S^{(7)}(E_d/\mathbb{Q}) \cong \left\{ \theta \in (L^\times/(L^\times)^7)^\chi \;\middle|\; \begin{array}{c} \mathrm{ord}_\mathfrak{P}(\theta) \equiv 0 \pmod 7 \text{ for all primes } \mathfrak{P} \\ \text{and } L_\mathfrak{Q}(\sqrt[7]{\theta})/L_\mathfrak{Q} \text{ is unramified} \end{array} \right\}.$$

Proof: The elliptic curve E_d has complex multiplication by $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$, explicitly $\zeta_3 : (x, y) \mapsto (\zeta_3 x, y)$.

Working over K we have $E_d[7] \cong E_d[2 - \zeta_3] \times E_d[3 + \zeta_3]$. Therefore by the inflation-restriction exact sequence $H^1(\mathbb{Q}, E_d[7]) \cong H^1(K, E_d[3 + \zeta_3])$. The torsion point $T \in E_d(L)$ defined above satisfies $\zeta_3 T = 2T$. So working over L we have $E_d[2 - \zeta_3] \cong \mathbb{Z}/7\mathbb{Z}$ and $E_d[3 + \zeta_3] \cong \mu_7$. Again by the inflation-restriction exact sequence

$$H^1(K, E_d[3 + \zeta_3]) \cong H^1(L, E_d[3 + \zeta_3])^{\mathrm{Gal}(L/K)} \cong (L^\times/(L^\times)^7)^\chi.$$

The Selmer group $S^{(7)}(E_d/\mathbb{Q}) \cong S^{(3+\zeta_3)}(E_d/K)$ is the subgroup of elements satisfying suitable local conditions. To determine these local conditions we may work over L, or even $L(\zeta_7) = \mathbb{Q}(E_d[7])$. (This is because any field extension of degree coprime to 7 does not affect local solubility.)

Taking $\lambda = -\zeta_3$ we find that $E_d \cong C_\lambda \cong D_\lambda$ over L and $\lambda^3 - 8\lambda^2 + 5\lambda + 1 = -\zeta_3^2(2-\zeta_3)^2$. We may further identify $[3+\zeta_3] : E_d \to E_d$ with $\phi : C_\lambda \to D_\lambda$. It follows by Lemma 6.1 that for all primes $\mathfrak{P} \neq \mathfrak{Q}$ the local conditions are as stated. Next we take $\lambda = -\zeta_3^2$ and note that over $L(\zeta_7)$ we may identify $[3+\zeta_3] : E_d \to E_d$ with $\widehat{\phi} : D_\lambda \to C_\lambda$. The local condition at $\mathfrak{Q}$ is now computed using the second part of Lemma 6.1. $\square$

Remark 6.3. If $(-d/7) = 1$ then $L_\mathfrak{Q} \cong \mathbb{Q}_7(\zeta_7)$. If moreover $\mathrm{ord}_\mathfrak{Q}(\theta) = 0$ then, by [CaFr, Exercises 2.12 and 2.13], the condition that $L_\mathfrak{Q}(\sqrt[7]{\theta})/L_\mathfrak{Q}$ is unramified is equivalent to $\theta^6 \equiv 1 \pmod{\mathfrak{Q}^7}$.

Example 6.4. Taking $d = -373$ we find using Magma that $S^{(7)}(E_d/\mathbb{Q})$ contains a subgroup $(\mathbb{Z}/7\mathbb{Z})^2$ generated by

$$\begin{aligned}
\theta_1 = &\left(\tfrac{1}{3}(25429\zeta_3 - 3109)\alpha + \tfrac{1}{3}(890126\zeta_3 - 68339)\right)\beta^2 \\
&+ \left(\tfrac{1}{3}(-43303\zeta_3 - 15062)\alpha + \tfrac{1}{3}(-1416721\zeta_3 - 546368)\right)\beta \\
&+ (19674\zeta_3 + 15329)\alpha + \tfrac{1}{3}(1967327\zeta_3 + 1525714), \\
\theta_2 = &\left(\tfrac{1}{3}(-10669\zeta_3 - 43556)\alpha + (272381\zeta_3 + 758092)\right)\beta^2 \\
&+ \left(\tfrac{1}{3}(-41063\zeta_3 - 49348)\alpha + (777437\zeta_3 + 853903)\right)\beta \\
&+ (-27508\zeta_3 - 13416)\alpha + (1400286\zeta_3 + 630112).
\end{aligned}$$

Since $E_d(\mathbb{Q}) = 0$ it follows that $\text{Ш}(E_d/\mathbb{Q})$ contains a subgroup $(\mathbb{Z}/7\mathbb{Z})^2$.

Acknowledgements

I would like to thank Michael Stoll for suggesting that the methods in [PSS] might be used to give examples of the form considered in this paper. All computer calculations were performed using Magma [BCP].

References

[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.

[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 the Magma home page at `http://magma.maths.usyd.edu.au/magma/`

[CaFr] J W.S. Cassels and A. Fröhlich (eds.), Algebraic number theory, Academic Press, London, 1967.

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

[CrFi] J.E. Cremona and T.A. Fisher, On the equivalence of binary quartics, *J. Symbolic Comput.* 44 (2009), no. 6, 673–682.

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

[D] H. Darmon, Serre's conjectures, in *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, 135–153, CMS Conf. Proc., 17, Amer. Math. Soc., Providence, RI, 1995.

[F1] T.A. Fisher, *On 5 and 7 Descents for Elliptic Curves*, PhD thesis, University of Cambridge, 2000, `http://www.dpmms.cam.ac.uk/~taf1000/thesis.html`

[F2] T.A. Fisher, Testing equivalence of ternary cubics, in *Algorithmic number theory (ANTS VII)*, F. Hess, S. Pauli, M. Pohst (eds.), Lecture Notes in Comput. Sci. 4076, Springer, 2006, 333-345.

[F3] T.A. Fisher, The Hessian of a genus one curve, *Proc. Lond. Math. Soc.* (3) 104 (2012) 613-648.

[F4] T.A. Fisher, *On families of n-congruent elliptic curves*, preprint, `http://arxiv.org/abs/1105.1706`

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

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

[Mi] J.S. Milne, Abelian varieties, in *Arithmetic geometry*, G. Cornell and J.H. Silverman (eds.), 103–150, Springer, New York, 1986.

[P] I. Papadopoulos, Courbes elliptiques ayant même 6-torsion qu'une courbe elliptique donnée, *J. Number Theory* 79 (1999), no. 1, 103–114.

[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.

[RS] K. Rubin and A. Silverberg, Mod 6 representations of elliptic curves, in *Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996)*, 213–220, Proc. Sympos. Pure Math., 66, Part 1, Amer. Math. Soc., Providence, RI, 1999.

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

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