ON FAMILIES OF 9-CONGRUENT ELLIPTIC CURVES

TOM FISHER

Abstract. We compute equations for the families of elliptic curves 9-congruent to a given elliptic curve. We use these to find infinitely many non-trivial pairs of 9-congruent elliptic curves over $\mathbb{Q}$, i.e. pairs of non-isogenous elliptic curves over $\mathbb{Q}$ whose 9-torsion subgroups are isomorphic as Galois modules.

Introduction

Elliptic curves E_1 and E_2 are *n-congruent* if their n-torsion subgroups $E_1[n]$ and $E_2[n]$ are isomorphic as Galois modules. They are *directly n-congruent* if the isomorphism $\phi : E_1[n] \to E_2[n]$ respects the Weil pairing e_n and *reverse n-congruent* if $e_n(\phi P, \phi Q) = e_n(P, Q)^{-1}$ for all $P, Q \in E_1[n]$. The elliptic curves directly and reverse n-congruent to a given elliptic curve E are parametrised by the modular curves $Y_E(n) = X_E(n) \setminus \{\text{cusps}\}$ and $Y_E^-(n) = X_E^-(n) \setminus \{\text{cusps}\}$. Finding equations for these modular curves can help with finding non-trivial pairs of n-congruent elliptic curves. Some of the potential applications are described in [1], [3], [8], [13], [19].

Equations for $X_E(n)$, and the family of curves it parametrises, have been computed for $n = 2, 3, 4, 5, 6, 7, 8, 11$ by Rubin and Silverberg [20], [21], [22], [23], Papadopoulos [18], Halberstadt and Kraus [14], Chen [6], and Fisher [12]. The analogous problem for n-congruences that do not respect the Weil pairing has been solved for the same values of n. The additional references for this include papers by Fisher [10], [11], Bruin and Doerksen [4, Section 7], and Poonen, Schaefer and Stoll [19, Section 7.2].

In this paper we treat the case $n = 9$. That is, we give equations for $X_E(9)$ and $X_E^-(9)$, and for the families of curves they parametrise. We use these formulae to exhibit non-trivial triples of 9-congruent elliptic curves over $\mathbb{Q}$, and non-trivial pairs of 9-congruent elliptic curves over $\mathbb{Q}(T)$. We also give equations for the modular diagonal quotient surfaces whose points parametrise pairs of 9-congruent elliptic curves.

We work over a field K of characteristic 0. We write $\overline{K}$ for the algebraic closure, and ζ_n for a primitive nth root of unity.

Date: 2nd June 2015.

1. Statement of results

If $n = 3$ or 9 then every element of $(\mathbb{Z}/n\mathbb{Z})^\times$ is either plus or minus a square. Therefore any pair of n-congruent elliptic curves are either directly or reverse n-congruent. In the case $n = 3$, we have $X_E^\pm(3) \cong \mathbb{P}^1$ and the families of curves parametrised are as follows.

Theorem 1.1. *Let E/K be the elliptic curve $y^2 = x^3 - 27c_4x - 54c_6$. Then the family of elliptic curves parametrised by $Y_E^\pm(3)$ is*

$$y^2 = x^3 - 27A^\pm(r,s)x - 54B^\pm(r,s) \tag{1}$$

where

$$\begin{aligned} A^+(r,s) &= c_4r^4 + 4c_6r^3s + 6c_4^2r^2s^2 + 4c_4c_6rs^3 - (3c_4^3 - 4c_6^2)s^4, \\ B^+(r,s) &= c_6r^6 + 6c_4^2r^5s + 15c_4c_6r^4s^2 + 20c_6^2r^3s^3 \\ &\qquad + 15c_4^2c_6r^2s^4 + 6(3c_4^4 - 2c_4c_6^2)rs^5 + (9c_4^3c_6 - 8c_6^3)s^6, \end{aligned}$$

and

$$\begin{aligned} A^-(r,s) &= -4(r^4 - 6c_4r^2s^2 - 8c_6rs^3 - 3c_4^2s^4)/(c_4^3 - c_6^2), \\ B^-(r,s) &= -8B^+(r,s)/(c_4^3 - c_6^2)^2. \end{aligned}$$

Proof. In the direct case this family of curves was first computed by Rubin and Silverberg [20]. The above formulae are taken from [10, Sections 8, 9 and 13], with $(r,s) = (\lambda,\mu)$, respectively $(r,s) = (c_6\xi + c_4^2\eta, -c_4\xi - c_6\eta)$. These formulae are available in Magma [2] via the function `HessePolynomials`. □

Our new results are in the case $n = 9$, where the curves $X_E^\pm(9)$ have genus 10. We write these curves as the complete intersection of two cubics in $\mathbb{P}^3$.

Theorem 1.2. *Let E/K be the elliptic curve $y^2 = x^3 + ax + b$. Then $X_E^\pm(9) = \{F_1^\pm = F_2^\pm = 0\} \subset \mathbb{P}^3$ where*

$$\begin{aligned} F_1^+(x,y,z,t) &= x^2t + 6xyz + 6bxt^2 + 6y^3 - 9ay^2t + 6a^2yt^2 - 3bz^3 \\ &\qquad + 3a^2z^2t + 9abzt^2 - (a^3 - 12b^2)t^3, \\ F_2^+(x,y,z,t) &= x^2z + 6xy^2 - 6axyt + 2a^2xt^2 - 9ay^2z - 18byz^2 + 12a^2yzt \\ &\qquad + a^2z^3 + 9abz^2t - 3a^3zt^2 + a^2bt^3, \end{aligned}$$

and

$$\begin{aligned} F_1^-(x,y,z,t) &= 9x^2y + 3x^2z - 6axyt + 6bxt^2 - 6ay^3 + 27by^2t + 3ayz^2 \\ &\qquad + 18byzt + 3a^2yt^2 + az^3 + 3bz^2t + a^2zt^2 - abt^3, \\ F_2^-(x,y,z,t) &= x^3 + 6axyz + 18bxyt + 3axz^2 + 6bxzt + a^2xt^2 + 9by^3 + 6a^2y^2t \\ &\qquad - 9byz^2 + 6a^2yzt - 3abyt^2 - 4bz^3 + 2a^2z^2t + 2b^2t^3. \end{aligned}$$

The families of curves parametrised by $X_E(9)$ and $X_E^-(9)$ are given by Theorem 1.1 and the following. By abuse of notation we write P both for a point in $\mathbb{P}^3$ and for a vector representing this point.

Theorem 1.3. *Let $X_E^{\pm}(3)$ and $X_E^{\pm}(9)$ be as described in Theorems 1.1 and 1.2, with $a = -27c_4$ and $b = -54c_6$. For $P \in X_E^{\pm}(9)$ with tangent line $P + \lambda Q$ we write $F_i^{\pm}(P + \lambda Q) = \gamma_i \lambda^2 + \delta_i \lambda^3$ for $i = 1, 2$. Then the forgetful map $X_E^{\pm}(9) \to X_E^{\pm}(3)$ is given by $(r : s) = (\gamma_2 : 3\gamma_1)$.*

Let $\mathcal{Z}(n)$ be the modular diagonal quotient surface whose points parametrise pairs of directly n-congruent elliptic curves, and likewise $\mathcal{Z}^-(n)$ in the reverse case. It is shown in [15, Theorem 4] that the surfaces $\mathcal{Z}^{\pm}(9)$ are each birational over $\mathbb{C}$ to an elliptic surface. Using Theorem 1.2 we are able to determine these elliptic surfaces explicitly.

Theorem 1.4. *The surface $\mathcal{Z}(9)$ is birational over $\mathbb{Q}$ to the elliptic surface*

$$\begin{aligned} y^2 + (6T^2 + 3T + 2)xy + T^2(T + 1)(4T^3 + 9T + 9)y& \\ = x^3 - (16T^4 + 12T^3 + 9T^2 + 6T + 1)x^2&. \end{aligned}$$

The surface $\mathcal{Z}^-(9)$ is birational over $\mathbb{Q}$ to the elliptic surface

$$\begin{aligned} y^2 + (12T^3 + 3T^2 - 6)xy + (T - 1)^3(T^3 - 1)(4T^3 - 3T - 7)y& \\ = x^3 - 3(T + 1)(T^3 - 1)(9T^2 + 2T + 1)x^2&. \end{aligned}$$

We use these results to prove [15, Conjecture 5] in the case $n = 9$.

Theorem 1.5. *There are infinitely many non-trivial pairs of directly 9-congruent elliptic curves over $\mathbb{Q}$, and these have infinitely many distinct pairs of j-invariants. By "non-trivial" we mean that the elliptic curves are not isogenous. The same result holds in the reverse case.*

Proof. For each positive integer m there are finitely many curves on $\mathcal{Z}^{\pm}(9)$ corresponding to pairs of elliptic curves related by a cyclic isogeny of degree m. Each of these curves comes with a non-constant morphism to $X_0(m)$ and so has positive genus for m sufficiently large. The elliptic surfaces in Theorem 1.4 each have a $\mathbb{Q}$-rational section of infinite order given by $(x, y) = (0, 0)$. Therefore the surfaces $\mathcal{Z}^{\pm}(9)$ each contain infinitely many curves birational to $\mathbb{P}^1$ over $\mathbb{Q}$. Since these curves have genus 0, we know by the above remarks that only finitely many correspond to pairs of isogenous elliptic curves. It follows that there are non-trivial pairs of 9-congruent elliptic curves over $\mathbb{Q}(T)$. In Section 6 we give a more explicit version of this first part of the proof by using Theorem 1.2 to exhibit some non-trivial pairs of 9-congruent elliptic curves over $\mathbb{Q}(T)$.

The proof is completed by specialising T to a rational number. In this way we obtain infinitely many pairs of elliptic curves that are not m-isogenous for any $m \leq d$ (for any fixed d). We are done by the theorem of Mazur [17], extended to composite m by Kenku [16], that any cyclic isogeny defined over $\mathbb{Q}$ has degree $m \leq 163$. $\square$

2. The modular curves $X(3)$ and $X(9)$

Let $M = \mu_n \times \mathbb{Z}/n\mathbb{Z}$ equipped with the pairing

$$\langle (\zeta, a), (\xi, b) \rangle = \zeta^b \xi^{-a}.$$

The modular curve $Y(n) = X(n) \backslash \{\text{cusps}\}$ parametrises pairs (E, ϕ) where E is an elliptic curve and $\phi : E[n] \to M$ is a symplectic isomorphism, i.e. an isomorphism that matches up the Weil pairing on $E[n]$ with the pairing $\langle \ , \ \rangle$ on M. We identify $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ with the group of symplectic automorphisms of M. There is then a natural action of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})/\{\pm I\}$ on $X(n)$ with quotient the j-line.

In the case $n = 3$ it is well known that $Y(3) = \mathbb{A}^1 \setminus \{t^3 = 1\}$ parametrises the non-singular fibres in the Hesse pencil of plane cubics:

$$\{x^3 + y^3 + z^3 - 3txyz = 0\} \subset \mathbb{P}^2. \tag{2}$$

We need an analogous result in the case $n = 9$.

Lemma 2.1. *The modular curve $X(9)$ has equations*

$$X(9) = \left\{ \begin{array}{l} a^2b + b^2c + c^2a = 0 \\ ab^2 + bc^2 + ca^2 = d^3 \end{array} \right\} \subset \mathbb{P}^3. \tag{3}$$

Moreover the forgetful map $X(9) \to X(3)$ is given by

$$t = -(a^3 + b^3 + c^3 + 6abc)/(3d^3). \tag{4}$$

Proof. In [12, Section 2] we showed, following work of Klein, Vélu and others, that if $n \geq 5$ is an odd integer then $Y(n) \subset Z(n)$ where $Z(n) \subset \mathbb{P}^{n-1}$ is defined as follows. We take co-ordinates $(a_0 : a_1 : \ldots : a_{n-1})$ on $\mathbb{P}^{n-1}$ and agree to read all subscripts mod n. Then $Z(n)$ is defined by $a_0 = 0$, $a_{n-i} = -a_i$ and

$$\operatorname{rank}(a_{i-j}a_{i+j})_{i,j=0}^{n-1} \leq 2.$$

In the case $n = 9$ we put

$$(a_0 : a_1 : \ldots : a_8) = (0 : a : -b : d : c : -c : -d : b : -a). \tag{5}$$

Then $Z(9) \subset \mathbb{P}^3$ is defined by

$$\operatorname{rank}\begin{pmatrix} 0 & -a^2 & -b^2 & -d^2 & -c^2 \\ a^2 & 0 & -ad & bc & cd \\ b^2 & ad & 0 & ac & -bd \\ d^2 & -bc & -ac & 0 & -ab \\ c^2 & -cd & bd & ab & 0 \end{pmatrix} \leq 2,$$

equivalently

$$\begin{aligned} (a^2b + b^2c + c^2a)d &= 0 & \qquad bc^3 - ba^3 - cd^3 &= 0 \\ ab^3 - ac^3 - bd^3 &= 0 & \qquad ca^3 - cb^3 - ad^3 &= 0. \end{aligned}$$

Adding together the last three equations and factoring shows that $Z(9)$ is the union of the curve defined in (3) and four isolated points

$$(0:0:0:1),\ (1:1:1:0),\ (1:\zeta_3:\zeta_3^2:0),\ (1:\zeta_3^2:\zeta_3:0).$$

Since $X(9)$ is a curve, it must therefore be as defined in (3).

Now writing $(x_0 : x_1 : \ldots : x_{n-1})$ for our co-ordinates on $\mathbb{P}^{n-1}$, and again agreeing to read all subscripts mod n, it is shown in [9, Section 3] that the family of elliptic curves parametrised by $Y(n)$ is defined by

$$\operatorname{rank}(a_{i-j}x_{i+j})_{i,j=0}^{n-1} \leq 2.$$

In the case $n = 9$ the elliptic curve E corresponding to $(a : b : c : d) \in Y(9)$ is the curve of degree 9 in $\mathbb{P}^8$ defined by the equations

$$\begin{aligned} adx_0^2 - b^2x_1x_8 + a^2x_2x_7 &= 0 \\ bcx_0^2 + d^2x_1x_8 - a^2x_3x_6 &= 0 \\ cdx_0^2 + c^2x_1x_8 - a^2x_4x_5 &= 0 \end{aligned}$$

and their cyclic permutes. Thus E is defined by a total of 27 quadrics.

Let 0_E be the point on E given by (5). In principle we could complete the proof by putting the elliptic curve $(E, 0_E)$ in Weierstrass form. However it is simpler to argue as follows. The action of $E[9]$ on E by translation is generated by the maps $x_i \mapsto x_{i+1}$ and $x_i \mapsto \zeta_9^i x_i$. From this we see that the morphism

$$(x_0 : x_1 : \ldots : x_8) \mapsto (x : y : z) = (x_0x_3x_6 : x_1x_4x_7 : x_2x_5x_8)$$

quotients out by the action of $E[3]$. We may therefore identify this morphism with the multiplication-by-3 map on E. On the other hand, we find by direct calculation that the image takes the form (2) with t as specified in (4). The forgetful map $X(9) \to X(3)$ is therefore as claimed. $\square$

Remark 2.2. The action of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ on $X(9) \subset \mathbb{P}^3$ is described by a projective representation $\overline{\rho} : \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) \to \mathrm{PGL}_4(\overline{K})$. According to [12, Section 2] it is given on the generators $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ for $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ by

$$\overline{\rho}(S) = \begin{pmatrix} \zeta_9 - \zeta_9^8 & \zeta_9^7 - \zeta_9^2 & \zeta_9^4 - \zeta_9^5 & \zeta_9^3 - \zeta_9^6 \\ \zeta_9^7 - \zeta_9^2 & \zeta_9^4 - \zeta_9^5 & \zeta_9 - \zeta_9^8 & \zeta_9^3 - \zeta_9^6 \\ \zeta_9^4 - \zeta_9^5 & \zeta_9 - \zeta_9^8 & \zeta_9^7 - \zeta_9^2 & \zeta_9^3 - \zeta_9^6 \\ \zeta_9^3 - \zeta_9^6 & \zeta_9^3 - \zeta_9^6 & \zeta_9^3 - \zeta_9^6 & 0 \end{pmatrix} \text{ and } \overline{\rho}(T) = \begin{pmatrix} \zeta_9 & 0 & 0 & 0 \\ 0 & \zeta_9^4 & 0 & 0 \\ 0 & 0 & \zeta_9^7 & 0 \\ 0 & 0 & 0 & \zeta_9^6 \end{pmatrix}.$$

In particular, the action of $\ker\big(\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})\big) \cong (\mathbb{Z}/3\mathbb{Z})^3$ is generated by

$$\begin{aligned} (a:b:c:d) &\mapsto (a:b:c:\zeta_3 d) \\ (a:b:c:d) &\mapsto (b:c:a:d) \\ (a:b:c:d) &\mapsto (\zeta_3 a + b + c : a + \zeta_3 b + c : a + b + \zeta_3 c : (\zeta_3 - 1)d). \end{aligned}$$

It may be checked that the map $X(9) \to X(3)$ in Lemma 2.1 quotients out by this action.

The pencil of cubics defining $X(9) \subset \mathbb{P}^3$ is naturally a copy of $X(3) \cong \mathbb{P}^1$. To explain this, let $F_1 = a^2b + b^2c + c^2a$ and $F_2 = ab^2 + bc^2 + ca^2 - d^3$ be the cubics defining $X(9)$. We write $\mathcal{H}(F)$ for the Hessian matrix of a form F, that is, the matrix of second partial derivatives. Then

$$\det \mathcal{H}(tF_1 - F_2) = -48(t^3 - 1)(a^3 + b^3 + c^3 - 3abc)d. \tag{6}$$

Therefore the Hessian vanishes for just 4 cubics in the pencil, and these correspond to the cusps of $X(3)$. The forgetful map $X(9) \to X(3)$ has the following geometric description.

Lemma 2.3. *For $P \in X(9)$ with tangent line $P + \lambda Q$ we write $F_i(P + \lambda Q) = \gamma_i \lambda^2 + \delta_i \lambda^3$ for $i = 1, 2$. Then the forgetful map $X(9) \to X(3)$ is given by $t = \gamma_2/\gamma_1$.*

Proof. We temporarily write a_1, a_2, a_3, a_4 for a, b, c, d and let Λ be the 4×4 alternating matrix with entries

$$\Lambda_{ij} = \frac{\partial F_1}{\partial a_k}\frac{\partial F_2}{\partial a_l} - \frac{\partial F_1}{\partial a_l}\frac{\partial F_2}{\partial a_k}$$

where (i, j, k, l) is an even permutation of $(1, 2, 3, 4)$. Then specialising Λ at $P = (a : b : c : d) \in X(9)$ gives a matrix whose rows (or columns) span the tangent line at P. Let $D = (a^3 + b^3 + c^3 - 3abc)d$. We find by direct calculation that

$$\Lambda\ \mathcal{H}(F_i)\ \Lambda \equiv \gamma_i\, D \begin{pmatrix} a^2 & ab & ac & ad \\ ab & b^2 & bc & bd \\ ac & bc & c^2 & cd \\ ad & bd & cd & d^2 \end{pmatrix} \mod (F_1, F_2)$$

for $i = 1, 2$, where $\gamma_1 = -18d^3$ and $\gamma_2 = 6(a^3 + b^3 + c^3 + 6abc)$. By Lemma 2.1 we have $t = \gamma_2/\gamma_1$. $\square$

3. Remarks on twisting

In this section we make some general remarks on computing twists of $X(n)$. These will be used to find equations for $X_E^-(9)$ once we have found equations for $X_E(9)$ by another method. We suppose that $X(n)$ has been embedded in (and spans) $\mathbb{P}^{N-1}$ and that the action of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is given by

$$\overline{\rho} : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PGL}_N(\overline{K}).$$

We write $\propto$ for equality in $\mathrm{PGL}_N(\overline{K})$, and a superscript $-T$ for the inverse transpose of a matrix. Let $\iota = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. We further suppose that

$$\overline{\rho}(\iota\gamma\iota) \propto \overline{\rho}(\gamma)^{-T}$$

for all $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. This condition is satisfied in the case of $X(9) \subset \mathbb{P}^3$ since the matrices $\overline{\rho}(S)$ and $\overline{\rho}(T)$ in Remark 2.2 are symmetric.

Lemma 3.1. *Let E/K be an elliptic curve and $\phi : E[n] \to M$ a symplectic isomorphism defined over $\overline{K}$. Suppose $h \in \mathrm{GL}_N(\overline{K})$ satisfies*

$$\sigma(h)h^{-1} \propto \overline{\rho}(\sigma(\phi)\phi^{-1})$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then $X_E(n) \subset \mathbb{P}^{N-1}$ and $X_E^-(n) \subset \mathbb{P}^{N-1}$ are the twists of $X(n) \subset \mathbb{P}^{N-1}$ given by $X_E(n) \cong X(n)$; $\mathbf{x} \mapsto h\mathbf{x}$ and $X_E^-(n) \cong X(n)$; $\mathbf{x} \mapsto h^{-T}\mathbf{x}$. Moreover these isomorphisms are compatible with the maps to the j-line.

Proof. This is a special case of [12, Lemma 3.2]. $\square$

The following lemma generalises [19, Proposition 7.5].

Lemma 3.2. *Let E/K be an elliptic curve. If $h \in \mathrm{GL}_N(\overline{K})$ describes $X_E(n) \subset \mathbb{P}^{N-1}$ as a twist of $X(n) \subset \mathbb{P}^{N-1}$ via $X_E(n) \cong X(n)$; $\mathbf{x} \mapsto h\mathbf{x}$, and this isomorphism is compatible with the maps to the j-line, then $X_E^-(n) \subset \mathbb{P}^{N-1}$ is the twist of $X(n) \subset \mathbb{P}^{N-1}$ via $X_E^-(n) \cong X(n)$; $\mathbf{x} \mapsto h^{-T}\mathbf{x}$.*

Proof. If h is the same as in Lemma 3.1 then the result is clear. In general if h_1 and h_2 are two such maps then there is a commutative diagram

$$\begin{array}{ccc} X_E(n) & \xrightarrow{h_1} & X(n) \\ \| & & \downarrow \beta \\ X_E(n) & \xrightarrow{h_2} & X(n) \end{array}$$

where β is an automorphism of $X(n)$ defined over $\overline{K}$. Since h_1 and h_2 are compatible with the maps to the j-line, it follows that $h_2 \propto \overline{\rho}(\gamma)h_1\alpha^{-1}$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ and $\alpha \in \mathrm{GL}_N(K)$. The change from h_1 to h_2 makes no difference to the desired conclusions. □

4. Formulae in the case of a rational 3-torsion point

In this section we find formulae for $X_E^{\pm}(9)$ and $X_E^{\pm}(9) \to X_E^{\pm}(3)$ in the case E has a rational 3-torsion point.

Lemma 4.1. *Let E/K be an elliptic curve with a rational 3-torsion point T, and discriminant Δ. Then E has a Weierstrass equation of the form*

$$y^2 + a_1xy + a_3y = x^3 \tag{7}$$

with $T = (0,0)$. Moreover $K(E[3]) = K(\zeta_3, \sqrt[3]{\Delta})$.

Proof. Moving T to $(0,0)$ gives a Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$. Since $2T \neq 0$ we have $a_3 \neq 0$. By a substitution $y \leftarrow y + rx$ we may assume $a_4 = 0$. Then E meets the line $y = 0$ in divisor $2(0,0) + (-a_2, 0)$. So for $3T = 0$ we need $a_2 = 0$. For the last statement we note that $\Delta = a_3^3(a_1^3 - 27a_3)$ and $E[3]$ has basis $T = (0,0)$ and $T' = (3a_3/(\delta - a_1), a_3(\zeta_3\delta - a_1)/(\delta - a_1))$ where $\delta = \sqrt[3]{a_1^3 - 27a_3}$. □

Lemma 4.2. *Let E/K be an elliptic curve with a rational 3-torsion point, and discriminant Δ.*

(i) *The family of elliptic curves parametrised by $Y(3) = \mathbb{A}^1 \setminus \{t^3 = 1\}$ is*

$$y^2 + 3txy + (t^3 - 1)y = x^3.$$

(ii) *The family of elliptic curves parametrised by $Y_E^{\pm}(3) = \mathbb{A}^1 \setminus \{t^3 = \Delta^{\pm 1}\}$ is*

$$y^2 + 3txy + (t^3 - \Delta^{\pm 1})y = x^3.$$

Proof. The family of elliptic curves in (i) is the same as that in (2), after a quadratic twist by -3 or a substitution $t \leftarrow (t+2)/(t-1)$. Let c_4, c_6, Δ be the usual quantities associated to the Weierstrass equation (7). Then part (ii) is the special case of Theorem 1.1 with $(r,s) = (a_1^2 t - a_1^3 a_3 + 36 a_3^2, t - a_1 a_3)$, respectively $(r,s) = ((a_1^3 a_3 - 36 a_3^2)t + 2a_1^2, a_1 a_3 t + 2)$. Alternatively the lemma may be proved directly by an argument similar to the proof of Lemma 4.1. $\square$

For $a \in K$ we write $\sqrt[3]{a}$ for the image of x in $K[x]/(x^3 - a)$. Each equation involving $\sqrt[3]{a}$ in the next theorem is written as a short-hand for three equations, one for each K-algebra homomorphism $K[x]/(x^3 - a) \to \overline{K}$.

Theorem 4.3. *Let E/K be the elliptic curve*

$$y^2 + 3t_E xy + (t_E^3 - \Delta)y = x^3. \tag{8}$$

Then $X(9)$ and $X_E^{\pm}(9)$ have equations in $\mathbb{A}^4$ (with co-ordinates t, u, v, w) given by

$$X(9) \qquad t - \sqrt[3]{1} = 9\left(u + v\sqrt[3]{1} + w(\sqrt[3]{1})^2\right)^3, \tag{9}$$

$$X_E(9) \qquad t - \sqrt[3]{\Delta} = (t_E - \sqrt[3]{\Delta})\left(u + v\sqrt[3]{\Delta} + w(\sqrt[3]{\Delta})^2\right)^3, \tag{10}$$

$$X_E^-(9) \qquad t - (\sqrt[3]{\Delta})^{-1} = \frac{3}{t_E - \sqrt[3]{\Delta}}\left(u + v\sqrt[3]{\Delta} + w(\sqrt[3]{\Delta})^2\right)^3. \tag{11}$$

Moreover the maps to $X(3)$ and $X_E^{\pm}(3)$ are given by $(t,u,v,w) \mapsto t$, where t is the co-ordinate in Lemma 4.2.

Remark 4.4. The equations in Theorem 4.3 may be re-written as follows. First we expand and equate coefficients of $1, \sqrt[3]{1}, (\sqrt[3]{1})^2$, respectively $1, \sqrt[3]{\Delta}, (\sqrt[3]{\Delta})^2$. We then eliminate t, and homogenise (introducing a new variable s) to give

$$X(9) = \left\{ \begin{array}{c} u^2 v + v^2 w + w^2 u = s^3 \\ u^2 w + v^2 u + w^2 v = 0 \end{array} \right\} \subset \mathbb{P}^3$$

$$X_E(9) = \left\{ \begin{array}{c} f_0(u,v,w) - t_E f_1(u,v,w) = s^3 \\ f_1(u,v,w) - t_E f_2(u,v,w) = 0 \end{array} \right\} \subset \mathbb{P}^3$$

$$X_E^-(9) = \left\{ \begin{array}{c} f_0(u,v,w) + t_E f_1(u,v,w) = 9s^3 \\ \Delta f_2(u,v,w) + 9t_E s^3 = 0 \end{array} \right\} \subset \mathbb{P}^3$$

where

$$\begin{aligned} f_0(u,v,w) &= u^3 + \Delta v^3 + \Delta^2 w^3 + 6\Delta uvw \\ f_1(u,v,w) &= 3(u^2 v + \Delta v^2 w + \Delta w^2 u) \\ f_2(u,v,w) &= 3(u^2 w + v^2 u + \Delta w^2 v). \end{aligned}$$

Proof of Theorem 4.3. The formulae for $X(9)$ and $X(9) \to X(3)$ were already established in Lemma 2.1.

Let $\mathbb{K}_n$ be the function field of $X(n)$ over $\overline{K}$. Let $B \subset \mathbb{K}_3^\times/(\mathbb{K}_3^\times)^3$ be the subgroup generated by all rational functions on $X(3)$ with zeros and poles only at the cusps. Since $X(3) \cong \mathbb{P}^1$ has 4 cusps, B has dimension 3 as an $\mathbb{F}_3$-vector space. By (9) we have $\mathbb{K}_9 = \mathbb{K}_3(\sqrt[3]{B})$. So if t is the co-ordinate on $X_E^\pm(3)$ in Lemma 4.2 then $X_E^\pm(9)$ has equations

$$t - (\sqrt[3]{\Delta})^{\pm 1} = c_\pm(E)\left(u + v\sqrt[3]{\Delta} + w(\sqrt[3]{\Delta})^2\right)^3$$

for some constant $c_\pm(E)$. Since on $X_E(9)$ there is a rational point (corresponding to E) above the point $t = t_E$ on $X_E(3)$, we can take $c_+(E) = t_E - \sqrt[3]{\Delta}$.

The equations (9) and (10) for $X(9)$ and $X_E(9)$ differ by a change of co-ordinates defined over $\overline{K}$. In writing down this change of co-ordinates it is important to remember that each of (9) and (10) is really three equations. Let $\alpha, \beta, \gamma, \delta \in \overline{K}$ satisfy

$$\alpha^3 = \frac{t_E - \delta}{9\delta}, \quad \beta^3 = \frac{t_E - \zeta_3\delta}{9\zeta_3\delta}, \quad \gamma^3 = \frac{t_E - \zeta_3^2\delta}{9\zeta_3^2\delta}, \quad \delta^3 = \Delta.$$

Then an isomorphism $X_E(9) \to X(9)$ is given by

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta_3 & \zeta_3^2 \\ 1 & \zeta_3^2 & \zeta_3 \end{pmatrix}^{-1} \begin{pmatrix} \alpha & & \\ & \beta & \\ & & \gamma \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta_3 & \zeta_3^2 \\ 1 & \zeta_3^2 & \zeta_3 \end{pmatrix} \begin{pmatrix} 1 & & \\ & \delta & \\ & & \delta^2 \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix}.$$

By Lemma 3.2 an isomorphism $X_E^-(9) \to X(9)$ is given by

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta_3^2 & \zeta_3 \\ 1 & \zeta_3 & \zeta_3^2 \end{pmatrix}^{-1} \begin{pmatrix} \alpha^{-1} & & \\ & \beta^{-1} & \\ & & \gamma^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta_3^2 & \zeta_3 \\ 1 & \zeta_3 & \zeta_3^2 \end{pmatrix} \begin{pmatrix} 1 & & \\ & \delta^{-1} & \\ & & \delta^{-2} \end{pmatrix} \begin{pmatrix} u \\ v \\ w \end{pmatrix}.$$

Therefore $X_E^-(9)$ has equations

$$t - (\sqrt[3]{\Delta})^{-1} = \frac{9^2}{t_E - \sqrt[3]{\Delta}}\left(u + v(\sqrt[3]{\Delta})^{-1} + w(\sqrt[3]{\Delta})^{-2}\right)^3. \tag{12}$$

The equations (11) and (12), though different, are related by a change of co-ordinates defined over K. □

5. Completion of proofs

In this section we complete the proofs of Theorems 1.2, 1.3 and 1.4. We start by using the results of the last section to prove Theorems 1.2 and 1.3 in the case

$E(K)[3] \neq 0$. By Lemma 4.1 we may assume E takes the form (8). Then E has shorter Weierstrass equation $y^2 = x^3 + ax + b$ where

$$\begin{aligned} a &= -24\Delta t_E - 3t_E^4, \\ b &= 16\Delta^2 + 40\Delta t_E^3 - 2t_E^6. \end{aligned}$$

The equations for $X_E(9)$ in Theorem 1.2 and Remark 4.4 are related by

$$\begin{pmatrix} u \\ v \\ w \\ s \end{pmatrix} = \begin{pmatrix} 1 & -3t_E^2 & 12\Delta t_E - 3t_E^4 & 36\Delta t_E^3 - 9t_E^6 \\ 0 & -12t_E & 24\Delta + 12t_E^3 & -216\Delta t_E^2 \\ 0 & -12 & 36t_E^2 & -144\Delta t_E - 72t_E^4 \\ 1 & 9t_E^2 & -36\Delta t_E + 9t_E^4 & 96\Delta^2 + 132\Delta t_E^3 + 15t_E^6 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}.$$

The equations for $X_E^-(9)$ in Theorem 1.2 and Remark 4.4 are related by

$$\begin{pmatrix} u \\ v \\ w \\ s \end{pmatrix} = \begin{pmatrix} \Delta t_E & -12\Delta^2 + 12\Delta t_E^3 & -4\Delta^2 + 7\Delta t_E^3 & -12\Delta^2 t_E^2 + 3\Delta t_E^5 \\ -2\Delta & 0 & -6\Delta t_E^2 & 18\Delta t_E^4 \\ t_E^2 & 0 & 4\Delta t_E - t_E^4 & -16\Delta^2 + 8\Delta t_E^3 - t_E^6 \\ -\Delta t_E & -4\Delta^2 + 4\Delta t_E^3 & -4\Delta^2 + \Delta t_E^3 & 12\Delta^2 t_E^2 - 3\Delta t_E^5 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}.$$

These 4 by 4 matrices have determinants $-2^{10}3^3(t_E^3 - \Delta)^3$ and $2^{10}\Delta^3(t_E^3 - \Delta)^4$, and so are non-singular by the discriminant condition for E. Theorem 1.2 in the case $E(K)[3] \neq 0$ now follows from Theorem 4.3.

Theorem 1.3 follows almost immediately from Lemma 2.3. The one detail we must check is how the pencil of cubics defining $X_E^{\pm}(9)$ in Theorem 1.2 matches up with the co-ordinates $(r : s)$ on $X_E^{\pm}(3) \cong \mathbb{P}^1$ in Theorem 1.1. Computing the discriminant of the Weierstrass equation (1), we find that the cusps of $X_E^{\pm}(3)$ are the roots of $f_{\pm}(r, s) = 0$ where

$$\begin{aligned} f_+(r, s) &= r^4 - 6c_4r^2s^2 - 8c_6rs^3 - 3c_4^2s^4 \\ f_-(r, s) &= c_4r^4 + 4c_6r^3s + 6c_4^2r^2s^2 + 4c_4c_6rs^3 - (3c_4^3 - 4c_6^2)s^4. \end{aligned}$$

On the other hand, writing $\mathcal{H}(F)$ for the Hessian matrix of F, we find that

$$\det \mathcal{H}(3rF_1^{\pm} - sF_2^{\pm}) = f_{\pm}(r, s)D_{\pm}(x, y, z, t)$$

for some quartic form $D_{\pm}(x, y, z, t)$. Comparing with (6) and Lemma 2.3 it follows that the forgetful map is as claimed in Theorem 1.3.

To extend the proofs of Theorems 1.2 and 1.3 to the case $E(K)[3] = 0$ we use the following two lemmas.

Lemma 5.1. *Let X, Y, Y' be curves defined over K. Suppose there is a commutative diagram*

$$\begin{tikzcd} Y \arrow[r, "\psi"] \arrow[d, "\pi"'] & Y' \arrow[d, "\pi'"] \\ X \arrow[r, equal] & X \end{tikzcd}$$

where π and π' are morphisms defined over K, and ψ is an isomorphism defined over a finite extension L/K. Suppose that π is the map that quotients out by a finite K-rational subgroup $A \subset \mathrm{Aut}(Y)$. If $[L:K]$ and $|A|$ are coprime then Y and Y' are isomorphic over K.

Proof. The curve Y' is the twist of Y by a class $\xi \in H^1(K, A)$ whose restriction to $H^1(L, A)$ is trivial. Since the composition

$$H^1(K, A) \xrightarrow{\text{res}} H^1(L, A) \xrightarrow{\text{cores}} H^1(K, A)$$

is multiplication by $[L:K]$, and this degree is coprime to $|A|$, it follows that ξ is trivial. $\square$

Lemma 5.2. *Let E/K be an elliptic curve and p a prime. Then $E(L)[p] \neq 0$ for some finite extension L/K with $[L:K]$ coprime to p.*

Proof. The orbits sizes for the action of Galois on $E[p] \setminus \{0\}$ add up to $p^2 - 1$. Therefore some orbit has size coprime to p. $\square$

To prove Theorem 1.2 we use Lemma 5.2 to find L/K an extension of degree coprime to 3 with $E(L)[3] \neq 0$. We already know that the theorem is true over L. We apply Lemma 5.1 with $X = X_E^{\pm}(3)$, $Y = X_E^{\pm}(9)$ and $Y' \subset \mathbb{P}^3$ the curve defined in the statement of Theorem 1.2. We further take π to be the forgetful map, and π' the map defined in the statement of Theorem 1.3. It follows that Theorem 1.2 is true over K. The proof of Theorem 1.3 goes through exactly the same as before.

Remark 5.3. If elliptic curves E and E' are quadratic twists, then it is easy to see that the modular curves $X_E^{\pm}(n)$ and $X_{E'}^{\pm}(n)$ are isomorphic. With $F_1^{\pm}$ and $F_2^{\pm}$ as defined in Theorem 1.2, this is borne out by the identities

$$\begin{aligned} F_1^+(\lambda^2 a, \lambda^3 b; \lambda^3 x, \lambda^2 y, \lambda z, t) &= \lambda^6 F_1^+(a, b; x, y, z, t), \\ F_2^+(\lambda^2 a, \lambda^3 b; \lambda^3 x, \lambda^2 y, \lambda z, t) &= \lambda^7 F_2^+(a, b; x, y, z, t), \end{aligned}$$

and

$$\begin{aligned} F_1^-(\lambda^2 a, \lambda^3 b; \lambda^2 x, \lambda y, \lambda z, t) &= \lambda^5 F_1^-(a, b; x, y, z, t), \\ F_2^-(\lambda^2 a, \lambda^3 b; \lambda^2 x, \lambda y, \lambda z, t) &= \lambda^6 F_2^-(a, b; x, y, z, t). \end{aligned}$$

Proof of Theorem 1.4. Treating a and b as additional variables, the equations for $X_E^{\pm}(9)$ in Theorem 1.2 define a threefold. Our task is to quotient out by the action of $\mathbb{G}_m$ in Remark 5.3, to give a surface birational to $\mathcal{Z}^{\pm}(9)$. One way to do this is by setting $a = b$, but this gives a highly singular model for $\mathcal{Z}^{\pm}(9)$, and does not seem to help in finding an elliptic fibration. Instead we make the following substitutions.

We start with the direct case. Putting $a = 12s - 3w^2$ and $b = us + 2w^3$ in Theorem 1.2, and expanding in powers of s, we find

$$\begin{aligned} F_1^+(6vs - 3w^3, 2sT - w^2, w, 1) &= 12s^2(g_0 + 4sg_1), \\ F_2^+(6vs - 3w^3, 2sT - w^2, w, 1) &= 36s^2(h_0 + 4sh_1), \end{aligned}$$

where

$$\begin{aligned} g_0 &= u^2 + 3uv + 3v^2 + 9uw + 6Tvw + 3(T^2 - 12T + 24)w^2, \\ g_1 &= T^3 - 9T^2 + 36T - 36, \\ h_0 &= v^2w - (T-1)uw^2 + 2(T-6)vw^2 + (T^2 - 24T + 48)w^3, \\ h_1 &= u + (T^2 - 6T + 12)v - 3(T-2)(T-6)w. \end{aligned}$$

The plane cubic $\{g_0h_1 - g_1h_0 = 0\} \subset \mathbb{P}^2$ is a smooth curve of genus one, defined over $\mathbb{Q}(T)$, with rational point $(u : v : w) = (12 : T-6 : -1)$. The elliptic surface in Theorem 1.4 is obtained by putting this curve in Weierstrass form, for example using the method in [5, Chapter 8]. To simplify the final answer we also made a substitution $T \leftarrow 2T + 3$.

In the reverse case we put $a = 3us - 3w^2$ and $b = 3vs^2 - 3uws + 2w^3$. We then compute

$$\begin{aligned} F_1^-(-3s^2T - w^2, s - w, 2w, 1) &= 9s^3q_1, \\ F_2^-(-3s^2T - w^2, s - w, 2w, 1) &= 9s^3(wq_1 - sq_2), \end{aligned}$$

where

$$\begin{aligned} q_1 &= 3u^2 - uv - 3uw + 2(3T-1)us - 6vw - 3(2T-3)vs + 2w^2 - 3T^2ws + 9T^2s^2, \\ q_2 &= 3(T-2)u^2 + 3uv + uw - 2v^2 - 6(2T-3)vw + 3(6T-1)vs + 9T^2ws + 3T^3s^2. \end{aligned}$$

The quadric intersection $\{q_1 = q_2 = 0\} \subset \mathbb{P}^3$ is a smooth curve of genus one, defined over $\mathbb{Q}(T)$, with rational point $(u : v : w : s) = (2 : 1 : 1 : 0)$. The elliptic surface in Theorem 1.4 is obtained by putting this curve in Weierstrass form, for example using the method in [5, Chapter 8]. To simplify the final answer we also made a substitution $T \leftarrow (2T-3)/(2T+1)$. $\square$

6. Examples

We use Theorems 1.2 and 1.3 to find some non-trivial pairs of 9-congruent elliptic curves over $\mathbb{Q}$ and $\mathbb{Q}(T)$. By "non-trivial" we mean that the elliptic curves are not isogenous. The examples may be checked independently of our work by comparing traces of Frobenius.

6.1. **Examples over $\mathbb{Q}$.** We refer to elliptic curves over $\mathbb{Q}$ by their labels in Cremona's tables [7]. For elliptic curves beyond the range of Cremona's tables we simply write the conductor followed by a $*$.

Example 6.1. Let E be the elliptic curve $47775z1$. The equations for $X_E(9)$ in Theorem 1.2 with $a = -41489280$ and $b = 102867483600$ may be simplified by substituting

$$\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \leftarrow \begin{pmatrix} 2520473760 & 937149484320 & -1998984627360 & -152410870080 \\ 0 & 79644600 & -185343480 & -3827880 \\ 0 & -22932 & 47040 & 6468 \\ 0 & -6 & 13 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}.$$

This gives a model for $X_E(9)$ with equations

$$\begin{aligned} -x^2z + x^2t + 4xyz + 2xyt - 3xz^2 + 2xzt - 3xt^2 + 6y^3 + 14y^2z \\ + y^2t + 6yz^2 - 4yzt + 9yt^2 - 6z^3 + 27z^2t - 13zt^2 - t^3 = 0 \\ -3x^2y + 4x^2z + 3x^2t + 3xy^2 + 20xyz - 12xyt - 3xz^2 - 32xzt + 25xt^2 + 21y^3 \\ +16y^2z - 24y^2t - 12yz^2 + 100yzt + 34yt^2 + 39z^3 - 21z^2t - 56zt^2 - 11t^3 = 0. \end{aligned}$$

On this curve we find rational points $P_1 = (1 : 0 : 0 : 0)$, $P_2 = (4 : -1 : -1 : 0)$ and $P_3 = (1 : 2 : -1 : 0)$. The corresponding elliptic curves directly 9-congruent to E are

P_1	$47775z1$	$y^2 + y = x^3 - x^2 - 32013x + 2215478$
P_2	$429975*$	$y^2 + y = x^3 - 314688780x - 2148671872069$
P_3	$494901225*$	$y^2 + y = x^3 - 23634650164230x - 21037908383222056594$

Since $X_E^-(9)$ is not locally soluble at $p = 7$ there are no elliptic curves reverse 9-congruent to E.

In addition to Example 6.1 we have found two further triples of directly 9-congruent non-isogenous elliptic curves over $\mathbb{Q}$. These are

$4650j1$	$y^2 + xy = x^3 + x^2 - 2700x + 54000$
$553350*$	$y^2 + xy = x^3 + x^2 - 10472207700x - 455228489646000$
$1966950*$	$y^2 + xy = x^3 - x^2 - 20654522386242x - 36130051534030639084$
$27606c1$	$y^2 + xy = x^3 - 10289707x + 12703497719$
$358878*$	$y^2 + xy = x^3 + 2940333x - 1416695391$
$1242270*$	$y^2 + xy + y = x^3 - x^2 - 359912x - 322105301$

The elliptic curves $1701a1$, $1701g1$ and $22113c1$ are also 9-congruent but only the last two of these are directly 9-congruent.

Example 6.2. Let E be the elliptic curve $201c1$. The equations for $X_E^-(9)$ in Theorem 1.2 with $a = -1029699$ and $b = 402173694$ may be simplified by substituting

$$\begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \leftarrow \begin{pmatrix} -26471709 & -23136696 & 20106774 & -20376135 \\ -45147 & -39828 & 33990 & -34509 \\ 90294 & 79332 & -68304 & 69342 \\ 77 & 68 & -58 & 59 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix}.$$

This gives a model for $X_E^-(9)$ with equations

$$\begin{aligned} &-x^3 + 4x^2y + 3x^2z - x^2t + 6xy^2 + 2xyz - 2xyt - 6xz^2 + 4xzt \\ &\quad -11xt^2 + y^3 + 7y^2t - 2yz^2 + 4yzt - 4yt^2 + 6z^3 - 7z^2t + 4zt^2 + t^3 = 0 \\ &2x^3 - x^2y + 5x^2t - 10xy^2 - 2xyz + 16xyt - 3xz^2 + 4xzt + 8xt^2 \\ &\quad -5y^3 - y^2z - 3y^2t - yz^2 - 2yzt + 12yt^2 + 3z^3 - 4z^2t + 2zt^2 - 3t^3 = 0. \end{aligned}$$

On this curve we find the rational point $(1 : -2 : -1 : 0)$. The corresponding elliptic curve reverse 9-congruent to E is

$$374865* \qquad y^2 + xy = x^3 + x^2 - 60068738107x + 4858035498982726.$$

6.2. **Examples over $\mathbb{Q}(T)$.** Again we start our investigations with the equations for $X_E^{\pm}(9)$ in Theorem 1.2. To find some interesting examples over $\mathbb{Q}(T)$, we set $a = b = -27j/(4(j - 1728))$ to obtain a model for $\mathcal{Z}^{\pm}(9)$, fibred over the j-line. We then looked for some rational curves on this surface, by intersecting with coordinate hyperplanes.

The following example gives a proof of Theorem 1.5 in the direct case, without going via Theorem 1.4.

Example 6.3. Let $E/\mathbb{Q}(T)$ be the elliptic curve $y^2 = x^3 + a(T)x + b(T)$ where

$$a(T) = \tfrac{1}{2}(39T^4 - 60T^3 - 162T^2 + 60T + 39),$$
$$b(T) = 47T^6 + 120T^5 + 21T^4 + 21T^2 - 120T + 47.$$

Then on $X_E(9)$, with equations as in Theorem 1.2, we find the rational point

$$(x : y : z : t) = (\tfrac{15}{2}(3T^4 + 8T^3 - 2T^2 - 8T + 3) : T^2 + 1 : 1 : 0).$$

The corresponding elliptic curve directly 9-congruent to E is the elliptic curve directly 3-congruent to E constructed in Theorem 1.1 with $c_4 = -a(T)/27, c_6 = -b(T)/54$ and $(r : s) = (47T^6 - 78T^5 - 153T^4 + 244T^3 + 153T^2 - 78T - 47 : 18(T^2+1)(T^2+6T-1))$. Specialising to $T = 0$ gives a pair of elliptic curves with conductors 80640 and 5886720. In particular these curves are not isogenous.

The following example gives a proof of Theorem 1.5 in the reverse case, without going via Theorem 1.4.

Example 6.4. Let $E/\mathbb{Q}(T)$ be the elliptic curve $y^2 = x^3 + a(T)x + b(T)$ where

$$a(T) = 3(3T + 1)(6T^3 - 3T - 1)(9T^3 - 9T - 4)^2,$$
$$b(T) = 2(3T^3 + 27T^2 + 21T + 4)(6T^3 - 3T - 1)^2(9T^3 - 9T - 4)^2.$$

Then on $X_E^-(9)$, with equations as in Theorem 1.2, we find the rational point

$$(x : y : z : t) = (-(6T^3 - 3T - 1)(9T^3 - 9T - 4) : T : 1 : 0).$$

The corresponding elliptic curve reverse 9-congruent to E is the elliptic curve reverse 3-congruent to E constructed in Theorem 1.1 with $c_4 = -a(T)/27, c_6 = -b(T)/54$ and $(r : s) = ((3T+1)(9T^3 - 9T - 4)(6T^3 - 3T - 1)(180T^4 + 321T^3 + 216T^2 + 66T + 8) : 3(369T^6 + 1107T^5 + 1431T^4 + 1017T^3 + 414T^2 + 90T + 8))$. Specialising to $T = -1/4$ gives the pair of elliptic curves 2304o1 and 343296g1. In particular these curves are not isogenous.

Acknowledgements

I would like to thank Zexiang Chen for some useful discussions that in particular helped to simplify the proof of Theorem 1.2. All computer calculations in support of this work were carried out using Magma [2].

References

[1] R. Barman and A. Saikia, A note on Iwasawa μ-invariants of elliptic curves, *Bull. Braz. Math. Soc.* 41 (2010), no. 3, 399–407.

[2] 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/`

[3] R. Bröker, E.W. Howe, K.E. Lauter and P. Stevenhagen, Genus-2 curves and Jacobians with a given number of points, to appear in *LMS J. Comput. Math.*

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

[5] J.W.S. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts, 24, Cambridge University Press, Cambridge, 1991.

[6] Z. Chen, *Families of elliptic curves with the same mod* 8 *representation*, in preparation.

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

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

[9] T.A. Fisher, Pfaffian presentations of elliptic normal curves, *Trans. Amer. Math. Soc.* 362 (2010), no. 5, 2525–2540.

[10] T.A. Fisher, The Hessian of a genus one curve, *Proc. Lond. Math. Soc.* (3) 104 (2012), no. 3, 613–648.

[11] T.A. Fisher, Invariant theory for the elliptic normal quintic, I. Twists of X(5), *Math. Ann.* 356 (2013), no. 2, 589–616.

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

[13] G. Frey, On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2, in *Elliptic curves, modular forms & Fermat's last theorem* (Hong Kong, 1993), J. Coates and S.-T. Yau (eds.), Ser. Number Theory I, Int. Press, Cambridge, MA, (1995) 79–98.

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

[15] E. Kani and W. Schanz, Modular diagonal quotient surfaces, *Math. Z.* 227 (1998), no. 2, 337–366.

[16] M.A. Kenku, On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class, *J. Number Theory* 15 (1982), no. 2, 199–202.

[17] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.* 44 (1978), no. 2, 129–162.

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

[19] 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.

[20] K. Rubin and A. Silverberg, Families of elliptic curves with constant mod p representations, in *Elliptic curves, modular forms & Fermat's last theorem* (Hong Kong, 1993), J. Coates and S.-T. Yau (eds.), Ser. Number Theory I, Int. Press, Cambridge, MA, (1995) 148–161.

[21] K. Rubin and A. Silverberg, Mod 6 representations of elliptic curves, in *Automorphic forms, automorphic representations, and arithmetic* (Fort Worth, TX, 1996), R.S. Doran, Z.-L. Dou and G.T. Gilbert (eds.), Proc. Sympos. Pure Math., 66, Part 1, Amer. Math. Soc., Providence, RI, (1999), 213-220.

[22] K. Rubin and A. Silverberg, Mod 2 representations of elliptic curves, *Proc. Amer. Math. Soc.* 129 (2001), no. 1, 53–57.

[23] A. Silverberg, Explicit families of elliptic curves with prescribed mod N representations, in *Modular forms and Fermat's last theorem* (Boston, MA, 1995), G. Cornell, J.H. Silverman and G. Stevens (eds.), Springer-Verlag, New York, (1997), 447–461.

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

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