ON FAMILIES OF n-CONGRUENT ELLIPTIC CURVES

T.A. FISHER

Abstract. We use an invariant-theoretic method to compute certain twists of the modular curves $X(n)$ for $n = 7, 9, 11$. Searching for rational points on these twists enables us to find non-trivial pairs of n-congruent elliptic curves over $\mathbb{Q}$, i.e. pairs of non-isogenous elliptic curves over $\mathbb{Q}$ whose n-torsion subgroups are isomorphic as Galois modules. We also show by giving explicit non-trivial examples over $\mathbb{Q}(T)$ that there are infinitely many examples over $\mathbb{Q}$ in the cases $n = 9$ and $n = 11$.

1. Introduction

Elliptic curves E_1 and E_2 over a field K 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 $\phi : E_1[n] \cong E_2[n]$ respects the Weil pairing 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 n-congruent to a given elliptic curve E are parametrised by the modular curve $Y_E(n) = X_E(n) \setminus \{\text{cusps}\}$.

For $n \leq 5$ we have $X_E(n) \cong \mathbb{P}^1$ and the corresponding families of elliptic curves were computed by Rubin and Silverberg [RS1], [RS2], [S]. However for $n \geq 7$ the genus is greater than 1. This prompted Mazur [M] to ask whether there are any pairs of non-isogenous elliptic curves over $\mathbb{Q}$ that are directly n-congruent for any $n \geq 7$. This was answered by Kraus and Oesterlé [KO] who gave the example of the directly 7-congruent elliptic curves $152a1$ and $7448e1$. The labels here are those in Cremona's tables [C]. Nowadays it is easy to find further examples by searching in Cremona's tables, for example

$$\begin{array}{lrcl} n = 11 & 190b1 & + & 2470a1, \\ n = 13 & 52a2 & + & 988b1, \\ n = 17 & 3675b1 & - & 47775b1. \end{array}$$

In each case the n-congruence is proved by computing sufficiently many traces of Frobenius; see [KO, Proposition 4]. Then [KO, Proposition 2] shows that the congruences are direct or reverse as indicated by the $\pm$.

Motivated by Mazur's question, Kani and Schanz [KS] studied the geometry of the surfaces that parametrise pairs of n-congruent of elliptic curves. This

Date: 9th May 2011.

prompted them to conjecture that for any $n \leq 12$ there are infinitely many pairs of n-congruent non-isogenous elliptic curves over $\mathbb{Q}$. It is understood that we are looking for examples with distinct j-invariants, since otherwise from any single example we could construct infinitely many by taking quadratic twists. The conjecture was proved in the case $n = 7$ by Halberstadt and Kraus [HK1], who subsequently [HK2] gave an explicit formula for $X_E(7)$ and used it to show that there are infinitely many 6-tuples of directly 7-congruent non-isogenous elliptic curves over $\mathbb{Q}$. We find the corresponding formulae for $X_E(9)$ and $X_E(11)$ and use them to construct explicit infinite families of pairs of elliptic curves that prove the conjecture for $n = 9$ and $n = 11$. In contrast the proof of the conjecture for $n = 11$ in [KR] does not yield a single explicit example.

We briefly mention three further motivations for studying n-congruence of elliptic curves.

- The modular approach to solving Diophantine equations sometimes requires us to find all elliptic curves n-congruent to a given elliptic curve. For example the paper of Poonen, Schaefer and Stoll [PSS] makes essential use of the formula for $X_E(7)$ due to Halberstadt and Kraus.
- There is a correspondence between pairs of reverse n-congruent elliptic curves and curves of genus 2 that admit a degree n morphism to an elliptic curve. See for example [Fr].
- It was observed by Cremona and Mazur [CM] that if elliptic curves E and F are n-congruent then the Mordell-Weil group of F can sometimes be used to explain elements of the Tate-Shafarevich group of E.

As each of these motivations makes clear, we should also be interested in congruences that do not respect the Weil pairing. The elliptic curves reverse n-congruent to E are parametrised by the modular curve $Y_E^-(n) = X_E^-(n) \setminus \{\text{cusps}\}$. The families of elliptic curves parametrised by $Y_E^-(3)$ and $Y_E^-(4)$ were computed in [F2], and the case of $Y_E^-(5)$ will be treated in [F3]. An equation for $X_E^-(7)$ was given in [PSS, Section 7.2]. We find corresponding formulae for $X_E^-(9)$ and $X_E^-(11)$. In the cases $n = 7$ and $n = 9$ we use these formulae to construct explicit infinite families of pairs of reverse n-congruent non-isogenous elliptic curves over $\mathbb{Q}$. We do not know if any such families exist in the case $n = 11$.

In Section 1.1 we recall the definitions of $X(n)$ and its twists. We then state the formulae for $X_E(n)$ and $X_E^-(n)$ for $n = 3, 7, 9, 11$ in Section 1.2. We include the cases $n = 3$ and $n = 7$ since our methods are quite different from those in [F2] and [HK2]. The results in the case $n = 3$ are also needed in Section 6 to treat the case $n = 9$. In the next two subsections we explain our basic strategy for computing twists and illustrate how it works in the case $n = 3$.

In Section 2 we recall Klein's equations for $X(n)$ for $n \geq 5$ an odd integer. The original approach of Klein was via theta functions, but our treatment is purely algebraic. We also recall explicit formulae for the action of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ on $X(n)$.

Then in Section 3 we use invariant theory for $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ to compute the twists $X_E(n)$ and $X_E^-(n)$ for $n = 7, 9, 11$.

In Section 4 we show that in the special case of an elliptic curve E whose n-torsion contains a copy of the Galois module μ_n, there are particularly simple formulae for $X_E(n)$ and $X_E^-(n)$. This section may be read independently of Section 3. Again the result for $X_E(7)$ is already given in [HK2].

Our formulae reduce the problem of finding elliptic curves n-congruent to E to that of finding rational points on $X_E(n)$ and $X_E^-(n)$. However before searching for rational points it helps to simplify the equations by making a change of coordinates. In Section 5 we describe how to do this in the case $K = \mathbb{Q}$. The problem naturally splits into two parts called minimisation and reduction.

In Section 6 we give formulae for the families of elliptic curves parametrised by $Y_E(n)$ and $Y_E^-(n)$ for $n = 7, 9, 11$. This is easiest in the case $n = 9$ since the natural maps $X_E(9) \to X_E(3)$ and $X_E^-(9) \to X_E^-(3)$ have a simple geometric description. In the cases $n = 7$ and $n = 11$ it is easy to compute the maps $j : X_E(n) \to \mathbb{P}^1$ and $j : X_E^-(n) \to \mathbb{P}^1$. However determination of the right quadratic twists takes considerably more work. (In specific numerical examples one can always fall back on the method in [KO], [HK1].) In the case of $Y_E(7)$ a formula is given in [HK2], although this formula does not quite cover all cases. We give a new proof leading to formulae that work in all cases. We then generalise to the families of elliptic curves parametrised by $Y_E^-(7)$, $Y_E(11)$ and $Y_E^-(11)$.

Finally in Section 7 we give examples of two different sorts. First we have written a program in Magma [BCP] that given an elliptic curve $E/\mathbb{Q}$ and $n \in \{7, 9, 11\}$ searches for rational points (up to a specified height bound) on minimised and reduced models for $X_E(n)$ and $X_E^-(n)$ and returns the corresponding list of elliptic curves n-congruent to E. For $n = 9$ and $n = 11$ we have run this program on every elliptic curve in the Cremona database. In particular we found three triples of directly 9-congruent non-isogenous elliptic curves over $\mathbb{Q}$.

Secondly we have found some non-trivial pairs of n-congruent elliptic curves over $\mathbb{Q}(T)$ for $n = 7, 9, 11$. The infinite families mentioned above are obtained by specialising T.

All computer calculations in support of this work were preformed using Magma [BCP]. A Magma file checking all our formulae, together with extended versions of the tables in Section 7, is available from the author's website [F4].

1.1. **Some modular curves.** We work over a field K of characteristic 0 and write $\overline{K}$ for the algebraic closure. Let $n \geq 3$ be an integer, and M a Galois module isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ as an abelian group and equipped with a non-degenerate alternating Galois equivariant pairing $M \times M \to \mu_n$. We temporarily write Y_M for the algebraic curve defined over K whose L-rational points (L a field extension of K) parametrise the isomorphism classes of pairs (E, ϕ), where E is an elliptic curve defined over L and $\phi : E[n] \cong M$ is a symplectic isomorphism

(i.e. one that matches up the given pairing on M with the Weil pairing on $E[n]$) commuting with the action of $\mathrm{Gal}(\overline{L}/L)$. Two such pairs (E_1, ϕ_1) and (E_2, ϕ_2) are isomorphic if there is an L-isomorphism $\alpha : E_1 \to E_2$ such that $\phi_1 = \phi_2 \circ (\alpha|_{E_1[n]})$.

Let X_M be the smooth projective model of Y_M. We define $X(n)$ to be X_M in the case $M = \mu_n \times \mathbb{Z}/n\mathbb{Z}$ with pairing

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

Given an elliptic curve E over K we define $X_E(n)$ to be X_M in the case M is $E[n]$ equipped with the Weil pairing. More generally we may take M to be $E[n]$ equipped with the rth power of the Weil pairing for any $r \in (\mathbb{Z}/n\mathbb{Z})^\times$. However the curve obtained only depends on the class of r mod squares. Since we will later be specialising to $n \in \{3, 7, 9, 11\}$ it suffices to take $r = \pm 1$. Taking $r = 1$ gives the curve $X_E(n)$ defined above. Taking $r = -1$ gives the curve $X_E^-(n)$.

We identify $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ with the group of symplectic automorphisms of $\mu_n \times \mathbb{Z}/n\mathbb{Z}$. There is then a natural action of $\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})/\{\pm I_2\}$ on $X(n)$ with quotient map $j : X(n) \to \mathbb{P}^1$. From the analytic theory we know that the j-map is ramified above 0, 1728 and ∞ with ramification indexes 3, 2 and n. Hence by the Riemann-Hurwitz formula the genus of $X(n)$ is

$$g(n) = \frac{n-6}{12n} \#\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z}) + 1$$

where for $n \geq 3$ we have $\#\mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z}) = (n^3/2) \prod_{p|n}(1 - 1/p^2)$. For some small values of n the genus is as follows.

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$g(n)$	0	0	0	0	1	3	5	10	13	26	25	50	49	73	81	133

1.2. **Statement of results.** The family of elliptic curves parametrised by $Y_E(n)$ for $n = 2, 3, 4, 5$ is given by formulae of Rubin and Silverberg [RS1], [RS2], [S]. In [F2] we developed an alternative invariant-theoretic approach that also gives formulae for $Y_E^-(n)$. In the case $n = 3$ we have

Theorem 1.1. *Let E be an elliptic curve with Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$. Then the families of elliptic curves parametrised by $Y_E(3)$ and $Y_E^-(3)$ are*

$$y^2 = x^3 - 27\mathbf{c}_4(\lambda, \mu)x - 54\mathbf{c}_6(\lambda, \mu)$$

and

$$y^2 = x^3 - 27\mathbf{c}_4^*(\lambda, \mu)x - 54\mathbf{c}_6^*(\lambda, \mu)$$

where

$$\begin{aligned}\mathbf{c}_4(\lambda,\mu) &= c_4\lambda^4 + 4c_6\lambda^3\mu + 6c_4^2\lambda^2\mu^2 + 4c_4c_6\lambda\mu^3 - (3c_4^3 - 4c_6^2)\mu^4,\\ \mathbf{c}_6(\lambda,\mu) &= c_6\lambda^6 + 6c_4^2\lambda^5\mu + 15c_4c_6\lambda^4\mu^2 + 20c_6^2\lambda^3\mu^3\\ &\qquad + 15c_4^2c_6\lambda^2\mu^4 + 6(3c_4^4 - 2c_4c_6^2)\lambda\mu^5 + (9c_4^3c_6 - 8c_6^3)\mu^6,\end{aligned}$$

and

$$\begin{aligned}\mathbf{c}_4^*(\lambda,\mu) &= -4(\lambda^4 - 6c_4\lambda^2\mu^2 - 8c_6\lambda\mu^3 - 3c_4^2\mu^4)/(c_4^3 - c_6^2),\\ \mathbf{c}_6^*(\lambda,\mu) &= -8\mathbf{c}_6(\lambda,\mu)/(c_4^3 - c_6^2)^2.\end{aligned}$$

Proof: These formulae (and their relation to those in [RS1]) may be found in [F2]. We recall the idea of the proof. Let F be the ternary cubic obtained by homogenising the Weierstrass equation for E. Then the family of curves parametrised by $X_E(3)$ is the pencil of plane cubics spanned by F and its Hessian, each with base point the same as that for E. It only remains to put these curves in Weierstrass form. One way of carrying out this final calculation is by using the formula for the Jacobian (due to Weil) coming from classical invariant theory. For this reason the polynomials $\mathbf{c}_4(\lambda,\mu)$ and $\mathbf{c}_6(\lambda,\mu)$ may already be found in [Sa, Art. 230], although not with the interpretation given here.

The corresponding formula for $Y_E^-(3)$ is obtained by replacing the Hessian (which is a covariant) by suitable contravariants. □

A formula for $X_E(7)$ was obtained by Halberstadt and Kraus [HK2]. Their method relies on studying the points on the Klein quartic

$$X(7) = \{x^3y + y^3z + z^3x = 0\} \subset \mathbb{P}^2$$

corresponding to an elliptic curve E and the elliptic curves E_a, E_b, E_c that are 2-isogenous to E. By combining this result with some classical invariant theory Poonen, Schaefer and Stoll [PSS, Section 7.2] then gave a formula for $X_E^-(7)$.

Theorem 1.2 (Halberstadt, Kraus, Poonen, Schaefer, Stoll)**.** *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 $\mathcal{F} = 0$ where*

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

and $X_E^-(7) \subset \mathbb{P}^2$ has equation $\mathcal{G} = 0$ where

$$\begin{aligned}\mathcal{G} = -a^2x^4 &+ 2abx^3y - 12bx^3z - (6a^3 + 36b^2)x^2y^2 + 6ax^2z^2\\ &+ 2a^2bxy^3 - 12abxy^2z + 18bxyz^2 + (3a^4 + 19ab^2)y^4\\ &- (8a^3 + 42b^2)y^3z + 6a^2y^2z^2 - 8ayz^3 + 3z^4.\end{aligned}$$

We give new proofs of Theorems 1.1 and 1.2. We then extend to the cases $n = 9$ and $n = 11$. Although we believe that the formulae in Theorems 1.3 and 1.4 below are correct for all elliptic curves E we assume for simplicity that $j(E) \neq 0, 1728$. In Section 2 we recall that $X(9)$ may be embedded in $\mathbb{P}^3$ as the complete intersection of two cubics:

$$X(9) = \left\{ \begin{array}{l} x^2y + y^2z + z^2x = 0 \\ xy^2 + yz^2 + zx^2 = t^3 \end{array} \right\} \subset \mathbb{P}^3.$$

Theorem 1.3. *Let E be an elliptic curve with Weierstrass equation $y^2 = x^3 + ax + b$. If $j(E) \neq 0, 1728$ then $X_E(9) \subset \mathbb{P}^3$ has equations $\mathcal{F}_1 = \mathcal{F}_2 = 0$ where*

$$\begin{aligned} \mathcal{F}_1 &= x^2t + 6xyz + 6bxt^2 + 6y^3 - 9ay^2t + 6a^2yt^2 - 3bz^3 + 3a^2z^2t \\ &\quad + 9abzt^2 - (a^3 - 12b^2)t^3, \\ \mathcal{F}_2 &= x^2z + 6xy^2 - 6axyt + 2a^2xt^2 - 9ay^2z - 18byz^2 + 12a^2yzt + a^2z^3 \\ &\quad + 9abz^2t - 3a^3zt^2 + a^2bt^3, \end{aligned}$$

and $X_E^-(9) \subset \mathbb{P}^3$ has equations $\mathcal{G}_1 = \mathcal{G}_2 = 0$ where

$$\begin{aligned} \mathcal{G}_1 &= 9x^2y + 3x^2z - 6axyt + 6bxt^2 - 6ay^3 + 27by^2t + 3ayz^2 \\ &\quad + 18byzt + 3a^2yt^2 + az^3 + 3bz^2t + a^2zt^2 - abt^3, \\ \mathcal{G}_2 &= x^3 + 6axyz + 18bxyt + 3axz^2 + 6bxzt + a^2xt^2 + 9by^3 + 6a^2y^2t \\ &\quad - 9byz^2 + 6a^2yzt - 3abyt^2 - 4bz^3 + 2a^2z^2t + 2b^2t^3. \end{aligned}$$

It was observed by Klein that $X(11)$ may be embedded in $\mathbb{P}^4$ as the singular locus of the Hessian of the cubic threefold

$$\{v^2w + w^2x + x^2y + y^2z + z^2v = 0\} \subset \mathbb{P}^4.$$

Theorem 1.4. *Let E be an elliptic curve with Weierstrass equation $y^2 = x^3 + ax + b$. If $j(E) \neq 0, 1728$ then $X_E(11) \subset \mathbb{P}^4$ is the singular locus of the Hessian of*

$$\begin{aligned} \mathcal{F} &= v^3 + av^2z - 2avx^2 + 4avxy - 6bvxz + avy^2 + 6bvyz + a^2vz^2 - w^3 \\ &\quad + aw^2z - 4awx^2 - 12bwxz + a^2wz^2 - 2bx^3 + 3bx^2y + 2a^2x^2z + 6bxy^2 \\ &\quad + 4abxz^2 + by^3 - a^2y^2z + abyz^2 + 2b^2z^3, \end{aligned}$$

and $X_E^-(11) \subset \mathbb{P}^4$ is the singular locus of the Hessian of

$$\begin{aligned} \mathcal{G} &= v^2z + 2vwy + 4vxy + 2w^2x - aw^2z + 2wx^2 - 2awy^2 - 6bwyz \\ &\quad + 6x^3 - 6ax^2z + 2a^2xz^2 + by^3 - 2a^2y^2z - 5abyz^2 - b^2z^3. \end{aligned}$$

1.3. **Preliminaries on twisting.** We identify $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ with the group of symplectic automorphisms of $\mu_n \times \mathbb{Z}/n\mathbb{Z}$ via $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : (\zeta_n^x, y) \mapsto (\zeta_n^{ax+by}, cx+dy)$, where ζ_n is a fixed primitive nth root of unity. The Galois action on $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ will be that arising from this identification. There is then a Galois equivariant group homomorphism

$$\overline{\rho} : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{Aut}(X(n)). \tag{1}$$

where the action of $\overline{\rho}(\gamma)$ on $Y(n)$ is given by $(E, \phi) \mapsto (E, \gamma \circ \phi)$.

Lemma 1.5. *Let E/K be an elliptic curve and $\phi : E[n] \cong \mu_n \times \mathbb{Z}/n\mathbb{Z}$ a symplectic, respectively anti-symplectic, isomorphism over $\overline{K}$. Then there is an isomorphism $\alpha : X_E(n) \to X(n)$, respectively $\alpha : X_E^-(n) \to X(n)$, over $\overline{K}$ such that*

$$\sigma(\alpha)\alpha^{-1} = \overline{\rho}(\sigma(\phi)\phi^{-1})$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Proof: The points on $Y_E(n)$, respectively $Y_E^-(n)$, correspond to pairs (F, ψ) where F is an elliptic curve and $\psi : F[n] \cong E[n]$ is a symplectic, respectively anti-symplectic, isomorphism. The modular interpretation of α is that it sends (F, ψ) to $(F, \phi \circ \psi)$. □

We are interested in the case $X(n)$ is embedded in $\mathbb{P}^{m-1}$ for some m, and $\overline{\rho}$ is realised as a projective representation (also denoted $\overline{\rho}$ by abuse of notation):

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

Writing $\propto$ for equality in $\mathrm{PGL}_m(\overline{K})$, we further suppose there exists[1] $\varepsilon \in \mathrm{GL}_m(K)$ such that

$$\overline{\rho}(\iota\gamma\iota) \propto \varepsilon\overline{\rho}(\gamma)^{-T}\varepsilon^{-1} \tag{2}$$

for all $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, where $\iota = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Our strategy for computing $X_E(n)$ and $X_E^-(n)$ as twists of $X(n)$ is explained by the following lemma.

Lemma 1.6. *Let E/K be an elliptic curve and $\phi : E[n] \cong \mu_n \times \mathbb{Z}/n\mathbb{Z}$ a symplectic isomorphism over $\overline{K}$. Suppose $h_1, h_2 \in \mathrm{GL}_m(\overline{K})$ satisfy*

$$\sigma(h_1)h_1^{-1} \propto \overline{\rho}(\sigma(\phi)\phi^{-1}) \qquad \sigma(h_2)h_2^{-1} \propto \overline{\rho}(\sigma(\phi)\phi^{-1})^{-T}$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then $X_E(n) \subset \mathbb{P}^{m-1}$ and $X_E^-(n) \subset \mathbb{P}^{m-1}$ are the twists of $X(n) \subset \mathbb{P}^{m-1}$ given by $X_E(n) \cong X(n)$; $\mathbf{x} \mapsto h_1\mathbf{x}$ and $X_E^-(n) \cong X(n)$; $\mathbf{x} \mapsto \varepsilon h_2\mathbf{x}$.

Proof: We apply Lemma 1.5 to the pairs (E, ϕ) and $(E, \iota \circ \phi)$. □

[1] By Remark 2.4(iii) below we can usually take $\varepsilon = I_m$.

Remark 1.7. If the projective representation $\overline{\rho}$ lifts to a representation

$$\rho : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_m(\overline{K})$$

then the existence of the matrix h_1 in Lemma 1.6 is clear from the generalised form of Hilbert's Theorem 90 which states that $H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{GL}_m(\overline{K})) = 0$. We could then take $h_2 = h_1^{-T}$. We will instead use invariant theory for the group $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ to give explicit formulae for h_1 and h_2.

1.4. **Introductory example: the case $n = 3$.** The family of curves parametrised by $X(3) \cong \mathbb{P}^1$ is the Hesse pencil of plane cubics

$$\{A(x^3 + y^3 + z^3) + Bxyz = 0\} \subset \mathbb{P}^2$$

with base point $(x : y : z) = (0 : 1 : -1)$. An equation for this family in Weierstrass form is $y^2 = x^3 - 27c_4(A, B)x - 54c_6(A, B)$ with discriminant $\Delta = (c_4^3 - c_6^2)/1728 = D^3$ where

$$\begin{aligned} D(A, B) &= -27A^4 - AB^3 \\ c_4(A, B) &= -216A^3B + B^4 \\ c_6(A, B) &= 5832A^6 - 540A^3B^3 - B^6. \end{aligned}$$

The action of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ on $X(3) \cong \mathbb{P}^1$ lifts to a representation

$$\rho : \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) \to \mathrm{SL}_2(\overline{K})$$

given on the generators $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ by

$$\rho(S) = \frac{-1}{\zeta_3 - \zeta_3^2} \begin{pmatrix} 1 & 1/3 \\ 6 & -1 \end{pmatrix}, \qquad \rho(T) = \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^2 \end{pmatrix}.$$

The hypothesis (2) is satisfied with $\varepsilon = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 18 \end{smallmatrix}\right)$.

Lemma 1.8. *Let E/K be an elliptic curve and $\phi : E[3] \cong \mu_3 \times \mathbb{Z}/3\mathbb{Z}$ a symplectic isomorphism over $\overline{K}$. Let $(A : B)$ be the corresponding $\overline{K}$-point on $X(3) \cong \mathbb{P}^1$ with co-ordinates (A, B) scaled so that*

$$c_4(A, B) = c_4(E) \quad \text{and} \quad c_6(A, B) = c_6(E) \tag{3}$$

where E has Weierstrass equation $y^2 = x^3 - 27c_4(E)x - 54c_6(E)$. If $j(E) \neq 0, 1728$ then

$$h_1 = \begin{pmatrix} A & -\frac{\partial D}{\partial B} \\ B & \frac{\partial D}{\partial A} \end{pmatrix}$$

satisfies the hypotheses of Lemma 1.6.

PROOF: Since $(A:B)\in X(3)$ is not a cusp we have $\det h_1 = 4D \neq 0$ and so $h_1 \in \mathrm{GL}_2(\overline{K})$. Let $G = \mathrm{Im}(\rho)$. There is a unique character $\chi : G \to \mu_3$ such that

$$\begin{aligned} D \circ g &= \chi(g) D \\ c_4 \circ g &= \chi(g)^2 c_4 \\ c_6 \circ g &= \chi(g)^3 c_6 \end{aligned} \tag{4}$$

for all $g \in G$. It follows by the chain rule that

$$\begin{pmatrix} -\frac{\partial D}{\partial B} \\ \frac{\partial D}{\partial A} \end{pmatrix} \circ g = \chi(g) g \begin{pmatrix} -\frac{\partial D}{\partial B} \\ \frac{\partial D}{\partial A} \end{pmatrix} \tag{5}$$

for all $g \in G$.

Let $\xi_\sigma = \sigma(\phi)\phi^{-1} \in \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. Since ρ describes the action of $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ on $X(3) \cong \mathbb{P}^1$ we have

$$\sigma \begin{pmatrix} A \\ B \end{pmatrix} = \lambda_\sigma \rho(\xi_\sigma) \begin{pmatrix} A \\ B \end{pmatrix} \tag{6}$$

for some $\lambda_\sigma \in \overline{K}^\times$. Then by (4) we have

$$\sigma(c_4(A,B)) = \lambda_\sigma^4 \chi_\sigma^2 c_4(A,B) \quad \text{and} \quad \sigma(c_6(A,B)) = \lambda_\sigma^6 \chi_\sigma^3 c_6(A,B)$$

where $\chi_\sigma = \chi(\rho(\xi_\sigma))$. Since $c_4(E), c_6(E) \in K$ it follows by (3) and our assumption $j(E) \neq 0, 1728$ that $\lambda_\sigma^2 \chi_\sigma = 1$. Using (5) and (6) we compute

$$\sigma(h_1) = h_1 \circ (\lambda_\sigma \rho(\xi_\sigma)) = \rho(\xi_\sigma) h_1 \begin{pmatrix} \lambda_\sigma & 0 \\ 0 & \lambda_\sigma^3 \chi_\sigma \end{pmatrix} \propto \rho(\xi_\sigma) h_1.$$

Hence $\sigma(h_1) h_1^{-1} \propto \rho(\xi_\sigma)$ as required. □

Lemma 1.6 shows that $X_E(3)$ and $X_E^-(3)$ are the twists of $X(3) \cong \mathbb{P}^1$ by h_1 and εh_1^{-T}. To compute the families of curves parametrised by $X_E(3)$ and $X_E^-(3)$ we put

$$\begin{aligned} \mathbf{c}_4(\lambda,\mu) &= c_4(\lambda A - \mu \tfrac{\partial D}{\partial B}, \lambda B + \mu \tfrac{\partial D}{\partial A}), \\ \mathbf{c}_6(\lambda,\mu) &= c_6(\lambda A - \mu \tfrac{\partial D}{\partial B}, \lambda B + \mu \tfrac{\partial D}{\partial A}), \end{aligned}$$

and

$$\begin{aligned} \mathbf{c}_4^*(\lambda,\mu) &= \frac{1}{(36D)^4} c_4(\lambda B + \mu \tfrac{\partial D}{\partial A}, -18(\lambda A - \mu \tfrac{\partial D}{\partial B})), \\ \mathbf{c}_6^*(\lambda,\mu) &= \frac{1}{(36D)^6} c_6(\lambda B + \mu \tfrac{\partial D}{\partial A}, -18(\lambda A - \mu \tfrac{\partial D}{\partial B})). \end{aligned}$$

The coefficients of $\mathbf{c}_4(\lambda,\mu)$, $\mathbf{c}_6(\lambda,\mu)$, $\mathbf{c}_4^*(\lambda,\mu)$, $\mathbf{c}_6^*(\lambda,\mu)$ may be written as rational functions in $c_4(A,B)$ and $c_6(A,B)$, thereby giving the formulae in Theorem 1.1. The following alternative proof of Theorem 1.1 has the advantage over that in [F2]

of not requiring any knowledge of the Hessian or the contravariants. We include it to illustrate the approach we take for $n = 7, 9, 11$.

Proof of Theorem 1.1: We assume $j(E) \neq 0, 1728$ so that Lemma 1.8 applies. By [RS1, Proposition 2.1] the formulae in the statement of the theorem define a family of elliptic curves with constant mod 3 Galois representation. In the case of $Y_E(3)$ the proof is completed by specialising to $(\lambda : \mu) = (1 : 0)$. In general, that is, to give an argument that also applies to $Y_E^-(3)$, we note that since we have specified a family of elliptic curves with the right j-invariant, it must be correct up to quadratic twist, say by $\delta \in K^\times$. It remains to show that δ is a square. As noted in [HK2, Section 7.1] it suffices to prove this in the case $\phi : E[3] \cong \mu_3 \times \mathbb{Z}/3\mathbb{Z}$ is defined over K. But in that case the families of curves parametrised by $X(3)$, $X_E(3)$ and $X_E^-(3)$ are the same, and this is born out by our construction. □

2. Equations for $X(n)$

We recall equations of Klein [K1], [K2], [K3] for the modular curves $X(n)$. Our treatment follows the survey in [F0, Chapter 4], but see also [AR], [V2].

2.1. **Klein's equations.** Let E be an elliptic curve and P, Q a basis for $E[n]$ with $e_n(P, Q) = \zeta_n$. If we embed $E \subset \mathbb{P}^{n-1}$ by a complete linear system $|D|$ of degree n then the translation maps τ_P and τ_Q extend to automorphisms of $\mathbb{P}^{n-1}$. The following lemma is recalled from [F1].

Lemma 2.1. *(i) We may change co-ordinates on $\mathbb{P}^{n-1}$ (over $\overline{K}$) so that τ_P and τ_Q are given by*

$$M_P = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta_n & 0 & \cdots & 0 \\ 0 & 0 & \zeta_n^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \zeta_n^{n-1} \end{pmatrix} \quad \text{and} \quad M_Q = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

(ii) If n is odd and $[-1]^*D \sim D$ then there is a unique choice of co-ordinates (over $\overline{K}$) such that τ_P, τ_Q and multiplication by -1 are given by M_P, M_Q and

$$[-1] = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \end{pmatrix}.$$

We restrict to $n \geq 5$ an odd integer. Given a symplectic isomorphism $\phi : E[n] \cong \mu_n \times \mathbb{Z}/n\mathbb{Z}$ we let P, Q be the basis for $E[n]$ with $\phi(iP + jQ) = (\zeta_n^i, j)$ for all $i, j \in \mathbb{Z}/n\mathbb{Z}$. If we embed $E \subset \mathbb{P}^{n-1}$ via the complete linear system $|n.0_E|$ and choose co-ordinates as in Lemma 2.1 then sending (E, ϕ) to the image of 0_E defines an embedding $Y(n) \subset \mathbb{P}^{n-1}$. Indeed if we know the co-ordinates of $0_E \in \mathbb{P}^{n-1}$ then M_P and M_Q allow us to write down n^2 points on E. Since E is defined by quadrics, it follows by Bézout's theorem that these n^2 points suffice to determine E. The embedding $Y(n) \subset \mathbb{P}^{n-1}$ is defined over K since $\langle M_P, M_Q \rangle \subset \mathrm{PGL}_n(\overline{K})$ is isomorphic to $\mu_n \times \mathbb{Z}/n\mathbb{Z}$ as a Galois module.

We write $(x_0 : x_1 : \ldots : x_{n-1})$ for our co-ordinates on $\mathbb{P}^{n-1}$ and agree to read all subscripts mod n. Since n is odd we have

$$n.0_E \sim 0_E + P + 2P + \ldots + (n-1)P.$$

Therefore 0_E belongs to exactly one of the hyperplanes fixed by M_P. But 0_E is fixed by $[-1]$ so we have either

$$\begin{array}{rrcll} & 0 & = & (0 : a_1 : a_2 : \ldots : a_2 : a_1) & (+) \\ \text{or} & 0 & = & (0 : a_1 : a_2 : \ldots : -a_2 : -a_1) & (-) \end{array}$$

where $a_1, a_2, \ldots$ are non-zero.

Let W be the vector space of quadrics on $\mathbb{P}^{n-1}$ and V the subspace of quadrics vanishing on E. Then $\dim W = n(n+1)/2$ and $\dim V = n(n-3)/2$. The action of M_P allows us to write these as direct sums $V = \oplus V_i$ and $W = \oplus W_i$ with

$$V_i \subset W_i = \langle x_i^2, x_{i-1}x_{i+1}, \ldots \rangle.$$

Since n is odd it follows by the action of M_Q that $\dim V_i = (n-3)/2$ and $\dim W_i = (n+1)/2$. The requirement that the quadrics in V_0 vanish at 0_E and its translates under M_Q imposes some linear conditions on the coefficients of these quadrics. This leads us to rule out the case $(+)$ and to make the following definition.

Definition 2.2. For $n \geq 5$ an odd integer let $Z(n) \subset \mathbb{P}^{n-1}$ be the subvariety defined by $a_0 = 0$, $a_{n-i} = -a_i$ and

$$\mathrm{rank}(a_{i-j}a_{i+j})_{i,j=0}^{n-1} \leq 2. \tag{7}$$

We note that (7) is equivalent to the vanishing of the 4×4 Pfaffians of this skew-symmetric matrix. The above construction shows that $Y(n) \subset Z(n)$. It is natural to ask whether $Z(n) = X(n)$. Vélu [V2] proved this in the case $n = p$ is a prime. However when n is composite $Z(n)$ has extra components.

When $n = 7$ we put $0_E = (0 : a : b : -c : c : -b : -a)$. Then $Z(7)$ is defined by

$$\operatorname{rank}\begin{pmatrix} 0 & -a^2 & -b^2 & -c^2 \\ a^2 & 0 & ac & -bc \\ b^2 & -ac & 0 & ab \\ c^2 & bc & -ab & 0 \end{pmatrix} \leq 2.$$

Thus $X(7) = Z(7)$ is the Klein quartic $\{a^3b + b^3c + c^3a = 0\} \subset \mathbb{P}^2$.

When $n = 9$ we put $0_E = (0 : a : -b : d : c : -c : -d : b : -a)$. Then $Z(9)$ 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

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

Adding together the last three equations and factoring shows that $Z(9)$ is the union of the curve

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

and four isolated points

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

When $n = 11$ we put $0_E = (0 : a : -c : b : e : d : -d : -e : -b : c : -a)$. Then $X(11) \subset \mathbb{P}^4$ is the singular locus of the Hessian of the cubic threefold

$$\{a^2b + b^2c + c^2d + d^2e + e^2a = 0\} \subset \mathbb{P}^4.$$

We refer to [AR] for further details. We checked using Magma that the homogeneous ideal of $X(11)$ is generated by the 4×4 minors of the Hessian matrix of the cubic form.

2.2. **The action of** $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$**.** We continue to take $n \geq 5$ odd. In Section 2.1 we defined an embedding $X(n) \subset \mathbb{P}^{m-1}$ where $m = (n-1)/2$. The action of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ on $X(n)$ extends to a projective representation $\overline{\rho} : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PGL}_m(\overline{K})$. We show that it lifts to a representation. See [AR, Appendix I] for a discussion of how this relates to work of Weil.

Proposition 2.3. *The projective representation* $\overline{\rho} : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PGL}_m(\overline{K})$ *lifts to a representation* $\rho : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_m(\overline{K})$.

Proof: The action of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ on $Y(n)$ is given by

$$\gamma : (E, P, Q) \mapsto (E, dP - cQ, -bP + aQ). \tag{8}$$

If we embed $X(n) \subset \mathbb{P}^{n-1}$ as described in Section 2.1 then the action (8) extends to a projective representation $\overline{\pi} : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{PGL}_n(\overline{K})$ where the image of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is uniquely determined by the properties that

$$\overline{\pi}(\gamma)^{-1} M_P^u M_Q^v \overline{\pi}(\gamma) \propto M_P^{du-bv} M_Q^{-cu+av} \tag{9}$$

for all $u, v \in \mathbb{Z}/n\mathbb{Z}$, and $\overline{\pi}(\gamma)$ commutes with $[-1]$. We regard $\overline{\pi}$ as describing an action on $\mathbb{P}^{n-1} = \mathbb{P}(W)$ where W is an n-dimensional vector space. The action of $[-1]$ gives an eigenspace decomposition $W = W_+ \oplus W_-$ with $\dim W_\pm = (n \pm 1)/2$. We may then identify $\overline{\rho}$ with the restriction of $\overline{\pi}$ to $\mathbb{P}(W_-) = \mathbb{P}^{m-1}$. To prove the proposition we show more generally that $\overline{\pi}$ lifts to a representation $\pi : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_n(\overline{K})$.

Let $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ be the usual generators of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. In view of the relations $(ST)^3 = S^4 = T^n = I_2$, the only 1-dimensional characters of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ are the ones in the case n is a multiple of 3 that factor via $\mathrm{PSL}_2(\mathbb{Z}/3\mathbb{Z}) \cong A_4$. Using (8) and (9) we compute

$$\overline{\pi}(S) \propto (\zeta_n^{ij})_{i,j=0}^{n-1} \qquad \overline{\pi}(T) \propto \mathrm{Diag}(\zeta_n^{i^2/2})_{i=0}^{n-1} \tag{10}$$

where the exponents are read as elements of $\mathbb{Z}/n\mathbb{Z}$.

If $M \in \mathrm{GL}_n(\overline{K})$ acts on $W_\pm$ then we write $M_\pm$ for its restriction to $W_\pm$. Since

$$3(1^2 + 2^2 + \ldots + m^2) \equiv 0 \pmod{n}$$

it is clear by (10) that there is a lift $\pi(T)$ of $\overline{\pi}(T)$ and 1-dimensional characters $\chi_\pm$ of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\det(\pi(T)_\pm) = \chi_\pm(T)$. Next we lift $\overline{\pi}(S)$ to a matrix $\pi(S)$ such that

$$\pi(S)\pi(T)^{-1}\pi(S) = \pi(T)\pi(S)\pi(T). \tag{11}$$

Restricting to $W_\pm$ and taking determinants it follows that $\det(\pi(S)_\pm) = 1 = \chi_\pm(S)$. For each $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ we now let $\pi(\gamma)$ be the unique lift of $\overline{\pi}(\gamma)$ such that $\det(\pi(\gamma)_\pm) = \chi_\pm(\gamma)$. These lifts exist since S and T generate $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ and are unique since $\dim W_-$ and $\dim W_+$ are coprime. It is evident that the map π so defined is a group homomorphism. □

Remark 2.4. (i) A calculation using (11) shows that $\pi(S) = g_n^{-1}(\zeta^{ij})_{i,j=0}^{n-1}$ where the Gauss sum $g_n = \sum_{i=0}^{n-1} \zeta^{-i^2/2}$ satisfies $g_n^2 = (-1)^{(n-1)/2} n$.

(ii) If we take $0_E = (0 : a_1 : a_2 : \ldots : -a_2 : -a_1)$ then with respect to co-ordinates $(a_1 : \ldots : a_m)$ we may take

$$\rho(S) = g_n^{-1}(\zeta^{ij} - \zeta^{-ij})_{i,j=1}^m \qquad \rho(T) = \mathrm{Diag}(\zeta^{i^2/2})_{i=1}^m.$$

In particular $\rho(-I_2) = (-1)^{(n+1)/2} I_m$.
(iii) Since $\rho(S)$ and $\rho(T)$ are symmetric we see that (2) holds with $\varepsilon = I_m$.
(iv) If $3 \nmid n$ then $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ has no 1-dimensional characters and so the lifts we have constructed are unique. If $3 \mid n$ then $3 \nmid m$ and we can make ρ unique by demanding that $\det \rho(T) = 1$, equivalently ρ takes values in $\mathrm{SL}_m(\overline{K})$.

3. Equations for $X_E(n)$ and $X_E^-(n)$

We derive our equations for $X_E(n)$ and $X_E^-(n)$ by using invariant theory for the group $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ to twist the equations for $X(n)$ in Section 2.1. We split into the cases $n = 7, 9, 11$.

3.1. **Formulae in the case $n = 7$.** We recall that $X(7)$ is the Klein quartic $\{F = 0\} \subset \mathbb{P}^2$ where $F = a^3b + b^3c + c^3a$. Let $G \cong \mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$ be the image of $\rho : \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) \to \mathrm{GL}_3(\overline{K})$. It is generated by

$$\frac{1}{g_7}\begin{pmatrix} \zeta_7 - \zeta_7^6 & \zeta_7^2 - \zeta_7^5 & \zeta_7^4 - \zeta_7^3 \\ \zeta_7^2 - \zeta_7^5 & \zeta_7^4 - \zeta_7^3 & \zeta_7 - \zeta_7^6 \\ \zeta_7^4 - \zeta_7^3 & \zeta_7 - \zeta_7^6 & \zeta_7^2 - \zeta_7^5 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \zeta_7 & 0 & 0 \\ 0 & \zeta_7^4 & 0 \\ 0 & 0 & \zeta_7^2 \end{pmatrix}$$

where $g_7 = 1 + 2(\zeta_7^3 + \zeta_7^5 + \zeta_7^6)$.

Definition 3.1. An invariant of degree m is a homogeneous polynomial $I = I(a, b, c)$ of degree m such that $I \circ g = I$ for all $g \in G$.

Recalling formulae of Klein we put

$$H = (-1/54) \times \begin{vmatrix} \frac{\partial^2 F}{\partial a^2} & \frac{\partial^2 F}{\partial a \partial b} & \frac{\partial^2 F}{\partial a \partial c} \\ \frac{\partial^2 F}{\partial a \partial b} & \frac{\partial^2 F}{\partial b^2} & \frac{\partial^2 F}{\partial b \partial c} \\ \frac{\partial^2 F}{\partial a \partial c} & \frac{\partial^2 F}{\partial b \partial c} & \frac{\partial^2 F}{\partial c^2} \end{vmatrix},$$

$$c_4 = (1/9) \times \begin{vmatrix} \frac{\partial^2 F}{\partial a^2} & \frac{\partial^2 F}{\partial a \partial b} & \frac{\partial^2 F}{\partial a \partial c} & \frac{\partial H}{\partial a} \\ \frac{\partial^2 F}{\partial a \partial b} & \frac{\partial^2 F}{\partial b^2} & \frac{\partial^2 F}{\partial b \partial c} & \frac{\partial H}{\partial b} \\ \frac{\partial^2 F}{\partial a \partial c} & \frac{\partial^2 F}{\partial b \partial c} & \frac{\partial^2 F}{\partial c^2} & \frac{\partial H}{\partial c} \\ \frac{\partial H}{\partial a} & \frac{\partial H}{\partial b} & \frac{\partial H}{\partial c} & 0 \end{vmatrix}, \qquad c_6 = (1/14) \times \begin{vmatrix} \frac{\partial F}{\partial a} & \frac{\partial F}{\partial b} & \frac{\partial F}{\partial c} \\ \frac{\partial H}{\partial a} & \frac{\partial H}{\partial b} & \frac{\partial H}{\partial c} \\ \frac{\partial c_4}{\partial a} & \frac{\partial c_4}{\partial b} & \frac{\partial c_4}{\partial c} \end{vmatrix}.$$

The ring of invariants $K[a,b,c]^G$ is generated by F, H, c_4 and c_6 subject to a single relation which reduces when we set $F = 0$ to

$$c_4^3 - c_6^2 \equiv 1728H^7 \pmod{F}.$$

Since F, H, c_4 and c_6 have degrees $4, 6, 14$ and 21 it is clear that every invariant of odd degree is divisible by c_6.

Lemma 3.2. *The j-invariant $X(7) \to \mathbb{P}^1$ is given by $j = c_4^3/H^7$.*

Proof: Both j and $j_0 = c_4^3/H^7$ define maps $X(7) \to \mathbb{P}^1$ that quotient out by the action of $G \cong \mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$. So they can differ by at most a Möbius map. We recall that j is ramified above 0, 1728 and ∞ with ramification indices 3, 2 and 7. Since

$$\begin{aligned} \#\{F = c_4 = 0\} &\leq 4\deg(c_4) = \tfrac{1}{3}|G| \\ \#\{F = c_6 = 0\} &\leq 4\deg(c_6) = \tfrac{1}{2}|G| \\ \#\{F = H = 0\} &\leq 4\deg(H) = \tfrac{1}{7}|G| \end{aligned}$$

and $j_0 - 1728 = c_6^2/H^7$ it follows that $j = j_0$ as required. □

Definition 3.3. A covariant column, respectively contravariant column, of degree m is a column vector $\mathbf{v} = (v_1, v_2, v_3)^T$ of homogeneous polynomials of degree m in variables a, b, c such that $\mathbf{v} \circ g = g\mathbf{v}$, respectively $\mathbf{v} \circ g = g^{-T}v$, for all $g \in G$.

We note that $\mathbf{x} = (a, b, c)^T$ is a covariant column of degree 1, whereas if I is an invariant of degree m then $\nabla I = (\frac{\partial I}{\partial a}, \frac{\partial I}{\partial b}, \frac{\partial I}{\partial c})^T$ is a contravariant column of degree $m - 1$.

Lemma 3.4. *Let E/K be an elliptic curve and $\phi : E[7] \cong \mu_7 \times \mathbb{Z}/7\mathbb{Z}$ a symplectic isomorphism over $\overline{K}$. Let $(a : b : c)$ be the corresponding $\overline{K}$-point on $X(7) \subset \mathbb{P}^2$ with co-ordinates (a, b, c) scaled so that*

$$c_4(a,b,c) = c_4(E) \quad \text{and} \quad c_6(a,b,c) = c_6(E) \tag{12}$$

where E has Weierstrass equation $y^2 = x^3 - 27c_4(E)x - 54c_6(E)$. If $j(E) \neq 0, 1728$ and $h \in \mathrm{GL}_3(\overline{K})$ is a matrix whose columns are covariant columns, respectively contravariant columns, of the same degree mod 7 evaluated at (a, b, c) then

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

respectively

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

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

PROOF: Let $\xi_\sigma = \sigma(\phi)\phi^{-1} \in \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. Recalling that ρ describes the action of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ on $X(7) \subset \mathbb{P}^2$ we have

$$\sigma((a,b,c)^T) = \lambda_\sigma \rho(\xi_\sigma)(a,b,c)^T \tag{13}$$

for some $\lambda_\sigma \in \overline{K}^\times$. Since c_4 and c_6 are invariants of degrees 14 and 21 we deduce

$$\sigma(c_4(a,b,c)) = \lambda_\sigma^{14} c_4(a,b,c) \quad \text{and} \quad \sigma(c_6(a,b,c)) = \lambda_\sigma^{21} c_6(a,b,c)$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Since $c_4(E), c_6(E) \in K$ it follows by (12) and our assumption $j(E) \neq 0, 1728$ that $\lambda_\sigma^{14} = \lambda_\sigma^{21} = 1$. Hence λ_σ is a 7th root of unity. Now suppose the columns of h are obtain by specialising polynomials whose degrees are all congruent to r mod 7. Then by (13) and Definition 3.3 we have

$$\sigma(h) = h \circ (\lambda_\sigma \rho(\xi_\sigma)) = \lambda_\sigma^r \rho(\xi_\sigma) h,$$

respectively

$$\sigma(h) = h \circ (\lambda_\sigma \rho(\xi_\sigma)) = \lambda_\sigma^r \rho(\xi_\sigma)^{-T} h.$$

Hence $\sigma(h)h^{-1} \propto \rho(\xi_\sigma)$, respectively $\sigma(h)h^{-1} \propto \rho(\xi_\sigma)^{-T}$, as required. □

We use Lemmas 1.6 and 3.4 to compute equations for $X_E(7)$ and $X_E^-(7)$. First we classify the covariant and contravariant columns. It is evident that

- The dot product of a covariant column and a contravariant column is an invariant.
- The cross product of two covariant columns is a contravariant column.
- The cross product of two contravariant columns is a covariant column.

We also write $[\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3] = (\mathbf{v}_1 \times \mathbf{v}_2) \cdot \mathbf{v}_3$ for the scalar triple product. It is easy to solve for the covariant and contravariant columns of any given degree by linear algebra. Let $\mathbf{e}$ and $\mathbf{f}$ be the covariant columns of degrees 9 and 11 given by

$$\mathbf{e} = \frac{I_{22}(\nabla F \times \nabla H) - c_4(\nabla F \times \nabla c_4) + 12H^2(\nabla H \times \nabla c_4)}{14c_6}$$

$$\mathbf{f} = \frac{I_{24}(\nabla F \times \nabla H) - (16F^4 - 104FH^2)(\nabla F \times \nabla c_4) + c_4(\nabla H \times \nabla c_4)}{14c_6}$$

where

$$I_{22} = 448F^4H - 48F^2c_4 - 2048FH^3$$
$$I_{24} = 128F^6 - 160F^3H^2 - 236FHc_4 - 336H^4.$$

Lemma 3.5. (i) *The covariant columns of odd degree, respectively even degree, form a free $k[F,H,c_4]$-module of rank 3 generated by $\mathbf{x}$, $\mathbf{e}$, $\mathbf{f}$, respectively $\nabla F \times \nabla H, \nabla F \times \nabla c_4, \nabla H \times \nabla c_4$.*

(ii) *The contravariant columns of odd degree, respectively even degree, form a free $k[F,H,c_4]$-module of rank 3 generated by ∇F, ∇H, ∇c_4, respectively $\mathbf{x} \times \mathbf{e}, \mathbf{x} \times \mathbf{f}, \mathbf{e} \times \mathbf{f}$.*

PROOF: By direct calculation we have $[\mathbf{x},\mathbf{e},\mathbf{f}] = -c_6$, whereas the definition of c_6 may be rewritten as $[\nabla F, \nabla H, \nabla c_4] = 14c_6$.

Let $\mathbf{v}$ be a covariant column of odd degree. We write $\mathbf{v} = I_1\mathbf{x} + I_2\mathbf{e} + I_3\mathbf{f}$ where I_1, I_2, I_3 are rational functions in a, b, c. Taking the dot product with $\mathbf{e}\times\mathbf{f}$ shows that $[\mathbf{v},\mathbf{e},\mathbf{f}] = I_1[\mathbf{x},\mathbf{e},\mathbf{f}]$. But $[\mathbf{v},\mathbf{e},\mathbf{f}]$ is an invariant of odd degree and therefore divisible by c_6. It follows that I_1 is an invariant and likewise for I_2 and I_3.

The other cases are similar. □

Theorem 3.6. *Let E/K be an elliptic curve with Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$ and let $\Delta = (c_4^3 - c_6^2)/1728$. If $j(E) \neq 0, 1728$ then $X_E(7) \subset \mathbb{P}^2$ has equation $\mathbf{F} = 0$ where*

$$\begin{aligned}\mathbf{F} = 12x^3z + 108x^2y^2 + 3c_4x^2z^2 + 72c_4xy^2z - 108c_4y^4 - 12c_6xyz^2 \\ + 84c_6y^3z + c_4^2xz^3 - 15c_4^2y^2z^2 + c_4c_6yz^3 + 768\Delta z^4,\end{aligned}$$

and $X_E^-(7) \subset \mathbb{P}^2$ has equation $\mathbf{G} = 0$ where

$$\begin{aligned}\mathbf{G} = 3x^4 + c_4x^3z - 18c_4x^2y^2 - 3c_6x^2yz + 24c_6xy^3 + 3c_4^2xy^2z \\ - 9c_4^2y^4 - c_4c_6y^3z + 168\Delta xz^3 + 1728\Delta y^2z^2 + 5c_4\Delta z^4.\end{aligned}$$

PROOF: The covariant columns $\mathbf{x}$, $\nabla F \times \nabla H$, $H\mathbf{e}$ have degrees 1, 8, 15, and the contravariant columns ∇F, $\mathbf{x}\times\mathbf{e}$, $H^2\nabla H$ have degrees 3, 10, 17. The determinants of the matrices formed from these columns are

$$\begin{aligned}\det(\mathbf{x}, (\nabla F \times \nabla H), H\mathbf{e}) &= 72H^4 - 4c_4FH \\ \det(\nabla F, (\mathbf{x}\times\mathbf{e}), H^2\nabla H) &= 72H^5 - 4c_4FH^2.\end{aligned} \tag{14}$$

The coefficients of the quartic $\widetilde{F}(x,y,z) = F(x\mathbf{x} + y(\nabla F \times \nabla H) + zH\mathbf{e})$ are invariants. Using linear algebra to rewrite these invariants as polynomials in F, H, c_4 and c_6 we find

$$\begin{aligned}\widetilde{F}(x,y,z) &= Fx^4 + 12H^3x^3z + (108H^3 - 6c_4F)x^2y^2 - 8c_6Fxy^3 \\ &+ 3c_4H^3x^2z^2 + (72c_4H^3 + 4128F^2H^4 + 48c_4F^3H - 768F^5H^2)xy^2z \\ &+ (-108c_4H^3 - 3c_4^2F - 11376F^2H^4 + 32c_4F^3H + 3392F^5H^2 - 256F^8)y^4 \\ &- 12c_6H^3xyz^2 + (84c_6H^3 - 16c_6F^3H)y^3z + (c_4^2H^3 + 688FH^7 \\ &+ 8c_4F^2H^4 - 128F^4H^5)xz^3 + (-15c_4^2H^3 - 10512FH^7 - 384c_4F^2H^4 \\ &+ 6144F^4H^5 + 96c_4F^5H^2 - 768F^7H^3)y^2z^2 + (c_4c_6H^3 - 8c_6F^2H^4)yz^3 \\ &+ (768H^{10} - 36c_4FH^7 - c_4^2F^2H^4 + 176F^3H^8 + 16c_4F^4H^5 - 64F^6H^6)z^4.\end{aligned}$$

Likewise $\widetilde{G}(x,y,z) = F(x\nabla F + y(\mathbf{x}\times\mathbf{e}) + zH^2\nabla H)$ becomes

$$\begin{aligned}\widetilde{G}(x,y,z) &= (3H^2+28F^3)x^4 + (c_4H^2+168F^2H^3)x^3z + (-18c_4H^2\\ &\quad - 816F^2H^3 - 24c_4F^3 + 192F^5H)x^2y^2 - 3c_6H^2x^2yz + 24c_6H^2xy^3\\ &\quad + (222FH^6 + 24F^4H^4)x^2z^2 + (3c_4^2H^2 + 3744FH^6 - 576F^4H^4)xy^2z\\ &\quad + (-9c_4^2H^2 - 5184FH^6 - 240c_4F^2H^3 - 4c_4^2F^3 + 2240F^4H^4 + 64c_4F^5H\\ &\quad - 256F^7H^2)y^4 + (-c_4c_6H^2 + 8c_6F^2H^3)y^3z + (168H^9 + 3c_4FH^6\\ &\quad + 24F^3H^7)xz^3 + (1728H^9 - 78c_4FH^6 + 816F^3H^7 + 24c_4F^4H^4\\ &\quad - 192F^6H^5)y^2z^2 + c_6FH^6yz^3 + (5c_4H^9 + 35F^2H^{10} - 4F^5H^8)z^4.\end{aligned}$$

Let $(a:b:c)$ be the $\overline{K}$-point on $X(7)$ corresponding to (E,ϕ) for some choice of symplectic isomorphism $\phi : E[7] \cong \mu_7\times\mathbb{Z}/7\mathbb{Z}$. By Lemma 3.2 we may scale (a,b,c) to satisfy (12). Then by Lemmas 1.6 and 3.4 a formula for $X_E(7)$, respectively $X_E^-(7)$, is given by specialising the coefficients of $\widetilde{F}$, respectively $\widetilde{G}$, to this choice of (a,b,c). Explicitly we set $F=0$, divide through by H^3, respectively H^2, and replace H^7 by Δ. □

Remark 3.7. The equations for $X_E(7)$ and $X_E^-(7)$ given in Theorems 1.2 and 3.6 are related by $\mathcal{F}(x,y,z) = \frac{1}{4}\mathbf{F}(6c_4z - \frac{1}{3}y, x, -18z)$ and $\mathcal{G}(x,y,z) = \mathbf{G}(9c_4y + z, 3x, 108y)$ where $a=-27c_4$ and $b=-54c_6$.

3.2. **Formulae in the case $n=9$.** We recall that $X(9) = \{F_1 = F_2 = 0\} \subset \mathbb{P}^3$ where $F_1 = a^2b+b^2c+c^2a$ and $F_2 = ab^2+bc^2+ca^2-d^3$. Let $G \cong \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ be the image of $\rho : \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}) \to \mathrm{SL}_4(\overline{K})$. It is generated by

$$\frac{1}{3}\begin{pmatrix} \zeta_9-\zeta_9^8 & \zeta_9^7-\zeta_9^2 & \zeta_9^4-\zeta_9^5 & \zeta_9^3-\zeta_9^6\\ \zeta_9^7-\zeta_9^2 & \zeta_9^4-\zeta_9^5 & \zeta_9-\zeta_9^8 & \zeta_9^3-\zeta_9^6\\ \zeta_9^4-\zeta_9^5 & \zeta_9-\zeta_9^8 & \zeta_9^7-\zeta_9^2 & \zeta_9^3-\zeta_9^6\\ \zeta_9^3-\zeta_9^6 & \zeta_9^3-\zeta_9^6 & \zeta_9^3-\zeta_9^6 & 0\end{pmatrix} \quad\text{and}\quad \begin{pmatrix}\zeta_9 & 0 & 0 & 0\\ 0 & \zeta_9^4 & 0 & 0\\ 0 & 0 & \zeta_9^7 & 0\\ 0 & 0 & 0 & \zeta_9^6\end{pmatrix}$$

Let $\chi : G \to \mu_3$ be the character given by $\mathrm{Diag}(\zeta_9,\zeta_9^4,\zeta_9^7,\zeta_9^6) \mapsto \zeta_9^3$.

Definition 3.8. An invariant of type $r\in\{0,1,2\}$ and degree m is a homogeneous polynomial $I = I(a,b,c,d)$ of degree m such that $I\circ g = \chi(g)^r I$ for all $g\in G$.

The type 0 invariants of smallest degree are $D = -(a^3+b^3+c^3-3abc)d$ and $I_6 = 2(a^5b+b^5c+c^5a)+5(a^4c^2+b^4a^2+c^4b^2)+20abc(a^2b+b^2c+c^2a)-3d^6$. Writing A and B for their matrices of second partial derivatives we find

$$\det(A+tB) = 81D^2 - 1620DI_6t + 2700I_{12}t^2 + 90000D^4t^4.$$

where I_{12} is a type 0 invariant of degree 12.

Definition 3.9. A covariant column, respectively contravariant column, of type $r \in \{0,1,2\}$ and degree m is a column vector $\mathbf{v} = (v_1, v_2, v_3, v_4)^T$ of homogeneous polynomials of degree m in variables a, b, c, d such that $\mathbf{v} \circ g = \chi(g)^r g\mathbf{v}$, respectively $\mathbf{v} \circ g = \chi(g)^r g^{-T}\mathbf{v}$, for all $g \in G$.

We note that $\mathbf{x}_1 = (a, b, c, d)^T$ is a covariant column of type 0 and degree 1, whereas if I is an invariant of type r and degree m then $\nabla I = (\frac{\partial I}{\partial a}, \frac{\partial I}{\partial b}, \frac{\partial I}{\partial c}, \frac{\partial I}{\partial d})^T$ is a contravariant column of type r and degree $m-1$. To construct some further examples we define 4×4 alternating matrices

$$\Lambda_i = \begin{pmatrix} 0 & \mathfrak{q}_i(a,b,c)d^2 & -\mathfrak{q}_i(c,a,b)d^2 & \mathfrak{r}_i(a,b,c) \\ -\mathfrak{q}_i(a,b,c)d^2 & 0 & \mathfrak{q}_i(b,c,a)d^2 & \mathfrak{r}_i(b,c,a) \\ \mathfrak{q}_i(c,a,b)d^2 & -\mathfrak{q}_i(b,c,a)d^2 & 0 & \mathfrak{r}_i(c,a,b) \\ -\mathfrak{r}_i(a,b,c) & -\mathfrak{r}_i(b,c,a) & -\mathfrak{r}_i(c,a,b) & 0 \end{pmatrix}$$

for $i = 0, 1, 2$ where

$$\begin{aligned} \mathfrak{q}_0(a,b,c) &= 3(a^2 + 2bc) & \mathfrak{r}_0(a,b,c) &= 2(a^3b + c^3b) - 3a^2c^2 - b^4 \\ \mathfrak{q}_1(a,b,c) &= 3(c^2 + 2ab) & \mathfrak{r}_1(a,b,c) &= 2(b^3c + a^3c) - 3b^2a^2 - c^4 \\ \mathfrak{q}_2(a,b,c) &= 3(b^2 + 2ac) & \mathfrak{r}_2(a,b,c) &= 2(c^3a + b^3a) - 3c^2b^2 - a^4. \end{aligned}$$

For M a 4×4 alternating matrix and $\mathbf{v}$ a column vector we define a column vector $M \star \mathbf{v}$ by the rule $(M \star \mathbf{v})_l = \sum M_{ij} v_k$ where the sum is over all (i, j, k) for which (i, j, k, l) is an even permutation of $(1, 2, 3, 4)$. We define covariant and contravariant columns

$$\begin{aligned} \mathbf{x}_7 &= \Lambda_0 \nabla D & \mathbf{e}_9 &= \Lambda_1 \nabla I_6 & \mathbf{u}_5 &= \Lambda_1 \star \mathbf{x}_1 \\ \mathbf{e}_7 &= \Lambda_1 \nabla D & \mathbf{f}_7 &= \Lambda_2 \nabla D & \mathbf{v}_{11} &= \Lambda_2 \star \mathbf{x}_7. \end{aligned}$$

Then $c_4 = \mathbf{x}_7 \cdot \mathbf{u}_5$ is an invariant of type 1 and degree 12, and $c_6 = \frac{1}{2}(\mathbf{x}_7 \cdot \nabla I_{12})$ is an invariant of type 0 and degree 18. Routine Gröbner basis calculations show that $c_4, c_6 \notin (F_1, F_2)$ yet

$$c_4^3 - c_6^2 \equiv 1728 D^9 \mod (F_1, F_2).$$

Lemma 3.10. *The j-invariant $X(9) \to \mathbb{P}^1$ is given by $j = c_4^3/D^9$.*

Proof: Both j and $j_0 = c_4^3/D^9$ define maps $X(9) \to \mathbb{P}^1$ that quotient out by the action of $G/\{\pm I\} \cong \mathrm{PSL}_2(\mathbb{Z}/9\mathbb{Z})$. So they can differ by at most a Möbius map.

We recall that j is ramified above 0, 1728 and ∞ with ramification indices 3, 2 and 9. Since

$$\begin{aligned}\#\{F_1 = F_2 = c_4 = 0\} &\leq 9\deg(c_4) = \tfrac{1}{3}|G/\{\pm I\}|\\ \#\{F_1 = F_2 = c_6 = 0\} &\leq 9\deg(c_6) = \tfrac{1}{2}|G/\{\pm I\}|\\ \#\{F_1 = F_2 = D = 0\} &\leq 9\deg(D) = \tfrac{1}{9}|G/\{\pm I\}|\end{aligned}$$

and $j_0 - 1728 = c_6^2/D^9$ it follows that $j = j_0$ as required. □

Lemma 3.11. *Let E/K be an elliptic curve and $\phi : E[9] \cong \mu_9 \times \mathbb{Z}/9\mathbb{Z}$ a symplectic isomorphism over $\overline{K}$. Let $(a : b : c : d)$ be the corresponding $\overline{K}$-point on $X(9) \subset \mathbb{P}^3$ with co-ordinates (a, b, c, d) scaled so that*

$$c_4(a, b, c, d) = c_4(E) \quad \text{and} \quad c_6(a, b, c, d) = c_6(E) \tag{15}$$

where E has Weierstrass equation $y^2 = x^3 - 27c_4(E)x - 54c_6(E)$. If $j(E) \neq 0, 1728$ and $h \in \mathrm{GL}_4(\overline{K})$ is a matrix whose columns are covariant columns, respectively contravariant columns, of types $r_1, \ldots, r_4$ and degrees $m_1, \ldots, m_4$ with $m_i + 6r_i$ constant mod 18, evaluated at (a, b, c, d) then

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

respectively

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

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Proof: Let $\xi_\sigma = \sigma(\phi)\phi^{-1} \in \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$. Recalling that ρ describes the action of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ on $X(9) \subset \mathbb{P}^3$ we have

$$\sigma((a, b, c, d)^T) = \lambda_\sigma \rho(\xi_\sigma)(a, b, c, d)^T \tag{16}$$

for some $\lambda_\sigma \in \overline{K}^\times$. Since c_4 and c_6 are invariants of types 1 and 0 and degrees 12 and 18 we deduce

$$\sigma(c_4(a, b, c, d)) = \lambda_\sigma^{12}\chi_\sigma c_4(a, b, c, d) \quad \text{and} \quad \sigma(c_6(a, b, c, d)) = \lambda_\sigma^{18} c_6(a, b, c, d)$$

where $\chi_\sigma = \chi(\rho(\xi_\sigma))$. Since $c_4(E), c_6(E) \in K$ it follows by (15) and our assumption $j(E) \neq 0, 1728$ that $\lambda_\sigma^{12}\chi_\sigma = \lambda_\sigma^{18} = 1$. Hence λ_σ is an 18th root of unity and $\chi_\sigma = \lambda_\sigma^6$. Now suppose the columns of h are obtained by specialising covariant columns, respectively contravariant columns, of types $r_1, \ldots, r_4$ and degrees $m_1, \ldots, m_4$ with $m_i + 6r_i \equiv r \pmod{18}$. Then by (16) and Definition 3.9 we have

$$\sigma(h) = h \circ (\lambda_\sigma \rho(\xi_\sigma)) = \lambda_\sigma^r \rho(\xi_\sigma)h,$$

respectively

$$\sigma(h) = h \circ (\lambda_\sigma \rho(\xi_\sigma)) = \lambda_\sigma^r \rho(\xi_\sigma)^{-T}h.$$

□

We use Lemmas 1.6 and 3.11 to compute equations for $X_E(9)$ and $X_E^-(9)$. First we construct some more covariant and contravariant columns. Let $\mathbf{v}_9$ be the contravariant column of type 2 and degree 9 given by

$$\mathbf{v}_9 = (f_1 d, f_2 d, f_3 d, -af_1 - bf_2 - cf_3)^T$$

where

$$\begin{aligned} f_1(a,b,c,d) &= a^8 + 35a^6bc + 42a^5b^3 + 7a^5c^3 + 105a^4b^2c^2 + 28a^4bd^3 \\ &+ 231a^3b^4c - 196a^3bc^4 + 14a^3c^2d^3 + 14a^2b^6 - 70a^2b^3c^3 - 84a^2b^2cd^3 \\ &- 21a^2c^6 + 28ab^4d^3 - 105ab^2c^5 - 14abc^3d^3 - 27acd^6 + 19b^7c \\ &- 35b^4c^4 + 14b^3c^2d^3 + 27b^2d^6 - 27bc^7 + 14c^5d^3, \end{aligned}$$

$f_2(a,b,c,d) = f_1(b,c,a,d)$ and $f_3(a,b,c,d) = f_1(c,a,b,d)$. We further put

$$\mathbf{x}_{13} = \Lambda_1 \mathbf{v}_9 \qquad \mathbf{x}_{15} = \Lambda_1 \mathbf{v}_{11} \qquad \mathbf{f}_{13} = \Lambda_0 \mathbf{v}_9.$$

In the following lemma the entries of the covariant and contravariant columns are viewed as elements of the co-ordinate ring $K[a,b,c,d]/(F_1,F_2)$. The lemma is included to show that we have been systematic, rather than because it is needed in what follows. We therefore omit the proof.

Lemma 3.12. *The covariant columns, respectively contravariant columns, of type $r \in \{0,1,2\}$, mod (F_1,F_2), form a free $K[D,c_6]$-module of rank 4 with basis as indicated in the following table.*

Covariants			*Contravariants*		
Type 0	*Type 1*	*Type 2*	*Type 0*	*Type 1*	*Type 2*
$\mathbf{x}_1$	$\mathbf{e}_7$	$\mathbf{f}_7$	∇D	$\mathbf{u}_5$	$\mathbf{v}_9$
$\mathbf{x}_7$	$\mathbf{e}_9$	$\mathbf{f}_{13}$	∇I_6	∇c_4	$\mathbf{v}_{11}$
$\mathbf{x}_{13}$	$c_4\mathbf{x}_1$	$c_4\mathbf{e}_7$	∇I_{12}	$c_4\nabla D$	$c_4\mathbf{u}_5$
$\mathbf{x}_{15}$	$c_4\mathbf{x}_7$	$c_4\mathbf{e}_9$	∇c_6	$c_4\nabla I_6$	$c_4\nabla c_4$

Theorem 3.13. *Let E/K be an elliptic curve with Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$. If $j(E) \neq 0, 1728$ then $X_E(9) \subset \mathbb{P}^3$ has equations $\mathbf{F}_1 = \mathbf{F}_2 = 0$*

where

$$\begin{aligned}\mathbf{F}_1 &= 24x^2t - 96xyz + 64y^3 + 24c_4y^2t + 48c_4yz^2 - 48c_6yzt + 12c_4^2yt^2 \\ &\quad - 8c_6z^3 + 12c_4^2z^2t - 6c_4c_6zt^2 - (c_4^3 - 2c_6^2)t^3, \\ \mathbf{F}_2 &= 16x^2z - 64xy^2 - 16c_4xyt - 16c_4xz^2 + 16c_6xzt - 4c_4^2xt^2 + 80c_4y^2z \\ &\quad - 32c_6y^2t - 32c_6yz^2 + 32c_4^2yzt - 8c_4c_6yt^2 + 8c_4^2z^3 - 12c_4c_6z^2t \\ &\quad + (2c_4^3 + 4c_6^2)zt^2 - c_4^2c_6t^3.\end{aligned}$$

and $X_E^-(9) \subset \mathbb{P}^3$ *has equations* $\mathbf{G}_1 = \mathbf{G}_2 = 0$ *where*

$$\begin{aligned}\mathbf{G}_1 &= -72x^2y - 144x^2z + 24c_4xyt - 48c_4xzt - 8c_6xt^2 - c_4y^3 + 18c_4y^2z \\ &\quad + 3c_6y^2t + 180c_4yz^2 + 12c_6yzt - 3c_4^2yt^2 + 792c_4z^3 + 12c_6z^2t \\ &\quad + 2c_4^2zt^2 + c_4c_6t^3, \\ \mathbf{G}_2 &= -864x^3 + 216c_4x^2t + 2592c_4xyz + 216c_6xyt + 15552c_4xz^2 \\ &\quad + 432c_6xzt - 72c_4^2xt^2 - 9c_6y^3 + 162c_6y^2z + 27c_4^2y^2t + 4212c_6yz^2 \\ &\quad + 108c_4^2yzt - 27c_4c_6yt^2 + 26136c_6z^3 + 972c_4^2z^2t + 18c_4c_6zt^2 \\ &\quad + (5c_4^3 + 4c_6^2)t^3.\end{aligned}$$

Proof: The covariant columns $\mathbf{x}_1, \mathbf{f}_7, D\mathbf{e}_9, D\mathbf{x}_{15}$ have types $0, 2, 1, 0$ and degrees $1, 7, 13, 19$. The contravariant columns $\mathbf{u}_5, D^2\nabla D, \nabla I_{12}, D^2\mathbf{v}_9$ have types $1, 0, 0, 2$ and degrees $5, 11, 11, 17$. The determinants of the matrices formed from these columns satisfy

$$\begin{aligned}\det(\mathbf{x}_1, \mathbf{f}_7, D\mathbf{e}_9, D\mathbf{x}_{15}) &\equiv 3456D^{10} \mod (F_1, F_2) \\ \det(\mathbf{u}_5, D^2\nabla D, \nabla I_{12}, D^2\mathbf{v}_9) &\equiv 1152D^{11} \mod (F_1, F_2).\end{aligned}$$

For certain 2×2 matrices $\alpha = (\alpha_{ij})$ and $\beta = (\beta_{ij})$, specified in Remark 3.14 below, we put

$$\begin{aligned}\mathbf{F}_i(x, y, z, t) &= (\alpha_{i1}F_1 + \alpha_{i2}F_2)(x\mathbf{x}_1 + y\mathbf{f}_7 + zD\mathbf{e}_9 + tD\mathbf{x}_{15}) \\ \mathbf{G}_i(x, y, z, t) &= (\beta_{i1}F_1 + \beta_{i2}F_2)(x\mathbf{u}_5 + yD^2\nabla D + z\nabla I_{12} + tD^2\mathbf{v}_9)\end{aligned}$$

for $i = 1, 2$. Using the Gröbner basis machinery in Magma to write each coefficient mod (F_1, F_2) as a polynomial in c_4 and c_6 we obtained the equations in the statement of the theorem. By Lemmas 1.6, 3.10 and 3.11 these are equations for $X_E(9)$ and $X_E^-(9)$. □

Remark 3.14. (i) The 2×2 matrices used in the proof of Theorem 3.13 were

$$\alpha = \frac{1}{9D^6}\begin{pmatrix} 3B & 9A \\ -(108A^3+B^3) & 9AB^2 \end{pmatrix} \text{ and } \beta = \frac{1}{D^6}\begin{pmatrix} 6A & -B \\ 162AB^2 & 9(108A^3+B^3) \end{pmatrix}$$

where $A = d^3$ and $B = a^3 + b^3 + c^3 + 6abc$.
(ii) The equations for $X_E(9)$ and $X_E^-(9)$ in Theorems 1.3 and 3.13 are related by

$$\mathcal{F}_i(x,y,z,t) \propto \mathbf{F}_i(x - 27c_4z - 162c_6t, 9y + 81c_4t, -54z, 324t)$$
$$\mathcal{G}_i(x,y,z,t) \propto \mathbf{G}_i(-x + 9c_4t, 36y + 36z, 6z, 108t)$$

for $i = 1, 2$ where $a = -27c_4$ and $b = -54c_6$.

3.3. **Formulae in the case $n = 11$.** We recall that $X(11)$ is the singular locus of the Hessian of the cubic threefold $\{F = 0\} \subset \mathbb{P}^4$ where

$$F = a^2b + b^2c + c^2d + d^2e + e^2a.$$

Let $G \cong \mathrm{PSL}_2(\mathbb{Z}/11\mathbb{Z})$ be the image of $\rho : \mathrm{SL}_2(\mathbb{Z}/11\mathbb{Z}) \to \mathrm{GL}_5(\overline{K})$. It is generated by

$$\frac{1}{g_{11}}\begin{pmatrix} \zeta_{11}-\zeta_{11}^{-1} & \zeta_{11}^{3}-\zeta_{11}^{-3} & \zeta_{11}^{9}-\zeta_{11}^{-9} & \zeta_{11}^{5}-\zeta_{11}^{-5} & \zeta_{11}^{4}-\zeta_{11}^{-4} \\ \zeta_{11}^{3}-\zeta_{11}^{-3} & \zeta_{11}^{9}-\zeta_{11}^{-9} & \zeta_{11}^{5}-\zeta_{11}^{-5} & \zeta_{11}^{4}-\zeta_{11}^{-4} & \zeta_{11}-\zeta_{11}^{-1} \\ \zeta_{11}^{9}-\zeta_{11}^{-9} & \zeta_{11}^{5}-\zeta_{11}^{-5} & \zeta_{11}^{4}-\zeta_{11}^{-4} & \zeta_{11}-\zeta_{11}^{-1} & \zeta_{11}^{3}-\zeta_{11}^{-3} \\ \zeta_{11}^{5}-\zeta_{11}^{-5} & \zeta_{11}^{4}-\zeta_{11}^{-4} & \zeta_{11}-\zeta_{11}^{-1} & \zeta_{11}^{3}-\zeta_{11}^{-3} & \zeta_{11}^{9}-\zeta_{11}^{-9} \\ \zeta_{11}^{4}-\zeta_{11}^{-4} & \zeta_{11}-\zeta_{11}^{-1} & \zeta_{11}^{3}-\zeta_{11}^{-3} & \zeta_{11}^{9}-\zeta_{11}^{-9} & \zeta_{11}^{5}-\zeta_{11}^{-5} \end{pmatrix}$$

and $\mathrm{Diag}(\zeta_{11}, \zeta_{11}^9, \zeta_{11}^4, \zeta_{11}^3, \zeta_{11}^5)$ where $g_{11} = 1 + 2(\zeta_{11} + \zeta_{11}^3 + \zeta_{11}^9 + \zeta_{11}^5 + \zeta_{11}^4)$. We define the invariants, covariant columns and contravariant columns exactly as in Section 3.1. Let $\sum$ denote a sum over all cyclic permutations, so that for example $F = \sum a^2b$. Other examples of invariants of small degree include

$$H = 3abcde + \sum(a^3c^2 - a^3de),$$
$$I_7 = \sum(a^6e + 3a^5d^2 - 15a^4bce + 5a^3b^3d + 15a^3bcd^2),$$
$$I_8 = \sum(a^7c - 7a^4bd^3 - 7a^4de^3 + 7a^3b^2c^3 + 21a^3c^2d^2e).$$

Writing A and B for the matrices of second partial derivatives of F and H we find

$$\det(A + tB) = 32H - 32I_7t - 24I_9t^2 - 8c_4t^3 + \dots$$

where I_9 and c_4 are invariants of degrees 9 and 11. We will not need a complete set of generators for the ring of invariants, but note that this is given in [A] and may also be computed using Magma. Let $\mathcal{I}$ be the homogeneous ideal of $X(11)$,

i.e. the ideal generated by the 4×4 minors of the Hessian matrix of F. The degree 19 polynomial

$$\begin{aligned}\widetilde{c}_6 &= a^9b^{10} - 509b^{18}d - 14107b^{14}d^4e + 510b^9c^{10} + 42326b^7d^{12} + 20669b^3d^{15}e \\ &- 14107b^2d^2e^{15} - 277419bc^2d^{10}e^6 - 248909bcd^{16}e - 209926bcd^5e^{12} \\ &+ 762409bd^{11}e^7 + be^{18} - 1018c^{18}e - 14107c^{16}de^2 - 586835c^{12}d^3e^4 \\ &+ 197780c^{10}d^4e^5 + 1019c^9d^{10} - 787130c^8d^5e^6 + 15634c^7d^{11}e + 42326c^7e^{12} \\ &+ 2007576c^6d^6e^7 + 247382c^5d^{12}e^2 - 528424c^5de^{13} - 616653c^4d^7e^8 \\ &+ 376744c^3d^{13}e^3 + 1067732c^3d^2e^{14} - 225004c^2d^8e^9 + 463659cd^{14}e^4 \\ &- 582142cd^3e^{15} + 70511d^9e^{10}\end{aligned}$$

is not an invariant but satisfies

$$\widetilde{c}_6^{\,2} \equiv abcde(c_4^3 - 1728F^{11}) \pmod{\mathcal{I}}.$$

Lemma 3.15. *The j-invariant $X(11) \to \mathbb{P}^1$ is given by $j = c_4^3/F^{11}$.*

Proof: Both j and $j_0 = c_4^3/F^{11}$ define maps $X(11) \to \mathbb{P}^1$ that quotient out by the action of $G \cong \mathrm{PSL}_2(\mathbb{Z}/11\mathbb{Z})$. So they can differ by at most a Möbius map. We recall that j is ramified above 0, 1728 and ∞ with ramification indices 3, 2 and 11. It is shown in [AR, Corollary 23.28] that $X(11) \subset \mathbb{P}^4$ has degree 20. Since

$$\begin{aligned}\#X(11) \cap \{c_4 = 0\} &\le 20\deg(c_4) = \tfrac{1}{3}|G| \\ \#X(11) \cap \{\widetilde{c}_6 = 0\} &\le 20\deg(\widetilde{c}_6) < |G| \\ \#X(11) \cap \{F = 0\} &\le 20\deg(F) = \tfrac{1}{11}|G|\end{aligned}$$

and $j_0 - 1728 = \widetilde{c}_6^{\,2}/((abcde)F^{11})$ it follows that $j = j_0$ as required. □

Lemma 3.16. *Let E/K be an elliptic curve and $\phi : E[11] \cong \mu_{11} \times \mathbb{Z}/11\mathbb{Z}$ a symplectic isomorphism over $\overline{K}$. Let $(a : b : c : d : e)$ be the corresponding $\overline{K}$-point on $X(11) \subset \mathbb{P}^4$ with co-ordinates (a, b, c, d, e) scaled so that*

$$c_4(a, b, c, d, e) = c_4(E) \tag{17}$$

where E has Weierstrass equation $y^2 = x^3 - 27c_4(E)x - 54c_6(E)$. If $j(E) \neq 0$ and $h \in \mathrm{GL}_5(\overline{K})$ is a matrix whose columns are covariant columns, respectively contravariant columns, of the same degree mod 11 evaluated at (a, b, c, d, e) then

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

respectively

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

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

PROOF: The proof is similar to that of Lemma 3.4. Recall that c_4 is a homogeneous polynomial of degree 11 and so (17) determines the scaling of (a, b, c, d, e) up to an 11th root of unity. □

We use Lemmas 1.6 and 3.16 to compute equations for $X_E(11)$ and $X_E^-(11)$. First we construct some covariant columns. Let $\mathbf{x}_1 = (a, b, c, d, e)^T$. If $\gamma \in \mathrm{SL}_2(\mathbb{Z}/11\mathbb{Z})$ is diagonal then $\rho(\gamma)$ cyclically permutes the co-ordinates a, b, c, d, e. A covariant column is therefore uniquely determined by its first entry. By averaging over the group we found covariant columns $\mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_9$ with first entries

$$\begin{aligned}
f_4 &= 2a^2e^2 + 4ab^2c - 4ac^2d + 4bce^2 + d^4,\\
f_5 &= -5a^3ce + 5a^2b^2d + 5a^2cd^2 + 5abc^2e - 10abde^2 + b^5 - 5b^3cd + 5bd^3e + 5c^2e^3,\\
f_9 &= -14a^6bde - 8a^5bd^3 + 9a^5c^2e^2 + 2a^5de^3 + 8a^4b^4e + 5a^4b^2c^3 + 63a^4b^2cde\\
&\quad + 6a^4c^4d - 18a^4c^2d^2e + 8a^4d^3e^2 + 31a^3b^4d^2 - 21a^3b^3e^3 + 47a^3b^2cd^3 + 35a^3bc^3e^2\\
&\quad + 14a^3bcde^3 - 12a^3c^2d^4 + 10a^3d^5e + 3a^2b^5ce - 26a^2b^3c^4 - 42a^2b^3c^2de\\
&\quad - 75a^2b^3d^2e^2 + 3a^2b^2e^5 + 18a^2bc^5d - 30a^2bc^3d^2e - 36a^2bcd^3e^2 + 2a^2c^3e^4\\
&\quad - 9a^2cde^5 + a^2d^7 - 2ab^7d - 6ab^5cd^2 + 50ab^4ce^3 - 7ab^3c^2d^3 - 6ab^3d^4e\\
&\quad - 54ab^2c^4e^2 - 3ab^2c^2de^3 - 9ab^2d^2e^4 - 29abc^3d^4 + 21abcd^5e + abe^7 + 9ac^5de^2\\
&\quad + 25ac^3d^2e^3 - 7acd^3e^4 - 10b^6c^2e - 2b^6de^2 + 4b^4c^5 + 40b^4c^3de - 6b^4cd^2e^2\\
&\quad + 13b^3ce^5 - 3b^3d^6 - 15b^2c^4d^2e - 54b^2c^2d^3e^2 + 31b^2d^4e^3 - 11bc^4e^4 + 3bc^2de^5\\
&\quad - 2bcd^7 - 7bd^2e^6 - c^7d^2 + 5c^5d^3e - 9c^3d^4e^2 + 8cd^5e^3 - e^9.
\end{aligned}$$

We temporarily write $a_1, \ldots, a_5$ for a, b, c, d, e and let Ξ be the 5×5 alternating matrix with entries

$$\Xi_{ij} = \frac{\partial F}{\partial a_r}\frac{\partial I_7}{\partial a_s} - \frac{\partial F}{\partial a_s}\frac{\partial I_7}{\partial a_r}$$

where $r \equiv (i-j-2)^3 + i + 3 \pmod 5$ and $s \equiv (j-i-2)^3 + j + 3 \pmod 5$. Then $\mathbf{x}_{14} = \Xi\nabla I_7$ is a covariant column of degree 14.

Theorem 3.17. *Let E/K be an elliptic curve with Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$ and let $\Delta = (c_4^3 - c_6^2)/1728$. If $j(E) \neq 0, 1728$ then $X_E(11) \subset \mathbb{P}^4$ is the singular locus of the Hessian of*

$$\begin{aligned}
\mathbf{F} &= v^3 + 3v^2w + c_4v^2y + 3vw^2 + 2c_4vwy - c_4\Delta vx^2 + 48\Delta vxy\\
&\quad + 9w^3 + 5c_4w^2y - c_4^2w^2z + c_4^2wy^2 - 576\Delta wyz + 72c_4\Delta wz^2\\
&\quad - 4\Delta^2x^3 - 72\Delta^2x^2z + 4c_4\Delta xy^2 + 2c_4^2\Delta xyz - (c_4^3\Delta - 1728\Delta^2)xz^2\\
&\quad + 64\Delta y^3 - 72c_4\Delta y^2z + 12c_4^2\Delta yz^2 + (c_4^3\Delta - 3456\Delta^2)z^3,
\end{aligned}$$

and $X_E^-(11) \subset \mathbb{P}^4$ *is the singular locus of the Hessian of*

$$\begin{aligned}\mathbf{G} = {} & 5v^3 - c_4v^2x - 60v^2y + 28c_4v^2z - 2c_4\Delta vw^2 - 48\Delta vwx \\ & - 240\Delta vwz - 16c_4vxy + 1680vy^2 - 872c_4vyz + 121c_4^2vz^2 \\ & + 8\Delta^2w^3 + 44c_4\Delta w^2y - 11c_4^2\Delta w^2z + c_4\Delta wx^2 + 336\Delta wxy \\ & - 122c_4\Delta wxz + 25c_4^2wy^2 - 14160\Delta wyz + 817c_4\Delta wz^2 - 20\Delta x^3 \\ & + 5c_4^2x^2y - 1884\Delta x^2z - 364c_4xy^2 + 160c_4^2xyz - 34764\Delta xz^2 \\ & + 19840y^3 - 10268c_4y^2z + 1643c_4^2yz^2 - 129220\Delta z^3.\end{aligned}$$

Proof: The covariant columns $\mathbf{x}_1, \mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_9, \mathbf{x}_{14}$ have degrees $1, 4, 5, 9, 14$ and the contravariant columns $\nabla F, \nabla I_7, \nabla I_8, \nabla I_9, \nabla c_4$ have degrees $2, 6, 7, 8, 10$. The determinants of the matrices formed from these columns satisfy

$$\begin{aligned}\det(\mathbf{x}_1, \mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_9, \mathbf{x}_{14}) &= c_4^3 - 1728F^{11} \pmod{\mathcal{I}} \\ \det(\nabla F, \nabla I_7, \nabla I_8, \nabla I_9, \nabla c_4) &= 55(c_4^3 - 1728F^{11}) \pmod{\mathcal{I}}.\end{aligned} \tag{18}$$

The coefficients of the cubic $\widetilde{F}(v, w, x, y, z) = F(v\mathbf{x}_1 + w\mathbf{x}_4 + x\mathbf{x}_5 + y\mathbf{x}_9 + z\mathbf{x}_{14})$ are invariants. Using the Gröbner basis machinery in Magma to rewrite the coefficients mod $\mathcal{I}$ as polynomials in c_4 and F we find

$$\begin{aligned}\widetilde{F} = {} & Fv^3 + 3F^2v^2w + c_4v^2y + 3F^3vw^2 + 2Fc_4vwy - c_4vx^2 + 48F^5vxy \\ & + 9F^4w^3 + 5F^2c_4w^2y - c_4^2w^2z + c_4^2wy^2 - 576F^9wyz + 72F^7c_4wz^2 \\ & - 4F^5x^3 - 72F^8x^2z + 4F^4c_4xy^2 + 2F^2c_4^2xyz - (c_4^3 - 1728F^{11})xz^2 \\ & + 64F^9y^3 - 72F^7c_4y^2z + 12F^5c_4^2yz^2 + (F^3c_4^3 - 3456F^{14})z^3.\end{aligned}$$

Likewise $\widetilde{G}(v, w, x, y, z) = F(v\nabla F + w\nabla I_7 + x\nabla I_8 + y\nabla I_9 + z\nabla c_4)$ becomes

$$\begin{aligned}\widetilde{G} = {} & 5F^2v^3 - c_4v^2x - 60F^4v^2y + 28Fc_4v^2z - 2Fc_4vw^2 - 48F^5vwx \\ & - 240F^6vwz - 16F^2c_4vxy + 1680F^6vy^2 - 872F^3c_4vyz + 121c_4^2vz^2 \\ & + 8F^6w^3 + 44F^3c_4w^2y - 11c_4^2w^2z + F^3c_4wx^2 + 336F^7wxy \\ & - 122F^4c_4wxz + 25c_4^2wy^2 - 14160F^8wyz + 817F^5c_4wz^2 - 20F^7x^3 \\ & + 5c_4^2x^2y - 1884F^8x^2z - 364F^4c_4xy^2 + 160Fc_4^2xyz - 34764F^9xz^2 \\ & + 19840F^8y^3 - 10268F^5c_4y^2z + 1643F^2c_4^2yz^2 - 129220F^{10}z^3.\end{aligned}$$

Let $(a : b : c : d : e)$ be the $\overline{K}$-point on $X(11)$ corresponding to (E, ϕ) for some choice of symplectic isomorphism $\phi : E[11] \cong \mu_{11} \times \mathbb{Z}/11\mathbb{Z}$. By Lemma 3.15 we may scale (a, b, c, d, e) to satisfy (17) and $F(a, b, c, d, e)^{11} = \Delta$. Moreover the determinants (18) are non-zero by our assumption $j(E) \neq 1728$. Then by Lemmas 1.6

and 3.16 cubics describing $X_E(11)$ and $X_E^-(11)$ are obtained by putting

$$\begin{aligned}\mathbf{F}(v,w,x,y,z) &= \frac{1}{F^4}\widetilde{F}(Fv,w,F^7x,F^2y,F^4z)\\ \mathbf{G}(v,w,x,y,z) &= \frac{1}{F^8}\widetilde{G}(F^2v,F^8w,F^4x,y,F^3z)\end{aligned} \tag{19}$$

and replacing F^{11} by Δ. □

Remark 3.18. The cubic forms describing $X_E(11)$ and $X_E^-(11)$ in Theorems 1.4 and 3.17 are related by

$$\begin{aligned}\mathcal{F}(v,w,x,y,z) &= \frac{1}{2^3c_6^3}\mathbf{F}(-v',w',-864x,-36c_4x-108c_6z,72y)\\ \mathcal{G}(v,w,x,y,z) &= \frac{1}{2^53^6(55c_6)^3}\mathbf{G}(v'',-427680y,x'',-y'',-z'')\end{aligned}$$

where $a=-27c_4$, $b=-54c_6$ and

$$\begin{aligned}v' &= c_6v+2c_6w-6c_4^2x+3c_4^2y-9c_4c_6z & w' &= c_6v+6c_4^2x+3c_4^2y+9c_4c_6z\\ v'' &= 44(2c_4v-6c_6w+33c_6x+135c_4^2y+810c_4c_6z) & x'' &= 60(5v+729c_4y+2187c_6z)\\ y'' &= 11(c_4v-3c_6w-6c_6x) & z'' &= 60(v+27c_4y+81c_6z).\end{aligned}$$

4. Diagonal twists

We give an alternative construction of $X_E(n)$ and $X_E^-(n)$ in the case E is an elliptic curve whose n-torsion contains a copy of the Galois module μ_n.

Let $C\to D$ be an isogeny of elliptic curves with kernel a labelled copy of μ_n. Then the dual isogeny has kernel a labelled copy of $\mathbb{Z}/n\mathbb{Z}$. The pairs of such curves are parametrised by the modular curve $Y_1(n)$. In the cases $n=7,9$ we choose a coordinate λ on $X_1(n)\cong\mathbb{P}^1$. In the case $n=11$ we recall that $X_1(11)$ is the elliptic curve $\nu^2+\nu=\lambda^3-\lambda^2$. We write $\boldsymbol{\lambda}$ to indicate λ in the cases $n=7,9$ and the pair λ,ν in the case $n=11$. Let $C_{\boldsymbol{\lambda}}$ and $D_{\boldsymbol{\lambda}}$ be the corresponding pairs of n-isogenous curves. By [Si, Exercise 8.13] $D_{\boldsymbol{\lambda}}$ has Weierstrass equation

$$\begin{aligned}
n=7 \qquad & y^2-(\lambda^2-\lambda-1)xy-(\lambda^3-\lambda^2)y = x^3-(\lambda^3-\lambda^2)x^2,\\
n=9 \qquad & y^2+(\lambda^3-3\lambda^2+4\lambda-1)xy+\lambda(\lambda-1)^4(\lambda^2-\lambda+1)y\\
& \qquad = x^3+\lambda(\lambda-1)(\lambda^2-\lambda+1)x^2,\\
n=11 \qquad & y^2+(\lambda\nu+2\lambda-(\nu+1)^2)xy-\lambda^2\nu(\nu+1)(\lambda-\nu-1)y\\
& \qquad = x^3-\lambda\nu(\nu+1)(\lambda-\nu-1)x^2.
\end{aligned}$$

On each of these curves $P = (0,0)$ is a point of order n. If we write the Weierstrass equation for $D_{\boldsymbol{\lambda}}$ as $y^2 + a_1xy + a_3y = x^3 + a_2x^2$ then by Vélu's formulae [V1] the n-isogenous curve $C_{\boldsymbol{\lambda}}$ has Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 - 5tx - (a_1^2 + 4a_2)t - 7w \tag{20}$$

where $t = 6s_2 + (a_1^2 + 4a_2)s_1 + a_1a_3s_0$, $w = 10s_3 + 2(a_1^2 + 4a_2)s_2 + 3a_1a_3s_1 + a_3^2s_0$ and $s_k = \sum_{j=1}^{(n-1)/2} x(jP)^k$. The Weierstrass equations (20) have discriminant

$$\begin{aligned} n = 7 \quad & \Delta(C_\lambda) = \lambda(\lambda-1)(\lambda^3 - 8\lambda^2 + 5\lambda + 1)^7 \\ n = 9 \quad & \Delta(C_\lambda) = \lambda(\lambda-1)(\lambda^2 - \lambda + 1)^3(\lambda^3 - 6\lambda^2 + 3\lambda + 1)^9 \\ n = 11 \quad & \Delta(C_{\lambda,\nu}) = \lambda(\lambda-1)(\lambda\nu + 2\lambda^2 - 2\lambda + 1)(\nu+1)^6 f(\lambda,\nu)^{11} \end{aligned} \tag{21}$$

where $f(\lambda,\nu) = (-3\lambda\nu + 2\nu - \lambda^3 + 5\lambda^2 - 5\lambda + 1)/(\lambda - 1)$.

Lemma 4.1. *Let E/K be an elliptic curve and $\iota : \mu_n \hookrightarrow E[n]$ an inclusion of Galois modules. Then there exists $Q \in E(\overline{K})[n]$ and $q \in K^\times/(K^\times)^n$ such that*

(i) $e_n(\iota(\zeta), Q) = \zeta^{-1}$ *for all* $\zeta \in \mu_n$,
(ii) $\sigma(Q) - Q = \iota(\frac{\sigma\sqrt[n]{q}}{\sqrt[n]{q}})$ *for all* $\sigma \in \mathrm{Gal}(\overline{K}/K)$, *and*
(iii) $K(E[n]) = K(\mu_n, \sqrt[n]{q})$.

Proof: This follows by standard properties of the Weil pairing, together with Hilbert's Theorem 90. □

Taking $E = C_{\boldsymbol{\lambda}}$ we compute $q = q(\boldsymbol{\lambda})$ as described in [F1, Section 1.2].

$$q(\boldsymbol{\lambda}) = \begin{cases} \lambda^4(\lambda-1) & \text{if } n = 7 \\ \lambda(\lambda-1)^7(\lambda^2-\lambda+1)^3 & \text{if } n = 9 \\ \lambda\nu^2(\lambda-1)(\lambda-\nu-1)^3 & \text{if } n = 11. \end{cases} \tag{22}$$

We consider the following diagonal twists of $X(n)$ for $n = 7, 9, 11$. Recall in the case $n = 11$ we take the singular locus of the Hessian of the cubic form.

$$X[\xi_1,\xi_2,\xi_3] = \{\xi_1x^3y + \xi_2y^3z + \xi_3z^3x = 0\} \subset \mathbb{P}^2$$
$$X[\xi_1,\xi_2,\xi_3;\eta] = \left\{ \begin{array}{c} \xi_1x^2y + \xi_2y^2z + \xi_3z^2x = 0 \\ \xi_1\xi_2xy^2 + \xi_2\xi_3yz^2 + \xi_1\xi_3zx^2 = \eta t^3 \end{array} \right\} \subset \mathbb{P}^3$$
$$X[\xi_1,\xi_2,\xi_3,\xi_4,\xi_5] \sim \{\xi_1v^2w + \xi_2w^2x + \xi_3x^2y + \xi_4y^2z + \xi_5z^2v = 0\} \subset \mathbb{P}^4.$$

Lemma 4.2. *The diagonal twists are determined up to K-isomorphism by $\theta \in K^\times/(K^\times)^n$ where*

$$\theta = \begin{cases} \xi_1\xi_2^2\xi_3^4 & \text{if } n = 7 \\ \xi_1\xi_2^7\xi_3^4\eta^3 & \text{if } n = 9 \\ (\xi_1\xi_2^5\xi_3^3\xi_4^4\xi_5^9)^2 & \text{if } n = 11. \end{cases}$$

Moreover if we replace θ by θ^k where k is a square in $(\mathbb{Z}/n\mathbb{Z})^\times$ then we obtain isomorphic twists.

Proof: The first part is proved by rescaling the co-ordinates and the second part by cyclically permuting them. (The expression for θ in the case $n = 11$ has been squared to simplify the statement of the next theorem.) □

Theorem 4.3. *Let E/K be an elliptic curve and $\iota : \mu_n \hookrightarrow E[n]$ an inclusion of Galois modules. If $q \in K^\times/(K^\times)^n$ is as specified in Lemma 4.1 then*

(i) *$X_E(n)$ is the diagonal twist with $\theta = q$, and*
(ii) *$X_E^-(n)$ is the diagonal twist with $\theta = q^{-1}$.*

Proof: Let $\chi : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}/n\mathbb{Z}$ be defined by $\sigma(\sqrt[n]{q})/\sqrt[n]{q} = \zeta_n^{\chi(\sigma)}$. Then the symplectic isomorphism $\phi : E[n] \cong \mu_n \times \mathbb{Z}/n\mathbb{Z};\ \iota(\zeta_n^x) + yQ \mapsto (\zeta_n^{-x}, y)$ satisfies

$$\sigma(\phi)\phi^{-1} : (\zeta_n^x, y) \mapsto (\zeta_n^{x+\chi(\sigma)y}, y).$$

Under our identification $\mathrm{Aut}(\mu_n \times \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ this corresponds to $T^{\chi(\sigma)}$. If $\rho(T) \propto \mathrm{Diag}(\zeta_n^{r_1}, \ldots, \zeta_n^{r_m})$ for some integers $r_1, \ldots, r_m$ then

$$h_1 = \mathrm{Diag}((\sqrt[n]{q})^{r_1}, \ldots, (\sqrt[n]{q})^{r_m})$$

and $h_2 = h_1^{-1}$ satisfy the hypotheses of Lemma 1.6.

If $n = 7$ then $(r_1, r_2, r_3) = (4, 2, 1)$ and we deduce

$$X_E(7) \cong X[q, 1, 1] \qquad X_E^-(7) \cong X[q^{-1}, 1, 1]$$

If $n = 9$ then $(r_1, r_2, r_3, r_4) = (5, 2, 8, 0)$ and we deduce

$$X_E(9) \cong X[1, 1, q; q^{-1}] \qquad X_E^-(9) \cong X[1, 1, q^{-1}; q]$$

If $n = 11$ then $(r_1, r_2, r_3, r_4, r_5) = (6, 10, 2, 7, 8)$ and we deduce

$$X_E(11) \cong X[1, 1, q^{-1}, 1, 1] \qquad X_E^-(11) \cong X[1, 1, q, 1, 1]$$

The descriptions of $X_E(n)$ and $X_E^-(n)$ now follow by Lemma 4.2. □

It is sometimes convenient to rewrite $X[\frac{1}{\xi_2}, \frac{1}{\xi_3}, \frac{1}{\xi_1}; \frac{\eta}{\xi_1\xi_2\xi_3}]$ as

$$X^-[\xi_1, \xi_2, \xi_3; \eta] = \left\{ \begin{array}{r} \xi_1\xi_3 x^2 y + \xi_1\xi_2 y^2 z + \xi_2\xi_3 z^2 x = 0 \\ \xi_1 x y^2 + \xi_2 y z^2 + \xi_3 z x^2 = \eta t^3 \end{array} \right\} \subset \mathbb{P}^3$$

For this twist we have $\theta = \xi_1^2\xi_2^5\xi_3^8\eta^3 \mod (K^\times)^9$.

Corollary 4.4. *Let E/K be an elliptic curve whose n-torsion contains a copy of the Galois module μ_n. Then writing $E = C_{\boldsymbol{\lambda}}$ we have*

$$X_E(7) = X[\lambda, \lambda-1, 1] \qquad X_E(9) = X[\lambda, \lambda-1, 1; \lambda^2-\lambda+1]$$
$$X_E^-(7) = X[\lambda-1, \lambda, \lambda(\lambda-1)] \qquad X_E^-(9) = X^-[\lambda, \lambda-1, 1; 1/(\lambda^2-\lambda+1)]$$

and

$$X_E(11) = X[\lambda^2(\lambda-1)^2, 1, (\lambda-\nu-1)^2, \nu, 1]$$
$$X_E^-(11) = X[\lambda(\lambda-1), 1, \lambda-\nu-1, \nu, \nu]$$

Proof: This follows from Theorem 4.3 and the formula (22) for $q(\boldsymbol{\lambda})$. □

Remark 4.5. The formula for $X_E(7)$ in Corollary 4.4 was found by Halberstadt and Kraus [HK2, Theorem 7.1] by specialising the formula in Theorem 1.2 and then making a (rather complicated) change of co-ordinates. We worked out the analogue of this in the case $n = 9$ before discovering the simpler proof presented here.

5. Minimisation and reduction

Let $n = 7, 9, 11$ and $m = (n-1)/2$. Given an elliptic curve $E/\mathbb{Q}$ the formulae in Section 1.2 give equations for $X_E(n) \subset \mathbb{P}^{m-1}$ and $X_E^-(n) \subset \mathbb{P}^{m-1}$. We search for elliptic curves n-congruent to E by searching for $\mathbb{Q}$-rational points on these curves. It helps with this search if we first make a change of co-ordinates over $\mathbb{Q}$ to simplify the equations, i.e. so that they have small integer coefficients. Following [CFS] this task naturally falls into two parts, called minimisation and reduction. In minimisation one seeks to remove primes from a suitably defined invariant. Then reduction, which may be thought of as the analogue of minimisation at the infinite place, makes a final $\mathrm{GL}_m(\mathbb{Z})$-transformation.

5.1. **The invariant.**

Definition 5.1. We split into the cases $n = 7, 9, 11$.
Case $n = 7$. The invariant of a twisted form of $F = x^3y + y^3z + z^3x$ is

$$\Psi(\mu(F \circ M)) = \mu^3(\det M)^4.$$

Case $n = 9$. The invariant of a twisted form of $(F_1, F_2) = (x^2y + y^2z + z^2x, xy^2 + yz^2 + zx^2 - t^3)$ is

$$\Psi((\alpha F_1 + \beta F_2) \circ M, (\gamma F_1 + \delta F_2) \circ M) = (\alpha\delta - \beta\gamma)^6 (\det M)^9.$$

Case $n = 11$. The invariant of a twisted form of $F = v^2w + w^2x + x^2y + y^2z + z^2v$ is

$$\Psi(\mu(F \circ M)) = \mu^5 (\det M)^3.$$

Lemma 5.2. *Let $\mathcal{F}$ be one of the twisted forms in Definition 5.1. Then*

(i) *$\Psi(\mathcal{F})$ is well-defined, i.e. it is independent of the choice of $M \in \mathrm{GL}_m(\overline{K})$.*
(ii) *If $\mathcal{F}$ has coefficients in K then $\Psi(\mathcal{F}) \in K$.*

Proof: (i) This is easy to check for M a scalar matrix. In general we use that $\mathrm{Aut}(X(n)) \cong \mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$. This is proved in [AR, Lemma 20.4] for $n \geq 7$ prime, and the same proof works for $n = 9$. We are reduced to considering $M = \rho(\gamma)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. It now suffices to recall (see the proof of Proposition 2.3) that the only 1-dimensional characters of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ are those of order 3 in the case $n = 9$. This explains why in the case $n = 9$ we defined the invariant as $(\alpha\delta - \beta\gamma)^6(\det M)^9$ and not just $(\alpha\delta - \beta\gamma)^2(\det M)^3$.
(ii) This follows from (i) by Galois theory. □

Remark 5.3. (i) In the case $n = 7$ it is shown in [PSS, Section 7.1] that $\Psi(\mathcal{F})$ is an integer coefficient polynomial in the coefficients of $\mathcal{F}$. We expect that similar formulae exist in the cases $n = 9$ and $n = 11$.
(ii) The twisted forms in Theorems 1.2, 1.3 and 1.4 have the following invariants. These were computed by following the proofs in Section 3.

	$X_E(n)$	$X_E^-(n)$
$n = 7$	$-4(4a^3 + 27b^2)$	$16(4a^3 + 27b^2)^2$
$n = 9$	$-2^{10}(4a^3 + 27b^2)^4$	$2^8(4a^3 + 27b^2)^5$
$n = 11$	$-4(4a^3 + 27b^2)^2$	$8(4a^3 + 27b^2)$.

(iii) The diagonal twists studied in Section 4 have invariants

$n = 7$	$X[\xi_1, \xi_2, \xi_3]$	$\Psi = \xi_1\xi_2\xi_3$
$n = 9$	$X[\xi_1, \xi_2, \xi_3; \eta]$	$\Psi = (\xi_1\xi_2\xi_3)^4\eta^3$
	$X^-[\xi_1, \xi_2, \xi_3; \eta]$	$\Psi = (\xi_1\xi_2\xi_3)^5\eta^3$
$n = 11$	$X[\xi_1, \xi_2, \xi_3, \xi_4, \xi_5]$	$\Psi = \xi_1\xi_2\xi_3\xi_4\xi_5$.

5.2. **Minimisation.** The level of a model $\mathcal{F}$ at a prime p is the p-adic valuation of the invariant, i.e. $v_p(\Psi(\mathcal{F}))$. We seek to make a change of co-ordinates that minimises the level. This is a local problem.

Theorem 5.4. *Let E be an elliptic curve over $\mathbb{Q}_p$ with $p \neq 2, 3$. If $n = 7, 9, 11$ then $X_E(n)$ and $X_E^-(n)$ admit models (with coefficients in $\mathbb{Z}_p$) with the following levels.*

Kodaira Symbol	$X_E(7)$	$X_E^-(7)$	$X_E(11)$	$X_E^-(11)$
$\mathrm{I}_m, \mathrm{I}_m^*$ $\quad m \equiv 0 \pmod{n}$	0	0	0	0
$\mathrm{I}_m, \mathrm{I}_m^*$ $\quad (m/n) = +1$	1	2	2	1
$\mathrm{I}_m, \mathrm{I}_m^*$ $\quad (m/n) = -1$	2	1	1	2
II, II*, III, III*, IV, IV*	2	2	2	2

Kodaira Symbol	$X_E(9)$	$X_E^-(9)$	*Kodaira Symbol*	$X_E(9)$	$X_E^-(9)$
$\mathrm{I}_m, \mathrm{I}_m^*$ $\quad m \equiv 0 \pmod{9}$	0	0	II, IV*	5	7
$\mathrm{I}_m, \mathrm{I}_m^*$ $\quad m \equiv 3, 6 \pmod{9}$	3	3	III, III*	6	6
$\mathrm{I}_m, \mathrm{I}_m^*$ $\quad m \equiv 1 \pmod{3}$	4	5	IV, II*	7	5
$\mathrm{I}_m, \mathrm{I}_m^*$ $\quad m \equiv 2 \pmod{3}$	5	4			

Proof: Replacing E by a quadratic twist does not change the curves $X_E(n)$ and $X_E^-(n)$. So we may assume that either (i) E has good reduction, or (ii) E has split multiplicative reduction, or (iii) E has additive reduction of type II, III or IV. We split into these three cases.
(i) If E has good reduction then by Remark 5.3(ii) the formulae in Theorems 1.2, 1.3 and 1.4 give models for $X_E(n)$ and $X_E^-(n)$ of level 0.
(ii) If E has split multiplicative reduction then by the Tate parametrisation $E[n]$ contains a copy of the Galois module μ_n. So we may apply the results of Section 4. More precisely if E has Kodaira symbol I_m then $E(\overline{\mathbb{Q}}_p) \cong \overline{\mathbb{Q}}_p^\times / q^{\mathbb{Z}}$ for some $q \in \mathbb{Q}_p$ with $v_p(q) = m \geq 1$. It may be verified by computing the Weil pairing that the conditions of Lemma 4.1 are satisfied. So by Theorem 4.3 the curves $X_E(n)$ and $X_E^-(n)$ are the diagonal twists with $\theta = q$ or q^{-1}. If $n = 7$ or 11 then by Lemma 4.2 they admit models of the form $X[\xi_1, \xi_2, \ldots]$ where at most two of the ξ_i have p-adic valuation 1 and the rest are units. We read off the level from Remark 5.3(iii). The case $n = 9$ is similar.
(iii) Finally suppose E has Kodaira symbol II, III or IV. In terms of a minimal

Weierstrass equation for E, say $y^2 = x^3 + ax + b$, these are the cases

$$\begin{array}{lll} \text{II} & v_p(a) \geq 1 & v_p(b) = 1, \\ \text{III} & v_p(a) = 1 & v_p(b) \geq 2, \\ \text{IV} & v_p(a) \geq 2 & v_p(b) = 2. \end{array}$$

Integer-coefficient models of the required level are obtained by modifying the formulae in Theorems 1.2, 1.3 and 1.4 as follows.

	$X_E(7)$	$X_E^-(7)$	$X_E(11)$	$X_E^-(11)$
II	$\mathcal{F}(x,y,z)$	$\frac{1}{p^2}\mathcal{G}(x,y,pz)$	$\frac{1}{p}\mathcal{F}(pv+w,w,x,y,z)$	$\mathcal{G}(v,w,x,y,z)$
III	$\frac{1}{p^3}\mathcal{F}(px,py,z)$	$\mathcal{G}(x,\frac{1}{p}y,z)$	$\frac{1}{p^2}\mathcal{F}(pv,pw,x,y,z)$	$\frac{1}{p^2}\mathcal{G}(pv,pw,px,y,z)$
IV	$\frac{1}{p^2}\mathcal{F}(x,py,z)$	$\frac{1}{p^2}\mathcal{G}(x,\frac{1}{p}y,pz)$	$\frac{1}{p^3}\mathcal{F}(pv,pw,x,py-x,z)$	$\frac{1}{p}\mathcal{G}(pv,w,px,y,\frac{1}{p}z)$

	$X_E(9)$	$X_E^-(9)$
II	$\frac{1}{p^2}\mathcal{F}_1(px,py,pz,t)$	$\frac{1}{p}\mathcal{G}_1(px,y,z,t)$
	$\frac{1}{p^3}\mathcal{F}_2(px,py,pz,t)$	$\frac{1}{p}\mathcal{G}_2(px,y,z,t)$
III	$\frac{1}{p^2}\mathcal{F}_1(px,py,z,t)$	$\frac{1}{p}\mathcal{G}_1(px,y,z,t)$
	$\frac{1}{p^2}\mathcal{F}_2(px,py,z,t)$	$\frac{1}{p^2}\mathcal{G}_2(px,y,z,t)$
IV	$\frac{1}{p^4}\mathcal{F}_1(p^2x,p^2y,pz,t)$	$\frac{1}{p^2}\mathcal{G}_1(px,y,z,t)$
	$\frac{1}{p^5}\mathcal{F}_2(p^2x,p^2y,pz,t)$	$\frac{1}{p^2}\mathcal{G}_2(px,y,z,t)$

□

To compute integer-coefficient models with level as specified in Theorem 5.4 we could in principle follow the proof of the theorem. In practice however it is simpler to use a range of ad hoc tricks. We have not proved that these tricks always get down to the level specified in the theorem, but this does at least happen in all numerical examples we have tried.

Again on the basis of some numerical experimentation, we conjecture that the levels in Theorem 5.4 are the minimal levels. At the primes 2 and 3 it seems the minimal levels can be larger. See Section 7 for some examples.

5.3. **Reduction.** In Section 2.2 we saw that the action of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ on $X(n) \subset \mathbb{P}^{m-1} = \mathbb{P}(V)$ lifts to an irreducible representation $\rho : \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}(V)$. So by the Weyl unitary trick there is an $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$-invariant inner product on V, and this is unique up to scalars. To reduce our equations for $X_E(n)$ and $X_E^-(n)$ we run the LLL algorithm on the Gram matrix for this inner product. In the untwisted

case it is clear that the $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$-invariant inner product is the standard one on $\mathbb{C}^m$, i.e. ρ is a unitary representation. So to compute the inner product it suffices to have numerical approximations to the matrices h_1 and h_2 in Lemma 1.6. Since our method for finding equations for $X_E(n)$ and $X_E^-(n)$ involved explicitly computing h_1 and h_2 this is obviously something we can do. To use these formulae we need numerical approximations for $a, b, c \ldots$ in Lemmas 3.4, 3.11 and 3.16. These are computed by evaluating suitable q-expansions. See [E] or [HK2] for the relevant formulae in the case $n = 7$.

6. Modular interpretation

In Section 3 we gave explicit formulae for $X_E(n)$ and $X_E^-(n)$ for $n = 7, 9, 11$. In this section we give equations for the families of curves they parametrise.

6.1. **Computing the j-invariant.** We first give formulae for the j-map $X_E(n) \to \mathbb{P}^1$ and $X_E^-(n) \to \mathbb{P}^1$. This is sufficient for some applications: see for example [PSS]. In each case we adapt the formulae in Lemmas 3.2, 3.10 and 3.15 by writing them in an way that behaves well under all changes of co-ordinates.

Case $n = 7$. Let $X = \{\mathcal{F} = 0\} \subset \mathbb{P}^2$ be a twist of $X(7)$. Starting with $\mathcal{F}$ in place of the Klein quartic F the formulae in Section 3.1 define polynomials $H(\mathcal{F})$, $c_4(\mathcal{F})$ and $c_6(\mathcal{F})$. If $\mathcal{F} = \mu(F \circ M)$ then $\Psi(\mathcal{F}) = \mu^3(\det M)^4$ and

$$\begin{aligned} H(\mathcal{F}) &= \mu^3(\det M)^2(H \circ M) \\ c_4(\mathcal{F}) &= \mu^8(\det M)^6(c_4 \circ M) \\ c_6(\mathcal{F}) &= \mu^{12}(\det M)^9(c_6 \circ M) \end{aligned} \tag{23}$$

As noted in [PSS] the syzygy $c_4^3 - c_6^2 \equiv 1728H^7 \pmod{F}$ becomes

$$c_4(\mathcal{F})^3 - c_6(\mathcal{F})^2 \equiv 1728\,\Psi(\mathcal{F})\,H(\mathcal{F})^7 \pmod{\mathcal{F}}.$$

In particular the j-map $X \to \mathbb{P}^1$ is given by

$$j = \frac{c_4(\mathcal{F})^3}{\Psi(\mathcal{F})H(\mathcal{F})^7}.$$

Case $n = 11$. Let $X \subset \mathbb{P}^4$ be a twist of $X(11)$ given as the singular locus of the Hessian of a cubic form $\mathcal{F} = \mathcal{F}(v, w, x, y, z)$. Starting with $\mathcal{F}$ in place of the cubic form $F = v^2w + w^2x + x^2y + y^2z + z^2v$ the formulae in Section 3.3 define polynomials $H(\mathcal{F})$ and $c_4(\mathcal{F})$. If $\mathcal{F} = \mu(F \circ M)$ then $\Psi(\mathcal{F}) = \mu^5(\det M)^3$ and

$$\begin{aligned} H(\mathcal{F}) &= \mu^5(\det M)^2(H \circ M) \\ c_4(\mathcal{F}) &= \mu^{17}(\det M)^8(c_4 \circ M) \end{aligned} \tag{24}$$

By Lemma 3.15 the j-map $X \to \mathbb{P}^1$ is given by

$$j = \frac{c_4(\mathcal{F})^3}{\Psi(\mathcal{F})^8 \mathcal{F}^{11}}.$$

Case $n = 9$. Our construction of $c_4(a, b, c, d)$ and $c_6(a, b, c, d)$ in Section 3.3 does not immediately generalise to twists of $X(9)$. Instead we exploit the fact that the pencil of cubics defining $X(9) \subset \mathbb{P}^3$ is naturally a copy of $X(3) \cong \mathbb{P}^1$. The notation X_M for a twist of $X(n)$ was introduced in Section 1.1.

Theorem 6.1. *Let $X_M = \{\mathcal{F}_1 = \mathcal{F}_2 = 0\} \subset \mathbb{P}^3$ be a twist of $X(9)$ where M is a symplectic Galois module with $M \cong (\mathbb{Z}/9\mathbb{Z})^2$ as an abelian group. Then*

(i) *Writing $\mathcal{H}$ for the determinant of the matrix of second partial derivatives we have*

$$\mathcal{H}(r\mathcal{F}_1 + s\mathcal{F}_2) = f(r, s)D(a, b, c, d)$$

where f and D are homogeneous polynomials of degree 4.

(ii) *We have $X_{M[3]} \cong \mathbb{P}^1$ with cusps at the roots of $f(r, s) = 0$.*

(iii) *For $P \in X_M$ with tangent line $P + tQ$ write $\mathcal{F}_i(P + tQ) = \gamma_i t^2 + \delta_i t^3$ for $i = 1, 2$. Then the forgetful map $X_M \to X_{M[3]}$ is $P \mapsto (-\gamma_2 : \gamma_1)$.*

Proof: We first prove the theorem in the case $M \cong \mu_9 \times \mathbb{Z}/9\mathbb{Z}$.
(i) Taking $F_1 = a^2b + b^2c + c^2a$ and $F_2 = ab^2 + bc^2 + ca^2 - d^3$ we compute

$$\mathcal{H}(rF_1 + sF_2) = 48(r^3 + s^3)s(a^3 + b^3 + c^3 - 3abc)d.$$

(ii) Since[2] $M[3] \cong \mu_3 \times \mathbb{Z}/3\mathbb{Z}$ we have $X_{M[3]} = X(3)$. We recall from Section 1.4 that $X(3) \cong \mathbb{P}^1$ with cusps at the roots of $A(27A^3 + B^3) = 0$. Our two choices of co-ordinates on $X(3)$ are now related by $(r : s) = (B : 3A)$.
(iii) We temporarily write a_1, a_2, a_3, a_4 for a, b, c, d and let Λ_2 be the 4×4 alternating matrix with (i, j) entry

$$\frac{\partial F_1}{\partial a_l}\frac{\partial F_2}{\partial a_k} - \frac{\partial F_1}{\partial a_k}\frac{\partial F_2}{\partial a_l}$$

where (i, j, k, l) is an even permutation of $(1, 2, 3, 4)$. This is the same as the matrix Λ_2 in Section 3.2. By direct calculation we find

$$\Lambda_2 \begin{pmatrix} \frac{\partial^2 F_i}{\partial a^2} & \cdots & \frac{\partial^2 F_i}{\partial a \partial d} \\ \vdots & & \vdots \\ \frac{\partial^2 F_i}{\partial a \partial d} & \cdots & \frac{\partial^2 F_i}{\partial d^2} \end{pmatrix} \Lambda_2 \equiv \gamma_i \, D \begin{pmatrix} a \\ \vdots \\ d \end{pmatrix} \begin{pmatrix} a & \cdots & d \end{pmatrix} \mod (F_1, F_2)$$

[2]The pairing e_9 on M induces a pairing e_3 on $M[3]$ by the rule $e_3(3S, T) = e_9(S, T)$ for all $S \in M$ and $T \in M[3]$.

for $i = 1, 2$, where $\gamma_1 = 18d^3$, $\gamma_2 = -6(a^3 + b^3 + c^3 + 6abc)$ and $D = -(a^3 + b^3 + c^3 - 3abc)d$.

In Corollary 6.5 below we show that the forgetful map $X(9) \to X(3)$ is

$$(a : b : c : d) \mapsto (A : B) = (d^3 : a^3 + b^3 + c^3 + 6abc). \tag{25}$$

Thus $(B : 3A) = (-\gamma_2 : \gamma_1)$ as required.

Relaxing our restriction on M, the general case of the theorem follows since the forgetful map $X_M \to X_{M[3]}$ may be characterised geometrically, i.e. it quotients out by the symplectic automorphisms of M that act trivially on $M[3]$. □

Remark 6.2. If we only use Theorem 6.1 to compute the j-invariant, then we can replace the forward reference (25) in the above proof by the observation that the polynomials $c_4(A, B)$ and $c_6(A, B)$ in Section 1.4 are related to the polynomials $c_4(a, b, c, d)$ and $c_6(a, b, c, d)$ in Section 3.2 by

$$\begin{aligned} c_4(d^3, a^3 + b^3 + c^3 + 6abc) &\equiv c_4(a, b, c, d) \mod (F_1, F_2), \\ c_6(d^3, a^3 + b^3 + c^3 + 6abc) &\equiv c_6(a, b, c, d) \mod (F_1, F_2). \end{aligned}$$

Since we already gave formulae for the universal families above $Y_E(3)$ and $Y_E^-(3)$ in Theorem 1.1, the following corollary gives formulae for the universal families above $Y_E(9)$ and $Y_E^-(9)$.

Corollary 6.3. *Let E/K be the elliptic curve $y^2 = x^3 - 27c_4x - 54c_6$. Let $X_E(3)$ and $X_E^-(3)$ be as given in Theorem 1.1, and let $X_E(9)$ and $X_E^-(9)$ be as given in Theorem 1.3 with $a = -27c_4$ and $b = -54c_6$. Then the forgetful maps $X_E(9) \to X_E(3)$ and $X_E^-(9) \to X_E^-(3)$ are given by $(\lambda : \mu) = (\gamma_2 : 3\gamma_1)$ where γ_1, γ_2 are computed by the tangent line construction in Theorem 6.1(iii).*

Proof: (i) We have $X_E(9) = \{\mathcal{F}_1 = \mathcal{F}_2 = 0\} \subset \mathbb{P}^3$ where $\mathcal{F}_1$ and $\mathcal{F}_2$ are as given in Theorem 1.3. We compute $\mathcal{H}(r\mathcal{F}_1 + s\mathcal{F}_2) = f(r, s)D(x, y, z, t)$ with

$$f(r, s) = r^4 + 2ar^2s^2 - 4brs^3 - \tfrac{1}{3}a^2s^4. \tag{26}$$

On the other hand the family of curves parametrised by $X_E(3)$ in Theorem 1.1 has cusps at the roots of

$$\mathbf{D}(\lambda, \mu) = \lambda^4 - 6c_4\lambda^2\mu^2 - 8c_6\lambda\mu^3 - 3c_4^2\mu^4. \tag{27}$$

Comparing (26) and (27) we see that our two choices of co-ordinates on $X_E(3) \cong \mathbb{P}^1$ are related by $(\lambda : \mu) = (r : -3s)$. Taking $(r : s) = (-\gamma_2 : \gamma_1)$ gives the result.

(ii) We have $X_E^-(9) = \{\mathcal{G}_1 = \mathcal{G}_2 = 0\} \subset \mathbb{P}^3$ where $\mathcal{G}_1$ and $\mathcal{G}_2$ are as given in Theorem 1.3. We compute $\mathcal{H}(r\mathcal{G}_1 + s\mathcal{G}_2) = f(r, s)D(x, y, z, t)$ with

$$f(r, s) = ar^4 - 6br^3s - 2a^2r^2s^2 + 2abrs^3 - (\tfrac{1}{3}a^3 + 3b^2)s^4. \tag{28}$$

On the other hand the family of curves parametrised by $X_E^-(3)$ in Theorem 1.1 has cusps at the roots of

$$\mathbf{c}_4(\lambda,\mu) = c_4\lambda^4 + 4c_6\lambda^3\mu + 6c_4^2\lambda^2\mu^2 + 4c_4c_6\lambda\mu^3 - (3c_4^3 - 4c_6^2)\mu^4. \tag{29}$$

Comparing (28) and (29) we see that our choices of co-ordinates on $X_E^-(3) \cong \mathbb{P}^1$ are related by $(\lambda : \mu) = (r : -3s)$. Taking $(r : s) = (-\gamma_2 : \gamma_1)$ gives the result. □

6.2. **Modular interpretation of $X(n)$.** In Section 2.1 we gave equations for $X(n)$. We recall from [F0] that (analogous to Definition 2.2) the elliptic curve $E \subset \mathbb{P}^{n-1}$ above $(0 : a_1 : a_2 : \ldots : -a_2 : -a_1) \in Y(n)$ has equations

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

Taking $n = 7, 9, 11$ we now put this curve in Weierstrass form. Notice that the Weierstrass equations have coefficients that are homogeneous polynomials of degree $4m$ and $6m$ for some integer m.

Theorem 6.4. *We split into the cases $n = 7, 9, 11$.*

(i) *The family of curves parametrised by $X(7) = \{a^3b + b^3c + c^3a = 0\} \subset \mathbb{P}^2$ is*

$$y^2 = x^3 - 27(abc)^2c_4(a,b,c)x - 54(abc)^3c_6(a,b,c) \tag{30}$$

where $c_4, c_6 \in K[a,b,c]$ are as defined in Section 3.1.

(ii) *The family of curves parametrised by $X(9) = \{F_1 = F_2 = 0\} \subset \mathbb{P}^3$ is*

$$y^2 = x^3 - 27c_4(a,b,c,d)x - 54c_6(a,b,c,d)$$

where $c_4, c_6 \in K[a,b,c,d]$ are as defined in Section 3.2.

(iii) *The family of curves parametrised by $X(11) \subset \mathbb{P}^4$ is*

$$y^2 = x^3 - 27(abcde)c_4(a,b,c,d,e)x - 54(abcde)\widetilde{c}_6(a,b,c,d,e). \tag{31}$$

where $c_4, \widetilde{c}_6 \in K[a,b,c,d,e]$ are as defined in Section 3.3.

Proof: In Section 4 we wrote $\boldsymbol{\lambda}$ for a co-ordinate (or pair of co-ordinates) on $X_1(n)$ for $n = 7, 9, 11$. With $q(\boldsymbol{\lambda})$ as defined in (22), we see by Lemma 4.1 that $X(n)$ is birational to $\{q(\boldsymbol{\lambda}) = \tau^n\} \subset X_1(n) \times \mathbb{G}_{\mathrm{m}}$. In the case $n = 7$ an explicit birational map is given in [F1, Section 2.2]. Applying the same method for $n = 9, 11$ we obtain

$$\begin{aligned}
n = 7 \qquad & (a : b : c) \mapsto (\lambda, \tau) = (-ac^2/b^3, ac/b^2),\\
n = 9 \qquad & (a : b : c : d) \mapsto (\lambda, \tau) = (-ac/b^2, a^2d/b^2c),\\
n = 11 \qquad & (a : b : c : d : e) \mapsto (\lambda, \nu, \tau) = (-abd/c^2e, ab^3/c^3e, -ab/c^2).
\end{aligned}$$

We checked directly that these are birational maps, and that the cusps of $X(n)$, i.e. $(1:0:\ldots:0)$ and its translates under the action of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, map to the cusps of $X_1(n)$, i.e. the roots of (21).

Let $c_4(\boldsymbol{\lambda})$ and $c_6(\boldsymbol{\lambda})$ be the invariants of the Weierstrass equation for $C_{\boldsymbol{\lambda}}$ in Section 4. Using Magma we compute

$$n=7 \qquad \begin{aligned} c_4(-ac^2/b^2) &\equiv \xi_7^4(abc)^2c_4(a,b,c) \mod (a^3b+b^3c+c^3a)\\ c_6(-ac^2/b^2) &\equiv \xi_7^6(abc)^3c_6(a,b,c) \mod (a^3b+b^3c+c^3a)\end{aligned}$$

$$n=9 \qquad \begin{aligned} c_4(-ac/b^2) &\equiv \xi_9^4c_4(a,b,c,d) \mod (F_1,F_2)\\ c_6(-ac/b^2) &\equiv \xi_9^6c_6(a,b,c,d) \mod (F_1,F_2)\end{aligned}$$

$$n=11 \qquad \begin{aligned} c_4(-abd/c^2e, ab^3/c^3e) &\equiv \xi_{11}^4(abcde)c_4(a,b,c,d,e) \mod \mathcal{I}\\ c_6(-abd/c^2e, ab^3/c^3e) &\equiv \xi_{11}^6(abcde)\widetilde{c}_6(a,b,c,d,e) \mod \mathcal{I}\end{aligned}$$

where $\xi_7 = a/b^5c$, $\xi_9 = a^2/b^4c$ and $\xi_{11} = a^3b/c^6e^2$.

See [HK2, Section 3] for a sketch of an alternative proof in the case $n=7$. □

Corollary 6.5. *The forgetful map $X(9)\to X(3)$ is given by*

$$(a:b:c:d)\mapsto (d^3 : a^3+b^3+c^3+6abc).$$

Proof: This follows from Theorem 6.4(ii) and Remark 6.2. □

6.3. **An alternative projective embedding.** We take $p\geq 5$ a prime and let $G=\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ act on $X(p)$ in the usual way.

Theorem 6.6 (Adler, Ramanan)**.** *The group of G-invariant divisor classes on $X(p)$ is free of rank 1 generated by a divisor class $[\Lambda]$ of degree $(p^2-1)/24$.*

Proof: See [AR, Theorem 24.1]. □

Let $m=(p-1)/2$. Klein showed there are embeddings $X(p)\subset\mathbb{P}^{m-1}$ and $X(p)\subset\mathbb{P}^m$ with linear G-action. The images are called the z-curve and the A-curve respectively. The corresponding hyperplane sections are $(m-1)\Lambda$ and $m\Lambda$, and indeed the divisor Λ in Theorem 6.6 is constructed by taking the difference of these. It is conjectured that each of these embeddings is via a complete linear system (the WYSIWYG Hypothesis in [AR]) and this is certainly known for $p=7$ and $p=11$. The equations for $X(p)$ we have used so far (introduced in Section 2.1) are for the z-curve. However in Sections 6.4 and 6.5 below we also need the A-curve.

Remark 6.7. Let $\pi : \mathfrak{X} \to X$ be the universal family over $X = X(p)$. It can be shown that $\pi_*(\Omega_{\mathfrak{X}/X}) \cong \mathcal{O}(p\Lambda)$. Hence the family of curves $\mathfrak{X} \to X$ has Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$ where

$$c_k \in H^0(X(p), \mathcal{O}(kp\Lambda))$$

for $k = 4, 6$. If we realise $X(p) \subset \mathbb{P}^{m-1}$ as the z-curve then to write c_k as a polynomial (in m variables) we need that $m - 1 = (p-3)/2$ divides kp. Thus in the case $p = 7$ we were able to write c_4 and c_6 as polynomials in $K[a, b, c]$. In the case $p = 11$ we likewise constructed $c_4 \in K[a, b, c, d, e]$, but there was no polynomial c_6.

Case $p = 7$. The z-curve is the Klein quartic

$$X(7) = \{x^3y + y^3z + z^3x = 0\} \subset \mathbb{P}^2.$$

The cusps of $X(7)$ are the 24 points of inflection. We recall from [PSS] that the cusps are naturally partitioned into eight sets of three $\{P_1, P_2, P_3\}$ with

$$P_1 + 3P_2 \sim P_2 + 3P_3 \sim P_3 + 3P_1 \sim H$$

where $H \sim 2\Lambda$ is the hyperplane section. We write $T_0, \ldots, T_7$ for the effective divisors of degree 3 of the form $P_1 + P_2 + P_3$ and note that one of these divisors, say T_0, satisfies $X(7) \cap \{xyz = 0\} = 4T_0$. We also recall from [PSS] that $2T_i \sim 2T_j$ for all $0 \le i, j \le 7$. It follows by Theorem 6.6 that $2T_0 \sim 3\Lambda$. Since $3\Lambda \sim 3H - 2T_0$ and $\mathcal{L}(3H - 2T_0)$ has basis x^2y, y^2x, z^2x, xyz the A-curve is the image of

$$X(7) \to \mathbb{P}^3\,; \quad (x : y : z) \mapsto (t_1 : t_2 : t_3 : t_4) = (x^2y : y^2z : z^2x : xyz)$$

with equations

$$\operatorname{rank} \begin{pmatrix} t_1 & 0 & t_4 & -t_2 \\ t_2 & -t_3 & 0 & t_4 \\ t_3 & t_4 & -t_1 & 0 \end{pmatrix} \le 2.$$

Case $p = 11$. The z-curve is the singular locus of the Hessian of

$$\{F = v^2w + w^2x + x^2y + y^2z + z^2v = 0\} \subset \mathbb{P}^4.$$

We write $H \sim 4\Lambda$ for the hyperplane section. The cusps are the 60 points of intersection of $X(11)$ with $\{F = 0\}$. They are naturally partitioned into twelve sets of five $\{P_1, \ldots, P_5\}$ with

$$P_1 + 6P_3 + 3P_4 + 10P_5 \sim H$$

and likewise under all cyclic permutations of the P_i. We write $T_0, \ldots, T_{11}$ for the effective divisors of degree 5 of the form $P_1 + \ldots + P_5$ and note that one of these

divisors, say T_0, satisfies $X(11) \cap \{vwxyz = 0\} = 20T_0$. It may be shown that $5T_i \sim 5T_j$ for all $0 \leq i, j \leq 11$ and hence $5T_0 \sim 5\Lambda$ by Theorem 6.6. Since $5\Lambda \sim 5H - 15T_0$ we find by computing a basis for $\mathcal{L}(5H - 15T_0)$ that the A-curve is the image of the morphism $X(11) \to \mathbb{P}^5$ given by

$$(t_1 : t_2 : t_3 : t_4 : t_5 : t_6) = (v^2wxz : vw^2xy : wx^2yz : vxy^2z : vwyz^2 : vwxyz).$$

It is shown in [AR, Theorem 51.1], and we checked using Magma, that this is the singular locus of the quartic hypersurface

$$t_6^4 - (t_1^2t_2 + t_2^2t_3 + t_3^2t_4 + t_4^2t_5 + t_5^2t_1)t_6 + t_1^2t_3t_5 + t_2^2t_4t_1 + t_3^2t_5t_2 + t_4^2t_1t_3 + t_5^2t_2t_4 = 0.$$

6.4. **Formulae in the case $n = 7$.**

Theorem 6.8. *Let $\mathcal{X} = \{\mathcal{F} = 0\} \subset \mathbb{P}^2$ be a twist of the Klein quartic, with hyperplane section H. Let $T = P_1 + P_2 + P_3$ where P_1, P_2, P_3 are points of inflection on $\mathcal{X}$ with*

$$P_1 + 3P_2 \sim P_2 + 3P_3 \sim P_3 + 3P_1 \sim H.$$

Let $d \in K[x, y, z]$ be a cubic form with $\{d = 0\}$ meeting $\mathcal{X}$ in a divisor $2D$ with $D \sim 2T$. Then there is a $\mathrm{Gal}(\overline{K}/K)$-module M such that for every field extension L/K and rational point $P = (x : y : z) \in \mathcal{X}(L) \setminus \{d = 0\}$, not a point of inflection, the elliptic curve

$$Y^2 = X^3 - 27\frac{c_4(\mathcal{F})(x, y, z)}{d(x, y, z)^2}X - 54\frac{c_6(\mathcal{F})(x, y, z)}{d(x, y, z)^3} \tag{32}$$

has 7-torsion isomorphic to M as a $\mathrm{Gal}(\overline{L}/L)$-module.

Proof: We first note that if $d_1, d_2 \in K[x, y, z]$ are cubic forms meeting $\mathcal{X}$ in divisors $2D_1$ and $2D_2$ with $D_1 \sim D_2$ then d_1/d_2 is the square of a rational function and hence the elliptic surfaces (32) with $d = d_1$ and $d = d_2$ are isomorphic over $\overline{K}$. Since $\mathcal{X}$ is a twist of the Klein quartic it follows (by taking $D = 2T_0$ as defined in the last section) that the elliptic surfaces (30) and (32) are isomorphic over $\overline{K}$. (Notice it does not matter whether we write the terms $d(x, y, z)$ in the numerator or in the denominator.) We are done by [RS1, Proposition 2.1]. □

In Theorem 6.10 below we determine rational functions d satisfying the hypothesis of Theorem 6.8 in the cases $\mathcal{X} = X_E(7)$ and $\mathcal{X} = X_E^-(7)$. We also show how to scale these functions to give the quadratic twist with $M \cong E[7]$.

Remark 6.9. Recall that $X_E(7)$ has a trivial K-rational point corresponding to E itself. Following [RS1] one method for finding the right quadratic twist would be to specialise at this point. However this approach fails when d vanishes at the trivial point. Neither does the method generalise to $X_E^-(7)$.

Theorem 6.10. *Let E/K be an elliptic curve with Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$ and let $\Delta = (c_4^3 - c_6^2)/1728$. If $j(E) \neq 0, 1728$ then the families of elliptic curves parametrised by $Y_E(7)$ and $Y_E^-(7)$ are given by (32) with $(\mathcal{F}, d) = (\mathbf{F}, d_1)$ and $(\mathbf{G}, d_2)$ where $\mathbf{F}$ and $\mathbf{G}$ are the quartics in Theorem 3.6 and*

$$d_1(x,y,z) = -6(3x^2 + c_4xz - 3c_4y^2 + c_6yz)z$$
$$d_2(x,y,z) = 2\Delta(4x^3 + c_4x^2z - 12c_4xy^2 - 2c_6xyz + 8c_6y^3 + c_4^2y^2z + 200\Delta z^3).$$

Proof: We fix a symplectic isomorphism $\phi : E[7] \cong \mu_7 \times \mathbb{Z}/7\mathbb{Z}$ and let $(a : b : c)$ be the $\overline{K}$-point on $X(7)$ corresponding to (E, ϕ). As in the proof of Theorem 3.6 we scale (a, b, c) so that $c_4(a, b, c) = c_4$ and $c_6(a, b, c) = c_6$.

Consideration of the action of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ on both the z-curve and the A-curve suggests we start with the forms

$$\begin{aligned} s_1(x,y,z) &= (a^2c^3 - 2ab^3c)x^2y + (a^3b^2 - 2abc^3)y^2z \\ &\qquad + (b^3c^2 - 2a^3bc)xz^2 + (a^3c^2 + a^2b^3 + b^2c^3)xyz, \\ s_2(x,y,z) &= a^2bx^2y + b^2cy^2z + c^2az^2x + 2abcxyz. \end{aligned}$$

We then let r_1 and r_2 be the unique cubic forms satisfying

$$r_i(x,y,z)xyz \equiv s_i(x,y,z)^2 \mod (x^3y + y^3z + z^3x) \tag{33}$$

for $i = 1, 2$. The coefficients of r_1 and r_2 are homogeneous polynomials in a, b, c of degrees 10 and 6. Recall that in the proof of Theorem 3.6 we put

$$\begin{aligned} \mathbf{F}(x,y,z) &= \frac{1}{H^3}F(x\mathbf{x} + y(\nabla F \times \nabla H) + zH\mathbf{e}), \\ \mathbf{G}(x,y,z) &= \frac{1}{H^2}F(x\nabla F + y(\mathbf{x} \times \mathbf{e}) + zH^2\nabla H). \end{aligned}$$

The cubics d_1 and d_2 in the statement of the theorem are likewise found by putting

$$\begin{aligned} d_1(x,y,z) &= \frac{1}{2abcH^4}r_1(x\mathbf{x} + y(\nabla F \times \nabla H) + zH\mathbf{e}), \\ d_2(x,y,z) &= \frac{2H^5}{abc}r_2(x\nabla F + y(\mathbf{x} \times \mathbf{e}) + zH^2\nabla H). \end{aligned} \tag{34}$$

It is clear from these constructions that $\{d_1 = 0\}$ and $\{d_2 = 0\}$ meet the corresponding twists of the Klein quartic in divisors of the form specified in Theorem 6.8. Hence our formulae for the families of elliptic curves parametrised by $Y_E(7)$ and $Y_E^-(7)$ are correct up to quadratic twist, say by $\delta \in K^\times$. It remains to show that δ is a square. As noted in [HK2, Section 7.1] it suffices to check this in the case $\phi : E[7] \cong \mu_7 \times \mathbb{Z}/7\mathbb{Z}$ is defined over K. Then $(a : b : c)$ is a K-rational point on $X(7)$. We write $(a, b, c) = (\lambda a_0, \lambda b_0, \lambda c_0)$ with $a_0, b_0, c_0 \in K$. By our earlier choice of scaling for a, b, c we have $\lambda^7 \in K$. Comparing the Weierstrass

equation (30) for E with that in the statement of the theorem we deduce that $\lambda^7 a_0 b_0 c_0 \in (K^\times)^2$. Hence $a^7, b^7, c^7 \in K$ and $(abc)^7 \in (K^\times)^2$. Using (14) and (23) we compute

$$\begin{aligned} c_k(\mathbf{F})(x,y,z) &= (2^9 3^6)^{k/2} c_k(x\mathbf{x} + y(\nabla F \times \nabla H) + zH\mathbf{e}) \\ c_k(\mathbf{G})(x,y,z) &= (2^9 3^6 H^7)^{k/2} c_k(x\nabla F + y(\mathbf{x} \times \mathbf{e}) + zH^2 \nabla H). \end{aligned}$$

for $k = 4, 6$. It follows by (34) that

$$\begin{aligned} \frac{c_k(\mathbf{F})(x,y,z)}{d_1(x,y,z)^{k/2}} &= \xi^k \frac{c_k(xH\mathbf{x} + yH(\nabla F \times \nabla H) + zH^2\mathbf{e})}{((abc)^6 r_1(xH\mathbf{x} + yH(\nabla F \times \nabla H) + zH^2\mathbf{e}))^{k/2}} \\ \frac{c_k(\mathbf{G})(x,y,z)}{d_2(x,y,z)^{k/2}} &= \eta^k \frac{c_k(xH^3\nabla F + yH^3(\mathbf{x} \times \mathbf{e}) + zH^5\nabla H)}{((abc)^6 H^{10} r_2(xH^3\nabla F + yH^3(\mathbf{x} \times \mathbf{e}) + zH^5\nabla H))^{k/2}} \end{aligned}$$

for some $\xi, \eta \in K^\times$. The covariant columns $H\mathbf{x}$, $H(\nabla F \times \nabla H)$, $H^2\mathbf{e}$ have degrees $7, 14, 21$ and the contravariant columns $H^3\nabla F$, $H^3(\mathbf{x} \times \mathbf{e})$, $H^5\nabla H$ have degrees $21, 28, 35$. Since each column has degree a multiple of 7, its evaluation at (a, b, c) is K-rational. Thus the families of curves in the statement of the theorem are K-isomorphic to

$$Y^2 = X^3 - 27\frac{c_4(x,y,z)}{((abc)^6 r_1(x,y,z))^2}X - 54\frac{c_6(x,y,z)}{((abc)^6 r_1(x,y,z))^3}$$

and

$$Y^2 = X^3 - 27\frac{c_4(x,y,z)}{((abc)^6 H^{10} r_2(x,y,z))^2}X - 54\frac{c_6(x,y,z)}{((abc)^6 H^{10} r_2(x,y,z))^3}.$$

To identify these with (30) we note that the cubic forms $(abc)^3 s_1(x,y,z)$ and $(abc)^3 H^5 s_2(x,y,z)$ have coefficients in K (since the degree of each coefficient is a multiple of 7) and then use (33). □

Making the change of co-ordinates in Remark 3.7 we can replace d_1 and d_2 by cubic forms that satisfy the conditions of Theorem 6.8 for $X_E(7) = \{\mathcal{F} = 0\} \subset \mathbb{P}^2$ and $X_E^-(7) = \{\mathcal{G} = 0\} \subset \mathbb{P}^2$ where $\mathcal{F}$ and $\mathcal{G}$ are the quartics in Theorem 1.2. Moreover having found one such form we can use the Riemann-Roch machinery in Magma to find further such forms.

In the case of $X_E(7)$ we obtain a cubic form d_{11} with $X_E(7) \cap \{d_{11} = 0\} = 2D_1$ for some divisor $D_1 \sim 2T$. Then $\mathcal{L}(3H - D_1)$ has basis

$$\begin{aligned} d_{11} &= -2(ax^2 + 3bxz + 3y^2 + 2ayz)z, \\ d_{12} &= 2(ax^2 + 3bxz + 3y^2 + 2ayz)x, \\ d_{13} &= 4(3bx^2 - 2axy - 2a^2xz - 3byz - 2abz^2)z, \\ d_{14} &= 4(a^2x^2 + 3bxy + 4abxz + ay^2 + 3b^2z^2)z. \end{aligned}$$

More generally we compute cubic forms d_{ij} for $1 \le i, j \le 4$ such that the matrix (d_{ij}) is symmetric and each 2×2 minor vanishes mod $\mathcal{F}$. The remaining d_{ij} are computed using $d_{11}d_{ij} \equiv d_{1i}d_{1j} \pmod{\mathcal{F}}$. Then $X_E(7) \cap \{d_{ij} = 0\} = D_i + D_j$ where $D_1, \ldots, D_4$ are divisors all linearly equivalent to $2T$. The family of elliptic curves parametrised by $Y_E(7)$ is now given by (32) with $(\mathcal{F}, d) = (\mathcal{F}, d_{ii})$ for any $1 \le i \le 4$. The A-curve is the image of $X_E(7) \to \mathbb{P}^3$; $(x : y : z) \mapsto (d_{11} : \ldots : d_{14})$ with equations

$$\operatorname{rank} \begin{pmatrix} 0 & t_3 & -t_4 & 2at_1 + t_4 \\ t_1 & 2at_1 + t_4 & 2bt_1 + at_2 + at_3 & 2at_2 + at_3 \\ t_2 & 2bt_1 + at_3 & -a^2t_1 + bt_3 - at_4 & 2bt_2 - bt_3 - at_4 \end{pmatrix} \le 2.$$

Our formula for the elliptic curve corresponding to $P \in Y_E(7)$ fails at points P with $d_{ii}(P) = 0$. These are the points whose image on the A-curve lies on the co-ordinate hyperplane $\{t_i = 0\}$. Therefore for any given point P we have $d_{ii}(P) \neq 0$ for some i. So unlike the treatment in [HK2, Theorem 5.2], where only the cubic form d_{11} was given, we have found formulae that cover all cases.

In the case of $X_E^-(7)$ we likewise find cubic forms d'_{ij} for $1 \le i, j \le 4$ such that the matrix (d'_{ij}) is symmetric and each 2×2 minor vanishes mod $\mathcal{G}$. Explicitly

$$\begin{aligned} d'_{11} &= -7ax^2y + 6x^2z + 3a^2y^3 - 8ay^2z + 3yz^2, \\ d'_{22} &= 2ax^3 + 12bx^2y - 2axyz - 3aby^3 + 6by^2z, \\ d'_{33} &= 2a^2xy^2 - 10axyz + 6xz^2 + 5aby^3 - 12by^2z, \\ d'_{44} &= 2a^2x^2y - 3ax^2z + 5abxy^2 - 12bxyz - 3a^2y^2z + 8ayz^2 - 3z^3. \end{aligned}$$

The remaining d'_{ij} are computed using $d'_{11}d'_{ij} \equiv d'_{1i}d'_{1j} \pmod{\mathcal{G}}$. The family of elliptic curves parametrised by $Y_E^-(7)$ is now given by (32) with $(\mathcal{F}, d) = (\mathcal{G}, \Delta d'_{ii})$ for any $1 \le i \le 4$. Exactly as before these formulae cover all cases.

6.5. **Formulae in the case $n = 11$.** Our approach is similar to that in the last section. As one would expect the formulae in the case $n = 11$ are more complicated than those in the case $n = 7$. There are however two further complications. One as

noted in Remark 6.7 is the absence of a polynomial c_6. The other is that the form we are looking for is no longer uniquely determined by its image in the co-ordinate ring. Indeed in the case $n = 7$ we were looking for a cubic form, and in the case $n = 11$ we are looking for a quintic form. But in both cases the homogeneous ideal is generated by quartics.

Consideration of the action of $\mathrm{SL}_2(\mathbb{Z}/11\mathbb{Z})$ on both the z-curve and the A-curve suggests we start with the forms

$$\begin{aligned} s_1(v,w,x,y,z) = {} & (a^3bc^3 + b^4cd^2 - ab^2c^2de - 2bc^2de^3)v^2wxz \\ & + (b^3cd^3 + c^4de^2 - abc^2d^2e - 2a^3cd^2e)vw^2xy \\ & + (c^3de^3 + a^2d^4e - abcd^2e^2 - 2ab^3de^2)wx^2yz \\ & + (a^3d^3e + ab^2e^4 - a^2bcde^2 - 2a^2bc^3e)vxy^2z \\ & + (ab^3e^3 + a^4bc^2 - a^2b^2cde - 2ab^2cd^3)vwyz^2 \\ & + 2(a^2b^2c^2e + a^2b^2de^2 + a^2cd^2e^2 + ab^2c^2d^2 + bc^2d^2e^2)vwxyz, \\ s_2(v,w,x,y,z) = {} & a^2bcev^2wxz + ab^2cdvw^2xy + bc^2dewx^2yz + acd^2evxy^2z \\ & + abde^2vwyz^2 + 2abcdevwxyz. \end{aligned}$$

We then solve for r_1 and r_2 satisfying

$$r_i(v,w,x,y,z)(vwxyz)^3 \equiv s_i(v,w,x,y,z)^4 \pmod{\mathcal{I}, \mathcal{I}'} \tag{35}$$

where $\mathcal{I}$ and $\mathcal{I}'$ are the homogeneous ideals for $X(11) \subset \mathbb{P}^4$ with respect to the two sets of variables a, b, c, d, e and v, w, x, y, z. The coefficients of r_1 and r_2 are homogeneous polynomials of degrees 28 and 20 in a, b, c, d, e. It is important to note that r_1 and r_2 are not uniquely determined by (35). However by averaging over the group we were able to choose $r_i = (abcde)^3\widetilde{r}_i$ in such a way that the coefficients of

$$\widetilde{r}_1(v\mathbf{x}_1 + w\mathbf{x}_4 + x\mathbf{x}_5 + y\mathbf{x}_9 + z\mathbf{x}_{14})$$

and

$$\widetilde{r}_2(v\nabla F + w\nabla I_7 + x\nabla I_8 + y\nabla I_9 + z\nabla c_4)$$

are congruent mod $\mathcal{I}$ to certain polynomials in F and c_4. The result is a pair of quintic forms $\widetilde{d}_1(v,w,x,y,z)$ and $\widetilde{d}_2(v,w,x,y,z)$ with coefficients in $\mathbb{Q}[F, c_4]$. We then put

$$\begin{aligned} d_1(v,w,x,y,z) &= \widetilde{d}_1(Fv, w, F^7x, F^2y, F^4z) \\ d_2(v,w,x,y,z) &= \frac{1}{F^4}\widetilde{d}_2(F^2v, F^8w, F^4x, y, F^3z) \end{aligned}$$

and replace F^{11} by Δ so that d_1 and d_2 have coefficients in $\mathbb{Q}[c_4, \Delta]$.

Remark 6.11. Unfortunately the polynomials $\widetilde{r}_i$ and d_i would take several pages to print out, so we must refer the reader to the accompanying Magma file [F4] for further details. We should also remark that the computation of d_1 and d_2 took several hours of computer time (whereas no other calculation up to this point took more than a few seconds).

Theorem 6.12. *Let E/K be an elliptic curve with Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$ and let $\Delta = (c_4^3 - c_6^2)/1728$. Assume $j(E) \neq 0, 1728$ and let $X = X_E(11)$, respectively $X_E^-(11)$, be as given in Theorem 3.17. If $(v : w : x : y : z) \in X(K) \setminus \{d_i = 0\}$, not a cusp, then the corresponding elliptic curve E'/K satisfies*

$$c_4(E') \equiv d_1(v,w,x,y,z)\, c_4(\mathbf{F})(v,w,x,y,z) \mod (K^\times)^4,$$

respectively

$$c_4(E') \equiv d_2(v,w,x,y,z)\, c_4(\mathbf{G})(v,w,x,y,z) \mod (K^\times)^4.$$

Proof: As noted in [HK2, Section 7.1] we are free to extend our field K so that $\phi : E[11] \cong \mu_{11} \times \mathbb{Z}/11\mathbb{Z}$ is defined over K. Let $(a : b : c : d : e)$ be the corresponding K-point on $X(11)$. We scale a, b, c, d, e so that $c_4(a,b,c,d,e) = c_4$. Then $a^{11}, \ldots, e^{11} \in K$ and by comparing the Weierstrass equation for E in the statement of the theorem with (31) we deduce $(abcde)^{11} \in (K^\times)^4$. The polynomials $\mathbf{F}$ and $\mathbf{G}$ were computed in Section 3.3 as twists of F. Putting

$$(v', w', x', y', z')^T = vF^7\mathbf{x}_1 + wF^6\mathbf{x}_4 + xF^{13}\mathbf{x}_5 + yF^8\mathbf{x}_9 + zF^{10}\mathbf{x}_{14},$$
$$(v'', w'', x'', y'', z'')^T = vF^3\nabla F + wF^9\nabla I_7 + xF^5\nabla I_8 + yF\nabla I_9 + zF^4\nabla c_4,$$

it follows by (18), (19) and (24) that

$$c_4(\mathbf{F})(v,w,x,y,z) = \frac{(c_4^3 - 1728F^{11})^8}{F^{22}} c_4(v',w',x',y',z'),$$
$$c_4(\mathbf{G})(v,w,x,y,z) = \frac{(55(c_4^3 - 1728F^{11}))^8}{F^{11}} c_4(v'',w'',x'',y'',z'').$$

By construction of d_1 and d_2 we have

$$d_1(v,w,x,y,z) = \frac{1}{(abcde)^3F^{30}} r_1(v',w',x',y',z'),$$
$$d_2(v,w,x,y,z) = \frac{1}{(abcde)^3F^{9}} r_2(v'',w'',x'',y'',z'').$$

In view of Theorem 6.4 our aim is to show that

$$d_1(v,w,x,y,z)\, c_4(\mathbf{F})(v,w,x,y,z) \equiv v'w'x'y'z'c_4(v',w',x',y',z') \mod (K^\times)^4,$$
$$d_2(v,w,x,y,z)\, c_4(\mathbf{G})(v,w,x,y,z) \equiv v''w''x''y''z''c_4(v'',w'',x'',y'',z'') \mod (K^\times)^4,$$

equivalently

$$(abcde)^8 F^{36} r_1(v', w', x', y', z') \equiv v'w'x'y'z' \mod (K^\times)^4,$$
$$(abcde)^8 F^{24} r_2(v'', w'', x'', y'', z'') \equiv v''w''x''y''z'' \mod (K^\times)^4.$$

To finish the proof we note that the quintic forms

$$(abcde)^2 F^9 s_1(v', w', x', y', z') \quad \text{and} \quad (abcde)^2 F^6 s_2(v'', w'', x'', y'', z'')$$

have coefficients in K (since the degree of each coefficient is a multiple of 11) and then use (35). □

We already gave a formula for the j-invariant in Section 6.1. So (assuming $j(E') \neq 0$) Theorem 6.12 determines E' up to quadratic twist by -1. In the case $K = \mathbb{Q}$ it is easy to decide which of the remaining two possibilities is correct by looking at traces of Frobenius.

In principle it should be possible to find alternative quintic forms to be used at points where d_1 or d_2 vanishes. (The quintic forms in question are those meeting the z-curve in a divisor $4D$ where D is a hyperplane section for the A-curve.) In the case $n = 7$ we managed to find the alternative forms using the Riemann-Roch machinery in Magma. Unfortunately the analogue of this in the case $n = 11$ does not appear to be practical. In the case of $X_E^-(11)$ this is not a problem, since the 25 points with $d_2 = 0$ correspond to the elliptic curves ℓ-isogenous to E for $\ell = 2, 7, 13$. We can also account for 7 of the points on $X_E(11)$ with $d_1 = 0$ as corresponding to the elliptic curve E itself and the elliptic curves 5-isogenous to E. We are yet to encounter an example (over $K = \mathbb{Q}$) where one of the remaining points with $d_1 = 0$ is rational.

7. Examples

We use the formulae in Theorems 1.2, 1.3 and 1.4 to give examples of non-trivial n-congruences for $n = 7, 9, 11$ over $\mathbb{Q}$ and $\mathbb{Q}(T)$. By "non-trivial" we mean that the elliptic curves are not isogenous. The examples over $\mathbb{Q}$ illustrate the value of minimising and reducing as described in Section 5. The examples over $\mathbb{Q}(T)$ were found by setting $a = b = -27j/(4(j - 1728))$ to obtain a surface fibred over the j-line and then intersecting with one of the co-ordinate hyperplanes in the hope of finding a rational curve. We refer to elliptic curves over $\mathbb{Q}$ by their labels in Cremona's tables [C]. For elliptic curves beyond the range of Cremona's tables we simply write the conductor followed by a $*$.

7.1. **Examples in the case $n = 7$.**

Example 7.1. Let E be the elliptic curve $162c1$. Let $\mathcal{F}$ and $\mathcal{G}$ be the equations for $X_E(7)$ and $X_E^-(7)$ as given in Theorem 1.2 with $a = 3645$ and $b = -13122$. These have invariants $\Psi(\mathcal{F}) = -2^{11} \cdot 3^{18}$ and $\Psi(\mathcal{G}) = 2^{22} \cdot 3^{36}$. Minimising and reducing suggests that we substitute

$$F(x, y, z) = \frac{1}{2^{10}3^{14}}\mathcal{F}(36y - 9z, 1944x - 972y - 1215z, z)$$
$$G(x, y, z) = \frac{1}{2^{12}3^{20}}\mathcal{G}(18x + 18y + 9z, z, -486x + 1458y + 1944z)$$

to give quartics

$$\begin{aligned} F(x, y, z) = 3x^3z + 3x^2y^2 - 6x^2yz + 3x^2z^2 - 3xy^3 \\ + 3xz^3 + 2y^4 - y^3z - 9y^2z^2 + 4yz^3 - 5z^4 \\ G(x, y, z) = -x^3y - x^3z - 6x^2z^2 + 6xy^2z - 6xyz^2 \\ + 6xz^3 + 2y^4 + 2y^3z - 6y^2z^2 - 38yz^3 - 8z^4 \end{aligned}$$

with invariants $\Psi(F) = -2 \cdot 3^4$ and $\Psi(G) = 2^2 \cdot 3^4$. We find rational points $P_1 = (1 : 0 : 0)$, $P_2 = (3 : -2 : -1)$ on $\{F = 0\} \subset \mathbb{P}^2$, and rational points $P_3 = (1 : 0 : 0)$, $P_4 = (1 : 1 : -1)$, $P_5 = (4 : -1 : 1)$ on $\{G = 0\} \subset \mathbb{P}^2$. The corresponding elliptic curves 7-congruent to E are

P_1	$162c1$	$y^2 + xy = x^3 - x^2 + 3x - 1$
P_2	$293706*$	$y^2 + xy = x^3 - x^2 - 62930562x - 192134303740$
P_3	$162c2$	$y^2 + xy = x^3 - x^2 - 42x - 100$
P_4	$17334f1$	$y^2 + xy = x^3 - x^2 - 5473977x - 4956193171$
P_5	$624186*$	$y^2 + xy = x^3 - x^2 - 11751402282x + 360746315347508.$

The fact $162c1$ and $162c2$ are reverse 7-congruent is already clear since they are 3-isogenous and $(3/7) = -1$.

It is shown in [HK2] that there are infinitely many 6-tuples of directly 7-congruent non-isogenous elliptic curves over $\mathbb{Q}$. The following example shows that there are infinitely many pairs of reverse 7-congruent non-isogenous elliptic curves over $\mathbb{Q}$.

Example 7.2. Let $E/\mathbb{Q}(T)$ be the elliptic curve $y^2 = x^3 + ax + b$ where $a = b = -27j/(4(j - 1728))$ and $j = 27T^3(5T - 56)/(T - 1)$. Then on $X_E^-(7)$, with equation as given in Theorem 1.2, we find the rational point

$$(x : y : z) = (0 : -4(T^2 - 12T + 8)(5T^2 + 4T + 8) : 9T^2(T + 4)(5T - 56)).$$

Specialising T (and taking quadratic twists by d as indicated) we obtain the following pairs of reverse 7-congruent elliptic curves E_1 and E_2.

T	d	E_1	E_2
-16	-38	$361a1$	$361a2$
8	-10	$700g1$	$2100q1$
2	-2	$2116b1$	$10580h1$
$16/5$	-42	$24255r1$	$24255m2$

The existence of specialisations E_1 and E_2 that are not isogenous is enough to show that there are infinitely many such specialisations.

7.2. **Examples in the case $n = 9$.**

Example 7.3. Let E be the elliptic curve $47775z1$. Let $\mathcal{F}_1 = \mathcal{F}_2 = 0$ be the equations for $X_E(9) \subset \mathbb{P}^3$ as given in Theorem 1.3 with $a = -41489280$ and $b = 102867483600$. The invariant is $\Psi(\mathcal{F}_1, \mathcal{F}_2) = -2^{42} \cdot 3^{60} \cdot 5^{12} \cdot 7^{32} \cdot 13^4$. Minimising and reducing suggests that we substitute

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

so that $X_E(9)$ is defined by

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

with invariant $-3^3 \cdot 5^6 \cdot 7^5 \cdot 13^4$. 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 7.3 we have found two further triples of directly 9-congruent non-isogenous elliptic curves over $\mathbb{Q}$. These are

$$\begin{array}{ll} 4650j1 & y^2+xy=x^3+x^2-2700x+54000 \\ 553350* & y^2+xy=x^3+x^2-10472207700x-455228489646000 \\ 1966950* & y^2+xy=x^3-x^2-20654522386242x-36130051534030639084 \end{array}$$

$$\begin{array}{ll} 27606c1 & y^2+xy=x^3-10289707x+12703497719 \\ 358878* & y^2+xy=x^3+2940333x-1416695391 \\ 1242270* & y^2+xy+y=x^3-x^2-359912x-322105301 \end{array}$$

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

Example 7.4. Let E be the elliptic curve $201c1$. Let $\mathcal{G}_1=\mathcal{G}_2=0$ be the equations for $X_E^-(9)\subset\mathbb{P}^3$ as given in Theorem 1.3 with $a=-1029699$ and $b=402173694$. The invariant is $\Psi(\mathcal{G}_1,\mathcal{G}_2)=2^{48}\cdot 3^{85}\cdot 67^5$. Minimising and reducing suggests that we substitute

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

so that $X_E^-(9)$ is defined by

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

with invariant $-3^4\cdot 67^5$. On this curve we find the rational point $(1:-2:-1:0)$. The corresponding elliptic curve reverse 9-congruent to E is

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

The following example shows that there are infinitely many pairs of directly 9-congruent non-isogenous elliptic curves over $\mathbb{Q}$.

Example 7.5. 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 given in Theorem 1.3, 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 curve directly 9-congruent to E is the curve directly 3-congruent to E constructed in Theorem 1.1 with $c_4 = -a(T)/27, c_6 = -b(T)/54$ and

$$(\lambda : \mu) = \big(47T^6 - 78T^5 - 153T^4 + 244T^3 + 153T^2 - 78T - 47 \\ : 18(T^2 + 1)(T^2 + 6T - 1)\big).$$

Specialising to $T = 0$ gives a pair of curves with conductors 80640 and 5886720. In particular these curves are not isogenous.

Next we give an example to show there are infinitely many non-trivial pairs of reverse 9-congruent elliptic curves over $\mathbb{Q}$.

Example 7.6. 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 $X_E^-(9)$, with equations as given in Theorem 1.3, has rational point

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

The corresponding curve reverse 9-congruent to E is the curve reverse 3-congruent to E constructed in Theorem 1.1 with $c_4 = -a(T)/27, c_6 = -b(T)/54$ and

$$(\lambda : \mu) = \big((3T + 1)(9T^3 - 9T - 4)(6T^3 - 3T - 1)(180T^4 + 321T^3 + 216T^2 + 66T + 8) \\ : 3(369T^6 + 1107T^5 + 1431T^4 + 1017T^3 + 414T^2 + 90T + 8)\big).$$

Specialising T (and taking quadratic twists by d as indicated) we obtain the following pairs of reverse 9-congruent elliptic curves E_1 and E_2.

T	d	E_1	E_2
-1	6	$24a4$	$24a5$
$-1/3$	6	$243a1$	$243b2$
$-1/4$	3	$768d1$	$114432o1$
$-1/2$	-6	$6400u1$	$6400u2$
$-2/3$	6	$23814v1$	$23814i1$

7.3. **Examples in the case $n = 11$.**

Example 7.7. Let E be the elliptic curve 1782b1. Let $\mathcal{F}$ be the cubic form describing $X_E(11) \subset \mathbb{P}^4$ as given in Theorem 1.4 with $a = 765$ and $b = 15102$. The invariant is $\Psi(\mathcal{F}) = -2^{28} \cdot 3^{12} \cdot 11^6$. Minimising and reducing suggests that we substitute

$$\begin{pmatrix} v \\ w \\ x \\ y \\ z \end{pmatrix} \leftarrow \begin{pmatrix} 984 & 12900 & -9093 & -34056 & 13689 \\ -2040 & -24252 & -3315 & 0 & -16857 \\ 328 & 164 & -435 & 0 & -57 \\ -352 & 88 & -264 & 264 & -1056 \\ -8 & -4 & -13 & 0 & 25 \end{pmatrix} \begin{pmatrix} v \\ w \\ x \\ y \\ z \end{pmatrix}$$

so that $X_E(11) \subset \mathbb{P}^4$ is the singular locus of the Hessian of

$$\begin{aligned} &-v^2w + v^2x - v^2y + 2v^2z - vw^2 + 4vwz - 4vx^2 - 8vxy + 2vxz + 6vyz \\ &+3vz^2 + 2w^3 - 3w^2x - 2w^2y + 8w^2z + 6wx^2 + 2wxy + 2wxz + 6wy^2 - 6wyz \\ &\qquad +9wz^2 - x^3 - x^2z - 3xy^2 - 6xyz - 9xz^2 - 6y^3 + 9y^2z + 3yz^2 - 7z^3 = 0 \end{aligned}$$

with invariant $2^2 \cdot 3^4 \cdot 11^2$. We find rational points $P_1 = (-1 : 5 : 1 : 2 : 1)$, $P_2 = (0 : 0 : 0 : 1 : 0)$ and $P_3 = (1 : 1 : -1 : 0 : -4)$. The corresponding elliptic curves directly 11-congruent to E are

P_1	$1782b1$	$y^2 + xy = x^3 - x^2 + 48x + 224$
P_2	$1782b2$	$y^2 + xy = x^3 - x^2 - 447x - 7795$
P_3	$447282*$	$y^2 + xy = x^3 - x^2 - 17552171922x - 227953575178678$

The fact $1782b1$ and $1782b2$ are directly 11-congruent is already clear since they are 3-isogenous and $(3/11) = 1$.

Example 7.8. Let E be the elliptic curve 4466c1. Let $\mathcal{G}$ be the cubic form describing $X_E^-(11) \subset \mathbb{P}^4$ as given in Theorem 1.4 with $a = 85$ and $b = -83162$. The invariant is $\Psi(\mathcal{F}) = 2^{21} \cdot 7 \cdot 11^2 \cdot 29^2$. Minimising and reducing suggests that we substitute

$$\begin{pmatrix} v \\ w \\ x \\ y \\ z \end{pmatrix} \leftarrow \begin{pmatrix} 4096 & -1408 & 128 & -1312 & 45088 \\ 0 & 128 & 128 & 32 & 110 \\ 0 & 0 & -256 & -96 & -103 \\ 0 & 0 & 0 & -32 & -11 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} v \\ w \\ x \\ y \\ z \end{pmatrix}$$

so that $X_E^-(11) \subset \mathbb{P}^4$ is the singular locus of the Hessian of

$$\begin{aligned}-2v^2z - 4vwy + 12vxy + 4vxz + 5vy^2 + 6vyz - 43vz^2 - w^2x + w^2y \\ -4wxy - 2wxz - 3wy^2 + 196wyz + 83wz^2 - 11x^3 - 12x^2y - 9x^2z \\ -11xy^2 + 366xyz + 125xz^2 + 322y^3 + 447y^2z + 275yz^2 + 632z^3 = 0\end{aligned}$$

with invariant $-2^2 \cdot 7 \cdot 11^2 \cdot 29^2$. We find rational points $P_1 = (-7 : 11 : 3 : 1 : 1)$ and $P_2 = (7830 : -3553 : 510 : -281 : 71)$. The corresponding elliptic curves reverse 11-congruent to E are

P_1	$4466c2$	$y^2 + xy + y = x^3 - x^2 - 1755x - 27349$
P_2	$1174558*$	$y^2 + xy + y = x^3 - x^2 + 117885809240x + 16240157710556505$

The fact $4466c1$ and $4466c2$ are reverse 11-congruent is already clear since they are 2-isogenous and $(2/11) = -1$.

We did not find any triples of 11-congruent non-isogenous elliptic curves over $\mathbb{Q}$. The following example shows that there are infinitely many pairs of directly 11-congruent non-isogenous elliptic curves over $\mathbb{Q}$.

Example 7.9. Let $E/\mathbb{Q}(T)$ be the elliptic curve $y^2 = x^3 + a(T)x + b(T)$ where

$$\begin{aligned}a(T) &= -3(T-3)(T^4 - 5T^2 - 24T - 92)/(T^3 - T^2 + 4T + 24) \\ b(T) &= -2(T-3)(T^5 - T^4 - 11T^3 - 43T^2 - 62T - 316)/(T^3 - T^2 + 4T + 24).\end{aligned}$$

Then $X_E(11)$, with equations as given in Theorem 1.4, has rational point

$$\begin{pmatrix} v \\ w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} T^6 + T^5 + 31T^4 + 259T^3 + 520T^2 + 676T + 1248 \\ -(T-3)(T^5 + 4T^4 + 43T^3 + 100T^2 - 44T - 320) \\ -(T^2 + 3T + 14)(T^3 - T^2 + 4T + 24) \\ 0 \\ (T+4)(T^3 - T^2 + 4T + 24) \end{pmatrix}$$

Specialising T (and taking quadratic twists by d as indicated) we obtain the following pairs of directly 11-congruent elliptic curves E_1 and E_2.

T	d	E_1	E_2
2	-6	$11a3$	$11a2$
1	42	$49a1$	$49a4$
-3	-2	$216b1$	$1512c1$
11	-426	$10082c1$	$70574h1$

The elliptic curve 11-congruent to E is $y^2 = x^3 + A(T)x + B(T)$ where

$$\begin{aligned}
A(T) = {} & -3(T-3)(T^2-8T-17)(T^3-T^2+4T+24)(T^{12}-250T^{11}+3473T^{10} \\
& -23824T^9+106654T^8-354556T^7+890186T^6-1710568T^5 \\
& +2386357T^4-2054170T^3+1799781T^2+956680T+3570796), \\
B(T) = {} & -2(T-3)(T^3-T^2+4T+24)^2(T^{20}+476T^{19}-27815T^{18}+556718T^{17} \\
& -6046664T^{16}+42450848T^{15}-213832636T^{14}+823702888T^{13} \\
& -2497998850T^{12}+5954643736T^{11}-10798748818T^{10}+13644339892T^9 \\
& -7927895108T^8-10398245632T^7+25581636532T^6-10366268760T^5 \\
& -60876061719T^4+164062110060T^3-98120800447T^2+262948421518T \\
& +141270230564).
\end{aligned}$$

These elliptic curves have discriminants

$$\begin{aligned}
& 2^{12}3^6(T-5)(T-3)^2(T+1)^5(T^2+7)/(T^3-T^2+4T+24)^3, \\
& -2^{12}3^6(T-5)^4(T-3)^2(T+1)^3(T^2+7)(T^3-T^2+4T+24)^3(T^3-T^2+15T-31)^{11}.
\end{aligned}$$

We did not find any pairs of reverse 11-congruent non-isogenous elliptic curves over $\mathbb{Q}(T)$. We note that according to [KS, Theorem 4] the modular diagonal surface in this case is of general type.

7.4. **Tables.** We have written a program in Magma that given an elliptic curve $E/\mathbb{Q}$ and $n \in \{7, 9, 11\}$ searches for elliptic curves n-congruent to E. For $n \in \{9, 11\}$ we have run these programs for all elliptic curves in the Cremona database (up to conductor 130000 at the time of our calculation). The resulting list of pairs of n-congruent elliptic curves is available from the author's website [F4]. We have been careful to remove all pairs that could be deduced from earlier entries by any combination of the following observations.

- n-congruence of elliptic curves is an equivalence relation.
- If $\phi : E \to E'$ is a rational isogeny of degree coprime to n then E and E' are n-congruent.
- If E and E' are n-congruent then so are their twists by the same quadratic character.

There is no guarantee that our tables are complete, since we have only searched for points of small height on the corresponding curves of genus 10 and 26. However the points we found (on minimised and reduced models) were generally much smaller than the search bound used. So in any given case it seems likely that we have found all the rational points, but there is little prospect of proving this for curves of such large genus.

Table 1 : Pairs of 9-congruent elliptic curves

$17a^2$	$+$	$493a$	$430b$	$+$	$20210b$	$968a$	$+$	$132616*$	$1950h$	$-$	$122850l$
$33a^2$	$-$	$297c$	$434c^2$	$+$	$62062h$	$1050j2$	$-$	$11550bg2$	$1950m2$	$+$	$17550ba2$
$35a2$	$-$	$77b2$	$446b$	$-$	$150302*$	$1066a$	$-$	$7462e$	$1952c$	$+$	$44896e$
$35a3$	$-$	$1015b1$	$456c$	$-$	$20520e$	$1106c$	$+$	$2281678*$	$1963a$	$+$	$374933*$
$66a1^2$	$+$	$3102c1$	$459c1$	$+$	$2295a1$	$1110n2$	$+$	$13098q2$	$1998d$	$-$	$3774c$
$84a3^2$	$-$	$1932b2$	$506b$	$+$	$2530b$	$1111a$	$+$	$121215655*$	$2040h$	$+$	$4073880*$
$91a$	$+$	$5005c$	$525c^2$	$+$	$4725r$	$1134d1$	$+$	$5670h1$	$2072c^2$	$-$	$184408*$
$106d$	$+$	$2438a$	$537b$	$+$	$148749*$	$1155j1$	$+$	$47355s1$	$2093c$	$+$	$2576483*$
$110c2$	$+$	$60610m2$	$570k3^2$	$-$	$1254j2$	$1176a$	$+$	$10584n$	$2118b1$	$-$	$7660806*$
$115a$	$+$	$366505*$	$573c$	$-$	$21491511*$	$1176b$	$+$	$34104b$	$2135d$	$+$	$207095*$
$118c$	$+$	$27494c$	$600c^2$	$+$	$5400r$	$1190c2$	$-$	$393890*$	$2190b$	$+$	$116070i$
$123b$	$+$	$3813a$	$606f^5$	$+$	$155742*$	$1209a$	$+$	$1357707*$	$2190e$	$+$	$15330k$
$131a$	$-$	$136633*$	$627b2$	$+$	$5643d2$	$1215b$	$-$	$1215g$	$2190l$	$+$	$24090k$
$140a2$	$-$	$3220c2$	$648b$	$+$	$26568a$	$1215c$	$+$	$23085b$	$2198b1$	$+$	$964922*$
$142c^2$	$+$	$232454*$	$696a$	$+$	$355656*$	$1218h^2$	$+$	$1218i$	$2209a$	$-$	$11045b$
$153a$	$-$	$117351a$	$702f$	$+$	$30186h$	$1275d$	$+$	$263925*$	$2211c$	$+$	$134871*$
$162a1$	$+$	$810c1$	$710a$	$+$	$137030*$	$1281d$	$+$	$4209c$	$2314b$	$-$	$363298*$
$166a$	$+$	$848426*$	$714c$	$+$	$6426n$	$1288e$	$+$	$240856*$	$2373f$	$-$	$21357c$
$174a1$	$+$	$17574f1$	$715b$	$+$	$1080365*$	$1330d1$	$+$	$860510*$	$2418a$	$+$	$2884674*$
$174c$	$+$	$1914g$	$741b$	$+$	$3335241*$	$1470e2$	$+$	$4998j2$	$2443c$	$+$	$925897*$
$195c$	$+$	$1755a$	$741d$	$+$	$65949e$	$1470n^2$	$+$	$13230dv$	$2450l^{13}$	$+$	$129850r$
$200b^2$	$-$	$20600v$	$768b^{2,5}$	$+$	$114432j$	$1482e1$	$+$	$16302l1$	$2451b^2$	$+$	$2451c$
$201a$	$+$	$82209a$	$781a$	$-$	$1349b$	$1482e2$	$+$	$117078p2$	$2530e$	$+$	$908270*$
$201c$	$-$	$374865*$	$805b^2$	$+$	$10465a$	$1482f2$	$+$	$8128770*$	$2537b$	$+$	$210571*$
$229a$	$+$	$2357555*$	$805c^2$	$+$	$24955b$	$1518r$	$+$	$13662m$	$2541a$	$-$	$22869o$
$235b$	$+$	$329a$	$808a$	$+$	$891224*$	$1617b$	$+$	$289443*$	$2568e$	$+$	$7408680*$
$238d^2$	$-$	$91154b$	$810a2$	$+$	$208170*$	$1653a$	$-$	$520695*$	$2571a$	$+$	$12749589*$
$243a1$	$-$	$243b2$	$810d2$	$+$	$23490n2$	$1701a$	$-$	$1701g$	$2616c$	$+$	$6574008*$
$246c^2$	$+$	$2214a$	$843a$	$+$	$1600857*$	$1701a$	$-$	$22113c$	$2646a1$	$+$	$60858h1$
$249a$	$+$	$42579e$	$850c$	$+$	$16150q$	$1725i^2$	$-$	$343275*$	$2646e1$	$+$	$13230e1$
$258c$	$+$	$1290h$	$858d2$	$+$	$4290l2$	$1757a$	$+$	$335587*$	$2674e$	$+$	$259378*$
$270a1$	$+$	$2970i1$	$861b$	$+$	$192003*$	$1771c1$	$+$	$2807035*$	$2678a$	$-$	$20806a$
$302b^2$	$+$	$226802*$	$861d$	$+$	$469245*$	$1782c$	$+$	$290466*$	$2699b$	$+$	$5249555*$
$338a^7$	$+$	$22646d$	$867b^2$	$+$	$141321*$	$1806a$	$+$	$2775822*$	$2706i^2$	$+$	$65855922*$
$350b2$	$-$	$6650bh2$	$897d^2$	$+$	$8073a$	$1830h$	$+$	$16470w$	$2728d$	$+$	$832040*$
$354a^2$	$+$	$55578e$	$906b$	$+$	$610222710*$	$1848g$	$+$	$9097704*$	$2758b$	$+$	$1069527578*$
$364a$	$+$	$26572d$	$906e$	$+$	$28086d$	$1862a2$	$+$	$102410n2$	$2787d$	$+$	$393187173*$
$390d3^2$	$+$	$3510f2$	$930d^2$	$+$	$564510*$	$1870e$	$+$	$136510*$	$2793b$	$+$	$790419*$
$406b2$	$-$	$62930k2$	$930i2$	$+$	$160890*$	$1887b$	$-$	$1054833*$	$2835a1$	$+$	$65205g1$
$430a$	$+$	$7310e$	$930l$	$+$	$8370n$	$1911a$	$-$	$17199o$	$2835d$	$+$	$53865d$

Table 2 : Pairs of 11-congruent elliptic curves

$138b^{2,3}$	+	$17526b$	$3910l$	+	$43010o$	$16354h$	+	$703222*$	$55470m^2$	+	$1275810*$
$190b$	+	$2470a$	$3990z$	+	$3990ba$	$16390m$	+	$23585210*$	$55594a$	−	$10062514*$
$216b$	+	$1512c$	$4046n$	+	$416738*$	$17550a$	+	$298350*$	$56100j^2$	−	$15539700*$
$238b^2$	+	$4522b$	$4158f$	+	$54054m$	$17550z$	+	$122850r$	$56154t$	−	$27346998*$
$258b^2$	+	$461562*$	$4200g^2$	+	$79800h$	$17556d$	+	$9778692*$	$57354j$	+	$3498594*$
$294a^7$	+	$4998ba$	$4275a^2$	−	$175275*$	$17710h$	+	$726110*$	$58968k$	+	$58968l$
$325a^3$	+	$23075e$	$4466c^2$	−	$1174558*$	$18850i$	+	$131950*$	$60088b$	+	$53658584*$
$329a$	+	$59549a$	$4598b$	+	$32186g$	$19950bl$	+	$618450*$	$64596b$	+	$53162508*$
$426b^2$	+	$77106c$	$4704a$	−	$192864*$	$20838f$	−	$10273134*$	$65220c$	+	$534086580*$
$497a$	+	$148603*$	$4760b$	+	$775880*$	$21175b$	+	$21175g$	$66300q$	+	$1259700*$
$513a$	+	$77463a$	$5070d$	−	$55770j$	$21760a$	+	$805120*$	$66930e$	+	$101265090*$
$600b$	+	$4200c$	$5265b$	+	$194805*$	$22950bi$	+	$849150*$	$67158c$	+	$3559374*$
$645f$	−	$70305g$	$5454b$	+	$59994e$	$23595g$	−	$165165*$	$67650v$	+	$16168350*$
$648b$	−	$4536c$	$5577b$	−	$39039b$	$24906a$	+	$70558698*$	$70890w$	+	$2197590*$
$700e^2$	−	$11900d$	$5880b$	−	$417480*$	$25110j$	−	$426870*$	$71610bj$	+	$109634910*$
$1080d$	+	$39960h$	$6710h$	+	$4381630*$	$26026d$	−	$2836834*$	$73255b$	−	$89151335*$
$1115a$	+	$125995a$	$7315e$	+	$8214745*$	$27610f^2$	+	$5273510*$	$73326t$	+	$3886278*$
$1134b$	−	$12474f$	$7350n$	+	$95550ch$	$27650j$	+	$1023050*$	$73370h$	+	$130790*$
$1155b$	−	$42735a$	$7830f^3$	+	$477630*$	$27885p$	−	$2704845*$	$78650w^2$	−	$78650bc$
$1176a$	−	$15288a$	$8096a$	−	$13984a$	$28420d$	+	$5087180*$	$79800s$	+	$16837800*$
$1210d$	+	$1210f$	$8120d$	+	$332920*$	$28830a$	−	$2219910*$	$80325u$	+	$80325v$
$1254b$	+	$264594*$	$8410c$	−	$58870e$	$28840c$	+	$30253160*$	$81675q$	+	$3348675*$
$1470j$	−	$16170bl$	$8670o$	−	$8670p$	$30774h$	+	$11417154*$	$83148g$	−	$582036*$
$1666a$	+	$18326b$	$9438d$	+	$1009866*$	$30855a$	+	$215985*$	$84270j$	+	$589890*$
$1782b^3$	+	$447282*$	$9450l$	+	$9450m$	$30888g$	+	$216216*$	$84930m$	+	$59196210*$
$1848f$	+	$97944h$	$9450o$	+	$292950*$	$31746q$	+	$222222*$	$84930p$	+	$31509030*$
$1870c$	+	$24310c$	$9450bo$	+	$160650*$	$32802d^2$	−	$117660774*$	$85050bf$	+	$2466450*$
$1925g$	+	$140525*$	$9555a$	−	$181545*$	$32856f$	+	$229992*$	$87210l$	+	$3226770*$
$2093b$	+	$26611d$	$9966h$	+	$827178*$	$34385a$	+	$378235*$	$87990d$	+	$5895330*$
$2184c$	+	$2184d$	$10010t$	+	$670670*$	$35574b$	−	$35574e$	$88842l$	+	$120198k$
$2755b$	+	$476615*$	$10082b$	+	$70574c$	$36498s$	+	$56406i$	$90986e$	+	$423175886*$
$3234e$	+	$947562*$	$11774a$	+	$24172022*$	$37446i$	−	$4456074*$	$92950s$	+	$9016150*$
$3322c$	+	$235862*$	$12376j$	+	$12376k$	$37830o$	+	$31285410*$	$93795r$	+	$2157285*$
$3325a$	+	$1173725*$	$12696b$	+	$12696c$	$38070k$	−	$5291730*$	$95370ch$	+	$667590*^2$
$3610d$	+	$25270j$	$13650ba$	+	$2716350*$	$39732a$	+	$24514644*$	$95550cb$	+	$95550cc$
$3718d$	+	$107822e$	$14196i$	−	$269724*$	$45738b$	+	$869022*$	$95700b$	+	$2201100*$
$3822u$	−	$42042ce$	$14844a$	+	$40182708*$	$47974d^2$	−	$48885506*$	$98070z$	+	$270771270*$
$3850a$	+	$65450b$	$14910ba$	+	$40450830*$	$53290a^2$	+	$53290b$	$98982c$	−	$19697418*$
$3850i^2$	+	$65450i$	$14950l$	+	$1599650*$	$53865e$	−	$10395945*$	$104910d$	+	$3252210*$
$3900e$	−	$66300t$	$16150p$	+	$4731950*$	$54813a$	−	$1589577*$	$105522e$	+	$139183518*$

The entries are given as $E_1 \pm E_2$ where the $\pm$ indicates whether the n-congruence respects the Weil pairing. In all cases except when $n = 9$ and the curves admit a rational 3-isogeny we have omitted the final number from the Cremona reference (which may be taken to be 1). A superscript ℓ indicates an elliptic curve that admits a rational ℓ-isogeny where ℓ is a prime not dividing n. If ℓ is not a square mod n then we may change the sign of the congruence by passing to an isogenous curve. For elliptic curves beyond the range of Cremona's tables we have again written the conductor followed by a $*$. The extended version of our tables [F4] also gives the Weierstrass equations.

References

[A] A. Adler, Invariants of $\mathrm{PSL}_2(\mathbf{F}_{11})$ acting on $\mathbf{C}^5$, *Comm. Algebra* **20** (1992), no. 10, 2837–2862.

[AR] A. Adler and S. Ramanan, *Moduli of abelian varieties*, Lect. Notes in Math. 1644, Springer (1996).

[BCP] MAGMA is described in 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/`

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

[CFS] J.E. Cremona, T.A. Fisher and M. Stoll, Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves, *Algebra & Number Theory* **4** (2010), no. 6, 763–820.

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

[E] N.D. Elkies, The Klein Quartic in Number Theory, in *The eightfold way, The beauty of Klein's quartic curve*, S. Levy (ed.), MSRI Publications **35**, Cambridge University Press, Cambridge (1999) 51–101.

[F0] T.A. Fisher, *On 5 and 7 descents for elliptic curves*, PhD thesis, University of Cambridge, 2000.

[F1] T. A. Fisher, Some examples of 5 and 7 descent for elliptic curves over $\mathbf{Q}$, *J. Eur. Math. Soc.* 3 (2001), no. 2, 169–201.

[F2] T. A. Fisher, *The Hessian of a genus one curve*, preprint, `arXiv:math/0610403v2`

[F3] T.A. Fisher, *Invariant theory for the elliptic normal quintic, I. Twists of* $X(5)$, in preparation.

[F4] T.A. Fisher, *On families of* n*-congruent elliptic curves*, electronic data accompanying this article, `http://www.dpmms.cam.ac.uk/~taf1000/papers/highercongr.html`

[Fr] 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.

[HK1] E. Halberstadt and A. Kraus, On the modular curves $Y_E(7)$, *Math. Comp.* **69** (2000), no. 231, 1193–1206.

[HK2] E. Halberstadt and A. Kraus, Sur la courbe modulaire $X_E(7)$, *Experiment. Math.* **12** (2003), no. 1, 27–40.

[KR] E.J. Kani and O.G. Rizzo, *Mazur's question on mod* 11 *representations of elliptic curves*, preprint, `http://www.mast.queensu.ca/~kani/mdqs.htm`

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

[K1] F. Klein, Über die Transformationen siebenter Ordnung der elliptischen Funktionen, *Math. Ann.* **14** (1878), 428-471. English translation in *The eightfold way, The beauty of Klein's quartic curve*, S. Levy (ed.), MSRI Publications **35**, Cambridge University Press, Cambridge 1999.

[K2] F. Klein, Über die Transformationen elfter Ordnung der elliptischen Funktionen, *Math. Ann.* **15** (1879), Reprinted in *Gesammelte Mathematische Abhandlungen III*, R. Fricke et al (eds.), Springer (1923) 140–168.

[K3] F. Klein, Über die elliptischen Normalkurven der n-ten Ordnung *(1885)*. Reprinted in *Gesammelte Mathematische Abhandlungen III*, R. Fricke et al (eds.), Springer (1923) 198–254.

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

[M] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), no. 2, 129–162.

[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.

[RS1] 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.

[RS2] K. Rubin and A. Silverberg, Mod 2 representations of elliptic curves, *Proc. Amer. Math. Soc.* **129** (2001), no. 1, 53–57.

[Sa] G. Salmon, *A treatise on the higher plane curves*, Third edition, Hodges, Foster and Figgis, Dublin, 1879.

[S] 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.

[Si] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM **106** (1986).

[V1] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sc. Paris*, **273** (1971) 238-241.

[V2] J. Vélu, Courbes elliptique munies d'un sous-group $\mathbb{Z}/n\mathbb{Z} \times \mu_n$, *Bull. Math. Soc. math. France*, Mémoire **57** (1978).

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

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