LMS J. Comput. Math. 17 (1) (2014) 536–564 © 2014 Author
doi:10.1112/S1461157014000059

On families of 7- and 11-congruent elliptic curves

Tom Fisher

Abstract

We use an invariant-theoretic method to compute certain twists of the modular curves $X(n)$ for $n = 7, 11$. Searching for rational points on these twists enables us to find non-trivial pairs of n-congruent elliptic curves over $\mathbb{Q}$, that is, pairs of non-isogenous elliptic curves over $\mathbb{Q}$ whose n-torsion subgroups are isomorphic as Galois modules. We also find a non-trivial pair of 11-congruent elliptic curves over $\mathbb{Q}(T)$, and hence give an explicit infinite family of non-trivial pairs of 11-congruent elliptic curves over $\mathbb{Q}$.

Supplementary materials are available with this article.

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 e_n, and *reverse n-congruent* if

$$e_n(\phi P, \phi Q) = e_n(P, Q)^{-1}$$

for all $P, Q \in E_1[n]$. The elliptic curves directly n-congruent to a given elliptic curve E are parameterised by the modular curve $Y_E(n) = X_E(n) \setminus \{\text{cusps}\}$.

For $n \leqslant 5$ we have $X_E(n) \cong \mathbb{P}^1$ and the corresponding families of elliptic curves were computed by Rubin and Silverberg [28, 30, 31]. It was shown independently by Papadopoulos [25] and Rubin and Silverberg [29] that $X_E(6)$ is the elliptic curve $y^2 = x^3 + \Delta_E$, where Δ_E is the discriminant of E. However for $n \geqslant 7$ the genus of $X_E(n)$ is greater than 1. This prompted Mazur [23] to ask whether there are any pairs of non-isogenous elliptic curves over $\mathbb{Q}$ that are directly n-congruent for any $n \geqslant 7$. This was answered by Kraus and Oesterlé [22] who gave the example of the directly 7-congruent elliptic curves $152a1$ and $7448e1$. The labels here are those in Cremona's tables [4]. Nowadays it is easy to find further examples by searching in Cremona's tables, for example

$$\begin{aligned} n &= 11 \quad 190b1 \text{ and } 2470a1,\\ n &= 13 \quad 52a2 \text{ and } 988b1,\\ n &= 17 \quad 3675b1 \text{ and } 47775b1. \end{aligned}$$

In each case the n-congruence is proved by computing sufficiently many traces of Frobenius. See for example [22, Proposition 4].

Motivated by Mazur's question, Kani and Schanz [18] studied the geometry of the surfaces that parametrise pairs of n-congruent elliptic curves. This prompted them to conjecture that for any $n \leqslant 12$ 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 pairs of j-invariants, since otherwise from any single example we could construct infinitely many examples by taking quadratic twists. The conjecture was proved in the case $n = 7$ by Halberstadt and Kraus [15],

Received 15 June 2011; revised 8 February 2014.

2010 Mathematics Subject Classification 11G05, 11F80 (primary).

who subsequently [16] 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 $\mathbb{Q}$. In this paper we find a formula for $X_E(11)$ and use it to construct a non-trivial pair of 11-congruent elliptic curves over $\mathbb{Q}(T)$. This proves the conjecture in the case $n = 11$. In contrast the proof by Kani and Rizzo [17] does not construct any explicit examples.

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 [26] 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 [14].
- It was observed by Cremona and Mazur [6] 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 parameterised by the modular curve $Y_E^-(n) = X_E^-(n) \setminus \{\text{cusps}\}$. The families of elliptic curves parameterised by $Y_E^-(3)$ and $Y_E^-(4)$ were computed in [11], and the analogous problem for $n = 5$ was solved in [12]. An equation for $X_E^-(7)$ was given in [26, § 7.2]. In this paper we find equations for $X_E^-(11)$.

In § 1.1 we recall the definitions of $X(n)$ and its twists. We then record the formulae for $X_E(n)$ and $X_E^-(n)$ for $n = 7, 11$ in § 1.2. In the case $n = 7$ these are the formulae given in [16, 26], but our method for finding them is new. In the case $n = 11$ the formulae themselves are new.

In § 2 we derive Klein's equations for $X(n)$ for $n \geqslant 5$ an odd integer. The original approach of Klein was via theta functions, but our treatment is purely algebraic. We also give explicit formulae for the action of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ on $X(n)$. Then in § 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 $n = 7, 11$.

In § 4 we work out formulae for the families of elliptic curves parameterised by $Y_E(n)$ and $Y_E^-(n)$ for $n = 7, 11$. Computing the j-invariant maps $j : X_E(n) \to \mathbb{P}^1$ and $j : X_E^-(n) \to \mathbb{P}^1$ is reasonably straightforward. Finding the right quadratic twists takes considerably more work, although in specific numerical examples one can always fall back on the method in [15, 22]. In the case of $Y_E(7)$ a formula is given in [16], but 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 parameterised by $Y_E^-(7)$, $Y_E(11)$ and $Y_E^-(11)$.

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 co-ordinates. We have written programs in Magma [3] to do this in the case $K = \mathbb{Q}$, using ideas of minimisation and reduction similar to those in [5]. We will report on this in future work. In fact we have written a program in Magma that given an elliptic curve $E/\mathbb{Q}$ and $n \in \{7, 11\}$ 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. In § 5 we give some examples over $\mathbb{Q}$ to illustrate how this works, and also some examples over $\mathbb{Q}(T)$, which by specialisation of T give infinite families of examples over $\mathbb{Q}$. The examples over $\mathbb{Q}$ may be checked, independent of the methods we use to find them, by checking that the traces of Frobenius are congruent mod n for sufficiently many primes.

All computer calculations in support of this work were performed using Magma [3]. A Magma file checking all our formulae, together with a table of 11-congruent elliptic curves over $\mathbb{Q}$, is available as supplementary material with the online version of this paper [13]. We have used

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

the same methods to study families of 9-congruent elliptic curves, and will report on this in future work. Our restriction to odd n is explained by our use of Klein's equations (see § 2.1).

1.1. *Some modular curves*

We work over a field K of characteristic 0 and write $\overline{K}$ for the algebraic closure. Let $n \geqslant 3$ 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 (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 write $X(n)$ and $Y(n)$ for X_M and Y_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/K, let $X_E(n)$ be X_M in the case M is $E[n]$ equipped with the Weil pairing. More generally let $X_E^{(r)}(n)$ be X_M in the case M is $E[n]$ equipped with the rth power of the Weil pairing for some $r \in (\mathbb{Z}/n\mathbb{Z})^\times$. Since multiplication by $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ is an automorphism of $E[n]$ that raises the Weil pairing to the power m^2, the curve $X_E^{(r)}(n)$ only depends on the class of r mod squares. Since we are interested in the cases $n = 7, 11$ it will suffice to take $r = \pm 1$. We write $X_E^-(n)$ for $X_E^{(-1)}(n)$.

Let $\zeta_n \in \overline{K}$ be a primitive nth root of unity. Over $K(\zeta_n)$ we may identify the Galois modules $\mu_n \times \mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^2$, and hence the group of symplectic automorphisms of $\mu_n \times \mathbb{Z}/n\mathbb{Z}$ with $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. 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 $n \geqslant 3$ 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*

A formula for $X_E(7)$ was obtained by Halberstadt and Kraus [16]. 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 [26, § 7.2] then gave a formula for $X_E^-(7)$.

THEOREM 1.1 (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*

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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

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 a new proof of Theorem 1.1 and then extend to the case $n = 11$. Although we believe our formulae in the case $n = 11$ are correct for all elliptic curves E, our proof does not naturally extend to the cases $j(E) = 0, 1728$. We therefore assume for simplicity that $j(E) \neq 0, 1728$. It was observed by Klein [20] (see also [2, Example 22.3]) 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 1.2. *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*

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

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

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

2. *Equations for* $X(n)$

We derive equations of Klein [19–21] for the modular curves $X(n)$. Our treatment follows the survey in [8, Chapter 4], but see also [2, 34].

2.1. *Klein's equations*

Suppose to begin with that $\zeta_n \in K$. Then the modular curve $Y(n)$ parametrises the triples (E, P, Q) where E is an elliptic curve and P, Q is 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 $\mathbb{P}^{n-1}$. In fact we have the following lemma, as proved in [9, § 2.1].

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*

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta_n & 0 & \cdots & 0 \\ 0 & 0 & \zeta_n^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \zeta_n^{n-1} \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

(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_1, M_2 and*

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

It is well known that if $n \geqslant 4$ then the image of $E \subset \mathbb{P}^{n-1}$ is defined by quadrics. In fact the homogeneous ideal is generated by a vector space of quadrics of dimension $n(n-3)/2$. See [**10**, § 5.1] for a short proof, or [**24**] for a more general result.

We restrict to $n \geqslant 5$ an odd integer. 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, P, Q) to the image of 0_E defines an embedding $Y(n) \subset \mathbb{P}^{n-1}$. We check injectivity as follows. If we know the co-ordinates of $0_E \in \mathbb{P}^{n-1}$ then M_1 and M_2 allow us to write down n^2 points on E. By Bezout's theorem any quadric not containing E meets E in at most $2n$ points. Therefore E is defined by the quadrics containing these n^2 points, and $P, Q \in E[n]$ are the translates of 0_E under M_1 and M_2.

We now drop our assumption that $\zeta_n \in K$. The subgroup of $\mathrm{PGL}_n(\overline{K})$ generated by M_1 and M_2 is isomorphic to $\mu_n \times \mathbb{Z}/n\mathbb{Z}$ as a Galois module. In view of the definition of $X(n)$ in § 1.1, it follows that the embedding $Y(n) \subset \mathbb{P}^{n-1}$ described in the last paragraph is defined over K, and not just over $K(\zeta_n)$.

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

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

The divisor on the right is a hyperplane section and is invariant under translation by P. It is also the only such divisor with 0_E in its support. Therefore 0_E belongs to exactly one of the hyperplanes fixed by M_1. But 0_E is fixed by $[-1]$, so we have either

$$\begin{aligned} 0_E &= (0 : a_1 : a_2 : \ldots : a_2 : a_1) \qquad (+) \\ \text{or} \quad 0_E &= (0 : a_1 : a_2 : \ldots : -a_2 : -a_1) \qquad (-) \end{aligned}$$

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_1 allows us to write these as direct sums $V = \oplus V_i$ and $W = \oplus W_i$ with

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

The V_i and W_i are the subspaces on which M_1 acts with eigenvalue ζ_n^{2i}. The action of M_2 shows that $V_i \cong V_{i+1}$ and $W_i \cong W_{i+1}$ for all i. Therefore $\dim V_i = (n-3)/2$ and $\dim W_i = (n+1)/2$. The requirement that the quadrics in V_0 vanish at $0_E = (a_0 : a_1 : \ldots : a_{n-1})$, and its translates under M_2, imposes some linear conditions on the coefficients of these quadrics. Since $V_0 \subset W_0$ has codimension 2 it follows that $\operatorname{rank}(a_{i-j}a_{i+j})_{i,j=0}^{n-1} \leqslant 2$.

If 0_E is of the form $(+)$ then this matrix is symmetric, and the vanishing of the top left 3×3 minor contradicts that a_1, a_2, a_3 are non-zero. Therefore 0_E must be of the form $(-)$. This motivates the following definition.

Definition 2.2. For $n \geqslant 5$ 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

$$\operatorname{rank}(a_{i-j}a_{i+j})_{i,j=0}^{n-1} \leqslant 2. \tag{2.1}$$

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

We note that (2.1) is equivalent to the vanishing of the 4×4 Pfaffians of this skew-symmetric matrix. Using minors instead of Pfaffians also works, but gives equations of larger degree. The above construction shows that $Y(n)\subset Z(n)$. It is natural to ask whether $X(n)=Z(n)$. Vélu [34] proved this in the case $n=p$ is a prime. However if n is composite then $Z(n)$ has extra components.

When $n=7$ we put $0_E=(0:a:b:-c:c:-b:-a)$ so that $Z(7)\subset\mathbb{P}^2$ with co-ordinates $(a:b:c)$. Then $Z(7)$ is defined by

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

Computing the Pfaffian of this matrix (that is, the square root of its determinant) shows that $X(7)=Z(7)$ is the Klein quartic $\{a^3b+b^3c+c^3a=0\}\subset\mathbb{P}^2$.

When $n=11$ we put $0_E=(0:a:-c:b:e:d:-d:-e:-b:c:-a)$ so that $Z(11)\subset\mathbb{P}^4$ with co-ordinates $(a:b:c:d:e)$. Computing 4×4 Pfaffians shows that $X(11)=Z(11)$ is the singular locus of the Hessian of the cubic threefold

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

In other words, $X(11)$ is defined by the vanishing of the partial derivatives of the determinant of the matrix

$$\begin{pmatrix}b & a & 0 & 0 & e\\ a & c & b & 0 & 0\\ 0 & b & d & c & 0\\ 0 & 0 & c & e & d\\ e & 0 & 0 & d & a\end{pmatrix}. \tag{2.2}$$

We refer to [2] for further details. In fact, as we checked using Magma, the homogeneous ideal of $X(11)$ is generated by the 4×4 minors of (2.2).

2.2. *The action of* $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$

We suppose $\zeta_n\in K$ so that $Y(n)$ parametrises the triples (E,P,Q) where E is an elliptic curve and P,Q is a basis for $E[n]$ with $e_n(P,Q)=\zeta_n$. The natural action of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ on $Y(n)$ is given by

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}:(E,P,Q)\mapsto(E,dP-cQ,-bP+aQ). \tag{2.3}$$

This extends to an action on $X(n)$, and so defines a group homomorphism

$$\overline{\rho}:\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})\rightarrow\mathrm{Aut}(X(n)). \tag{2.4}$$

We now take $n\geqslant 5$ an odd integer. In § 2.1 we defined an embedding $X(n)\subset\mathbb{P}^{m-1}$ where $m=(n-1)/2$. In this setting (2.4) becomes a projective representation $\overline{\rho}:\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})\rightarrow\mathrm{PGL}_m(\overline{K})$. We show that it lifts to a representation. See [2, Appendix I] for a discussion of how this relates to work of Weil. We write $\propto$ for equality in $\mathrm{PGL}_n(\overline{K})$.

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

Proof. If we embed $X(n)\subset\mathbb{P}^{n-1}$ as described in § 2.1 then the action (2.3) extends to a projective representation $\overline{\pi}:\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})\rightarrow\mathrm{PGL}_n(\overline{K})$ where the image of $\gamma=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ is uniquely determined by the properties that

$$\overline{\pi}(\gamma)^{-1}M_1^uM_2^v\overline{\pi}(\gamma)\propto M_1^{du-bv}M_2^{-cu+av} \tag{2.5}$$

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

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 prove the stronger result 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 non-trivial one-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 (2.5) we compute

$$\overline{\pi}(S) \propto (\zeta_n^{ij})_{i,j=0}^{n-1}, \quad \overline{\pi}(T) \propto \mathrm{Diag}(\zeta_n^{i^2/2})_{i=0}^{n-1} \tag{2.6}$$

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

If $M \in \mathrm{GL}_n(\overline{K})$ acts on each of the subspaces $W_\pm$ then we write $M_\pm$ for the endomorphisms obtained by restricting to $W_\pm$. Since

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

it is clear that if $M = \mathrm{Diag}(\zeta_n^{i^2/2})_{i=0}^{n-1}$ then the determinants of M_+ and M_- are cube roots of unity. So by (2.6) there is a lift $\pi(T)$ of $\overline{\pi}(T)$, and one-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

$$\pi(S)\pi(T)^{-1}\pi(S) = \pi(T)\pi(S)\pi(T). \tag{2.7}$$

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 (2.7) shows that $\pi(S) = g_n^{-1}(\zeta_n^{ij})_{i,j=0}^{n-1}$ where the Gauss sum $g_n = \sum_{i=0}^{n-1} \zeta_n^{-i^2/2}$ 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

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

In particular $\rho(-I_2) = (-1)^{(n+1)/2} I_m$.

(iii) If n is not divisible by 3 then $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ has no one-dimensional characters, and so the lift we have constructed is unique. If n is divisible by 3 then m is not divisible by 3 and we can make ρ unique by demanding that $\det \rho(T) = 1$, equivalently that 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 § 2.1. We first make some general remarks about twisting and then split into the cases $n = 7, 11$.

3.1. *Preliminaries on twisting*

Let $n \geqslant 3$ be an integer. We recall that $Y(n)$ parametrises the pairs (E, ϕ) where E is an elliptic curve and $\phi : E[n] \cong \mu_n \times \mathbb{Z}/n\mathbb{Z}$ is a symplectic isomorphism. We temporarily write Γ

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

for the group of symplectic automorphisms of $\mu_n \times \mathbb{Z}/n\mathbb{Z}$. Then Γ acts on $Y(n)$ by $\gamma : (E, \phi) \mapsto (E, \gamma\,\phi)$. This action extends to $X(n)$, and so defines a group homomorphism

$$\overline{\rho} : \Gamma \to \mathrm{Aut}(X(n)). \tag{3.1}$$

If X_1 and X_2 are varieties defined over K, and $\alpha : X_1 \to X_2$ is a morphism defined over $\overline{K}$, then for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we write $\sigma(\alpha)$ for the morphism $X_1 \to X_2$ given on $\overline{K}$-points by $P \mapsto \sigma(\alpha(\sigma^{-1}P))$.

Lemma 3.1. *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 defined over $\overline{K}$. Then there is an isomorphism $\alpha : X_E(n) \to X(n)$, respectively $\alpha : X_E^-(n) \to X(n)$, defined 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 of $Y_E(n)$, 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. For ϕ as in the statement of the lemma, the composite $\phi\,\psi : F[n] \cong \mu_n \times \mathbb{Z}/n\mathbb{Z}$ is a symplectic isomorphism. Let $\alpha : Y_E^{\pm}(n) \to Y(n)$ be the isomorphism defined by $(F, \psi) \mapsto (F, \phi\,\psi)$. Then $\sigma(\alpha)$ maps $(F, \psi) \mapsto (F, \sigma(\phi)\,\psi)$. Therefore $\sigma(\alpha)\alpha^{-1}$ maps $(F, \psi') \mapsto (F, \sigma(\phi)\phi^{-1}\psi')$. In our notation this automorphism of $Y(n)$ is denoted $\overline{\rho}(\sigma(\phi)\phi^{-1})$. □

Fixing a primitive nth root of unity $\zeta_n \in \overline{K}$, we identify $\mu_n \times \mathbb{Z}/n\mathbb{Z}$ with $(\mathbb{Z}/n\mathbb{Z})^2$ via $(\zeta_n^a, b) \mapsto (a, b)$. Then $\Gamma = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, and the maps $\overline{\rho}$ defined in (2.4) and (3.1) are the same. We now suppose, as happened in § 2 for $n \geqslant 5$ an odd integer, that $X(n)$ 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)

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

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

$$\overline{\rho}(\iota\gamma\iota) \propto \overline{\rho}(\gamma)^{-T} \tag{3.2}$$

for all $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. Equivalently, $\overline{\rho}(S)$ and $\overline{\rho}(T)$ are symmetric matrices, where S and T are the generators for $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ defined in § 2.2. Our strategy for computing $X_E(n)$ and $X_E^-(n)$ as twists of $X(n)$ is explained by the following lemma.

Lemma 3.2. *Let E/K be an elliptic curve and $\phi : E[n] \cong \mu_n \times \mathbb{Z}/n\mathbb{Z}$ a symplectic isomorphism defined 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 $X_E^-(n) \cong X(n)$; $\mathbf{x} \mapsto h_2\mathbf{x}$, where $\mathbf{x}$ is a point in projective space written as a column vector.

Proof. Let $X' = \{\mathbf{x} \in \mathbb{P}^{n-1} \mid h_1\mathbf{x} \in X(n)\}$. Since $\sigma(h_1)h_1^{-1}$ is an automorphism of $X(n)$, we see that X' is defined over K. Then by Lemma 3.1 the curves $X_E(n)$ and X' are twists of $X(n)$ by the same cocycle. They are therefore isomorphic over K. The proof is the same for $X_E^-(n)$, except that we apply Lemma 3.1 to the pair $(E, \iota\phi)$, and observe by (3.2) that

$$\overline{\rho}(\sigma(\iota\phi)\,(\iota\phi)^{-1}) = \overline{\rho}(\iota\sigma(\phi)\phi^{-1}\iota) \propto \overline{\rho}(\sigma(\phi)\phi^{-1})^{-T}.$$

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

For the first equality we use that ι corresponds to an automorphism of $\mu_n \times \mathbb{Z}/n\mathbb{Z}$ which is defined over K. □

Remark 3.3. If, as happened in § 2 for $n \geqslant 5$ an odd integer, 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 a matrix h_1 satisfying the conditions in Lemma 3.2 follows 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 $h_2 = h_1^{-T}$. In the next two sections we use invariant theory for $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ to compute suitable matrices h_1 and h_2.

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

We saw in § 2.1 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 $g_7 = 1 + 2(\zeta_7^3 + \zeta_7^5 + \zeta_7^6) = \sqrt{-7}$.

Definition 3.4. 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 $g \in G$.

Following Klein (see, for example, [7, 16, 19]) we put

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

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

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.

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

Lemma 3.5. *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

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

and $j_0 - 1728 = c_6^2/H^7$, we see that j_0 is ramified above 0, 1728 and ∞ with ramification indices at least 3, 2 and 7. It follows that $j = j_0$ as required. □

Definition 3.6. 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 $\mathbf{v} \circ g = g^{-T}\mathbf{v}$, 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 $\nabla I = (\partial I/\partial a, \partial I/\partial b, \partial I/\partial c)^T$ is a contravariant column of degree $m - 1$.

Lemma 3.7. *Let E/K be an elliptic curve and $\phi : E[7] \cong \mu_7 \times \mathbb{Z}/7\mathbb{Z}$ a symplectic isomorphism defined 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*

$$c_4(a, b, c) = c_4(E) \quad \text{and} \quad c_6(a, b, c) = c_6(E) \tag{3.3}$$

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

$$\sigma((a, b, c)^T) = \lambda_\sigma \rho(\xi_\sigma)(a, b, c)^T \tag{3.4}$$

for some $\lambda_\sigma \in \overline{K}^\times$. Now $\rho(\xi_\sigma) \in G$, whereas c_4 and c_6 are homogeneous polynomials of degrees 14 and 21 invariant under the action of G. Therefore

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

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We are given that $c_4(E), c_6(E) \in K$. So by (3.3), and our assumption $j(E) \neq 0, 1728$, we have $\lambda_\sigma^{14} = \lambda_\sigma^{21} = 1$. Hence λ_σ is a 7th root of unity. Now suppose the columns of h are obtained by specialising polynomials whose degrees are all congruent to r mod 7. Then by (3.4) and Definition 3.6 we have

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

respectively

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

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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

We use Lemmas 3.2 and 3.7 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 straightforward to solve for the covariant and contravariant columns of any given degree by linear algebra. As above we put $\mathbf{x} = (a, b, c)^T$. Let $\mathbf{e}$ and $\mathbf{f}$ be the covariant columns of degrees 9 and 11 given by

$$\begin{aligned} \mathbf{e} &= \frac{I_{22}(\nabla F \times \nabla H) - c_4(\nabla F \times \nabla c_4) + 12H^2(\nabla H \times \nabla c_4)}{14c_6}, \\ \mathbf{f} &= \frac{I_{24}(\nabla F \times \nabla H) - (16F^4 - 104FH^2)(\nabla F \times \nabla c_4) + c_4(\nabla H \times \nabla c_4)}{14c_6} \end{aligned}$$

where

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

We describe the covariant and contravariant columns as modules over the ring $K[F, H, c_4]$ of invariants of even degree.

LEMMA 3.8. (i) *The covariant columns of odd, 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, 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 $[\nabla F, \nabla H, \nabla c_4] = 14c_6$. Since c_6 is not identically zero it follows that $\mathbf{x}, \mathbf{e}, \mathbf{f}$ are linearly independent over $K(a, b, c)$, and likewise for $\nabla F, \nabla H, \nabla c_4$.

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 3.9. *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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

from these columns are

$$\begin{aligned} \det(\mathbf{x}, (\nabla F \times \nabla H), H\mathbf{e}) &= 72H^4 - 4c_4FH, \\ \det(\nabla F, (\mathbf{x} \times \mathbf{e}), H^2\nabla H) &= 72H^5 - 4c_4FH^2. \end{aligned} \tag{3.5}$$

Therefore the matrices h_1 and h_2 obtained by evaluating at a point of $Y(7)$ are non-singular.

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

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

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 3.5 we may scale (a,b,c) to satisfy (3.3). With this choice of scaling we also have $H(a,b,c)^7 = \Delta$. By Lemma 3.7 the matrix h_1, respectively h_2, formed by evaluating the covariant, respectively contravariant, columns at (a,b,c), satisfies the conditions of Lemma 3.2. Therefore 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 3.10. It is not immediately clear how the equations for $X_E(7)$ and $X_E^-(7)$ found by our method (see Theorem 3.9) are related to those already in the literature (see Theorem 1.1). In fact writing $a = -27c_4$ and $b = -54c_6$ we have

$$\mathcal{F}(x,y,z) = \tfrac{1}{4}\mathbf{F}(6c_4z - \tfrac{1}{3}y, x, -18z), \qquad \mathcal{G}(x,y,z) = \mathbf{G}(9c_4y + z, 3x, 108y).$$

3.3. *Formulae in the case $n = 11$*

We saw in § 2.1 that $X(11)$ is the singular locus of the Hessian of the cubic threefold $\{F = 0\} \subset \mathbb{P}^4$ where

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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

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 $g_{11} = 1 + 2(\zeta_{11} + \zeta_{11}^3 + \zeta_{11}^9 + \zeta_{11}^5 + \zeta_{11}^4) = \sqrt{-11}$.

We define the invariants, covariant columns and contravariant columns exactly as in § 3.2. Let $\sum$ denote a sum over all cyclic permutations, so that for example $F = \sum a^2 b$. Other examples of invariants of small degree include

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

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. Although we will not need a complete set of generators for the ring of invariants, we remark that such a set is given in [1], and may also be computed using Magma. Let $\mathcal{I}$ be the homogeneous ideal of $X(11)$, that is, 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 3.11. *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 [2, Corollary 23.28] that $X(11) \subset \mathbb{P}^4$ has degree 20. Since

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

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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

Lemma 3.12. *Let E/K be an elliptic curve and $\phi : E[11] \cong \mu_{11} \times \mathbb{Z}/11\mathbb{Z}$ a symplectic isomorphism defined 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*

$$c_4(a, b, c, d, e) = c_4(E) \tag{3.6}$$

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 3.7. Recall that c_4 is a homogeneous polynomial of degree 11 and so (3.6) determines the scaling of (a, b, c, d, e) up to an 11th root of unity. □

We use Lemmas 3.2 and 3.12 to compute equations for $X_E(11)$ and $X_E^-(11)$. First we compute 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 3.13. *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*

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

the Hessian of

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

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

$$\begin{aligned}\det(\mathbf{x}_1, \mathbf{x}_4, \mathbf{x}_5, \mathbf{x}_9, \mathbf{x}_{14}) &= c_4^3 - 1728F^{11} \pmod{\mathcal{I}}, \\ \det(\nabla F, \nabla I_7, \nabla I_8, \nabla I_9, \nabla c_4) &= 55(c_4^3 - 1728F^{11}) \pmod{\mathcal{I}}.\end{aligned} \tag{3.7}$$

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 3.11 we may scale (a, b, c, d, e) to satisfy (3.6) and $F(a, b, c, d, e)^{11} = \Delta$. Moreover the determinants (3.7) are non-zero by our assumption $j(E) \neq 1728$. By Lemmas 3.2 and 3.12 we obtain cubic forms describing $X_E(11)$ and $X_E^-(11)$ by putting

$$\begin{aligned}\mathbf{F}(v, w, x, y, z) &= \frac{1}{F^4}\widetilde{F}(Fv, w, F^7x, F^2y, F^4z), \\ \mathbf{G}(v, w, x, y, z) &= \frac{1}{F^8}\widetilde{G}(F^2v, F^8w, F^4x, y, F^3z)\end{aligned} \tag{3.8}$$

and replacing F^{11} by Δ. □

REMARK 3.14. We simplify the cubic forms $\mathbf{F}$ and $\mathbf{G}$ in Theorem 3.13 by putting

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

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

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

This gives the cubic forms $\mathcal{F}$ and $\mathcal{G}$ in Theorem 1.2.

4. *Modular interpretation*

In § 3 we computed equations for $X_E(n)$ and $X_E^-(n)$ for $n=7,11$. In this section we compute equations for the families of curves they parametrise.

4.1. *Computing the j-invariant*

We give formulae for the j-maps $X_E(n)\to\mathbb{P}^1$ and $X_E^-(n)\to\mathbb{P}^1$ by adapting the formulae in Lemmas 3.5 and 3.11.

First we define the *invariant* $\Psi(F)$ of a polynomial F of the form considered in Theorems 1.1 and 1.2. For F a polynomial in variables $x_1,\dots,x_m$ and $M=(M_{ij})$ an $m\times m$ matrix we write $F\circ M$ for $F(x_1',\dots,x_m')$ where $x_i'=\sum_j M_{ij}x_j$.

DEFINITION 4.1. We split into the cases $n=7,11$.

(i) The invariant Ψ of a twisted form $\mu(F\circ M)$ of $F=x^3y+y^3z+z^3x$ is

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

(ii) The invariant Ψ of a twisted form $\mu(F\circ M)$ of $F=v^2w+w^2x+x^2y+y^2z+z^2v$ is

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

LEMMA 4.2. *Let $\mathcal{F}$ be one of the twisted forms in Definition 4.1. Then:*

(i) *$\Psi(\mathcal{F})$ is well-defined, that is, 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 appeal to the fact, proved in [**2**, Lemma 20.40], that $\mathrm{Aut}(X(n))\cong \mathrm{PSL}_2(\mathbb{Z}/n\mathbb{Z})$. Therefore it suffices to consider $M=\rho(\gamma)$ for $\gamma\in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. We then use that $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ has no non-trivial one-dimensional characters.

(ii) This follows from (i) by Galois theory. □

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

Remark 4.3. (i) In the case $n = 7$ it is shown in [**26**, § 7.1] that $\Psi(\mathcal{F})$ is an integer coefficient polynomial in the coefficients of $\mathcal{F}$. We expect this is also true in the case $n = 11$, but we have not worked out the details.

(ii) By following the proofs in § 3, the twisted forms in Theorems 1.1 and 1.2 have invariants

$$\begin{array}{lcc} & X_E(n) & X_E^-(n) \\ n=7 & -4(4a^3+27b^2) & 16(4a^3+27b^2)^2 \\ n=11 & -4(4a^3+27b^2)^2 & 8(4a^3+27b^2). \end{array}$$

We now split into the cases $n = 7, 11$ and give formulae for the j-map.

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 § 3.2 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

$$\begin{aligned} H(\mathcal{F}) &= \mu^3(\det M)^2(H \circ M),\\ c_4(\mathcal{F}) &= \mu^8(\det M)^6(c_4 \circ M),\\ c_6(\mathcal{F}) &= \mu^{12}(\det M)^9(c_6 \circ M). \end{aligned} \tag{4.1}$$

As observed in [**26**, Lemma 7.2], 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 § 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

$$\begin{aligned} H(\mathcal{F}) &= \mu^5(\det M)^2(H \circ M),\\ c_4(\mathcal{F}) &= \mu^{17}(\det M)^8(c_4 \circ M). \end{aligned} \tag{4.2}$$

By Lemma 3.11 the j-map $X \to \mathbb{P}^1$ is given by

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

4.2. *Modular interpretation of $X(n)$*

In § 2.1 we gave equations for $X(n)$. In [**8**, Chapter 4] it is shown that (analogous to Definition 2.2) the elliptic curve $E \subset \mathbb{P}^{n-1}$ above $(0 : a_1 : a_2 : \ldots : -a_2 : -a_1) \in Y(n)$ is defined by

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

The following theorem gives an equation for this curve in Weierstrass form. Notice that the coefficients are homogeneous polynomials of degrees $4t$ and $6t$ for some integer t. An alternative proof in the case $n = 7$ is sketched in [**16**, § 3].

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

THEOREM 4.4. *We split into the cases $n = 7, 11$.*

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

$$y^2 = x^3 - 27(abc)^2c_4(a,b,c)x - 54(abc)^3c_6(a,b,c) \tag{4.3}$$

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

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

$$y^2 = x^3 - 27(abcde)c_4(a,b,c,d,e)x - 54(abcde)\widetilde{c}_6(a,b,c,d,e) \tag{4.4}$$

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

Proof. The modular curve $Y_1(n)$ parametrises pairs (E, P) where E is an elliptic curve and $P \in E$ is a point of order n. If $n = 7$ then we choose a co-ordinate λ on $X_1(7) \cong \mathbb{P}^1$. If $n = 11$ then $X_1(11)$ is the elliptic curve $\nu^2 + \nu = \lambda^3 - \lambda^2$. We write $\boldsymbol{\lambda}$ to indicate λ in the case $n = 7$, and the pair λ, ν in the case $n = 11$. By [32, Exercise 8.13] the elliptic curves $D_{\boldsymbol{\lambda}}$ parameterised by $Y_1(7)$ and $Y_1(11)$ have Weierstrass equations

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

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 [33] the n-isogenous elliptic curve $C_{\boldsymbol{\lambda}} = D_{\boldsymbol{\lambda}}/\langle P \rangle$ has Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 - 5tx - (a_1^2 + 4a_2)t - 7w \tag{4.5}$$

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 (4.5) have discriminant

$$\begin{aligned} n = 7 \qquad & \Delta(C_\lambda) = \lambda(\lambda-1)(\lambda^3 - 8\lambda^2 + 5\lambda + 1)^7, \\ n = 11 \quad & \Delta(C_{\lambda,\nu}) = \lambda(\lambda-1)(\lambda\nu + 2\lambda^2 - 2\lambda + 1)(\nu+1)^6 f(\lambda,\nu)^{11}, \end{aligned} \tag{4.6}$$

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

Let $\phi : C_{\boldsymbol{\lambda}} \to D_{\boldsymbol{\lambda}}$ and $\widehat{\phi} : D_{\boldsymbol{\lambda}} \to C_{\boldsymbol{\lambda}}$ be the dual isogenies of degree n with $\ker \widehat{\phi} = \langle P \rangle$. Then by properties of the Weil pairing $\ker \phi$ is isomorphic to μ_n as a Galois module. Let $Q \in C_{\boldsymbol{\lambda}}(\overline{K})$ with $\phi(Q) = P$. Then $\sigma \mapsto \sigma(Q) - Q$ is a cocycle taking values in μ_n. By Hilbert's Theorem 90 there exists $q \in K^\times/(K^\times)^n$ such that $\sigma(Q) - Q = \sigma(\sqrt[n]{q})/\sqrt[n]{q}$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Computing $q = q(\boldsymbol{\lambda})$ as described in [9, § 1.2] we find

$$q(\boldsymbol{\lambda}) = \begin{cases} \lambda^4(\lambda - 1) & \text{if } n = 7 \\ \lambda\nu^2(\lambda-1)(\lambda-\nu-1)^3 & \text{if } n = 11. \end{cases} \tag{4.7}$$

Now $X(n)$ 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 [9, § 2.2]. Applying the same method for $n = 11$ we obtain

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

We checked directly that these are birational maps, and that the cusps of $X(n)$, that is, $(1 : 0 : \ldots : 0)$ and its translates under the action of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, map to the cusps of $X_1(n)$, that is, the roots of (4.6).

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

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

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

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

where $\xi_7 = a/b^5c$ and $\xi_{11} = a^3b/c^6e^2$. Since we are free to cancel 4th powers and 6th powers from the coefficients of a shorter Weierstrass equation, the result follows. □

4.3. *An alternative projective embedding*

We take $p \geqslant 5$ a prime and let $G = \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ act on $X(p)$ in the usual way.

THEOREM 4.5 (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 [2, 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 4.5 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 [2]) and this is known for $p = 7, 11$. The equations for $X(p)$ introduced in § 2.1 are for the z-curve. However in §§ 4.4 and 4.5 we also need the A-curve.

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 [26] 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 $P_1+P_2+P_3$. One of these divisors, T_0 say, satisfies $X(7) \cap \{xyz = 0\} = 4T_0$. As observed in [26, §11] we have $2T_i \sim 2T_j$ for all $0 \leqslant i, j \leqslant 7$. It follows by Theorem 4.5 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

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

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

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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

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 $P_1 + \ldots + P_5$. One of these divisors, T_0 say, satisfies $X(11) \cap \{vwxyz = 0\} = 20T_0$. It may be shown that $5T_i \sim 5T_j$ for all $0 \leqslant i, j \leqslant 11$ and hence $5T_0 \sim 5\Lambda$ by Theorem 4.5. 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

$$(v : w : x : y : z) \mapsto (t_1 : \ldots : t_6) = (v^2wxz : vw^2xy : wx^2yz : vxy^2z : vwyz^2 : vwxyz).$$

It is shown in [2, Theorem 51.1], and we checked using Magma, that this is the singular locus of the quartic hypersurface

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

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

THEOREM 4.6. *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

$$Y^2 = X^3 - 27\frac{c_4(\mathcal{F})(x, y, z)}{d(x, y, z)^2}X - 54\frac{c_6(\mathcal{F})(x, y, z)}{d(x, y, z)^3} \tag{4.8}$$

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

Proof. 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 (4.8) 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 (4.3) and (4.8) 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 [28, Proposition 2.1]. □

In Theorem 4.8 below we determine rational functions d satisfying the hypothesis of Theorem 4.6 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 4.7. Recall that $X_E(7)$ has a trivial K-rational point corresponding to E itself. Following [28] 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, and also does not generalise to $X_E^-(7)$.

THEOREM 4.8. *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 parameterised by $Y_E(7)$ and $Y_E^-(7)$ are given by (4.8) with $(\mathcal{F}, d) = (\mathbf{F}, d_1)$ and $(\mathbf{G}, d_2)$ where $\mathbf{F}$ and $\mathbf{G}$ are the quartics in Theorem 3.9 and*

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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

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 3.9 we scale (a, b, c) so that $c_4(a, b, c) = c_4$ and $c_6(a, b, c) = c_6$. 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

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

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

$$r_i(x, y, z)xyz \equiv s_i(x, y, z)^2 \mod (x^3y + y^3z + z^3x) \tag{4.9}$$

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 3.9 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

$$\begin{aligned} d_1(x, y, z) &= \frac{1}{2abcH^4}r_1(x\mathbf{x} + y(\nabla F \times \nabla H) + zH\mathbf{e}), \\ d_2(x, y, z) &= \frac{2H^5}{abc}r_2(x\nabla F + y(\mathbf{x} \times \mathbf{e}) + zH^2\nabla H). \end{aligned} \tag{4.10}$$

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 4.6. So our formulae for the families of elliptic curves parameterised 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 [**16**, § 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 (4.3) for E with that in the statement of the theorem it follows that $\lambda^7 a_0b_0c_0 \in (K^\times)^2$. So $a^7, b^7, c^7 \in K$ and $(abc)^7 \in (K^\times)^2$. Using (3.5) and (4.1) 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 (4.10) 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. Therefore the families of curves in the statement of the theorem are K-isomorphic to

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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

and

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

To identify these with (4.3) we note that the cubic forms $(abc)^3s_1(x,y,z)$ and $(abc)^3H^5s_2(x,y,z)$ have coefficients in K (since the degree of each coefficient is a multiple of 7) and then use (4.9). □

Making the change of co-ordinates in Remark 3.10, we can replace d_1 and d_2 by cubic forms that satisfy the conditions of Theorem 4.6 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 1.1. 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 there are cubic forms d_{ij} for $1 \leqslant i,j \leqslant 4$ 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 parameterised by $Y_E(7)$ is now given by (4.8) with $(\mathcal{F}, d) = (\mathcal{F}, d_{ii})$ for any $1 \leqslant i \leqslant 4$.

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

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

Our formula for the elliptic curve corresponding to $P \in Y_E(7)$ fails when $d_{ii}(P) = 0$. However the zeros of d_{ii} correspond to the hyperplane section $\{t_i = 0\}$ on the A-curve. Therefore, for any given point P, we have $d_{ii}(P) \neq 0$ for some i. So unlike the treatment in [**16**, 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 $1 \leqslant i,j \leqslant 4$ such that the matrix (d'_{ij}) is symmetric and each 2×2 minor vanishes mod $\mathcal{G}$. Explicitly,

$$\begin{aligned}
d'_{11} &= -7ax^2y + 6x^2z + 3a^2y^3 - 8ay^2z + 3yz^2,\\
d'_{12} &= 2ax^3 + 12bx^2y - 2axyz - 3aby^3 + 6by^2z,\\
d'_{13} &= 2a^2xy^2 - 10axyz + 6xz^2 + 5aby^3 - 12by^2z,\\
d'_{14} &= 2a^2x^2y - 3ax^2z + 5abxy^2 - 12bxyz - 3a^2y^2z + 8ayz^2 - 3z^3.
\end{aligned}$$

The remaining d'_{ij} are computed using $d'_{11}d'_{ij} \equiv d'_{1i}d'_{1j} \pmod{\mathcal{G}}$. The family of elliptic curves parameterised by $Y_E^-(7)$ is now given by (4.8) with $(\mathcal{F}, d) = (\mathcal{G}, \Delta d'_{ii})$ for any $1 \leqslant i \leqslant 4$. Exactly as before, these formulae cover all cases.

4.5. *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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

complications. One is that there is no invariant 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 our twist of $X(n)$ is defined by quartics.

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

$$r_i(v,w,x,y,z)(vwxyz)^3 \equiv s_i(v,w,x,y,z)^4 \pmod{\mathcal{I}, \mathcal{I}'} \tag{4.11}$$

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 (4.11). 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 4.9. 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 [**13**] for further details. The computation of d_1 and d_2 took several hours of computer time, whereas all other calculations up to this point ran in a few seconds.

THEOREM 4.10. *Let E/K be an elliptic curve with Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$ and let $\Delta = (c_4^3 - c_6^2)/1728$. Assume $j(E) \neq 0, 1728$ and let $X = X_E(11)$, respectively $X_E^-(11)$, be as given in Theorem 3.13. If $(v:w:x:y:z) \in X(K) \setminus \{d_i = 0\}$, not a cusp, then the corresponding elliptic curve E'/K satisfies*

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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

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 [16, § 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 (4.4) we deduce that $(abcde)^{11} \in (K^\times)^4$. The polynomials $\mathbf{F}$ and $\mathbf{G}$ were computed in § 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 (3.7), (3.8) and (4.2) 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

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

In view of Theorem 4.4 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 (4.11). □

We already gave a formula for the j-invariant in § 4.1. So (assuming $j(E') \neq 0$) Theorem 4.10 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 seven 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.

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

5. *Examples*

We use the formulae in Theorems 1.1 and 1.2 to give examples of non-trivial n-congruences for $n = 7, 11$ 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 mentioned in the introduction. 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 [4]. For elliptic curves beyond the current range of Cremona's tables we simply write the conductor followed by a $*$.

Remark 5.1. If elliptic curves E and E' are related by an isogeny of degree d coprime to n, then they are clearly n-congruent. Since dual isogenies are adjoints with respect to the Weil pairing, the curves are directly n-congruent if d is a square in $(\mathbb{Z}/n\mathbb{Z})^\times$ and reverse n-congruent if $-d$ is a square in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Remark 5.2. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. As the referee points out, by Ribet's level raising theorem [**27**], there are (under suitable hypotheses) infinitely many primes p such that there is a newform of weight 2 for $\Gamma_0(Np)$ with the same mod 7 (or mod 11) representation as E. However only finitely many of these will have rational Hecke eigenvalues and so correspond to an elliptic curve. It is nonetheless interesting to note that many of the examples found by our methods (and likewise those in [**15**, **16**]) can be explained by Ribet's theorem.

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

Example 5.3. Let E be the elliptic curve $162c1$. Let $\mathcal{F}$ and $\mathcal{G}$ be the equations for $X_E(7)$ and $X_E^-(7)$ in Theorem 1.1 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

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

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	$293706x2$	$y^2 + xy = x^3 - x^2 - 62930562x - 192134303740,$
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	$624186*$	$y^2 + xy = x^3 - x^2 - 11751402282x + 360746315347508.$

Since the elliptic curves $162c1$ and $162c2$ are 3-isogenous, it was already clear from Remark 5.1 that they are reverse 7-congruent.

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

It is shown in [16, Proposition 6.3] 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 5.4. 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 $X_E^-(7)$, with equation as given in Theorem 1.1, has 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.

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

EXAMPLE 5.5. Let E be the elliptic curve 1782b1. Let $\mathcal{F}$ be the cubic form describing $X_E(11) \subset \mathbb{P}^4$ in Theorem 1.2 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

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

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	$447282*$	$y^2 + xy = x^3 - x^2 - 17552171922x - 227953575178678.$

Since the elliptic curves $1782b1$ and $1782b2$ are 3-isogenous, it was already clear from Remark 5.1 that they are directly 11-congruent.

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

EXAMPLE 5.6. Let E be the elliptic curve 4466c1. Let $\mathcal{G}$ be the cubic form describing $X_E^-(11) \subset \mathbb{P}^4$ in Theorem 1.2 with $a = 85$ and $b = -83162$. The invariant is $\Psi(\mathcal{G}) = 2^{21} \cdot 7 \cdot 11^2 \cdot 29^2$. 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

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

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$*$	$y^2 + xy + y = x^3 - x^2 + 117885809240x + 16240157710556505.$

Since the elliptic curves 4466c1 and 4466c2 are 2-isogenous, it was already clear from Remark 5.1 that they are reverse 11-congruent.

A table of pairs of 11-congruent elliptic curves over $\mathbb{Q}$ is available from the website [**13**]. These were found by searching for rational points on $X_E(11)$ and $X_E^-(11)$ for all elliptic curves $E/\mathbb{Q}$ in Cremona's tables. As happened in Examples 5.5 and 5.6, the elliptic curves 11-congruent to E that we find often have conductor beyond the current range of Cremona's tables.

The following example shows that there are infinitely many pairs of directly 11-congruent non-isogenous elliptic curves over $\mathbb{Q}$.

EXAMPLE 5.7. 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 1.2, 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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

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

$$2^{12}3^6(T-5)(T-3)^2(T+1)^5(T^2+7)/(T^3-T^2+4T+24)^3,$$

and

$$-2^{12}3^6(T-5)^4(T-3)^2(T+1)^3(T^2+7)(T^3-T^2+4T+24)^3(T^3-T^2+15T-31)^{11}.$$

We did not find any pairs of reverse 11-congruent non-isogenous elliptic curves over $\mathbb{Q}(T)$. We note that according to [**18**, Theorem 4] the modular diagonal surface in this case is of general type.

References

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

2. A. Adler and S. Ramanan, *Moduli of abelian varieties*, Lecture Notes in Mathematics 1644 (Springer, 1996).

3. W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system I: The user language', *J. Symbolic Comput.* 24 (1997) 235–265; see also the Magma home page at http://magma.maths.usyd.edu.au/magma/.

4. J. E. Cremona, *Algorithms for modular elliptic curves* (Cambridge University Press, Cambridge, 1997); see also http://www.warwick.ac.uk/~masgaj/ftp/data/.

5. 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.

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

7. N. D. Elkies, 'The Klein quartic in number theory', *The eightfold way: The beauty of Klein's quartic curve*, Mathematical Sciences Research Institute Publications 35 (ed. S. Levy; Cambridge University Press, Cambridge, 1999) 51–101.

8. T. A. Fisher, 'On 5 and 7 descents for elliptic curves', PhD Thesis, University of Cambridge, 2000, http://www.dpmms.cam.ac.uk/~taf1000/thesis.html.

9. T. A. Fisher, 'Some examples of 5 and 7 descent for elliptic curves over **Q**', *J. Eur. Math. Soc.* 3 (2001) no. 2, 169–201.

10. T. A. Fisher, 'The invariants of a genus one curve', *Proc. Lond. Math. Soc.* (3) 97 (2008) 753–782.

11. T. A. Fisher, 'The Hessian of a genus one curve', *Proc. Lond. Math. Soc.* (3) 104 (2012) 613–648.

12. T. A. Fisher, 'Invariant theory for the elliptic normal quintic, I. Twists of $X(5)$', *Math. Ann.* 356 (2013) no. 2, 589–616.

13. T. A. Fisher, 'On families of 7- and 11-congruent elliptic curves', Electronic data accompanying this article, http://journals.cambridge.org/sup_S1461157014000059sup001.

14. G. Frey, 'On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2', *Elliptic curves, modular forms & Fermat's Last Theorem,* Hong Kong, 1993, Series on Number Theory I (eds J. Coates and S.-T. Yau; International Press, Cambridge, MA, 1995) 79–98.

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

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press

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

17. 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.

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

19. 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*, Mathematical Sciences Research Institute Publications 35 (ed. S. Levy; Cambridge University Press, Cambridge 1999).

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

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

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

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

24. D. Mumford, 'Varieties defined by quadratic equations', *Questions on algebraic varieties* (C.I.M.E., III Ciclo, Varenna, 1969) (Edizioni Cremonese, Rome, 1970) 29–100.

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

26. 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.

27. K. A. Ribet, 'Raising the levels of modular representations', *Séminaire de Théorie des Nombres,* Paris, 1987–1988, Progress in Mathematics 81 (ed. C. Goldstein; Birkhäuser, Boston, 1990) 259–271.

28. K. Rubin and A. Silverberg, 'Families of elliptic curves with constant mod p representations', *Elliptic curves, modular forms & Fermat's Last Theorem,* Hong Kong, 1993, Series in Number Theory I (eds J. Coates and S.-T. Yau; International Press, Cambridge, MA, 1995) 148–161.

29. K. Rubin and A. Silverberg, 'Mod 6 representations of elliptic curves', *Automorphic Forms, Automorphic representations, and arithmetic,* Fort Worth, TX, 1996, Proceedings of Symposia in Pure Mathematics, Part 1 66 (American Mathematical Society, Providence, RI, 1999) 213–220.

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

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

32. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Text in Mathematics 106 (Springer, New York, 1986).

33. J. Vélu, 'Isogénies entre courbes elliptiques', *C. R. Math. Acad. Sci. Paris* 273 (1971) 238–241.

34. J. Vélu, 'Courbes elliptique munies d'un sous-group $\mathbb{Z}/n\mathbb{Z} \times \mu_n$', *Mém. Soc. Math. Fr.* 57 (1978).

Tom Fisher
University of Cambridge
DPMMS
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB
United Kingdom

T.A.Fisher@dpmms.cam.ac.uk

https://doi.org/10.1112/S1461157014000059 Published online by Cambridge University Press