EXPLICIT MODULI SPACES FOR CONGRUENCES OF ELLIPTIC CURVES

TOM FISHER

Abstract. We determine explicit birational models over $\mathbb{Q}$ for the modular surfaces parametrising pairs of N-congruent elliptic curves in all cases where this surface is an elliptic surface. In each case we also determine the rank of the Mordell-Weil lattice and the geometric Picard number.

1. Introduction

Let $N \geq 2$ be an integer. A pair of elliptic curves are said to be *N-congruent*, if their N-torsion subgroups are isomorphic as Galois modules. Such an isomorphism raises the Weil pairing to the power ε for some $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$. In this situation we say that the N-congruence has *power* ε. Since multiplication-by-m on one of the elliptic curves (for m an integer coprime to N) changes ε to $m^2\varepsilon$, we are only ever interested in the class of $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$ mod squares.

Let $Z(N, \varepsilon)$ be the surface that parametrises pairs of N-congruent elliptic curves with power ε. This is a surface defined over $\mathbb{Q}$. We only consider $Z(N, \varepsilon)$ up to birational equivalence. Kani and Schanz [14, Theorem 4] classified the geometry of these surfaces, explicitly determining the pairs (N, ε) for which $Z(N, \varepsilon)$ is birational over $\mathbb{C}$ to either (i) a rational surface, (ii) an elliptic $K3$-surface, (iii) an elliptic surface with Kodaira dimension one (also known as a properly elliptic surface), or (iv) a surface of general type. In case (i) it is known that the surface is rational over $\mathbb{Q}$. We show in cases (ii) and (iii) that the surface is birational over $\mathbb{Q}$ to an elliptic surface, determining in each case a Weierstrass equation for the generic fibre as an elliptic curve over $\mathbb{Q}(T)$. One application of these explicit equations is that we are then able to use the methods of van Luijk and Kloosterman to compute the geometric Picard number of each surface.

The problem of computing $Z(N, \varepsilon)$ is closely related to that of computing the modular curves $X_E(N, \varepsilon)$ parametrising the elliptic curves N-congruent (with power ε) to a given elliptic curve E. Equations for $X_E(N, \varepsilon)$, and the family of curves it parametrises, have been determined as follows. The cases $N \leq 5$ were treated by Rubin and Silverberg [21], [23], [25] for $\varepsilon = 1$, and by Fisher [7], [8]

Date: 26th April 2018.

2010 *Mathematics Subject Classification.* 11G05, 11F80, 14J27.

Key words and phrases. elliptic curves, Galois representations, elliptic surfaces.

for $\varepsilon \neq 1$. The case $N = 7$ was treated by Halberstadt and Kraus [12] for $\varepsilon = 1$, and by Poonen, Schaefer and Stoll [20] for $\varepsilon \neq 1$. The case $N = 8$ was treated by Chen [6], and the cases $N = 9$ and $N = 11$ by Fisher [9], [10].

If N is not a prime power, then in principle we obtain equations for $X_E(N, \varepsilon)$ as a fibre product of modular curves of smaller level. Equations that are substantially better than this have been obtained in the case $(N, \varepsilon) = (6, 1)$ by Rubin and Silverberg [22], and independently Papadopoulos [19], and in the cases $(N, \varepsilon) = (12, 1)$ and $(12, 7)$ by Chen [5, Chapter 7]. Chen also gives equations for $X_E(N, \varepsilon)$ in the cases $(N, \varepsilon) = (6, 5)$ and $(10, 1)$.

The equations for $X_E(N, \varepsilon)$ do immediately give us equations for $Z(N, \varepsilon)$, but unfortunately this does not always make it easy to find the elliptic fibrations. The main purpose of this note is to record the transformations that work in each case.

According to [14, Theorem 4] the surface $Z(N, \varepsilon)$ is rational over $\mathbb{C}$ for all $N \leq 5$, and in the cases $N = 6, 7, 8$ with $\varepsilon = 1$. In each of these cases $Z(N, \varepsilon)$ is rational over $\mathbb{Q}$, as follows (see [5, Chapter 8]) from the results cited above.

In our terminology, it is part of the definition of an elliptic surface that it has a section. As we describe below, some of the cases in the next two theorems were already treated in [6], [10], [16].

Theorem 1.1. *The surfaces $Z(N, \varepsilon)$ that are birational over $\mathbb{C}$ to an elliptic $K3$-surface, are in fact birational over $\mathbb{Q}$ to an elliptic surface. The generic fibres are the elliptic curves over $\mathbb{Q}(T)$ with the following Weierstrass equations.*

$$
\begin{aligned}
Z(6,5): &\quad y^2 + 3T(T-2)xy + 2(T-1)(T+2)^2(T^3-2)y = x^3 - 6(T-1)(T^3-2)x^2,\\
Z(7,3): &\quad y^2 = x^3 + (4T^4 + 4T^3 - 51T^2 - 2T - 50)x^2 + (6T+25)(52T^2 - 4T + 25)x,\\
Z(8,3): &\quad y^2 = x^3 - (3T^2-7)x^2 - 4T^2(4T^4 - 15)x + 4T^2(53T^4 + 81T^2 + 162),\\
Z(8,5): &\quad y^2 = x^3 - 2(T^2+19)x^2 - (4T^2-49)(T^4 - 6T^2 + 25)x,\\
Z(9,1): &\quad y^2 + (6T^2 + 3T + 2)xy + T^2(T+1)(4T^3 + 9T + 9)y\\
&\qquad\qquad = x^3 - (16T^4 + 12T^3 + 9T^2 + 6T + 1)x^2,\\
Z(12,1): &\quad y^2 + 2(5T^2+9)xy + 96(T^2+3)(T^2+1)^2 y = x^3 + (T^2+3)(11T^2+1)x^2.
\end{aligned}
$$

Theorem 1.2. *The surfaces $Z(N, \varepsilon)$ that are birational over $\mathbb{C}$ to a properly elliptic surface, are in fact birational over $\mathbb{Q}$ to an elliptic surface. The generic fibres are the elliptic curves over $\mathbb{Q}(T)$ with the following Weierstrass equations.*

$$
\begin{aligned}
Z(8,7): &\quad y^2 = x^3 + 2(4T^6 - 15T^4 + 14T^2 - 1)x^2 + (T^2-1)^4(16T^4 - 24T^2 + 1)x,\\
Z(9,2): &\quad y^2 + 3(4T^3 + T^2 - 2)xy + (T-1)^3(T^3-1)(4T^3 - 3T - 7)y\\
&\qquad\qquad = x^3 - 3(T+1)(T^3-1)(9T^2 + 2T + 1)x^2,
\end{aligned}
$$

$$\begin{aligned}
Z(10,1):\ & y^2-(3T-2)(6T^2-5T-2)xy \\
&\quad -4T^2(T-1)^2(4T^2-2T-1)(27T^3-54T^2+16T+12)y \\
&\quad =x^3+T^2(T-1)(27T^3-54T^2+16T+12)x^2,\\
Z(10,3):\ & y^2+(T^3-8T^2-9T-8)xy+2T^2(T^3-T^2-3T-3)(7T^2+2T+3)y \\
&\quad =x^3+2(3T+2)(T^3-T^2-3T-3)x^2,\\
Z(11,1):\ & y^2+(T^3+T)xy=x^3-(4T^5-17T^4+30T^3-18T^2+4)x^2 \\
&\quad +T^2(2T-1)(3T^2-7T+5)^2x.
\end{aligned}$$

Although we have not made it formally part of the statements of Theorems 1.1 and 1.2, our methods do also give the moduli interpretations of these surfaces. In other words, given a point on one of these surfaces (away from a certain finite set of curves) we can determine the corresponding pair of N-congruent elliptic curves. The fact that N-congruent elliptic curves over $\mathbb{Q}$ have traces of Frobenius (at all primes of good reduction) that are congruent mod N, then provides some very useful check on our calculations.

The second part of the following corollary was conjectured by Kani and Schanz [14, Conjecture 5], and its proof (for $\varepsilon = 1$) was completed by Zexiang Chen in his PhD thesis [5]. For N sufficiently large it is expected (with variants of this conjecture variously attributed to Frey, Mazur, Kani and Darmon) that the conclusions of the corollary are false.

Corollary 1.3. *Let $N \le 12$ and $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$ with $\varepsilon = 1$ if $N = 11$ or 12.*

(i) *There are infinitely many pairs of non-isogenous elliptic curves over $\mathbb{Q}(T)$ that are N-congruent with power ε.*

(ii) *There are infinitely many pairs of non-isogenous elliptic curves over $\mathbb{Q}$ that are N-congruent with power ε.*

Moreover the j-invariants j_1 and j_2 of the elliptic curves in (i) (resp. (ii)) correspond to infinitely many curves (resp. points) in the (j_1, j_2)-plane.

Proof. In Table 3 we list at least one $\mathbb{Q}$-rational section of infinite order for each of the elliptic surfaces in Theorems 1.1 and 1.2. This proves the first part. The second part follows by specialising T. See the proof of [10, Theorem 1.5] for further details. The final sentence of the statement is included to guard against various "cheat" proofs, where new examples are generated from old by taking quadratic twists, or making substitutions for T. □

Remark 1.4. If elliptic curves E_1 and E_2 are N-congruent with power $\varepsilon = -1$, then the quotient of $E_1 \times E_2$ by the graph of the N-congruence is a principally polarised abelian surface. The surface $Z(N, -1)$ may then be interpreted as a

Hilbert modular surface, parametrising degree N morphisms from a genus 2 curve to an elliptic curve. At the outset of our work, this moduli interpretation had not been made explicit for any $N > 5$. Remarkably however, this approach has been used by A. Kumar [16] to independently obtain results equivalent to the first two parts of Theorem 1.1 and the first three parts of Theorem 1.2. As far as we are aware, his methods do not generalise to $\varepsilon \neq -1$.

In Tables 1 and 2 we record some further data concerning the elliptic surfaces in Theorems 1.1 and 1.2. Since a K3-surface may admit many elliptic fibrations, the data in Table 1 comes with the caveat that it relates to the elliptic fibration we happened to find in Theorem 1.1. Since a properly elliptic surface has a unique elliptic fibration, there is no such caveat for Table 2. We list in each case the Kodaira symbols of the singular fibres (with bracketing to indicate fibres that are Galois conjugates), the order of the torsion subgroup over $\mathbb{Q}(T)$, the ranks of the group of sections over $\mathbb{Q}(T)$ and $\overline{\mathbb{Q}}(T)$, and finally the geometric Picard number ρ. The lower bounds on the ranks are immediate from the independent sections of infinite order listed in Tables 3 and 4. The upper bounds on the ranks, and the geometric Picard numbers are justified in Section 4.

TABLE 1. The elliptic K3-surfaces in Theorem 1.1

(N, ε)	singular fibres	|tors|	rank/$\mathbb{Q}$	rank/$\overline{\mathbb{Q}}$	ρ
$(6, 5)$	$(\mathrm{I}_2, \mathrm{I}_2), \mathrm{I}_3, (\mathrm{I}_3, \mathrm{I}_3, \mathrm{I}_3), \mathrm{I}_4, \mathrm{I}_4$	1	2	2	20
$(7, 3)$	$\mathrm{I}_1, \mathrm{I}_2, (\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_2, \mathrm{I}_2), \mathrm{I}_3, \mathrm{I}_{10}$	2	2	2	20
$(8, 3)$	$(\mathrm{I}_1, \mathrm{I}_1), \mathrm{I}_2, (\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_3, \mathrm{I}_3), \mathrm{I}_0^*$	1	4	5	20
$(8, 5)$	$\mathrm{I}_2, \mathrm{I}_2, (\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_3, \mathrm{I}_3), \mathrm{I}_0^*$	2	2	4	20
$(9, 1)$	$(\mathrm{I}_1, \mathrm{I}_1, \mathrm{I}_1), \mathrm{I}_2, (\mathrm{I}_2, \mathrm{I}_2, \mathrm{I}_2), \mathrm{I}_3, \mathrm{I}_4, \mathrm{I}_0^*$	1	3	4	19
$(12, 1)$	$(\mathrm{I}_1, \mathrm{I}_1, \mathrm{I}_1, \mathrm{I}_1, \mathrm{I}_1, \mathrm{I}_1, \mathrm{I}_1, \mathrm{I}_1), (\mathrm{I}_4, \mathrm{I}_4), (\mathrm{I}_4, \mathrm{I}_4)$	1	3	5	19

TABLE 2. The properly elliptic surfaces in Theorem 1.2

(N, ε)	singular fibres	|tors|	rank/$\mathbb{Q}$	rank/$\overline{\mathbb{Q}}$	ρ
$(8, 7)$	$\mathrm{I}_2, (\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_3, \mathrm{I}_3), \mathrm{I}_4, \mathrm{I}_8, \mathrm{I}_8$	2	1	2	30
$(9, 2)$	$(\mathrm{I}_2, \mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_3, \mathrm{I}_3), (\mathrm{I}_3, \mathrm{I}_3, \mathrm{I}_3), \mathrm{I}_9, \mathrm{I}_0^*$	1	2	2	29
$(10, 1)$	$(\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_3, \mathrm{I}_3, \mathrm{I}_3), \mathrm{I}_5, \mathrm{I}_{10}, \mathrm{IV}$	1	1	1	28
$(10, 3)$	$(\mathrm{I}_1, \mathrm{I}_1, \mathrm{I}_1), \mathrm{I}_2, (\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_2, \mathrm{I}_2), (\mathrm{I}_3, \mathrm{I}_3, \mathrm{I}_3), \mathrm{I}_4, \mathrm{I}_4, \mathrm{I}_6$	1	3	4	28
$(11, 1)$	$(\mathrm{I}_1, \mathrm{I}_1, \mathrm{I}_1), \mathrm{I}_2, (\mathrm{I}_2, \mathrm{I}_2, \mathrm{I}_2), \mathrm{I}_3, \mathrm{I}_4, (\mathrm{I}_4, \mathrm{I}_4), \mathrm{I}_{10}$	2	2	2	28

TABLE 3. Mordell-Weil generators over $\mathbb{Q}(T)$

(N,ε)	x-coordinates of independent sections of infinite order
$(6,5)$	$0,\ 2T^4-4T,$
$(7,3)$	$4T^2+20T+25,\ 6T+25,$
$(8,3)$	$-7,\ -T^2+9,\ -4T^2-6T,\ (4T^5-2T^4+10T^3+6T^2+18T)/(T-1)^2,$
$(8,5)$	$-4T^2+49,\ 2T^3+19T^2+60T+63,$
$(9,1)$	$0,\ 4T^4+2T^3-2T^2,\ 4T^4+4T^3+9T^2+18T+9,$
$(12,1)$	$0,\ -12T^4-24T^2-12,\ 4T^6+12T^4-4T^2-12,$
$(8,7)$	$4T^6+4T^5-9T^4-10T^3+4T^2+6T+1,$
$(9,2)$	$0,\ 2T^5-8T^3+4T^2+6T-4,$
$(10,1)$	$0,$
$(10,3)$	$0,\ 2T^5-4T^4-4T^3+6T,\ 4T^5-2T^4-14T^3-18T^2-6T,$
$(11,1)$	$T^4+4T^2+4,\ 3T^2-7T+5.$

TABLE 4. Additional Mordell-Weil generators over $\overline{\mathbb{Q}}(T)$

(N,ε)	d	section of infinite order defined over $\mathbb{Q}(\sqrt{d})$
$(8,3)$	-2	$(-2T^4-5T^2-9, (2T^6+5T^4+20T^2+9)\sqrt{-2}),$
$(8,5)$	-3	$(-2T^3+T^2+18T-35, (12T^3-6T^2-108T+210)\sqrt{-3}),$
$(8,5)$	-1	$(16T^2-196, (8T^4-346T^2+3038)\sqrt{-1}),$
$(9,1)$	-3	$(-(19/3)T^4-15T^3-9T^2,\ \dots),$
$(12,1)$	-3	$(-12T^4-40T^2-12,\ \dots),$
$(12,1)$	-1	$(-16T^4-64T^2-48,\ \dots),$
$(8,7)$	-3	$(-4T^6-20T^5-39T^4-36T^3-14T^2+1,\ \dots),$
$(10,3)$	-3	$(-7T^6-23T^5-30T^4-15T^3-9T^2,\ \dots).$

We organise the proofs of Theorems 1.1 and 1.2 as follows. The cases $N=8$ and $N=9$ were already treated in [6], [10], by starting from equations for $X_E(N,\varepsilon)$. In Section 2 we use a similar approach to treat the cases $(N,\varepsilon)=(7,3)$, $(11,1)$ and $(12,1)$. Then in Section 3 we treat the cases $(N,\varepsilon)=(6,5)$, $(10,1)$ and $(10,3)$ by exhibiting $Z(N,\varepsilon)$ as a degree 3 cover of a K3-surface.

The calculations described in this paper were carried out using Magma [1]. Accompanying Magma files are available from the author's website. We assume that the reader is familiar with the standard techniques for putting an elliptic curve in Weierstrass form, as described in [2, §8], or as implemented in Magma.

2. Proofs via equations for $X_E(N,\varepsilon)$

We prove Theorems 1.1 and 1.2 in the cases $(N,\varepsilon) = (7,3)$, $(11,1)$ and $(12,1)$. The case $(N,\varepsilon) = (7,3)$ was treated in [5, Section 8.2], but as this has not been published before, we include the details for completeness.

Case $(N,\varepsilon) = (7,3)$. Let E be the elliptic curve $y^2 = x^3 + ax + b$. The following equation for $X_E(7,3)$, as a quartic curve in $\mathbb{P}^2$, was computed by Poonen, Schaefer and Stoll [20, Section 7.2], building on work of Halberstadt and Kraus [12].

$$\begin{aligned} F(a,b;x,y,z) = {} & -a^2x^4 + 2abx^3y - 12bx^3z - 6(a^3+6b^2)x^2y^2 + 6ax^2z^2 \\ & + 2a^2bxy^3 - 12abxy^2z + 18bxyz^2 + (3a^4+19ab^2)y^4 \\ & - 2(4a^3+21b^2)y^3z + 6a^2y^2z^2 - 8ayz^3 + 3z^4. \end{aligned}$$

Replacing E by a quadratic twist does not change the isomorphism class of $X_E(7,3)$. This is borne out by the identity

$$F(\lambda^2 a, \lambda^3 b; \lambda x, y, \lambda^2 z) = \lambda^8 F(a,b;x,y,z).$$

The surface $Z(7,3)$ is the quotient of $\{F = 0\} \subset \mathbb{A}^2 \times \mathbb{P}^2$ by this $\mathbb{G}_m$-action. We have $F(y, x_1y; x_2, T, y) = y^2(cy^2 + hy - f)$ where

$$\begin{aligned} c &= (T^2+1)(3T^2 - 8T + 3), \\ h &= T^3(19T - 42)x_1^2 + 2T(T-3)^2x_1x_2 - 6(T^2-1)x_2^2, \\ f &= 36T^2x_1^2x_2^2 - 2(T-6)x_1x_2^3 + x_2^4. \end{aligned}$$

Therefore $Z(7,3)$ is birational to the total space for the genus one curve over $\mathbb{Q}(T)$ with equation $Y^2 = h^2 + 4cf$. This is a double cover of $\mathbb{P}^1$ with a rational point above $(x_1 : x_2) = (1 : 0)$. Putting this elliptic curve in Weierstrass form, and replacing T by $(6T-3)/(4T+4)$, gives the equation in the statement of Theorem 1.1.

Case $(N,\varepsilon) = (11,1)$. Let E be the elliptic curve $y^2 = x^3 + ax + b$. Equations for $X_E(11,1)$ as a curve in $\mathbb{P}^4$ were computed in [9, Theorem 1.2]. These equations are the 4×4 minors of the 5×5 Hessian matrix of the cubic form

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

Replacing E by a quadratic twist does not change the isomorphism class of $X_E(11,1)$. This is borne out by the identity

$$F(\lambda^2 a, \lambda^3 b; \lambda^2 v, \lambda^2 w, \lambda x, \lambda y, z) = \lambda^6 F(a,b;v,w,x,y,z).$$

We may describe $Z(11,1)$ as the quotient of a 3-fold in $\mathbb{A}^2 \times \mathbb{P}^4$ by this $\mathbb{G}_m$-action.

We start by using the discriminant condition $4a^3 + 27b^2 \neq 0$ to simplify the equations for $X_E(11,1)$. The polynomials

$$\begin{aligned}
F_1 &= vz + 2wz + x^2 - xy - y^2,\\
F_2 &= axz + bz^2 - vx + vy - 2wx,\\
F_3 &= a^2z^2 + 2awz - 4ax^2 - 12bxz - 3w^2,\\
F_4 &= a^2z^2 + 2avz - 2ax^2 + 4axy + ay^2 - 6bxz + 6byz + 3v^2,\\
F_5 &= 2a^2yz - abz^2 - 4avx - 2avy - 6bvz - 3bx^2 - 12bxy - 3by^2,
\end{aligned}$$

are linear combinations of the derivatives of F, where the matrix implicit in taking these linear combinations is invertible if $4a^3 + 27b^2 \neq 0$. Now $X_E(11,1)$ is defined by the 4×4 minors of the 5×5 Jacobian matrix (M say) of $F_1, \ldots, F_5$.

We make the substitutions

$$\begin{aligned}
a &= (4U + 3x_3)x_4 - 3x_5^2,\\
b &= x_2(x_1 + x_3)x_4 - (4U + 3x_3)x_4x_5 + 2x_5^3,\\
(v, w, x, y, z) &= (x_2x_4 + x_4x_5 + x_5^2, x_3x_4 - x_5^2, x_5, x_4, 1).
\end{aligned}$$

We have $4a^3 + 27b^2 = x_4h$ for some polynomial h. We add x_5 times the first row of M to the second row. We then divide all but the first row by x_4. Let $I \subset \mathbb{Q}[U, x_1, x_2, x_3, x_4, x_5]$ be the ideal generated by the 4×4 minors of M, and

$$J = \{f \in \mathbb{Q}[U, x_1, x_2, x_3, x_4, x_5] : x_2hf \in I\}.$$

Using the Gröbner basis machinery in Magma we find that $J \cap \mathbb{Q}[U, x_1, x_2, x_3, x_4]$ is generated by 3 homogeneous polynomials of degree 4. These define a surface in $\mathbb{P}^4$ of degree 12. By the substitution

$$T = \frac{4(2x_1 - x_2 + x_3)U + (x_1x_2 - x_2^2 + x_3x_4)}{2(2x_4 - x_2)U + 2(x_1x_2 - x_2^2 + x_3x_4)}$$

this surface is birational to the surface $\{Q_1 = Q_2 = 0\}$ in $\mathbb{A}^1 \times \mathbb{P}^3$ where

$$\begin{aligned}
Q_1 = {} & 4(T-2)x_1x_2 + 8x_1x_3 + (T-2)^2x_2^2\\
& + 4(T-2)x_2x_3 + 2(T^2 - T + 1)x_2x_4 + 4x_3^2 - 4Tx_3x_4,\\
Q_2 = {} & 8x_1^2 + 16x_1x_3 - 4(2T-1)x_1x_4 - T(T-2)x_2^2 - T^2x_2x_3\\
& - 2(T^2 - T + 1)x_2x_4 - 2(T-4)x_3^2 - 2(T^2 + 4T - 1)x_3x_4.
\end{aligned}$$

These same equations define a genus one curve in $\mathbb{P}^3$ defined over $\mathbb{Q}(T)$, with a rational point at $(x_1 : x_2 : x_3 : x_4) = (0 : 0 : 0 : 1)$. Putting this elliptic curve in Weierstrass form gives the equation in the statement of Theorem 1.2.

Case $(N,\varepsilon) = (12,1)$. Let E be the elliptic curve $y^2 = x^3+ax+b$. Equations for $X_E(12,1)$ as a curve in $\mathbb{P}^5$ were computed in [5, Theorem 1.7.10]. These equations are $F_0 = F_1 = F_2 = F_3 = 0$ where

$$\begin{aligned}
F_0 &= -X^2Z + aXY^2 + 6bY^3 - 6aY^2Z - 12Z^3,\\
F_1 &= X^2 + 12XZ + 36Z^2 - 2u_0u_2 - u_1^2 + au_2^2,\\
F_2 &= 4aXY + 36bY^2 - 24aYZ - 2u_0u_1 + 2au_1u_2 + bu_2^2,\\
F_3 &= 8aXZ - 4a^2Y^2 - u_0^2 + 2bu_1u_2.
\end{aligned}$$

These polynomials satisfy

$$F_i(\lambda^2 a, \lambda^3 b; \lambda X, Y, \lambda Z, \lambda^2 u_0, \lambda u_1, u_2) = \lambda^{m_i} F_i(a, b; X, Y, Z, u_0, u_1, u_2)$$

where $(m_0, m_1, m_2, m_3) = (3, 2, 3, 4)$. Again, it is our aim to quotient out by this $\mathbb{G}_m$-action. We do this by setting $(X + 6Z)Y = u_2^2$. Specifically, we substitute $(X, Y, Z, u_0, u_1, u_2) = (x^2 - 6y, 1, y, vx, wx, x)$ and then solve for a and b so that the first two equations are satisfied. In the remaining two equations we substitute

$$v = 2(w - 2y)y + \frac{T+1}{T-1}(x^2(y+1) - (w+2y)^2).$$

The resultant with respect to w is $f(T)x^{14}y^2g(x,y)^2h(x,\widetilde{y})$ where $f(T)$ is a rational function in T, $g(x,y) = x^6(y+1) - 9y^2(x^2+4)^2$,

$$\begin{aligned}
h(x,y) = (T+1)^2x^2y^2 + (T+2)(T^2+3)^2x^2 \\
- 4(T-1)(T+3)^2xy + 4(T+3)^2y^2 + 12T(T+1)^2(T+3)^2
\end{aligned}$$

and $\widetilde{y} = (144(T+1)y + (T+3)^2((T-3)x^2 + 12(T+1)))/(8(T+3)x)$. Therefore $Z(12,1)$ is birational to the total space for the genus one curve $C = \{h = 0\}$ in $\mathbb{A}^2$ defined over $\mathbb{Q}(T)$. Replacing x by $2(T+3)/(T^2+3)x$, and completing the square in y shows that C has equation

$$Y^2 = -(T+2)x^4 - (4T^3 + 5T^2 + 6T + 9)x^2 - 3T(T^2+3)^2. \tag{1}$$

This gives a genus one fibration on $Z(12,1)$ defined over $\mathbb{Q}$, but without a $\mathbb{Q}$-rational section. Indeed the fibres with $T > 0$ have no real points.

We now find another genus one fibration that does have a $\mathbb{Q}$-rational section. Let $F(x_1, x_2, x_3)$ be the unique homogeneous polynomial of degree 6 with the property that $F(x, T, 1)$ is the right hand side of (1). Then F is the discriminant of the following quadratic in T.

$$x_1^2x_2 + (T^2+2)x_1^2x_3 + 2Tx_1x_2^2 - 2Tx_1x_2x_3 + T^2x_2^3 + 3x_2^2x_3 + 3T^2x_2x_3^2 + 9x_3^3 = 0$$

This same equation defines a genus one curve in $\mathbb{P}^2$ defined over $\mathbb{Q}(T)$, with a rational point at $(x_1 : x_2 : x_3) = (1 : 0 : 0)$. Putting this elliptic curve in Weierstrass form gives the equation in the statement of Theorem 1.1.

3. Degree 3 covers of K3-surfaces

We prove Theorems 1.1 and 1.2 in the cases $(N,\varepsilon) = (6,5)$, $(10,1)$ and $(10,3)$. In the first of these cases, Chen's equations for $X_E(6,5)$ already give a genus one fibration on $Z(6,5)$, but one without a section. The content of Theorem 1.1 in this case is that we can find another genus one fibration that does have a section.

For N an odd integer, let $Z^*(N,\varepsilon)$ be the double cover of $Z(N,\varepsilon)$ that parametrises pairs of elliptic curves whose ratio of discriminants is a square.

Theorem 3.1. *If $(N,\varepsilon) = (3,2)$, $(5,1)$ or $(5,2)$ then $Z^*(N,\varepsilon)$ is a double cover of $\mathbb{P}^2$, ramified over the union of two cuspidal cubics, with equation*

$$y^2 = F_+(u,v,w)F_-(u,v,w) \tag{2}$$

where

$$\begin{aligned}
Z^*(3,2):&\quad F_\pm = u(u+3v\pm w)^2 + 4v^3,\\
Z^*(5,1):&\quad F_\pm = u(u^2-11uv-v^2) + w^2(12u+v) \pm 2w(3u^2-4uv+4w^2),\\
Z^*(5,2):&\quad F_\pm = u^2(11v+8w) + w^2(8u-v+4w) \pm 2u(2v-w)(4u-v+4w).
\end{aligned}$$

Proof. Let E be the elliptic curve $y^2 = x^3+ax+b$. We put $\Delta = -4a^3-27b^2$, and define polynomials

$$\begin{aligned}
f(x) &= x^3+ax+b,\\
g(x) &= 3ax^4+18bx^3-6a^2x^2-6abx-a^3-9b^2,\\
h(x) &= 3ax^2+9bx-a^2,\\
j(x) &= 27bx^3-18a^2x^2-27abx-2a^3-27b^2.
\end{aligned}$$

If we assign the variables x,a,b weights 1, 2, 3, then each of these polynomials is homogeneous. We note that $j^2 = -4h^3-27\Delta f^2$.

Case $(N,\varepsilon) = (3,2)$. The following equations for the family of curves parametrised by $X_E(3,2)$ are taken from [7, Section 13]. Starting from the Klein form[1]

$$D(\xi,\eta) = -27a\xi^4-54b\xi^3\eta-18a^2\xi^2\eta^2-54ab\xi\eta^3+(a^3-27b^2)\eta^4,$$

we define

$$A(\xi,\eta) = \frac{1}{108}\begin{vmatrix} D_{\xi\xi} & D_{\xi\eta}\\ D_{\eta\xi} & D_{\eta\eta}\end{vmatrix}, \quad \text{and} \quad B(\xi,\eta) = \frac{1}{36}\begin{vmatrix} D_\xi & D_\eta\\ A_\xi & A_\eta\end{vmatrix},$$

where the subscripts denote partial derivatives. These forms satisfy the syzygy

$$-4A^3-27B^2 = 16(4a^3+27b^2)^2D^3. \tag{3}$$

[1]We obtain D from $\mathfrak{D}(\xi,\eta)$ in [7, Section 9] by putting $c_4 = -48a$, $c_6 = -864b$, multiplying ξ by 12, and dividing through by $2^{12}3^3$.

The family of elliptic curves 3-congruent to E with power $\varepsilon = 2$ is given by

$$y^2 = x^3 + A(\xi,\eta)x + B(\xi,\eta).$$

We dehomogenise by putting $(\xi,\eta) = (x,1)$. Then $D = f_x^3 - 27f^2 = j - 3f_x h$ where $f_x = 3x^2 + a$. The quantities $(u,v,r,s) = (D, f_x h, h^3, 3^6\Delta f^4)$ are related by

$$(4r + (u+3v)^2)(ru - v^3) = rs. \tag{4}$$

As we verify in Remark 3.2 below, this is an equation for $Z(3,2)$ in $\mathbb{P}(1,1,2,3)$ where the coordinates u,v,r,s have weights $1,1,2,3$. We see by (3) that, up to squared factors, the ratio of discriminants is s/u. We substitute $s = uw^2$ in (4) to give a quadratic in r whose discriminant is the polynomial F_+F_- in the statement of the theorem.

Case $(N,\varepsilon) = (5,1)$. The following equations for the family of curves parametrised by $X_E(5,1)$ are taken from [7, Section 13]. Starting from the Klein form[2]

$$\begin{aligned} D(\lambda,\mu) = {} & \lambda^{12} + 22a\lambda^{10}\mu^2 + 220b\lambda^9\mu^3 - 165a^2\lambda^8\mu^4 - 528ab\lambda^7\mu^5 \\ & - 220(a^3 + 12b^2)\lambda^6\mu^6 + 264a^2b\lambda^5\mu^7 - 165a(5a^3 + 32b^2)\lambda^4\mu^8 \\ & - 880b(3a^3 + 20b^2)\lambda^3\mu^9 + 22a^2(25a^3 + 168b^2)\lambda^2\mu^{10} \\ & + 20(19a^4b + 128ab^3)\lambda\mu^{11} + (125a^6 + 1792a^3b^2 + 6400b^4)\mu^{12}, \end{aligned}$$

we define

$$A(\lambda,\mu) = \frac{1}{5808}\begin{vmatrix} D_{\lambda\lambda} & D_{\lambda\mu} \\ D_{\mu\lambda} & D_{\mu\mu} \end{vmatrix}, \quad \text{and} \quad B(\lambda,\mu) = \frac{1}{360}\begin{vmatrix} D_\lambda & D_\mu \\ A_\lambda & A_\mu \end{vmatrix},$$

where the subscripts denote partial derivatives. These forms satisfy the syzygy

$$4A^3 + 27B^2 = (4a^3 + 27b^2)D^5. \tag{5}$$

The family of elliptic curves 5-congruent to E with power $\varepsilon = 1$ is given by

$$y^2 = x^3 + A(\lambda,\mu)x + B(\lambda,\mu).$$

We dehomogenise by putting $(\lambda,\mu) = (x,1)$. Then

$$D = 4kf - 3(f^2+g)^2 + 32\Delta(f^2+g),$$

where $k(x) = f^3 + fj + 4\Delta f + 3g(xf_x - 2f) = x^9 + 12ax^7 + 84bx^6 + \ldots$

The quantities $(t,u,v,r,s) = (4f, 2(f^2+g), 16\Delta, 4k, D)$ are related by

$$\begin{aligned} r^2 + st^2 &= u(u^2 - 11uv - v^2) + (12u + v)s, \\ rt &= 3u^2 - 4uv + 4s. \end{aligned} \tag{6}$$

[2]We obtain D from $\mathbf{D}(\lambda,\mu)$ in [7, Section 8] by putting $c_4 = -48a$, $c_6 = -864b$, multiplying λ by 12, and dividing through by $2^{24}3^{12}$.

These are equations for $Z(5,1)$ in $\mathbb{P}(1,2,2,3,4)$ where the coordinates t,u,v,r,s have weights $1,2,2,3,4$. We see by (5) that, up to squared factors, the ratio of discriminants is s. Putting $s=w^2$ we obtain from (6) the equation

$$(r^2-st^2)^2=(r^2+st^2)^2-4s(rt)^2=F_+(u,v,w)F_-(u,v,w)$$

where $F_\pm$ are the polynomials in the statement of the theorem.

Case (N,ε) = (5,2). The following equations for the family of curves parametrised by $X_E(5,2)$ are taken from [8, Theorem 5.8]. Starting from the Klein form[3]

$$\begin{aligned}D(\lambda,\mu)&=(125a^3-432b^2)\lambda^{12}+2430a^2b\lambda^{11}\mu-22a(25a^3-378b^2)\lambda^{10}\mu^2\\&\quad-110b(11a^3-108b^2)\lambda^9\mu^3-165a^2(5a^3-27b^2)\lambda^8\mu^4-132ab(53a^3-189b^2)\lambda^7\mu^5\\&\quad+220(a^6-123a^3b^2+81b^4)\lambda^6\mu^6+132a^2b(19a^3-297b^2)\lambda^5\mu^7\\&\quad-165(a^7-26a^4b^2+189ab^4)\lambda^4\mu^8-110(3a^6b-34a^3b^3+135b^5)\lambda^3\mu^9\\&\quad-22a^2(a^3-3b^2)(a^3+27b^2)\lambda^2\mu^{10}-10ab(5a^6+82a^3b^2+189b^4)\lambda\mu^{11}\\&\quad+(a^9-a^6b^2-181a^3b^4-675b^6)\mu^{12},\end{aligned}$$

we define

$$A(\lambda,\mu)=\frac{1}{1452}\begin{vmatrix}D_{\lambda\lambda}&D_{\lambda\mu}\\D_{\mu\lambda}&D_{\mu\mu}\end{vmatrix},\quad\text{and}\quad B(\lambda,\mu)=\frac{-1}{180}\begin{vmatrix}D_\lambda&D_\mu\\A_\lambda&A_\mu\end{vmatrix},$$

where the subscripts denote partial derivatives. These forms satisfy the syzygy

$$-4A^3-27B^2=16(4a^3+27b^2)^2D^5. \tag{7}$$

The family of elliptic curves 5-congruent to E with power $\varepsilon=2$ is given by

$$y^2=x^3+A(\lambda,\mu)x+B(\lambda,\mu).$$

We dehomogenise by putting $(\lambda,\mu)=(x,1)$. Then

$$D=16\Delta f^4-g^3+4(2g^3-g^2j-4\Delta f^2g). \tag{8}$$

The quantities $(r,s,v,w)=(\Delta f^4,\Delta f^2g,g^3,2g^3-g^2j-4\Delta f^2g)$ are related by

$$r(4s-2v+w)^2+27rsv+sw^2-s^2(v-4w)=0. \tag{9}$$

This is an equation for $Z(5,2)$ as a cubic surface in $\mathbb{P}^3$. We see from (7) and (8) that, up to squared factors, the ratio of discriminants is $r(16r-v+4w)$. Putting $r(16r-v+4w)=(4r-u)^2$, where u is a new variable, and using this equation to eliminate r from (9), we obtain a quadratic in s whose discriminant is the polynomial F_+F_- in the statement of the theorem. □

[3]We obtain D from $\mathbf{D}(\lambda,\mu)$ in [8, Section 5] by putting $c_4=-48a$, $c_6=-864b$, multiplying λ by 12, and dividing through by $2^{36}3^{15}$.

Remark 3.2. Let $(N,\varepsilon) = (3,2)$, $(5,1)$ or $(5,2)$. We saw in the proof of Theorem 3.1 that one model for $Z(N,\varepsilon)$ is the weighted projective plane $\mathbb{P}(1,2,3)$ where the co-ordinates x,a,b have weights $1,2,3$. We mapped this to another model for $Z(N,\varepsilon)$ defined by (4), (6) or (9). The inverse maps are as follows.

$$(3,2)\quad \begin{cases} x = r + v^2, \\ a = -3r(r + uv + 2v^2), \\ b = r(u+3v)(ru+v^3) + 2r^2(r+3v^2), \end{cases}$$

$$(5,1)\quad \begin{cases} x = 32u - v + 5t^2, \\ a = -3(8u-v)(32u-v) - 288rt + 30(28u+v)t^2 - 75t^4, \\ b = -2(32u-v)^2(4u+v) - 144(32u-v)rt + 6(32u-v)(88u-5v)t^2 \\ \qquad\qquad + 1008rt^3 - 150(28u+v)t^4 + 250t^6, \end{cases}$$

$$(5,2)\quad \begin{cases} x = 4rs + 4rv + rw - s^2, \\ a = 3(8rs^3 + 4rs^2v + 6rs^2w + rsw^2 - s^4), \\ b = r^2s(16s^3 - 8s^2v - 24s^2w - 40svw - 15sw^2 + 4vw^2 - 2w^3) \\ \qquad\qquad + rs^3(24s^2 + 8sv + 34sw + 7w^2) - 2s^6. \end{cases}$$

Remark 3.3. There are two naturally defined involutions on the K3-surfaces in Theorem 3.1. The first switches the sign of y, and corresponds to swapping over the pair of N-congruent elliptic curves. The second is given on $Z^*(3,1)$ and $Z^*(5,1)$ by switching the sign of w, and on $Z^*(5,2)$ by $(u,v,w,y) \mapsto (\widetilde{u},v,w,(\widetilde{u}/u)^2y)$ where $\widetilde{u} = u(v-4w)/(8u-(v-4w))$. This second involution switches the choice of square root for the ratio of discriminants. The two involutions commute, and the second swaps over the curves $F_+ = 0$ and $F_- = 0$.

Remark 3.4. For a suitable parametrisation of the cuspidal cubic $F_+ = 0$, we obtain a family of elliptic curves with j-invariant

$$\begin{aligned} (3,1):&\qquad j = 27(T-3)^3(T+1)^3/T^3, \\ (5,1):&\qquad j = (T+5)^3(T^2-5)^3(T^2+5T+10)^3/(T^2+5T+5)^5, \\ (5,2):&\qquad j = 125T(2T+1)^3(2T^2+7T+8)^3/(T^2+T-1)^5. \end{aligned}$$

These correspond to $X_{\mathrm{s}}^+(3)$, $X_{\mathrm{s}}^+(5)$ and $X_{\mathrm{ns}}^+(5)$, where $X_{\mathrm{s}}^+(N)$ and $X_{\mathrm{ns}}^+(N)$ are the modular curves associated to the normaliser of a split or non-split Cartan subgroup of level N. We may compute $X_{\mathrm{s}}^+(N)$ as the quotient of $X_0(N^2)$ by the Fricke involution, whereas the formula for $X_{\mathrm{ns}}^+(5)$ is taken from [4, Corollary 5.3]. The use of these modular curves to construct pairs of N-congruent elliptic curves is described further in [11].

Let N be an odd integer and let $\varepsilon \in (\mathbb{Z}/2N\mathbb{Z})^\times$. Then $X_E(2N,\varepsilon) \to X_E(N,\varepsilon)$ is geometrically a Galois covering with Galois group $\mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$. Since elliptic curves which are 2-congruent have ratio of discriminants a square, it follows that $Z(2N,\varepsilon) \to Z^*(N,\varepsilon)$ is a degree 3 cover. In the cases $(2N,\varepsilon) = (6,5)$, $(10,1)$ and $(10,3)$ the surface $Z(2N,\varepsilon)$ has an elliptic fibration. The pushfoward of a fibre gives a divisor class D on the K3-surface $Z^*(N,\varepsilon)$ with $D^2 = 2$. Using this divisor class D we may write $Z^*(N,\varepsilon)$ as a double cover of $\mathbb{P}^2$. We have arranged (with the benefit of hindsight) that the equations in Theorem 3.1 write $Z^*(N,\varepsilon)$ as a double cover of $\mathbb{P}^2$ in exactly this way.

The equations for $Z(2N,\varepsilon)$ in Theorems 1.1 and 1.2 may be obtained from the equations for $Z^*(N,\varepsilon)$ in Theorem 3.1 as follows. The tangent line to a general point on the cuspidal cubic $F_+(u,v,w) = 0$ has equation:

$$(2N,\varepsilon) = (6,5) \qquad (T^3-1)u + 3(T-1)v - w = 0, \tag{10}$$

$$(2N,\varepsilon) = (10,1) \qquad (T-2)u - T(T-1)^2 v + 2(T-1)w = 0, \tag{11}$$

$$(2N,\varepsilon) = (10,3) \qquad T^3 u - (T+1)v - T^2 w = 0. \tag{12}$$

We parametrise this line, and substitute into the right hand side of the equation $y^2 = F_+(u,v,w)F_-(u,v,w)$. After cancelling a squared factor (which arises since we chose a tangent line) the right hand side is a binary quartic with a linear factor. We now have the equation for a genus one curve over $\mathbb{Q}(T)$ with a rational point. Putting this elliptic curve in Weierstrass form gives the equations for $Z(6,5)$, $Z(10,1)$ and $Z(10,3)$ in Theorems 1.1 and 1.2.

It remains to show that these degree 3 covers of $Z^*(N,\varepsilon)$ are the ones we wanted. We use the following lemma.

Lemma 3.5. *Let K be a field of characteristic not 2 or 3. Elliptic curves E_1 and E_2 over K with j-invariants j_1 and j_2, with $j_1, j_2 \notin \{0, 1728\}$, are 2-congruent if and only if there exist $m, x \in K$ satisfying $(j_1 - 1728)(j_2 - 1728) = m^2$ and*

$$x^3 - 3j_1j_2x - 2j_1j_2(m + 1728) = 0.$$

Proof. This follows from the formulae in [23] or [7, Sections 8 and 13] by a generic calculation. □

We illustrate the use of Lemma 3.5 in the case $(2N,\varepsilon) = (10,3)$, the other cases being similar. Above each point $(u : v : w) \in \mathbb{P}^2$ there are a pair of points on $Z^*(5,2)$ possibly defined over a quadratic extension. These points correspond to a pair of elliptic curves, say with j-invariants j_1 and j_2. A calculation using the formulae in Remark 3.2 shows that, for m a suitable choice of square root of $(j_1 - 1728)(j_2 - 1728)$, we have

$$j_1j_2 = G_6(u,v,w)H(u,v,w)^2$$
$$j_1j_2(m + 1728) = G_9(u,v,w)H(u,v,w)^3$$

where

$$G_6(u,v,w) = 640u^4v^2 - 768u^4vw - 72u^3v^3 - 240u^3v^2w + \dots$$
$$G_9(u,v,w) = 6912u^7v^2 - 1376u^6v^3 - 14976u^6v^2w + \dots$$

are irreducible homogeneous polynomials of degrees 6 and 9, and $H \in \mathbb{Q}(u,v,w)$ is a rational function. Finally we claim that the polynomials

$$X^3 - 3G_6(u,v,w)X - 2G_9(u,v,w) = 0, \tag{13}$$

arising from Lemma 3.5, and

$$uT^3 - wT^2 - vT - v = 0, \tag{14}$$

appearing in (12), define the same cubic extension. Indeed we find by computer algebra that if (14) has root T_0 then (13) has root

$$X_0 = 3u^2(8u - 3v - 4w)T_0^2 + 12u(2uv - 4uw + vw)T_0 \\ - 16u^2v + 6uv^2 + 8uw^2 - vw^2 + 4w^3.$$

4. Computing the Picard numbers

Let $E/\mathbb{Q}(T)$ be one of the elliptic curves in Theorems 1.1 and 1.2. We write $X \to \mathbb{P}^1$ for the minimal fibred surface with generic fibre E. The reduction of E mod p is an elliptic curve $E_p/\mathbb{F}_p(T)$, and the reduction of X mod p is a surface $X_p/\mathbb{F}_p$. We will always take p to be a prime of good reduction.

Let $\overline{X} = X \times_{\mathbb{Q}} \overline{\mathbb{Q}}$ and $\overline{X}_p = X_p \times_{\mathbb{F}_p} \overline{\mathbb{F}}_p$. The Shioda-Tate formula [24, Corollary 5.3] tells us that

$$\mathrm{rank} E(\overline{\mathbb{Q}}(T)) + 2 + \textstyle\sum_{t \in \mathbb{P}^1(\overline{\mathbb{Q}})}(m_t - 1) = \mathrm{rank}\,\mathrm{NS}(\overline{X}), \tag{15}$$

and

$$\mathrm{rank} E_p(\overline{\mathbb{F}}_p(T)) + 2 + \textstyle\sum_{t \in \mathbb{P}^1(\overline{\mathbb{F}}_p)}(m_t - 1) = \mathrm{rank}\,\mathrm{NS}(\overline{X}_p), \tag{16}$$

where m_t is the number of irreducible components in the fibre above t. We write ρ and ρ_p for the numbers on the right of (15) and (16). These are the geometric Picard numbers of X and X_p. The sections exhibited in Tables 3 and 4 give a lower bound for $\mathrm{rank} E(\overline{\mathbb{Q}}(T))$ and hence by (15) a lower bound for ρ. These lower bounds are exactly the values recorded in Tables 1 and 2.

Let $X \to \mathbb{P}^1$ be a minimal elliptic surface with non-constant j-invariant, and let $m = \chi(\mathcal{O}_X)$. This may be computed from the fact that sum of the Euler numbers

of the singular fibres is $12m$. By [17, Lemma IV.1.1] the Hodge diamond of X is

$$\begin{array}{ccccc} & & h^{0,0} & & \\ & h^{1,0} & & h^{0,1} & \\ h^{2,0} & & h^{1,1} & & h^{0,2} \\ & h^{2,1} & & h^{1,2} & \\ & & h^{2,2} & & \end{array} \qquad \begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ m-1 & & 10m & & m-1 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

The surfaces in Theorem 1.1 have $m = 2$ and those in Theorem 1.2 have $m = 3$. To tie in with [14, Theorem 4], we note that $p_g = h^{2,0} = m - 1$. By the Lefschetz theorem on $(1,1)$-classes we have $\rho \leq h^{1,1} = 10m$. This already determines ρ in all cases with $N \leq 8$. It remains for us to improve this upper bound by 1 in the cases $(N, \varepsilon) = (9,1), (12,1), (9,2)$, and to improve it by 2 in the cases $(N, \varepsilon) = (10,1), (10,3), (11,1)$.

The main tool we wish to use (see [26, Proposition 6.2]) is that there is an injective map $\mathrm{NS}(\overline{X}) \to \mathrm{NS}(\overline{X}_p)$ that preserves the intersection pairing.

Let $f_p(x)$ be the characteristic polynomial of Frobenius acting on $H^2_{\text{ét}}(\overline{X}_p, \mathbb{Q}_\ell(1))$, normalised so that $f_p(0) = 1$. This is a polynomial of degree $b_2 = 12m - 2$, independent of the choice of prime $\ell \neq p$. By the Weil conjectures it satisfies the functional equation $f_p(x) = \pm x^{b_2} f_p(1/x)$. The polynomials $f_p(x)$ may be computed from the numbers $n_r = |X_p(\mathbb{F}_{p^r})|$ using the Lefschetz trace formula. See for example [27, Section 3], where f_p is denoted $\widetilde{f}_p$. We used both the functional equation and the Magma function `FrobeniusActionOnTrivialLattice` to limit how many n_r we had to compute. The polynomials $f_p(x)$ for two carefully chosen primes of good reduction are recorded in Table 5.

Let $\Delta_p \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ be the absolute value of the determinant of the intersection pairing on $\mathrm{NS}(\overline{X}_p)$. It may be computed using either of the following two lemmas.

Lemma 4.1. *Write $f_p(x) = g_p(x)h_p(x)$ where every root of g_p is a root of unity, and no root of h_p is a root of unity. Then $\rho_p \leq \deg g_p$ and in the case of equality we have $\Delta_p \equiv h_p(1)h_p(-1) \mod (\mathbb{Q}^\times)^2$.*

Proof. The first part is described for example in [27]. The Tate conjecture predicts that this inequality is always an equality, and this has been proved in many cases. See [13, Section 17.3] for the history of this problem and further references. The formula for Δ_p is a small refinement of a result of Kloosterman, that in turn depends on known cases of the Artin-Tate conjecture.

Let $F_k(x) = \prod(1 - p^k \alpha_i^k x)$ where $f_p(x) = \prod(1 - \alpha_i x)$. The result of Kloosterman [15, Proposition 4.7], is that if k is an even integer with $\alpha_i^k = 1$ for all α_i which

TABLE 5

(N,ε)	Characteristic polynomial of Frobenius
$(9,1)$	$f_5(x) = (x-1)^{16}(x+1)^2(x^2+x+1)(x^2+\frac{7}{5}x+1)$
	$f_7(x) = (x-1)^{18}(x+1)^2(x^2+\frac{10}{7}x+1)$
$(12,1)$	$f_5(x) = (x-1)^{16}(x+1)^4(x^2+\frac{6}{5}x+1)$
	$f_{11}(x) = (x-1)^{12}(x+1)^8(x^2+\frac{6}{11}x+1)$
$(9,2)$	$f_7(x) = (x-1)^{24}(x+1)^2(x^2+x+1)^2(x^2+\frac{10}{7}x+1)(x^2+\frac{13}{7}x+1)$
	$f_{13}(x) = (x-1)^{24}(x^2+x+1)^3(x^2+\frac{1}{13}x+1)(x^2+\frac{25}{13}x+1)$
$(10,1)$	$f_7(x) = (x-1)^{24}(x+1)^2(x^2+x+1)^2(x^2+\frac{10}{7}x+1)^2$
	$f_{17}(x) = -(x-1)^{25}(x+1)^5(x^2-\frac{2}{17}x+1)(x^2+\frac{25}{17}x+1)$
$(10,3)$	$f_{31}(x) = (x-1)^{24}(x+1)^2(x^2+x+1)^2(x^2+\frac{46}{31}x+1)(x^2+\frac{58}{31}x+1)$
	$f_{37}(x) = (x-1)^{28}(x+1)^2(x^2+\frac{70}{37}x+1)^2$
$(11,1)$	$f_{23}(x) = (x-1)^{28}(x+1)^2(x^2+\frac{42}{23}x+1)(x^2+\frac{45}{23}x+1)$
	$f_{53}(x) = (x-1)^{28}(x^2+x+1)(x^2+\frac{25}{53}x+1)(x^2+\frac{70}{53}x+1)$

are roots of unity, then

$$\Delta_p = \lim_{s\to 1} \frac{F_k(p^{-ks})}{(1-p^{k(1-s)})^\rho}. \tag{17}$$

Let $H_k(x) = \prod(1-p^k\beta_i^k x)$ where $h_p(x) = \prod(1-\beta_i x)$. Then $F_k(x) = (1-p^k x)^\rho H_k(x)$, and (17) becomes

$$\Delta_p = H_k(p^{-k}) = \prod_i(\beta_i^k - 1) = h_p(1)h_p(-1)\prod_{\substack{d|k\\ d>2}}\prod_i \Phi_d(\beta_i)$$

where Φ_d is the dth cyclotomic polynomial. For $d>2$ we claim that $\prod_i \Phi_d(\beta_i)$ is a rational square. By the functional equation we have

$$\beta_1,\dots,\beta_{2m} = \gamma_1,\dots,\gamma_m,\gamma_1^{-1},\dots,\gamma_m^{-1}.$$

Since $d>2$ we have $\Phi_d(x) = x^{\phi(d)}\Phi_d(1/x)$ where $\phi(d)$ is even, say $\phi(d)=2n$. Therefore $\gamma_i^{-n}\Phi_d(\gamma_i) = \gamma_i^n\Phi_d(\gamma_i^{-1})$. It follows that $\prod_{i=1}^m \gamma_i^{-n}\Phi_d(\gamma_i) \in \mathbb{Q}$ and

$$\prod_{i=1}^{2m}\Phi_d(\beta_i) = \prod_{i=1}^{2m}\beta_i^{-n}\Phi_d(\beta_i) = \left(\prod_{i=1}^{m}\gamma_i^{-n}\Phi_d(\gamma_i)\right)^2. \qquad \square$$

Lemma 4.2. *Suppose that $P_1,\dots P_r$ generate a finite index subgroup of $E_p(\overline{\mathbb{F}}_p(T))$. Then we have $\Delta_p \equiv (\prod_t c_t)\operatorname{Reg}(P_1,\dots,P_r) \mod (\mathbb{Q}^\times)^2$ where the product is over*

$t \in \mathbb{P}^1(\overline{\mathbb{F}}_p)$ and c_t is the number of irreducible components of multiplicity one in the fibre of $\overline{X}_p$ above t.

Proof. See [24, Theorem 8.7 and (7.8)]. □

In the calculations below, we sometimes needed to find explicit generators for $E_p(\mathbb{F}_p(T))$. These were found by searching on 2-coverings, computed using 2-descent in Magma, as implemented in the function field case by S. Donnelly.

If $\rho = \rho_p = \rho_q$ for distinct primes p and q, then we have $\Delta_p \equiv \Delta_q \mod (\mathbb{Q}^\times)^2$. As observed by van Luijk [27], this can sometimes be used to improve our upper bound on ρ by 1. This is particularly useful since (assuming the Tate conjecture) ρ_p is always even. Indeed $\rho_p = \deg g_p = b_2 - \deg h_p$, and $\deg h_p$ is even by the functional equation. See [15] and [18] for further examples.

Case $(N,\varepsilon) = (9,1)$. We already know that $\rho = 19$ or 20. Since the Tate conjecture has been proved for elliptic K3-surfaces, equality holds in Lemma 4.1. By Lemma 4.1 we compute $\Delta_5 = 3 \cdot 17$ and $\Delta_7 = 2 \cdot 3$. Since these are different, it follows by the method of van Luijk that $\rho = 19$.

Case $(N,\varepsilon) = (12,1)$. This is identical to the previous example, except that now $\Delta_5 = 1$ and $\Delta_{11} = 7$.

Case $(N,\varepsilon) = (9,2)$. We already know that $\rho = 29$ or 30. Let $p = 7$ or 13. By Lemma 4.1 and (16) we have rank $E_p(\overline{\mathbb{F}}_p(T)) \leq 3$. We prove equality by exhibiting three independent points of infinite order in $E_p(\mathbb{F}_p(T))$. In addition to the reductions of the two points in Table 3, we have when $p = 7$ the point

$$(5T^5 + 6T^4 + 4T^2 + 6T, T^7 + 3T^6 + 6T^3 + 2T^2 + 2T),$$

and when $p = 13$ the point

$$(4T^6 + 8T^5 + 3T^4 + 7T^3 + 5T^2 + 10T + 2, 10T^9 + 4T^8 + 5T^6 + 5T^5 + 12T^3 + 4T^2 + 12).$$

Using either Lemma 4.1 or Lemma 4.2 we find that $\Delta_7 = 2$ and $\Delta_{13} = 17$. Since these are different, it follows that $\rho = 29$.

In the cases $(N,\varepsilon) = (10,1), (10,3), (11,1)$ we aim to show that $\rho = 28$. We were unable[4] to find a prime p with $\rho_p = 28$, despite computing the polynomials $f_p(x)$ for all $p < 150$. This prompted us to try a variant of van Luijk's method, were we use the intersection pairing to improve our upper bound for ρ by 2.

Case $(N,\varepsilon) = (10,1)$. We already know that $\rho = 28$, 29 or 30. In addition to the point $P_1 = (0,0)$ in Table 3 we have when $p = 7$ the points

$$Q_1 = (6T^6 + 6T^4 + 4T^3 + 5T^2, 4T^9 + 6T^8 + 6T^7 + T^6 + T^5 + 3T^4),$$
$$Q_2 = (T^6 + 5T^5 + 6T^4 + 4T^3 + 5T^2, 2T^9 + 6T^8 + 2T^7 + T^6 + 3T^4),$$

[4]There is presumably a systematic reason for this, similar to that described in [3].

and when $p = 17$ the points

$$R_1 = (16T^6 + 13T^5 + 6T^4 + 4T^3 + 12T^2, 4T^9 + 2T^8 + 5T^7 + 8T^5 + 15T^4),$$
$$R_2 = ((6T^8 + 8T^7 + 2T^6 + 5T^5 + 8T^4 + 4T^3 + T^2)/(T + 6)^2, \ \dots).$$

Using either Lemma 4.1 or Lemma 4.2 we find that $\Delta_7 = 1$ and $\Delta_{17} = 2 \cdot 59$. Since these are different, it follows that $\rho \leq 29$.

Reducing mod 7 or 17 does not change the Kodaira symbols of the singular fibres. So by Lemma 4.2 it will be enough for us to work with the height pairing on the Mordell-Weil group, rather than the intersection pairing on the full Néron-Severi group. We compute

$$\mathrm{Reg}(P_1, uQ_1 + vQ_2) = \tfrac{2}{75}(7u^2 - 12uv + 18v^2),$$
$$\mathrm{Reg}(P_1, xR_1 + yR_2) = \tfrac{1}{450}(139x^2 + 76xy + 316y^2).$$

If $\rho = 29$ then the equation $\frac{2}{75}(7u^2 - 12uv + 18v^2) = \frac{1}{450}(139x^2 + 76xy + 316y^2)$ has a solution in rational numbers u, v, x, y not all zero. However this quadratic form of rank 4 is not locally soluble over the 3-adics. Therefore $\rho = 28$.

Case $(N,\varepsilon) = (10,3)$. We already know that $\rho = 28$, 29 or 30. Let $p = 31$ or 37. Since $p \equiv 1 \pmod 3$ the reductions of the points in Tables 3 and 4 give us points $P_1, P_2, P_3, P_4 \in E_p(\mathbb{F}_p(T))$. In addition when $p = 31$ we have

$$Q_1 = (20T^4 + 13T^3 + 30T^2 + 6T, 5T^5 + 4T^4 + 29T^3 + 4T^2 + 5T),$$
$$Q_2 = (7T^6 + 12T^5 + 9T^4 + 19T^2 + 13T + 4)/(T + 29)^2, \ \dots),$$

and when $p = 37$ we have

$$R_1 = (36T^4 + 11T^3 + 4T^2, 26T^5 + 34T^4 + 2T^3 + 15T^2),$$
$$R_2 = (6T^4 + 5T^3 + T^2 + 26T + 32, 29T^5 + 35T^4 + 2T^3 + 15T^2 + 19T + 10).$$

Using either Lemma 4.1 or Lemma 4.2 we find that $\Delta_{31} = 2 \cdot 5$ and $\Delta_{37} = 1$. Therefore $\rho \leq 29$.

As in the previous example, reducing mod 31 or 37 does not change the singular fibres. We compute

$$\mathrm{Reg}(P_1, P_2, P_3, P_4, uQ_1 + vQ_2) = \tfrac{5}{96}(25u^2 - 4uv + 52v^2),$$
$$\mathrm{Reg}(P_1, P_2, P_3, P_4, xR_1 + yR_2) = \tfrac{1}{8}(5x^2 + 8y^2).$$

If $\rho = 29$ then the equation $\frac{5}{96}(25u^2 - 4uv + 52v^2) = \frac{1}{8}(5x^2 + 8y^2)$ has a solution in rational numbers u, v, x, y not all zero. However this quadratic form is not locally soluble over the 3-adics. Therefore $\rho = 28$.

Case $(N,\varepsilon) = (11,1)$. We already know that $\rho = 28$, 29 or 30. Let P_1 and P_2 be the reductions mod p of the points in Table 3. In addition, when $p = 23$ we have

$$Q_1 = (16T^2 + 5T + 5, 21T^3 + 15T^2 + 3T + 18),$$
$$Q_2 = (18T^6 + 5T^5 + 5T^4 + 22T^3 + 9T^2)/(T + 16)^2, \ \dots),$$

and when $p = 53$ we have

$$R_1 = (28T^5 + T^4 + 23T^3 + 40T^2 + 15T, \ \dots),$$
$$R_2 = (49T^6 + 44T^5 + 38T^4)/(T^2 + 42T + 5)^2, \ \dots).$$

Using either Lemma 4.1 or Lemma 4.2 we find that $\Delta_{23} = 2 \cdot 7 \cdot 11 \cdot 13$ and $\Delta_{53} = 11 \cdot 131$. Therefore $\rho \leq 29$.

Again, reducing mod 23 or 53 does not change the singular fibres. We compute

$$\mathrm{Reg}(P_1, P_2, uQ_1 + vQ_2) = \tfrac{11}{480}(57u^2 - 46uv + 137v^2),$$
$$\mathrm{Reg}(P_1, P_2, xR_1 + yR_2) = \tfrac{1}{240}(541x^2 - 228xy + 1196y^2).$$

If $\rho = 29$ then the equation $\frac{11}{480}(57u^2-46uv+137v^2) = \frac{1}{240}(541x^2-228xy+1196y^2)$ has a solution in rational numbers u, v, x, y not all zero. However this quadratic form is not locally soluble over the 11-adics. Therefore $\rho = 28$.

References

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

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

[3] F. Charles, On the Picard number of K3 surfaces over number fields, *Algebra Number Theory* **8** (2014), no. 1, 1–17.

[4] I. Chen, On Siegel's modular curve of level 5 and the class number one problem, *J. Number Theory* **74** (1999), no. 2, 278–297.

[5] Z. Chen, *Congruences of elliptic curves*, PhD thesis, University of Cambridge, 2016. `http://zc231.user.srcf.net/Maths/PhDThesis.pdf`

[6] Z. Chen, Families of elliptic curves with the same mod 8 representation, to appear in *Math. Proc. Cambridge Philos. Soc.*, `https://doi.org/10.1017/S0305004117000354`

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

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

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

[10] T.A. Fisher, On families of 9-congruent elliptic curves, *Acta Arith.* **171** (2015), no. 4, 371–387.

[11] E. Halberstadt, Sur la courbe modulaire $X_{\mathrm{ndép}}(11)$, *Experiment. Math.* **7** (1998), no. 2, 163–174.

[12] E. Halberstadt and A. Kraus, Sur la courbe modulaire $X_E(7)$, *Experiment. Math.* **12** (2003), no. 1, 27–40.
[13] D. Huybrechts, *Lectures on K3 surfaces*, Cambridge Studies in Advanced Mathematics, **158**, Cambridge University Press, Cambridge, 2016.
[14] E. Kani and W. Schanz, Modular diagonal quotient surfaces, *Math. Z.* **227** (1998), no. 2, 337–366.
[15] R. Kloosterman, Elliptic K3 surfaces with geometric Mordell-Weil rank 15, *Canad. Math. Bull.* **50** (2007), no. 2, 215–226.
[16] A. Kumar, Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields, *Res. Math. Sci.* **2** (2015), Art. 24, 46 pages.
[17] R. Miranda, *The basic theory of elliptic surfaces*, Dottorato di Ricerca in Matematica, ETS Editrice, Pisa, 1989.
[18] B. Naskręcki, Mordell-Weil ranks of families of elliptic curves associated to Pythagorean triples, *Acta Arith.* **160** (2013), no. 2, 159–183.
[19] I. Papadopoulos, Courbes elliptiques ayant même 6-torsion qu'une courbe elliptique donnée, *J. Number Theory* **79** (1999), no. 1, 103–114.
[20] 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.
[21] K. Rubin and A. Silverberg, Families of elliptic curves with constant mod p representations, in *Elliptic curves, modular forms & Fermat's last theorem* (Hong Kong, 1993), J. Coates and S.-T. Yau (eds.), Ser. Number Theory I, Int. Press, Cambridge, MA, (1995) 148–161.
[22] K. Rubin and A. Silverberg, Mod 6 representations of elliptic curves, in *Automorphic forms, automorphic representations, and arithmetic* (Fort Worth, TX, 1996), R.S. Doran, Z.-L. Dou and G.T. Gilbert (eds.), Proc. Sympos. Pure Math., **66**, Part 1, Amer. Math. Soc., Providence, RI, (1999), 213–220.
[23] K. Rubin and A. Silverberg, Mod 2 representations of elliptic curves, *Proc. Amer. Math. Soc.* **129** (2001), no. 1, 53–57.
[24] T. Shioda, On the Mordell-Weil lattices, *Comment. Math. Univ. St. Paul.* **39** (1990), no. 2, 211–240.
[25] A. Silverberg, Explicit families of elliptic curves with prescribed mod N representations, in *Modular forms and Fermat's last theorem* (Boston, MA, 1995), G. Cornell, J.H. Silverman and G. Stevens (eds.), Springer-Verlag, New York, (1997), 447–461.
[26] R. van Luijk, An elliptic K3 surface associated to Heron triangles, *J. Number Theory* **123** (2007), no. 1, 92–119.
[27] R. van Luijk, K3 surfaces with Picard number one and infinitely many rational points, *Algebra Number Theory* **1** (2007), no. 1, 1–15.

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK
E-mail address: T.A.Fisher@dpmms.cam.ac.uk