ON PAIRS OF 17-CONGRUENT ELLIPTIC CURVES

T.A. FISHER

Abstract. We compute explicit equations for the surfaces $Z(17,1)$ and $Z(17,3)$ parametrising pairs of 17-congruent elliptic curves. We find that each is a double cover of the same elliptic $K3$-surface. We use these equations to exhibit the first non-trivial example of a pair of symplectically 17-congruent elliptic curves over the rationals. We also compute the corresponding genus 2 curve whose Jacobian has a $(17,17)$-splitting.

1. Introduction

Let p be a prime number. Elliptic curves over the rationals are said to be *p-congruent* if their p-torsion subgroups are isomorphic as Galois modules, and *symplectically* p-congruent if the isomorphism can be chosen to respect the Weil pairing. For example if $\phi : E \to E'$ is an isogeny of degree d, and d is coprime to p, then E and E' are p-congruent, and symplectically p-congruent if d is a quadratic residue mod p. Such congruences, arising from an isogeny, are said to be trivial.

Examples of non-trivial symplectic p-congruences were previously known for all primes $p \le 13$. We exhibit the first such example with $p = 17$. Specifically, the elliptic curves

$$E_1 : \quad y^2 + xy = x^3 - x^2 - 128973503459x + 17827877649739965$$

$$E_2 : \quad y^2 + xy = x^3 - x^2 - 1842012155425437 14x - 341876083324832144918 62380$$

with conductors

$$N(E_1) = 279809270 = 2 \cdot 5 \cdot 13 \cdot 59 \cdot 191^2,$$
$$N(E_2) = 3077901970 = 2 \cdot 5 \cdot 11 \cdot 13 \cdot 59 \cdot 191^2,$$

are symplectically 17-congruent. This claim may be verified using either of the techniques we review in Sections 2 and 3.

A pair of anti-symplectically 17-congruent elliptic curves was previously found by Cremona [B, CF, F1]. These are the elliptic curves

$$E_1' : \quad y^2 + xy = x^3 - 8x + 27$$
$$E_2' : \quad y^2 + xy = x^3 + 8124402x - 11887136703$$

Date: 3rd June 2021.

with conductors

$$N(E_1') = 3675 = 3 \cdot 5^2 \cdot 7^2,$$
$$N(E_2') = 47775 = 3 \cdot 5^2 \cdot 7^2 \cdot 13.$$

In [F3] we completed the proof that for all primes $p \leq 13$ there are infinitely many non-trivial pairs of p-congruent elliptic curves (with infinitely many pairs of j-invariants) both symplectic and anti-symplectic. The Frey-Mazur conjecture predicts that for p sufficiently large, there are no such examples. We suggest the following strong form of their conjecture.

Conjecture 1.1. *Let $p \geq 17$ be a prime. Then any pair of p-congruent elliptic curves over the rationals is either explained by an isogeny, or the elliptic curves are simultaneous quadratic twists of one of the pairs (E_1, E_2) or (E_1', E_2').*

We say that a p-congruence has *power k* if the isomorphism of p-torsion subgroups raises the Weil pairing to the power k. Let $Z(p,k)$ be the surface parametrising all pairs of elliptic curves that are p-congruent with power k, up to simultaneous quadratic twist. This surface comes with an involution ι whose moduli interpretation is that we swap over the two elliptic curves. We write $W(p,k)$ for the quotient of $Z(p,k)$ by ι. These surfaces only depend (up to isomorphism) on whether k is a quadratic residue or a quadratic non-residue mod p. As above, we call these the *symplectic* and *anti-symplectic* cases.

For $p \leq 13$ it is known [F2, F3, Kum] that the surfaces $W(p,k)$ are rational (i.e., birational to $\mathbb{P}^2$) over $\mathbb{Q}$.

Theorem 1.2. *The surfaces $W(17,1)$ and $W(17,3)$ are birational over $\mathbb{Q}$ to the elliptic K3-surface with Weierstrass equation*

$$y^2 + (T+1)(T-2)xy + T^3 y = x^3 - x^2. \tag{1}$$

The surfaces $Z(17,1)$ and $Z(17,3)$ are birational over $\mathbb{Q}$ to the double covers $z^2 = F_1(T,x,y)$ and $z^2 = F_3(T,x,y)$ where F_1 and F_3 are recorded in Appendix A.

Let j_1 and j_2 be the rational functions on $Z(p,k)$ giving the j-invariants of the two elliptic curves. Then $j_1 + j_2$ and $j_1 j_2$ are rational functions on $W(p,k)$. In the cases $(p,k) = (17,1)$ and $(17,3)$ we have also computed these rational functions. The formulae are too complicated to record here, but are available electronically from [F4].

We used these formulae to find the pairs of elliptic curves (E_1, E_2) and (E_1', E_2') specified above. In each case the curves are not isogenous, since for example they do not have the same conductor. The only previous method for finding such examples was to search in tables of elliptic curves with small conductor. (See for example [CF, Section 3] or [BM, Section 4.3].) Accordingly only the second pair was previously known.

Our evidence for Conjecture 1.1 when $p = 17$ is that we searched for further rational points on $Z(17, 1)$ and $Z(17, 3)$, but none of the points we found give rise to new pairs of 17-congruent elliptic curves. Conjecture 1.1 has also been verified by Cremona and Freitas [CF, Theorem 1.3 and Section 3.7] for all pairs of elliptic curves with conductor less than 500 000.

We have no theoretical explanation for our observation that the surfaces $W(17, 1)$ and $W(17, 3)$ are birational. It would of course be interesting to find one. We note that a wealth of information about the complex geometry of the surfaces $Z(n, k)$ was computed by Kani and Schanz [KS]. In particular the surfaces $Z(17, 1)$ and $Z(17, 3)$ are surfaces of general type with geometric genus 10. We do not expect that these surfaces are birational.

In Section 2 we verify the 17-congruences claimed above by comparing traces of Frobenius mod 17. In Section 3 we compute a genus 2 curve whose Jacobian is isogenous to $E_1 \times E_2$, and note that this gives another proof that E_1 and E_2 are 17-congruent. We construct our birational models for $Z(17, 1)$ and $Z(17, 3)$ as quotients of $X(17) \times X(17)$. In Section 4 we give explicit equations for $X(17)$, and in Sections 5 and 6 we compute the quotients in the symplectic and anti-symplectic cases. In the final two sections we describe some of the interesting curves and points that we have so far found on these surfaces.

2. Verification via modularity

In [Ma, p.133] Mazur asked whether there are any non-trivial symplectic n-congruences for any integer $n \geq 7$. The question was answered by Kraus and Oesterlé [KO] who gave the example of the pair of symplectically 7-congruent elliptic curves $152a1$ and $7448e1$. (We use the subsequent labelling of these curves in Cremona's tables.) They also established the following results.

Lemma 2.1. [KO, Proposition 2] *Let p be a prime number. Let E and E' by p-congruent elliptic curves over $\mathbb{Q}$, with minimal discriminants Δ and Δ'. Suppose that E and E' have multiplicative reduction at a prime $\ell \neq p$ and that the exponent $v_\ell(\Delta)$ is coprime to p. Then $v_\ell(\Delta')$ is coprime to p, and the p-congruence is symplectic if and only if the ratio $v_\ell(\Delta)/v_\ell(\Delta')$ is a square mod p.*

Lemma 2.2. [KO, Proposition 4] *Let E and E' be modular elliptic curves over $\mathbb{Q}$ with conductors N and N'. Let S be the set of primes for which one of the curves has split multiplicative reduction, and the other has non-split multiplicative reduction. Let $M = \operatorname{lcm}(N, N') \prod_{\ell \in S} \ell$ and*

$$\mu(M) = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(M)] = \#\mathbb{P}^1(\mathbb{Z}/M\mathbb{Z}) = M \prod_{\ell | M} (1 + \ell^{-1}).$$

Then the following conditions are equivalent.

(i) *The Galois modules $E[p]$ and $E'[p]$ have isomorphic semi-simplifications.*
(ii) $a_\ell(E) \equiv a_\ell(E') \pmod p$ *for all primes* $\ell < \mu(M)/6$ *with* $v_\ell(NN') = 0$*; and* $a_\ell(E)a_\ell(E') \equiv \ell+1 \pmod p$ *for all primes* $\ell < \mu(M)/6$ *with* $v_\ell(NN') = 1$.

Since $X_0(17)$ is a rank 0 elliptic curve, there are only finitely many j-invariants of elliptic curves over $\mathbb{Q}$ admitting a rational 17-isogeny. As noted in [C, Section 3.8], the exceptional j-invariants are $-17^2 \cdot 101^3/2$ and $-17 \cdot 373^3/2^{17}$. Ignoring these two j-invariants, the conclusion of Lemma 2.2(i), when $p = 17$, is that E and E' are 17-congruent.

Example 2.3. Let E_1 and E_2 be the elliptic curves defined in the introduction. For the primes $\ell < 50$ the traces of Frobenius are as follows.

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$a_\ell(E_1)$	−1	0	1	−1	−5	1	2	4	−1	−3	−2	−11	5	−4	−9
$a_\ell(E_2)$	−1	0	1	−1	1	1	2	4	−1	−3	−2	6	−12	−4	−9

In the notation of Lemma 2.2 we have $S = \emptyset$ and $M = N(E_2)$. It takes about three hours[1] to verify that $a_\ell(E_1) \equiv a_\ell(E_2) \pmod{17}$ for all primes $\ell < \mu(M)/6 \approx 1.033 \times 2^{30}$ with $\ell \neq 11$. This shows that E_1 and E_2 are 17-congruent. Since

$$\Delta(E_1) = 2^3 \cdot 5^3 \cdot 13 \cdot 59^2 \cdot 191^3,$$
$$\Delta(E_2) = -2^{14} \cdot 5^{11} \cdot 11^{17} \cdot 13 \cdot 59 \cdot 191^9,$$

it follows by Lemma 2.1 (with $\ell = 2, 5, 13$ or 59) that the congruence is symplectic.

Example 2.4. Let E_1' and E_2' be the elliptic curves defined in the introduction. For the primes $\ell < 50$ the traces of Frobenius are as follows.

ℓ	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$a_\ell(E_1')$	−1	1	0	0	0	−3	2	−1	−2	−8	8	−7	0	8	−10
$a_\ell(E_2')$	−1	1	0	0	0	1	2	−1	−2	9	−9	10	0	8	7

In the notation of Lemma 2.2 we have $S = \emptyset$ and $M = N(E_2')$. It takes a fraction of a second to verify that $a_\ell(E_1) \equiv a_\ell(E_2) \pmod{17}$ for all primes $\ell < \mu(M)/6 = 15680$ with $\ell \neq 13$. This shows that E_1' and E_2' are 17-congruent. Since

$$\Delta(E_1') = -3^5 \cdot 5^2 \cdot 7^2,$$
$$\Delta(E_2') = -3^2 \cdot 5^2 \cdot 7^2 \cdot 13^{17},$$

it follows by Lemma 2.1 (with $\ell = 3$) that the congruence is anti-symplectic.

[1]Running Magma on a single core of the author's desktop.

Remark 2.5. (i) It may be possible to reduce the Sturm bound, and hence the runtime, in Example 2.3 by using a result similar to [St, Theorem 9.21] or by using level lowering. We did not pursue this.
(ii) Methods for determining the symplectic type in situations where Lemma 2.1 does not apply have recently been studied in [CF, FKr].
(iii) The existence of a prime ℓ for which Lemma 2.1 applies, together with the Weil pairing and the fact our elliptic curves do not admit a rational 17-isogeny, is already enough (see [Se, Chapter IV, Section 3.2]) to show that in each case the mod 17 Galois representation is surjective.

3. Verification via genus 2 Jacobians

Let E_1 and E_2 be n-congruent elliptic curves over $\mathbb{Q}$, where the congruence ψ reverses the sign of the Weil pairing. Then the quotient J of $E_1 \times E_2$ by the graph of ψ is a principally polarised abelian surface. It is shown in [FKa, Section 1] that if n is odd and E_1 and E_2 are not isogenous, then J is the Jacobian of a genus 2 curve C defined over $\mathbb{Q}$, and there are degree n morphisms $C \to E_1$ and $C \to E_2$, also defined over $\mathbb{Q}$. For further details of this construction of reducible genus 2 Jacobians, see for example [BHLS, BD, FKa, Kum, Kuh, Sh].

Since -1 is a quadratic residue mod 17, the elliptic curves E_1 and E_2 defined in the introduction are of the form considered in the last paragraph. In this section we compute the corresponding genus 2 curve, and note that this gives another proof that E_1 and E_2 are 17-congruent.

Lemma 3.1. *Let $E_1 = \mathbb{C}/(\mathbb{Z}+\tau_1\mathbb{Z})$ and $E_2 = \mathbb{C}/(\mathbb{Z}+\tau_2\mathbb{Z})$ with $\mathrm{Im}(\tau_1), \mathrm{Im}(\tau_2) > 0$. Let $\psi : E_1[n] \to E_2[n]$ be the isomorphism given by $\frac{1}{n}(r + s\tau_1) \mapsto \frac{1}{n}(r - s\tau_2)$ for $r, s = 0, 1, \ldots, n-1$. (Note the minus sign!) Then the quotient J of $E_1 \times E_2$ by the graph of ψ is represented in the Siegel upper half-space by*

$$\tau = \begin{pmatrix} n\tau_1 & \tau_1 \\ \tau_1 & (\tau_1 + \tau_2)/n \end{pmatrix}.$$

Proof. We have $J \cong \mathbb{C}^2/\Lambda$ where Λ is the lattice spanned by the columns $b_1, \ldots, b_4$ of the matrix

$$\begin{pmatrix} \tau_1 & \tau_1/n & 1/n & 0 \\ 0 & -\tau_2/n & 1/n & -1 \end{pmatrix}.$$

The principal polarisation on J is given by the Hermitian Riemann form

$$H((z_1, z_2), (w_1, w_2)) = n\left(\frac{z_1\overline{w}_1}{\mathrm{Im}(\tau_1)} + \frac{z_2\overline{w}_2}{\mathrm{Im}(\tau_2)}\right),$$

whose imaginary part is given with respect to the basis $b_1, \ldots, b_4$ for Λ by

$$\begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}.$$

We therefore take

$$\tau = (b_3|b_4)^{-1}(b_1|b_2) = \begin{pmatrix} n & 0 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \tau_1 & \tau_1/n \\ 0 & -\tau_2/n \end{pmatrix} = \begin{pmatrix} n\tau_1 & \tau_1 \\ \tau_1 & (\tau_1+\tau_2)/n \end{pmatrix}. \qquad \square$$

The elliptic curves E_1 and E_2 defined in the introduction are represented in the upper half-plane by $\tau_1 \approx 0.1142862335i$ and $\tau_2 \approx 0.5000000000+1.415897663i$. We computed τ in the Siegel upper half-space corresponding to our genus 2 Jacobian by applying Lemma 3.1 (with $n = 17$) to τ_1 and $\tau_2' = (64\tau_2 - 15)/(-17\tau_2 + 4)$. The formula for τ_2' had to be guessed, but since the congruence must respect complex conjugation there were only 8 possibilities to try. We then used the methods described by van Wamelen [W] to compute the Igusa-Clebsch invariants of our genus 2 curve to 300 decimal digits of precision. Recognising these as rational numbers, we next used the method of Mestre [Me] to find a genus 2 curve over $\mathbb{Q}$ with these invariants. Up to quadratic twist, this gave the genus 2 curve C with equation $y^2 = f_1(x)f_2(x)$ where

$$\begin{aligned} f_1(x) &= 196081931x^3 + 1143338037x^2 - 801791940x + 135616700, \\ f_2(x) &= -25996x^3 + 1698260x^2 - 6845267x + 3822078. \end{aligned}$$

We chose this particular quadratic twist since it satisfies $\#\operatorname{Jac}(C)(\mathbb{F}_p) = \#E_1(\mathbb{F}_p) \cdot \#E_2(\mathbb{F}_p)$ for many primes p of good reduction.

To prove that our equation for C is correct (without relying on the numerical approximations in the last paragraph) we also computed the degree 17 morphisms $\phi_1 : C \to E_1$ and $\phi_2 : C \to E_2$. The x-coordinate of ϕ_i is given by $\xi_i(x) = h_i(x)/(f_i(x)g_i(x)^2)$ where g_i and h_i are certain polynomials of degrees 7 and 17. Working mod $p = 101$ we find

$$\begin{aligned} g_1(x) &= 25x^7 + 56x^6 + 31x^5 + 99x^4 + 100x^3 + 42x^2 + 79x + 5, \\ g_2(x) &= 3x^7 + 76x^6 + 44x^5 + 97x^4 + 52x^3 + 38x^2 + 75x + 2, \\ h_1(x) &= 16x^{17} + 6x^{16} + 57x^{15} + 54x^{14} + 94x^{13} + 79x^{12} + 77x^{11} + 55x^{10} \\ &\quad + 74x^9 + 78x^8 + 97x^7 + 79x^6 + 25x^5 + 96x^4 + 98x^3 + 46x^2 + 4x + 99, \\ h_2(x) &= 67x^{17} + 25x^{16} + x^{15} + 22x^{14} + 84x^{13} + 94x^{12} + 93x^{11} + 95x^{10} \\ &\quad + 34x^9 + 40x^8 + 99x^7 + 84x^6 + 43x^5 + 12x^4 + 59x^3 + 13x^2 + 26x + 98. \end{aligned}$$

The full expressions for $g_1, g_2, h_1, h_2 \in \mathbb{Z}[x]$ may be found in [F4]. We do not record these here, since some of the coefficients have nearly 100 decimal digits.

Our method to compute these polynomials was to compute them mod p for many primes p and then use the Chinese remainder theorem. To compute them mod p we looped over all possibilities for the map $C(\mathbb{F}_p) \to E_i(\mathbb{F}_p)$, compatible with the group laws on the Jacobians, and then solved for the rational function ξ_i (with numerator and denominator of degree at most 17) by interpolation.

The y-coordinates of the maps $\phi_i : C \to E_i$ are of course even more complicated to write down. However, a convenient alternative to recording these directly is to note that the invariant differentials on E_1 and E_2 pull back to the following "elliptic differentials" on C:

$$\phi_1^* \left(\frac{dx}{2y + x} \right) = \frac{(273857x - 336364)dx}{y},$$
$$\phi_2^* \left(\frac{dx}{2y + x} \right) = \frac{(2758x + 1630)dx}{y}.$$

Our second proof that E_1 and E_2 are 17-congruent is completed by the next lemma, which we record for convenience, but is essentially well known. Compared to the proof in Section 2, this proof takes a fraction of the computer time, since we only have to check that our formulae for ϕ_1 and ϕ_2 do indeed define morphisms $C \to E_1$ and $C \to E_2$.

Lemma 3.2. *Let C be a genus 2 curve and let p be a prime. Let $\phi_1 : C \to E_1$ and $\phi_2 : C \to E_2$ be morphisms of degree p, where E_1 and E_2 are non-isogenous elliptic curves. Then E_1 and E_2 are p-congruent.*

Proof. Since E_1, E_2 and $J = \operatorname{Jac} C$ are principally polarised abelian varieties, we identify them with their duals without further comment.

The map $\phi_1 : C \to E_1$ induces by pull back a map $E_1 \to J$. This map is injective since otherwise, by [BL, Proposition 11.4.3], ϕ_1 would have to factor via a non-trivial isogeny of elliptic curves, which is not possible by our assumption that ϕ_1 has prime degree. Since E_1 and E_2 are not isogenous, the composite of the maps $E_1 \to J$ and $J \to E_2$ induced by ϕ_1 and ϕ_2 must be the zero map. The same observations apply with the roles of E_1 and E_2 swapped over. The pull back and push forward maps associated to ϕ_1 and ϕ_2 therefore define dual isogenies

$$E_1 \times E_2 \xrightarrow{\widehat{\phi}} J \xrightarrow{\phi} E_1 \times E_2$$

whose composite is multiplication-by-p. In particular $\deg \phi = \deg \widehat{\phi} = p^2$ and there are isomorphisms of Galois modules $E_1[p] \cong J[\phi] \cong E_2[p]$. □

4. The modular curve $X(17)$

Let $\zeta = e^{2\pi i/17}$ and $\xi_k = \zeta^k + \zeta^{-k}$. Let $G \cong \mathrm{PSL}_2(\mathbb{Z}/17\mathbb{Z})$ be the subgroup of $\mathrm{SL}_9(\mathbb{C})$ generated by M_2 and M_{17} where

$$M_2 = \frac{-1}{\sqrt{17}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & \xi_3 & \xi_8 & \xi_7 & \xi_4 & \xi_5 & \xi_2 & \xi_6 & \xi_1 \\ 2 & \xi_8 & \xi_7 & \xi_4 & \xi_5 & \xi_2 & \xi_6 & \xi_1 & \xi_3 \\ 2 & \xi_7 & \xi_4 & \xi_5 & \xi_2 & \xi_6 & \xi_1 & \xi_3 & \xi_8 \\ 2 & \xi_4 & \xi_5 & \xi_2 & \xi_6 & \xi_1 & \xi_3 & \xi_8 & \xi_7 \\ 2 & \xi_5 & \xi_2 & \xi_6 & \xi_1 & \xi_3 & \xi_8 & \xi_7 & \xi_4 \\ 2 & \xi_2 & \xi_6 & \xi_1 & \xi_3 & \xi_8 & \xi_7 & \xi_4 & \xi_5 \\ 2 & \xi_6 & \xi_1 & \xi_3 & \xi_8 & \xi_7 & \xi_4 & \xi_5 & \xi_2 \\ 2 & \xi_1 & \xi_3 & \xi_8 & \xi_7 & \xi_4 & \xi_5 & \xi_2 & \xi_6 \end{pmatrix}$$

and $M_{17} = \mathrm{Diag}(1, \zeta, \zeta^9, \zeta^{13}, \zeta^{15}, \zeta^{16}, \zeta^8, \zeta^4, \zeta^2)$. The pattern of subscripts in the definition of M_2 is the sequence of powers of 3 in $(\mathbb{Z}/17\mathbb{Z})/\{\pm 1\}$.

We write $\mathbb{C}[x_0, \ldots, x_8]_d$ for the space of homogeneous polynomials of degree d. An *invariant* of degree d is a polynomial $I \in \mathbb{C}[x_0, \ldots, x_8]_d$ satisfying $I \circ g = I$ for all $g \in G$. In degrees 2 and 3 the only invariants are

$$\begin{aligned} Q &= x_0^2 + x_1x_5 + x_2x_6 + x_3x_7 + x_4x_8, \\ D &= 2x_0(x_1x_5 - x_2x_6 + x_3x_7 - x_4x_8) \\ &\qquad - x_1^2x_4 + x_2^2x_5 - x_3^2x_6 + x_4^2x_7 - x_5^2x_8 + x_6^2x_1 - x_7^2x_2 + x_8^2x_3. \end{aligned}$$

In degree 4 we have the invariants Q^2 and

$$\begin{aligned} F = {} & x_0^4 + x_0(x_1^2x_4 + x_2^2x_5 + x_3^2x_6 + x_4^2x_7 + x_5^2x_8 + x_1x_6^2 + x_2x_7^2 + x_3x_8^2) \\ & + x_1x_3x_5x_7 + x_2x_4x_6x_8 + x_1x_2x_5x_6 + x_2x_3x_6x_7 + x_3x_4x_7x_8 + x_1x_4x_5x_8 \\ & + x_1^2x_3x_8 + x_1x_2^2x_4 + x_2x_3^2x_5 + x_3x_4^2x_6 + x_4x_5^2x_7 + x_5x_6^2x_8 + x_1x_6x_7^2 + x_2x_7x_8^2. \end{aligned}$$

Proposition 4.1. *Let $C \subset \mathbb{P}^8$ be the curve defined by the vanishing of Q and all partial derivatives of F. Then $C = C_1 \cup C_2$ where C_1 and C_2 are curves of degrees 96 and 168, each isomorphic to the modular curve $X(17)$. The 144 cusps on C_1 are cut out (each with multiplicity 2) by the cubic form D. Moreover D vanishes identically on C_2.*

Proof. Let $p \geq 5$ be a prime. The group $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ acts on $X(p)$ with quotient the j-line, and the group of divisor classes fixed by this group action is an infinite cyclic group, generated by λ of degree $(p^2-1)/24$. Let $m = (p-1)/2$. Klein gave equations for $X(p)$ embedded in $\mathbb{P}^{m-1}$ and $\mathbb{P}^m$ with hyperplane sections $(m-1)\lambda$

and $m\lambda$. Following [AR] we call these models the z-curve and the A-curve. See [AR, Section 24] or [F3, Section 4] for further details.

We take $p = 17$. Let $z_1, \dots, z_8$ be coordinates on $\mathbb{P}^7$. We write $z_0 = 0$, $z_{-i} = -z_i$ and agree to read all subscripts mod 17. According to [F1, Section 2] the z-curve for $X(17)$ is the curve in $\mathbb{P}^7$ defined by the 4 by 4 Pfaffians of the 17 by 17 skew symmetric matrix $(z_{i-j}z_{i+j})$. We define maps $\phi_i : X(17) \to \mathbb{P}^8$ for $i = 1, 2$ by

$$\phi_1 = \left(1 : \frac{z_2}{z_1} : \frac{z_6}{z_3} : \frac{-z_1}{z_8} : \frac{-z_3}{z_7} : \frac{z_8}{z_4} : \frac{-z_7}{z_5} : \frac{z_4}{z_2} : \frac{-z_5}{z_6}\right)$$

and

$$\begin{aligned}\phi_2 = \Bigg(& z_1z_4 + z_2z_8 + z_3z_5 - z_6z_7 - \frac{2z_4z_7z_2}{z_1} \\ & : -z_8^2 - \frac{2z_5z_7z_2}{z_1} : z_7^2 - \frac{2z_2z_4z_6}{z_3} : -z_4^2 + \frac{2z_5z_6z_1}{z_8} : z_5^2 + \frac{2z_1z_2z_3}{z_7} \\ & : -z_2^2 + \frac{2z_3z_6z_8}{z_4} : z_6^2 - \frac{2z_1z_8z_7}{z_5} : -z_1^2 - \frac{2z_3z_7z_4}{z_2} : z_3^2 + \frac{2z_4z_8z_5}{z_6}\Bigg).\end{aligned}$$

Let C_1 and C_2 be the images of ϕ_1 and ϕ_2. We find using Magma [BCP] that Q, the partial derivatives of F, and the quartics $x_0^4 + x_1x_3x_5x_7$ and $x_0^4 + x_2x_4x_6x_8$ vanish on C_1. Likewise, Q, D, and the partial derivatives of F vanish on C_2. These equations are sufficient to define each curve set-theoretically. In fact, the homogeneous ideal of C_1 is generated by one quadratic form, 9 cubic forms and 117 quartic forms, and the homogeneous ideal of C_2 is generated by one quadratic form and 28 cubic forms. To prove the decomposition $C = C_1 \cup C_2$ we checked that $(x_0^4 + x_1x_3x_5x_7)D^2$ and $(x_0^4 + x_2x_4x_6x_8)D^2$ belong to the ideal generated by Q and the partial derivatives of F.

Since Q and F are invariants, the group G acts on C, and hence on C_1 and C_2. It is shown in [AR, Lemma 20.40] that for $p \geq 7$ a prime, the curve $X(p)$ has automorphism group $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. So up to an automorphism of G, the G-actions on C_1 and C_2 correspond to the usual action of $\mathrm{PSL}_2(\mathbb{Z}/17\mathbb{Z})$ on $X(17)$. The points on $X(17)$ above $j = 0, 1728, \infty$ form G-orbits of sizes 816, 1224, 144. All other G-orbits have size $|G| = 2448$. The intersection of C_1 with $\{D = 0\}$ has $3 \times 96 = 288$ points counted with multiplicity. Being preserved by the G-action, it must therefore be the set of cusps, each counted with multiplicity 2. □

Remark 4.2. The formula for ϕ_1 (up to signs and ordering) is that given in [AR, Section 51], and accordingly C_1 is the A-curve. The formula for ϕ_2 was found by using the G-actions to compute a complement to the image of $S^2\mathcal{L}(\zeta)$ in $\mathcal{L}(2\zeta)$, where $\mathcal{L}(\delta)$ denotes the Riemann Roch space of a divisor δ, and $\zeta \sim 7\lambda$ is the hyperplane section for the z-curve.

Definition 4.3. A *covariant* of degree d is a column vector $\mathbf{v}$ of polynomials in $\mathbb{C}[x_0,\ldots,x_8]_d$ satisfying $\mathbf{v}\circ g = g\mathbf{v}$ for all $g\in G$.

Starting from an invariant I of degree d we may construct a covariant of degree $d-1$ as

$$\nabla_Q I = H(Q)^{-1}\begin{pmatrix}\partial I/\partial x_0\\ \vdots \\ \partial I/\partial x_8\end{pmatrix} \tag{2}$$

where $H(Q)$ is the 9 by 9 matrix of second partial derivatives of Q. Going in the other direction, if $\mathbf{v}$ and $\mathbf{w}$ are covariants of degrees d and e then

$$\mathbf{v}\cdot\mathbf{w} := \mathbf{v}^T H(Q)\mathbf{w} = \operatorname{coeff}(Q(\mathbf{v}+t\mathbf{w}),t) \tag{3}$$

is an invariant of degree $d+e$. If we think of a covariant as a G-equivariant polynomial map $\mathbb{C}^9\to\mathbb{C}^9$ then the composition of covariants $\mathbf{v}$ and $\mathbf{w}$ of degrees d and e is a covariant $\mathbf{v}\circ\mathbf{w}$ of degree de.

We put $\mathbf{v}_1=(x_0,\ldots,x_8)^T$, $\mathbf{v}_2=\nabla_Q D$, $\mathbf{v}_3=\nabla_Q F$, $\mathbf{v}_4=\mathbf{v}_2\circ\mathbf{v}_2$ and $\mathbf{v}_6=\mathbf{v}_3\circ\mathbf{v}_2$. Then $c_4=\mathbf{v}_4\cdot\mathbf{v}_6$ is an invariant of degree 10.

Lemma 4.4. *Let $X=X(17)$ be the curve denoted C_1 in Proposition 4.1. Then the j-map $X\to\mathbb{P}^1$ is given by $j=-2^7c_4^3/D^{10}$.*

Proof. The calculation at the end of this proof shows that c_4 does not vanish identically on X. So the intersection of X with $\{c_4=0\}$ is a set of $10\times 96 = 816+144$ points. Arguing as in the proof of Proposition 4.1, this set is the union of the points above $j=0$ and $j=\infty$. Our formula for the j-invariant therefore has the correct divisor, and so is correct up to scaling.

Let $u=(\theta^3-\theta^2-\theta+2i-1)/4$ where $\theta=\sqrt[4]{1-4i}$ and $i=\sqrt{-1}$. Let σ be the generator for $\operatorname{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(i))$ given by $\sigma(\theta)=i\theta$. The point

$$(1:u:\sigma(u):\sigma^2(u):\sigma^3(u):u:\sigma(u):\sigma^2(u):\sigma^3(u))\in X$$

is fixed by a permutation matrix of order 2 in G, and so lies above $j=1728$. The function c_4^3/D^{10} takes the value $-1728/2^7$ at this point. □

5. Computations in the symplectic case

Let $X=X(17)\subset\mathbb{P}^8$ be the curve denoted C_1 in Proposition 4.1. By [F3, Lemma 3.2] the surface $Z(17,1)$ is birational to the quotient of $X\times X\subset\mathbb{P}^8\times\mathbb{P}^8$ by the diagonal action of $G\cong\mathrm{PSL}_2(\mathbb{Z}/17\mathbb{Z})$. We write $x_0,\ldots,x_8$ and $y_0,\ldots,y_8$ for our coordinates on the first and second copies of $\mathbb{P}^8$.

Definition 5.1. A *bi-invariant* of degree (m, n) is a polynomial in $x_0, \ldots, x_8$ and $y_0, \ldots, y_8$, that is homogeneous of degrees m and n in the two sets of variables, and is invariant under the diagonal action of G.

In principle we may find equations for $Z(17, 1)$ by computing generators and relations for the ring of bi-invariants mod $I(X \times X)$. In practice we find it is sufficient to compute only some of the generators and some of the relations.

The calculations that follow rely on showing that certain bi-invariants vanish identically on $X \times X$. Initially we only checked that they vanish at many $\mathbb{F}_p$-points for some moderately large prime p. For a full proof in characteristic 0 we used the G-action and numerical approximations to verify the conditions in the following lemma. This is sufficient since if the absolute value of the norm of an algebraic integer is less than one, then it must be zero.

Lemma 5.2. *Let I be a bihomogeneous form of degree (m, n) with $m, n \leq 22$. If I vanishes at all points $(P, Q) \in X \times X$ with $j(P), j(Q) \in \{0, 1728, \infty\}$ then I vanishes on $X \times X$.*

Proof. This follows from Bezout's theorem, using that $144+816+1224 > 22 \times 96$. The argument is then identical to that used in the proof of [F3, Lemma 6.2]. □

It is easy to compute the dimension of the space of bi-invariants of any given degree from the character table of G. However we need to work with explicit bases for these spaces. Let Q, D and F be the invariants of degrees 2, 3 and 4 defined in Section 4. We define bi-invariants Q_{ij}, D_{ij} and F_{ij} by the rules

$$\begin{aligned} Q(\lambda x_0 + \mu y_0, \ldots, \lambda x_8 + \mu y_8) &= \lambda^2 Q_{20} + \lambda\mu Q_{11} + \mu^2 Q_{02}, \\ D(\lambda x_0 + \mu y_0, \ldots, \lambda x_8 + \mu y_8) &= \lambda^3 D_{30} + \lambda^2\mu D_{21} + \ldots + \mu^3 D_{03}, \\ F(\lambda x_0 + \mu y_0, \ldots, \lambda x_8 + \mu y_8) &= \lambda^4 F_{40} + \lambda^3\mu F_{31} + \ldots + \mu^4 F_{04}. \end{aligned}$$

Then, writing H for the 9 by 9 matrix of second partial derivatives with respect to $x_0, \ldots, x_8$, we put

$$D_x = H(Q)^{-1}H(D_{30}), \;\; D_y = H(Q)^{-1}H(D_{21}), \;\; F_{xy} = H(Q)^{-1}H(F_{31}).$$

The space of bi-invariants of degree $(2, 2)$ has dimension 4, with basis $A_1, \ldots, A_4$ where $A_1 = Q_{20}Q_{02}$, $A_2 = Q_{11}^2$, $A_3 = F_{22}$, and

$$\mathrm{tr}(D_x D_y F_{xy}) = -16A_1 + 8A_2 - 8A_4.$$

Each of these bi-invariants is symmetric (under interchanging the x's and y's), but only the first vanishes identically on $X \times X$.

The space of bi-invariants of degree $(3, 3)$ has dimensional 16. Under interchanging the x's and y's, this breaks up as the direct sum of symmetric and skew-symmetric subspaces of dimensions 14 and 2. The subspace of symmetric bi-invariants has basis $B'_1, \ldots, B'_{14}$ given by

$$\begin{aligned} & Q_{11}A_2,\ Q_{11}A_3,\ Q_{11}A_4,\ D_{30}D_{03},\ D_{21}D_{12},\ \operatorname{tr}(D_x^3 D_y^3),\ \operatorname{tr}(D_x^2 D_y D_x D_y^2), \\ & \operatorname{tr}(D_x^2 D_y^2 F_{xy}),\ \operatorname{tr}(D_x D_y D_x D_y F_{xy}),\ \operatorname{tr}(D_x D_y F_{xy}^2),\ \operatorname{tr}(F_{xy}^3), \\ & Q_{11}A_1,\ Q_{20}F_{13} + Q_{02}F_{31},\ 2\nabla_Q F(x_0, \ldots, x_8) \cdot \nabla_Q F(y_0, \ldots, y_8), \end{aligned}$$

where in the final expression (for B'_{14}) we use the notation (2) and (3).

We changed our choice of basis for this space of bi-invariants first so that the bi-invariants themselves have small integer coefficients, then so that the relations considered below have small integer coefficients, and finally to facilitate writing down an elliptic fibration. To simplify the calculations that follow, we therefore (with the benefit of hindsight) switch to the basis $B_1, \ldots, B_{14}$ that is related to the basis $B'_1, \ldots, B'_{14}$ (as specified in the last paragraph) by the first change of basis matrix recorded in Appendix A. In fact we keep the first and last three basis elements the same, i.e. $B_i = B'_i$ for $i = 1, 2, 3, 12, 13, 14$.

The subspace of bi-invariants vanishing on $X \times X$ is spanned by B_{12}, B_{13}, B_{14}. We write $\mathcal{I}_1 \subset \mathbb{Q}[z_1, \ldots, z_{11}]$ for the ideal generated by all quadratic and cubic forms vanishing on the image of the map

$$X \times X \to \mathbb{P}^{10}; \quad (x_0, \ldots, x_8; y_0, \ldots, y_8) \mapsto (B_1 : \ldots : B_{11}).$$

We find that $\mathcal{I}_1$ is minimally generated by 13 quadratic forms and 21 cubic forms. Moreover the subvariety $\Sigma_1 \subset \mathbb{P}^{10}$ defined by $\mathcal{I}_1$ is a surface of degree 29.

Proposition 5.3. *The surface Σ_1 is birational over $\mathbb{Q}$ to the elliptic surface Σ defined by the Weierstrass equation* (1) *in the statement of Theorem 1.2.*

Proof. The rational map $\Sigma_1 \to \mathbb{P}^3 \times \mathbb{A}^1$ given by

$$(z_1 : \ldots : z_{11}) \mapsto ((z_1 : z_2 : z_3 : z_4), T) = ((z_1 : z_2 : z_3 : z_4), z_5/z_6)$$

has image satisfying

$$\begin{aligned} & 2Tz_1^2 + 3Tz_1z_2 - (5T-2)z_1z_3 - 3T^2z_1z_4 + Tz_2^2 - 4Tz_2z_3 - 2T^2z_2z_4 \\ & \qquad + 2(2T-1)z_3^2 + T(4T-1)z_3z_4 + T^3z_4^2 = 0, \\ & (T+1)^2z_1^2 + T(2T+1)z_1z_2 - (T+1)^2z_1z_3 - T(T+1)^2z_1z_4 + T^2z_2^2 \\ & \qquad - 2T^2z_2z_3 - T^3z_2z_4 = 0. \end{aligned}$$

These same equations define a genus one curve in $\mathbb{P}^3$ over the function field $\mathbb{Q}(T)$. Making the linear change of coordinates

$$\begin{aligned} u_1 &= T(T+1)z_1, & u_3 &= (T+1)z_3, \\ u_2 &= T(z_1 + z_2 - 2z_3 - Tz_4), & u_4 &= T(-z_1 + 2z_3 + Tz_4), \end{aligned}$$

gives the simplified quadric intersection

$$u_1u_2 + u_1u_3 + (T+1)u_2^2 - u_3u_4 = 0,$$
$$u_1u_4 + Tu_2^2 - T^2u_2u_4 - Tu_3u_4 = 0,$$

which in turn is isomorphic to the elliptic curve (1) via

$$x = \frac{-Tu_1}{u_4}, \quad y = \frac{Tu_1(u_1 - u_2 - u_4)}{u_2u_4}.$$

Composing these maps gives a birational map $\Sigma_1 \to \Sigma$. The inverse map, represented as an explicit 11-tuple of elements in the function field $\mathbb{Q}(\Sigma)$, is recorded in the accompanying computer file [F4]. □

Since the rational map $X \times X \to \Sigma$ is defined by symmetric bi-invariants, it factors via a rational map $\pi : W(17,1) \to \Sigma$. We will see below that π is birational, thereby proving the first part of Theorem 1.2.

One way to compute equations for the double cover $Z(17,1) \to W(17,1)$ is to find a skew-symmetric bi-invariant of degree $(3,3)$ that does not vanish identically on $X \times X$, and then write its square, modulo $I(X \times X)$, as a quadratic form in $B_1, \ldots, B_{11}$. We omit the details, since this calculation is superceded by the calculation of the j-maps, which we do next.

We consider the symmetric bi-invariants $\alpha_1 = D_{30}D_{03}$, $\alpha_2 = D_{12}D_{21}$, $\alpha_3 = D_{21}^3D_{03} + D_{12}^3D_{30}$, $\alpha_4 = c_4(x_0, \ldots, x_8)c_4(y_0, \ldots, y_8)$ and

$$\alpha_5 = c_4(x_0, \ldots, x_8)D_{03}^3D_{12} + c_4(y_0, \ldots, y_8)D_{30}^3D_{21},$$

of degrees (m,m) for $m = 3, 3, 6, 10, 11$. Let $S = \mathbb{Q}[u, v, w, z_4, \ldots, z_{11}]$ be the graded polynomial ring where the variables have weights $1, 2, 2, 3, \ldots, 3$. In the accompanying Magma file [F4] we record $g_1, \ldots, g_5 \in S$ of weighted degrees $3, 3, 9, 15, 15$ and $h_1, \ldots, h_5 \in S$ of weighted degrees $0, 0, 3, 5, 4$, such that each of the bi-invariants

$$g_i(Q_{11}, A_3, A_4, B_4, \ldots, B_{11}) - h_i(Q_{11}, A_3, A_4, B_4, \ldots, B_{11})\alpha_i$$

vanishes on $X \times X$. We use these expressions to solve for the α_i as elements of the function field $\mathbb{Q}(\Sigma)$. Then the polynomials $f_1(Y) = Y^2 - \alpha_3 Y + \alpha_1\alpha_2^3$ and $f_2(Y) = Y^2 - \alpha_5 Y + \alpha_1^3\alpha_2\alpha_4$ have roots defined over the same quadratic extension of $\mathbb{Q}(\Sigma)$. Let these roots be r_1, s_1 and r_2, s_2. If we order these roots appropriately then by Lemma 4.4, and the definition of the α_i, we have

$$j_1 + j_2 = \frac{-2^7}{\alpha_1^9}\left(\frac{r_2^3}{r_1} + \frac{s_2^3}{s_1}\right) \qquad \text{and} \qquad j_1j_2 = \frac{2^{14}\alpha_4^3}{\alpha_1^{10}}.$$

Let $\widetilde{\Sigma} \to \Sigma$ be the double cover defined by the requirement that disc f_1, disc f_2, or $(j_1 + j_2)^2 - 4j_1j_2$ is a square. Then the product of j-maps $X \to \mathbb{P}^1$ factors as

$$X \times X \longrightarrow Z(17,1) \longrightarrow \widetilde{\Sigma} \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1. \tag{4}$$

The composite corresponds to a Galois extension of function fields, with Galois group $G \times G$. Since $G \cong \mathrm{PSL}_2(\mathbb{Z}/17\mathbb{Z})$ is a simple group, the diagonal subgroup $\Delta_G \subset G \times G$ is a maximal subgroup. Therefore one of the last two maps in (4) is birational. However if the last map were birational, then this would mean that in attempting to quotient out by Δ_G, we had in fact quotiented out by $G \times G$. To exclude this possibility we may check, for example, that the rational function F_{22}/Q_{11}^2 on $X \times X$ is not $G \times G$-invariant.

In conclusion, $Z(17,1)$ is birational to $\widetilde{\Sigma}$, and $W(17,1)$ is birational to Σ. This completes the proof of Theorem 1.2 in the symplectic case.

Remark 5.4. We initially hoped that we might compute $W(17,1)$ using the bi-invariants of degree $(2,2)$, without needing those of degree $(3,3)$. In hindsight we see that this is not possible, since the map $W(17,1) \to \mathbb{P}^2$ given by $(A_2 : A_3 : A_4)$ is generically 5-to-1. This may be seen by eliminating z_4 from the first quadric intersection in the proof of Proposition 5.3, and noting that the resulting quartic in z_1, z_2, z_3 has degree 5 in T.

6. Computations in the anti-symplectic case

In Section 4 we defined G as the subgroup of $\mathrm{SL}_9(\mathbb{C})$ generated by certain matrices with entries in $\mathbb{Q}(\zeta)$, where ζ is a primitive 17th root of unity. Replacing each matrix entry by its image under the automorphism $\zeta \mapsto \zeta^3$ of $\mathbb{Q}(\zeta)$ defines an outer automorphism $g \mapsto \widetilde{g}$ of G.

Definition 6.1. A *skew bi-invariant* of degree (m,n) is a polynomial in $x_0, \ldots, x_8$ and $y_0, \ldots, y_8$, that is homogeneous of degrees m and n in the two sets of variables, and is invariant under the action of G via $g : (x,y) \mapsto (gx, \widetilde{g}y)$.

Since the map $g \mapsto \widetilde{\widetilde{g}}$ is an inner automorphism of G we see that if f is a skew bi-invariant, then so too is

$$f^\dagger(x_0, \ldots, x_8; y_0, \ldots, y_8) := f(y_0, \ldots, y_8; -x_0, -x_2, -x_3, \ldots, -x_8, -x_1).$$

We have $f^{\dagger\dagger} = f$.

The space of skew bi-invariants of degree $(2,2)$ has basis A_1, A_2, A_3 where $A_1 = Q_{20}Q_{02}$ and

$$\begin{aligned} A_2 = 4x_0^2y_0^2 + \textstyle\sum(&2x_0x_1y_3y_4 + 2x_4x_5y_0y_1 + x_1^2y_1y_7 + x_2x_8y_1^2 + x_1x_2y_2y_5 \\ &+ x_3x_6y_1y_2 + x_1x_3y_5y_8 + x_1x_6y_1y_3 + \tfrac{1}{2}(x_1x_5y_2y_6 + x_3x_7y_1y_5)), \\ A_3 = 4x_0^2y_0^2 + \textstyle\sum(&2x_0x_1y_2y_8 + 2x_1x_3y_0y_1 + x_1^2y_2y_3 + x_3x_4y_1^2 + x_1x_2y_2y_5 \\ &+ x_3x_6y_1y_2 + x_1x_3y_5y_8 + x_1x_6y_1y_3 + \tfrac{1}{2}(x_1x_5y_1y_5 + x_2x_6y_1y_5)). \end{aligned}$$

Here $\sum$ denotes the sum over all simultaneous cyclic permutations of $x_1, \ldots, x_8$ and $y_1, \ldots, y_8$ (fixing x_0 and y_0). We have $A_i^\dagger = A_i$ for $i = 1, 2, 3$.

The space of skew bi-invariants of degree $(3,1)$ is 1-dimensional, spanned by

$$S_{31} = -16x_0^3y_0 + \sum((3x_0x_1x_5 + 3x_1^2x_4)y_0 + (6x_0x_1x_3 + 6x_0x_4x_5 + 3x_2^2x_3 + 3x_1x_4^2 + x_5^3 + 3x_4x_6^2 + 6x_1x_2x_7 + 6x_3x_5x_8 + 6x_6x_7x_8)y_1).$$

We write $S_{13} = S_{31}^\dagger$ for the corresponding skew bi-invariant of degree $(1,3)$.

Earlier we wrote $H(f)$ for the 9 by 9 matrix of second partial derivatives of f with respect to $x_0, \ldots, x_8$. We now write $H = H_{xx}$ and define H_{xy}, H_{yx}, H_{yy} in the analogous way. We further put $\mathcal{H}_{xx}(f) = H(Q)^{-1}H_{xx}(f)$, $\mathcal{H}_{xy}(f) = H(Q)^{-1}H_{xy}(f)$ and so on. The following are skew bi-invariants of degree $(3,3)$.

$$\begin{aligned} P &= 2(Q_{20}S_{13} + Q_{02}S_{31}), \\ \Theta_{ij} &= \operatorname{tr}(\mathcal{H}_{xx}(D_{30})\mathcal{H}_{xy}(A_i)\mathcal{H}_{yy}(D_{03})\mathcal{H}_{yx}(A_j)), \\ \Psi_{ij} &= \operatorname{tr}(\mathcal{H}_{xx}(S_{31})\mathcal{H}_{xy}(A_i)\mathcal{H}_{yx}(A_j)), \\ U_i &= \operatorname{tr}(\mathcal{H}_{xy}(P)\mathcal{H}_{yx}(A_i)), \\ V &= \operatorname{tr}(\mathcal{H}_{xy}(\Theta_{12})\mathcal{H}_{yx}(A_3)). \end{aligned}$$

The space of skew bi-invariants of degree $(3,3)$ has dimension 15. The subspace fixed by the involution $f \mapsto f^\dagger$ has basis $B_1', \ldots, B_{12}'$ given by

$$D_{30}D_{03},\ P,\ \Theta_{12},\ \Theta_{13},\ \Theta_{22},\ \Theta_{23},\ \Theta_{33},\ U_2,\ U_3,\ \Psi_{22} + \Psi_{22}^\dagger, \Psi_{23} + \Psi_{23}^\dagger,\ V.$$

For the calculations that follow we switch (with the benefit of hindsight) to the basis $B_1, \ldots, B_{12}$ that is related to the basis $B_1', \ldots, B_{12}'$ by the second change of basis matrix recorded in Appendix A.

The subspace of bi-invariants vanishing on $X \times X$ has basis B_{11}, B_{12}. We write $\mathcal{I}_3 \subset \mathbb{Q}[z_1, \ldots, z_{10}]$ for the ideal generated by all quadratic and cubic forms vanishing on the image of the map

$$X \times X \to \mathbb{P}^9; \quad (x_0, \ldots, x_8; y_0, \ldots, y_8) \mapsto (B_1 : \ldots : B_{10}).$$

We find that $\mathcal{I}_3$ is minimally generated by 14 quadratic forms and 2 cubic forms. Moreover the variety $\Sigma_3 \subset \mathbb{P}^9$ defined by $\mathcal{I}_3$ is a surface of degree 24.

Proposition 6.2. *The surface Σ_3 is birational over $\mathbb{Q}$ to the elliptic surface Σ defined by the Weierstrass equation* (1) *in the statement of Theorem 1.2.*

Proof. The rational map $\Sigma_3 \to \mathbb{P}^3 \times \mathbb{A}^1$ given by

$$(z_1 : \ldots : z_{10}) \mapsto ((z_1 : z_2 : z_3 : z_4), T) = ((z_1 : z_2 : z_3 : z_4), z_5/z_6)$$

has image satisfying

$$\begin{aligned} z_1^2 - Tz_1z_2 + Tz_1z_3 + Tz_2z_3 - Tz_3^2 + Tz_3z_4 &= 0, \\ z_1z_3 - Tz_2z_3 + 2(T+1)z_1z_4 - (T^2-1)z_2z_4 + (T+1)z_4^2 &= 0. \end{aligned}$$

These same equations define a genus one curve in $\mathbb{P}^3$ over $\mathbb{Q}(T)$. Making the linear change of coordinates

$$u_1 = z_1 - Tz_2, \qquad u_3 = (T+1)z_3,$$
$$u_2 = (T+2)z_1 + z_2 - (T+1)(z_3 - z_4), \qquad u_4 = (T+1)z_4$$

gives the simplified quadric intersection

$$u_1^2 + Tu_1u_2 + Tu_2u_3 - Tu_1u_4 = 0,$$
$$u_1u_3 + Tu_1u_4 + u_2u_4 + u_3u_4 = 0,$$

which in turn is isomorphic to the elliptic curve (1) via

$$x = \frac{T(u_1 + Tu_2)}{u_4}, \quad y = \frac{T(u_1 + Tu_2)^2}{u_1u_4}.$$

Composing these maps gives a birational map $\Sigma_3 \to \Sigma$. The inverse map, represented as an explicit 10-tuple of elements in the function field $\mathbb{Q}(\Sigma)$, is recorded in the accompanying computer file [F4]. □

Since the B_i are skew bi-invariants satisfying $B_i^\dagger = B_i$, the rational map $X \times X \to \Sigma$ factors via a rational map $\pi : W(17,3) \to \Sigma$. We will see below that π is birational, thereby proving the first part of Theorem 1.2.

For the purpose of computing the j-maps we decided to work with the skew bi-invariants of degree $(2,2)$, alongside those of degree $(3,3)$. We consider the map from $X \times X$ to the weighted projective space $\mathbb{P}(2,2,3,\ldots,3)$ given by

$$(v, w, z_1, \ldots, z_{10}) = (A_2, A_3, B_1, \ldots, B_{10}).$$

Among the equations defining the image of this map we found the relations

$$vz_5z_{10} - w(z_1z_5 - z_3z_5 + z_1z_6 - z_5z_8 + z_5z_9) = 0,$$
$$vw^2z_7 - (z_2 - z_3 - z_5)(z_6 - z_7)z_{10} + z_5z_8z_{10} = 0.$$

We used these relations to extend our map $\Sigma \to \mathbb{P}^9$ to a map $\Sigma \to \mathbb{P}(2,2,3,\ldots,3)$.

The space of skew bi-invariants of degree $(3,2)$ has dimension 5. We picked one of these skew bi-invariants, not vanishing on $X \times X$, and called it T_{32}. We also put $T_{23} = T_{32}^\dagger$. We define skew bi-invariants $\alpha_1 = D_{30}D_{03}$, $\alpha_2 = S_{31}S_{13}$, $\alpha_3 = T_{32}T_{23}$, $\alpha_4 = D_{03}S_{31}T_{32} + D_{30}S_{13}T_{23}$, $\alpha_5 = S_{31}T_{23}^2 + S_{13}T_{32}^2$,

$$\alpha_6 = c_4(x_0, \ldots, x_8)c_4(y_0, \ldots, y_8),$$
$$\alpha_7 = D_{03}^3T_{23}c_4(x_0, \ldots, x_8) + D_{30}^3T_{32}c_4(y_0, \ldots, y_8),$$

of degrees (m,m) for $m = 3,4,5,6,7,10,12$. Let $S = \mathbb{Q}[v, w, z_1, \ldots, z_{10}]$ be the coordinate ring of $\mathbb{P}(2,2,3,\ldots,3)$, i.e., the graded polynomial ring where the variables have these weights. In the accompanying Magma file [F4], we record

$g_1, \ldots, g_7 \in S$ of weighted degrees $3, 6, 8, 8, 12, 18, 18$, and $h_1, \ldots, h_7 \in S$ of weighted degrees $0, 2, 3, 2, 5, 8, 6$, such that each of the skew bi-invariants

$$g_i(A_2, A_3, B_1, \ldots, B_{10}) - h_i(A_2, A_3, B_1, \ldots, B_{10})\alpha_i$$

vanishes on $X \times X$. We use these expressions to solve for the α_i as elements of the function field $\mathbb{Q}(\Sigma)$. Then the polynomials

$$\begin{aligned} f_1(Y) &= Y^2 - \alpha_4 Y + \alpha_1\alpha_2\alpha_3, \\ f_2(Y) &= Y^2 - \alpha_5 Y + \alpha_2\alpha_3^2, \\ f_3(Y) &= Y^2 - \alpha_7 Y + \alpha_1^3\alpha_3\alpha_6, \end{aligned}$$

have roots defined over the same quadratic extension of $\mathbb{Q}(\Sigma)$. Let f_i have roots r_i, s_i. If we order these roots appropriately then by Lemma 4.4, and the definition of the α_i, we have

$$j_1 + j_2 = \frac{-2^7\alpha_2}{\alpha_1^9}\left(\frac{r_3^3}{r_1 r_2} + \frac{s_3^3}{s_1 s_2}\right) \quad \text{and} \quad j_1 j_2 = \frac{2^{14}\alpha_6^3}{\alpha_1^{10}}.$$

Let $\widetilde{\Sigma} \to \Sigma$ be the double cover defined by the requirement that $\operatorname{disc} f_1$, $\operatorname{disc} f_2$, $\operatorname{disc} f_3$ or $(j_1 + j_2)^2 - 4j_1 j_2$ is a square. Then the product of j-maps $X \to \mathbb{P}^1$ factors as

$$X \times X \longrightarrow Z(17,3) \longrightarrow \widetilde{\Sigma} \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1.$$

Exactly as in Section 5 it follows that $Z(17,3)$ is birational to $\widetilde{\Sigma}$ and $W(17,3)$ is birational to Σ. This completes the proof of Theorem 1.2 in the anti-symplectic case.

Remark 6.3. The elliptic $K3$-surface (1) admits many different elliptic fibrations. The fibrations we initially found on $W(17,1)$ and $W(17,3)$ were different, and it was only after we discovered that these surfaces are birational that we adjusted the calculations in this section so as to find the same elliptic fibration.

7. Some modular curves

Let $m \geq 2$ be an integer coprime to 17. Then any pair of m-isogenous elliptic curves are 17-congruent with power k, where $k = 1$ if m is a quadratic residue mod 17, and $k = 3$ otherwise. There is therefore a copy of the modular curve $X_0(m)$ on the surface $Z(17,k)$. In Table 1 we explicitly identify these curves in all cases where $X_0(m)$ has genus 0 or 1. The polynomials F_1 and F_3 are those appearing in the statement of Theorem 1.2, and explicitly recorded in Appendix A.

Table 1. Copies of $X_0(m)$ on $Z(17,1)$ and $Z(17,3)$

m	Formula specifying a curve on (a blow up of) $z^2 = F_k(T,x,y)$
2	$F_1(-2+\varepsilon, -4+8\varepsilon-5\varepsilon^2+\varepsilon^3+t\varepsilon^4, 4+O(\varepsilon)) = 2^{18}(8t+1)\varepsilon^4+O(\varepsilon^5)$
3	$F_3(-1/2+\varepsilon, 1/2-\varepsilon+t\varepsilon^3, 1/4+O(\varepsilon^2)) = -2^{-20}(27t-16)\varepsilon^4+O(\varepsilon^5)$
4	$F_1(1+\varepsilon, -t\varepsilon^2, -1+O(\varepsilon)) = 2^4(32t+1)\varepsilon^2+O(\varepsilon^3)$
5	$F_3(-2+\varepsilon, 2-\varepsilon+t\varepsilon^2, 2+O(\varepsilon)) = -2^{12}3^4(t^2-11t-1)\varepsilon^4+O(\varepsilon^5)$
6	$F_3(-1+\varepsilon, 1-2\varepsilon+t\varepsilon^2, 2\varepsilon+O(\varepsilon^2)) = (t^2-36t+36)\varepsilon^{10}+O(\varepsilon^{11})$
7	$F_3(t\varepsilon^{-2}, t\varepsilon^{-3}, \varepsilon^{-2}+O(\varepsilon^{-1})) = t^{22}(t+1)(t-27)\varepsilon^{-48}+O(\varepsilon^{-47})$
8	$F_1(\varepsilon, \varepsilon^2+\varepsilon^3+8t\varepsilon^4, \varepsilon^2+2\varepsilon^3+O(\varepsilon^4)) = 2^4(t^2+6t+1)\varepsilon^{18}+O(\varepsilon^{19})$
9	$F_1(\varepsilon^{-1}, \varepsilon^{-3}+t\varepsilon^{-1}, O(\varepsilon^{-4})) = (t^2+20t-8)\varepsilon^{-24}+O(\varepsilon^{-23})$
10	$F_3((t+1)\varepsilon^2, t^{-1}(t+1)^3\varepsilon^4, t^{-1}(t+1)^3(\varepsilon^4+\varepsilon^5)+O(\varepsilon^6))$ $= t^{-4}(t+1)^{16}(t^2+18t+1)\varepsilon^{32}+O(\varepsilon^{33})$
11	$F_3(\varepsilon^2-\varepsilon^3, \varepsilon^3+\varepsilon^4+(t-1)\varepsilon^5, \varepsilon^3+2\varepsilon^4+O(\varepsilon^5))$ $= t(t^3+20t^2+56t+44)\varepsilon^{36}+O(\varepsilon^{37})$
12	$F_3(\varepsilon^{-1}, -\varepsilon^{-1}-(t+1), t\varepsilon^{-2}+O(\varepsilon^{-1})) = (t^2-14t+1)\varepsilon^{-24}+O(\varepsilon^{-23})$
13	$F_1(-t\varepsilon^{-1}, (t+1)\varepsilon^{-1}, t^{-2}(t+1)^3+O(\varepsilon)) = t^{16}(t^2+12t-16)\varepsilon^{-20}+O(\varepsilon^{-19})$
14	$F_3(\varepsilon^{-1}, -t\varepsilon^{-3}, t\varepsilon^{-5}+O(\varepsilon^{-4})) = t^2(t+1)^4(t^4-14t^3+19t^2-14t+1)\varepsilon^{-30}+O(\varepsilon^{-29})$
15	$F_1(\varepsilon^{-1}, t\varepsilon^{-2}, -t\varepsilon^{-4}+O(\varepsilon^{-3})) = t^2(t-1)^2(t^2-t-1)(t^2+11t-1)\varepsilon^{-24}+O(\varepsilon^{-23})$
16	$F_1(-1+\varepsilon, t\varepsilon, 1+O(\varepsilon)) = (t^2-12t+4)\varepsilon^4+O(\varepsilon^5)$
18	$F_1(t, -t, -t(t+1)) = t^{16}(t+1)^2(t^2+10t+1)$
19	$F_1(-1+2\varepsilon, (t+4)\varepsilon, (t+4)^2\varepsilon^2+O(\varepsilon^3)) = -8(t+3)(t^3-2t+2)\varepsilon^4+O(\varepsilon^5)$
20	$F_3(-\varepsilon+t^2\varepsilon^2, \varepsilon-t\varepsilon^2, \varepsilon-\varepsilon^2+O(\varepsilon^3)) = (t^4+8t^3-2t^2+8t+1)\varepsilon^{12}+O(\varepsilon^{13})$
21	$F_1(-\varepsilon, t(t+1)\varepsilon^3, (t+1)^2\varepsilon^3+O(\varepsilon^4)) = (t^4+6t^3-17t^2+6t+1)\varepsilon^{16}+O(\varepsilon^{17})$
24	$F_3(t,1,0) = (t+1)^8(t^3+t^2-1)^4(t^4-8t^3+2t^2+8t+1)$
25	$F_1(t, t^2, t^2) = -t^{18}(t+1)^4(16t^2+4t-1)$
27	$F_3(t, t^2(t+1), t^2(t+1)^2) = -t^{18}(t^2+2t+2)^4(t-1)(11t^3+15t^2+9t+1)$
32	$F_1(t, t^2(t+1), -t^2(t^3+t^2-1))$ $= t^{16}(t+1)^4(t^2+t+1)^4(t^4+8t^3+12t^2+16t+4)$
36	$F_1(t, (t+1)(t^2+t+1), (t+1)^2(t^2+2t+2))$ $= (t+1)^4(t^3+t^2+2t+1)^2(t^3+2t^2+3t+1)^4(4t^4+8t^3+12t^2+8t+1)$
49	$F_1(t, t(t^2-1), -t(t^2-1)^2) = t^{20}(t+1)^4(t^2-t-1)^2(t^4+6t^3+3t^2-18t-19)$

In compiling Table 1 we used the `SmallModularCurve` database in Magma [BCP] to check the moduli interpretations. For example, the entry with $m = 18$ shows that $Z(17, 1)$ contains a curve isomorphic to $y^2 = t^2 + 10t + 1$. We parametrise this curve by putting $t = -T/((T + 2)(T + 3))$, and find, using our expressions for $j_1 + j_2$ and $j_1 j_2$ as rational functions on $W(17, 1)$, that

$$X^2 - (j_1 + j_2)X + j_1 j_2 = \big(X - j_{18}(T)\big)\big(X - j_{18}(6/T)\big)$$

where

$$j_{18}(T) = \frac{((T+2)^{12} - 8(T+2)^9 + 16(T+2)^3 + 16)^3}{(T+2)^9((T+2)^3 - 8)((T+2)^3 + 1)^2}$$

is the j-map on $X_0(18)$.

To find most of these curves it was necessary to blow up the surfaces in Theorem 1.2. In such cases we specify the arguments T, x, y of F_k as power series in ε, given to sufficient precision to determine a unique solution of (1). For example, the entry with $m = 20$ shows that blowing up our model for $Z(17, 3)$ above $(T, x, y) = (0, 0, 0)$ we found a curve isomorphic to $y^2 = t^4 + 8t^3 - 2t^2 + 8t + 1$. Putting this elliptic curve in Weierstrass form we find it has Cremona label $20a1$, and in particular is isomorphic to $X_0(20)$.

8. Examples and further questions

We restate Conjecture 1.1 in the case $p = 17$. As usual we say a p-congruence is trivial if it is explained by an isogeny of degree coprime to p.

Conjecture 8.1. (i) *The only non-trivial pairs of symplectically* 17*-congruent elliptic curves over* $\mathbb{Q}$ *are the simultaneous quadratic twists of the elliptic curves* E_1 *and* E_2 *(with conductors* 279809270 *and* 3077901970*) as defined in the introduction.*

(ii) *The only non-trivial pairs of anti-symplectically* 17*-congruent elliptic curves over* $\mathbb{Q}$ *are the simultaneous quadratic twists of the elliptic curves* E_1' *and* E_2' *(with conductors* 3675 *and* 47775*) as defined in the introduction.*

We make a related conjecture.

Conjecture 8.2. *Let* $\widetilde{Z}(17, k)$ *be the surface in* $\mathbb{A}^4$ *with equations*

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

and $z^2 = F_k(T, x, y)$ *where* F_k *is as recorded in Appendix A.*

(i) *The only* $\mathbb{Q}$*-points on* $\widetilde{Z}(17, 1)$ *lie above one of the curves*

$$(x, y) = (0, -T^3), (-T, -T^2 - T), (-T, -T), (T^2, T^2), (T^2, -T^4 + T^2),$$
$$(T^3 + T^2, T^4 + 2T^3 + T^2), (T^3 - T, T^4 - T^2 - T),$$

or the curve $T = 0$*, or one of the points in Table 2.*

(ii) *The only* $\mathbb{Q}$*-points on* $\widetilde{Z}(17,3)$ *lie above one of the curves*

$$(x,y) = (-T,-T), (-T,-T^2-T), (T^2,-T^4+T^2), \\ (T^3+T^2,-T^5-T^4+T^2),$$

or the curve $T=0$*, or one of the points in Table 2.*

The points on $\widetilde{Z}(17,k)$ lying above one of the curves listed in Conjecture 8.2 do not correspond to non-trivial pairs of 17-congruent elliptic curves, either because there is an m-isogeny (with $m=18$ or 25), or the j-maps have a pole, or the point is spurious since F_k vanishes to even multiplicity.

It should be possible to prove that Conjectures 8.1 and 8.2 are equivalent by computing biregular (not just birational) models for $Z(17,1)$ and $Z(17,3)$. This belief is based on the fact that in compiling Table 1 we carried out some of the necessary blow ups, but did not find any new examples of 17-congruences. Nonetheless we leave the full verification to future work.

The height of a rational number $x = a/b$ (where a, b are coprime integers) is $H(x) = \max(|a|,|b|)$. Our evidence for Conjecture 8.2 is that we found no further points with $H(T) \le 3000$ and $H(x) \le 10000$. We see little hope of proving this conjecture using existing methods. A possibly more tractable problem, the answer to which would still be interesting, would be to determine all curves of genus 0 or 1 on these surfaces (either over $\mathbb{Q}$ or over $\overline{\mathbb{Q}}$).

In Table 2 we list elliptic curves via their Cremona labels [C], writing instead the conductor followed by a star for curves beyond the range of Cremona's tables. The latter convention is only needed for the first entry, where the relevant elliptic curves are the ones defined in the introduction. The first column records whether the congruence is symplectic ($k=1$) or anti-symplectic ($k=3$). The final column records the degree of the isogeny when the curves are isogenous. Each pair of elliptic curves we list is only determined up to simultaneous quadratic twist.

TABLE 2. Some rational points on $Z(17,1)$ and $Z(17,3)$

k	T	x	y	17-congruent ell. curves	degree
1	$1/3$	$-2/75$	$-11/125$	279809270∗, 3077901970∗	–
1	-3	-27	108	1849a1, 1849a2	43
1	$-5/6$	$-5/24$	$5/16$	4489a1, 4489a2	67
3	1	2	4	27a2, 27a4	27
3	$9/7$	$27/49$	$-54/49$	3675b1, 47775b1	–
3	$-5/14$	$125/392$	$375/1568$	1225h1, 1225h2	37
3	$11/39$	$1771/6591$	$116380/257049$	26569a1, 26569a2	163

Appendix A. Formulae

We record the polynomials $F_1(T,x,y)$ and $F_3(T,x,y)$ in Theorem 1.2. These define the double covers $Z(17,1) \to W(17,1)$ and $Z(17,3) \to W(17,3)$.

$$
\begin{aligned}
F_1(T,x,y) &= x^{10} - 2T(T-1)x^8y + T(T^3-2T^2-11T+4)x^9 \\
&- T^2(T^4-3T^3-3T^2+3T-10)x^7y + T^2(8T^4+58T^3+15T^2-64T+5)x^8 \\
&- T^3(8T^5+51T^4+80T^3+51T^2-2T-20)x^6y - 2T^4(16T^4-41T^3-205T^2 \\
&- 97T+71)x^7 + 2T^4(16T^6+49T^5-13T^4-142T^3-113T^2-T+10)x^5y \\
&- T^4(149T^6+576T^5+180T^4-956T^3-579T^2+148T+5)x^6 - 2T^5(13T^7 \\
&- 39T^6-229T^5-202T^4+126T^3+169T^2+9T-5)x^4y + T^5(80T^8+318T^7 \\
&- 192T^6-1800T^5-1376T^4+819T^3+750T^2-67T-4)x^5 - T^6(T+1)(24T^7 \\
&+ 156T^6-24T^5-558T^4-285T^3+192T^2+21T-2)x^3y - T^6(16T^{10}+72T^9 \\
&- 239T^8-1300T^7-870T^6+1952T^5+2295T^4+18T^3-449T^2+4T+1)x^4 \\
&+ T^8(T+1)^2(12T^6-50T^5-226T^4+36T^3+292T^2-31T-6)x^2y \\
&- T^8(T+1)(76T^8+273T^7-275T^6-1505T^5-631T^4+1016T^3+472T^2 \\
&- 94T-4)x^3 - T^{10}(T+1)^3(T^5-14T^4+55T^3+118T^2-68T-4)xy \\
&- T^{10}(T+1)^2(131T^6+328T^5-234T^4-700T^3-18T^2+138T+3)x^2 \\
&- T^{13}(T+1)^4(T^2-2T+28)y - 2T^{13}(T+1)^3(49T^3+63T^2-63T-27)x \\
&- 27T^{16}(T+1)^4.
\end{aligned}
$$

$$
\begin{aligned}
F_3(T,x,y) &= x^{10} - 14Tx^8y - T(4T^2-71T-16)x^9 + T^2(17T^2-89T-18)x^7y \\
&- T^2(14T^4+288T^3+165T^2-220T-19)x^8 + T^3(76T^4+480T^3+545T^2 \\
&- 176T-4)x^6y + T^3(94T^6+513T^5+234T^4-1412T^3-732T^2+242T+4)x^7 \\
&- T^5(163T^5+837T^4+1320T^3-72T^2-898T+106)x^5y - T^5(159T^7+590T^6 \\
&- 103T^5-3276T^4-3150T^3+1326T^2+820T-112)x^6 + T^6(80T^7+418T^6 \\
&+ 501T^5-936T^4-2496T^3-948T^2+390T-4)x^4y + T^6(98T^9+386T^8 \\
&- 350T^7-3439T^6-3894T^5+3010T^4+4872T^3-306T^2-284T+4)x^5 \\
&+ T^8(4T^8+130T^7+917T^6+2787T^5+4078T^4+2292T^3-482T^2-480T \\
&- 60)x^3y - T^8(27T^{10}+122T^9-177T^8-1496T^7-987T^6+5032T^5+8446T^4 \\
&+ 1124T^3-2621T^2+54T-61)x^4 - T^{10}(10T^9+132T^8+738T^7+2126T^6 \\
&+ 3179T^5+1902T^4-718T^3-1376T^2-482T-256)x^2y + T^{10}(T^{10}-48T^9
\end{aligned}
$$

$$
\begin{aligned}
&- 122T^8 + 882T^7 + 4304T^6 + 6244T^5 + 973T^4 - 4506T^3 - 1714T^2 + 428T \\
&- 242)x^3 - T^{12}(T^{10} - T^9 - 70T^8 - 368T^7 - 814T^6 - 714T^5 + 237T^4 + 963T^3 \\
&+ 800T^2 + 522T + 312)xy - T^{12}(26T^9 + 283T^8 + 1018T^7 + 1256T^6 - 810T^5 \\
&- 3237T^4 - 1848T^3 + 648T^2 + 108T - 265)x^2 - T^{14}(T + 2)(T^8 + 12T^7 + 44T^6 \\
&+ 74T^5 + 64T^4 + 20T^3 - 43T^2 - 92T - 60)y - 2T^{14}(10T^8 + 94T^7 + 323T^6 \\
&+ 471T^5 + 129T^4 - 367T^3 - 263T^2 + 69T + 36)x + T^{16}(T^8 + 4T^7 - 8T^6 \\
&- 66T^5 - 120T^4 - 56T^3 + 53T^2 + 36T - 16).
\end{aligned}
$$

We also record the change of basis matrices we used in Sections 5 and 6. In each case the rows of the matrix give the B_i' in terms of the B_i.

$$
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-24 & -12 & 28 & 8 & -4 & 0 & 4 & 4 & 0 & -4 & 4 & 0 & 0 & 0 \\
-34 & -15 & 34 & 7 & -8 & -3 & 0 & 5 & -2 & -9 & 7 & 0 & -1 & 0 \\
-480 & -288 & 320 & 160 & -64 & -32 & 192 & 160 & 0 & -96 & 96 & 512 & -96 & 0 \\
248 & 144 & -96 & -144 & 0 & -16 & -192 & -144 & -32 & 48 & 16 & 448 & -48 & 16 \\
-24 & -56 & -128 & -40 & 0 & -24 & 32 & 56 & -16 & -24 & -8 & -32 & -40 & 8 \\
-384 & -144 & 688 & 96 & -64 & 0 & 32 & -48 & -16 & 0 & 128 & -64 & 0 & 8 \\
328 & 204 & -240 & -76 & 32 & 4 & -144 & -92 & 8 & 36 & -20 & 24 & 20 & -12 \\
-366 & -180 & 96 & 72 & -48 & 12 & 192 & 168 & -12 & -48 & -84 & 36 & 0 & 36 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
$$

$$
\begin{pmatrix}
-4 & -12 & 8 & -4 & -8 & -8 & 0 & -4 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\
-56 & -176 & 148 & -68 & -160 & -140 & 36 & -52 & 24 & 24 & -8 & 4 \\
-104 & -240 & 156 & -76 & -128 & -164 & 12 & -92 & 8 & 8 & 8 & 4 \\
-16 & -128 & 124 & -36 & -144 & -92 & 12 & -36 & 8 & 8 & 8 & 12 \\
-40 & -48 & 48 & -24 & -32 & -40 & 48 & -24 & 32 & 32 & 0 & 16 \\
-64 & -176 & 132 & -60 & -128 & -148 & 4 & -76 & -8 & -8 & 24 & -12 \\
-36 & -72 & 96 & -96 & 12 & 24 & -36 & -12 & 0 & 24 & 24 & -12 \\
-60 & -48 & 48 & -24 & -12 & -48 & 60 & -60 & 48 & 48 & 72 & 24 \\
36 & 72 & -72 & 24 & 60 & 24 & -60 & 12 & -72 & -72 & 24 & -48 \\
-72 & -84 & 108 & -48 & 0 & 24 & -12 & -24 & 12 & 24 & 0 & 12 \\
-208 & 204 & -72 & 28 & 364 & 116 & 288 & -44 & 208 & 224 & 32 & 104
\end{pmatrix}
$$

References

[AR] A. Adler and S. Ramanan, *Moduli of abelian varieties*, Lecture Notes in Mathematics, **1644**, Springer-Verlag, Berlin, 1996.

[BM] A.J. Best, B. Matschke, Elliptic curves with good reduction outside of the first six primes, preprint, 2020, `arXiv:2007.10535[math.NT]`

[B] N. Billerey, On some remarkable congruences between two elliptic curves, preprint, 2016, `arXiv:1605.09205[math.NT]`

[BL] C. Birkenhake and H. Lange, *Complex abelian varieties*, Second edition, Springer-Verlag, Berlin, 2004.

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

[BHLS] R. Bröker, E.W. Howe, K.E. Lauter and P. Stevenhagen, Genus-2 curves and Jacobians with a given number of points, *LMS J. Comput. Math.* **18** (2015), no. 1, 170–197.

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

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

[CF] J.E. Cremona and N. Freitas, Global methods for the symplectic type of congruences between elliptic curves, to appear in a *Revista Matemática Ibroamericana*, `arXiv:1910.12290[math.NT]`

[F1] T.A. Fisher, On families of 7- and 11-congruent elliptic curves, *LMS J. Comput. Math.* **17** (2014), no. 1, 536–564.

[F2] T.A. Fisher, Explicit moduli spaces for congruences of elliptic curves, *Math. Z.* **295** (2020), no. 3-4, 1337–1354.

[F3] T.A. Fisher, On families of 13-congruent elliptic curves, preprint, 2019, `arXiv:1912.10777[math.NT]`

[F4] T.A. Fisher, On pairs of 17-congruent elliptic curves, *Magma files accompany this article*, `https://www.dpmms.cam.ac.uk/~taf1000/papers/congr17.html`

[FKr] N. Freitas and A. Kraus, On the symplectic type of isomorphisms of the p-torsion of elliptic curves, to appear in *Memoirs of AMS*, `arXiv:1607.01218[math.NT]`

[FKa] G. Frey and E. Kani, Curves of genus 2 covering elliptic curves and an arithmetical application, *Arithmetic algebraic geometry* (Texel, 1989), G. van der Geer, F. Oort and J. Steenbrink (eds.), Progr. Math., **89**, Birkhäuser Boston, Boston, MA, 1991, 153–176.

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

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

[Kuh] R.M. Kuhn, Curves of genus 2 with split Jacobian, *Trans. Amer. Math. Soc.* **307** (1988), no. 1, 41–49.

[Kum] A. Kumar, Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields, *Res. Math. Sci.* **2** (2015), Art. 24.

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

[Me] J.-F. Mestre, Construction de courbes de genre 2 à partir de leurs modules, *Effective methods in algebraic geometry*, T. Mora and C. Traverso (eds.), Progr. Math., **94**, Birkhäuser Boston, Boston, MA, 1991, 313–334.

[Se] J.-P. Serre, Abelian ℓ-adic representations and elliptic curves, McGill University lecture notes, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Sh] T. Shaska, Curves of genus 2 with (N, N) decomposable Jacobians, *J. Symbolic Comput.* **31** (2001), no. 5, 603–617.

[St] W. Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics, **79**, American Mathematical Society, Providence, RI, 2007.

[W] P.B. van Wamelen, Computing with the analytic Jacobian of a genus 2 curve, *Discovering mathematics with Magma*, W. Bosma and J. Cannon (eds.), Algorithms Comput. Math., **19**, Springer, Berlin, 2006, 117–135.

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

Email address: T.A.Fisher@dpmms.cam.ac.uk