ON FAMILIES OF 13-CONGRUENT ELLIPTIC CURVES

T.A. FISHER

Abstract. We compute twists of the modular curve $X(13)$ that parametrise the elliptic curves 13-congruent to a given elliptic curve. Searching for rational points on these twists enables us to find non-trivial pairs of 13-congruent elliptic curves over $\mathbb{Q}$, i.e. pairs of non-isogenous elliptic curves over $\mathbb{Q}$ whose 13-torsion subgroups are isomorphic as Galois modules. We also find equations for the surfaces parametrising pairs of 13-congruent elliptic curves. There are two such surfaces, corresponding to 13-congruences that do, or do not, respect the Weil pairing. We write each as a double cover of the projective plane ramified over a highly singular model for Baran's modular curve of level 13. By finding suitable rational curves on these surfaces, we show that there are infinitely many non-trivial pairs of 13-congruent elliptic curves over $\mathbb{Q}$.

1. Introduction

Elliptic curves E and E' are *n-congruent* if their n-torsion subgroups are isomorphic as Galois modules. We say the n-congruence has *power* k if the isomorphism raises the Weil pairing to the power k. Since multiplication-by-m, where m is an integer coprime to n, is an automorphism of the n-torsion subgroup, we are only interested in $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ up to multiplication by squares. Taking $n = p$ an odd prime, we say the congruence is *direct* if k is a quadratic residue, and *skew* if k is a quadratic non-residue.

The elliptic curves n-congruent with power k to a given elliptic curve E are parametrised by (the non-cuspidal points of) the curve $X_E(n, k)$. The pairs of elliptic curves that are n-congruent with power k, up to simultaneous quadratic twist, are parametrised by (a Zariski open subset of) the surface $Z(n, k)$.

If elliptic curves E and E' are related by an isogeny of degree d, with d coprime to n, then by standard properties of the Weil pairing, E and E' are n-congruent with power d. Congruences of this form are said to be trivial. We are interested in the following two basic questions.

(i) For which prime numbers p do there exist non-trivial pairs of p-congruent elliptic curves over $\mathbb{Q}$?
(ii) For which prime numbers p do there exist infinitely many non-trivial pairs of p-congruent elliptic curves over $\mathbb{Q}$?

Date: 23rd December 2019.

To be more precise, in (ii) we ask for infinitely many pairs of j-invariants, otherwise from any non-trivial pair of p-congruent elliptic curves we could construct infinitely many by taking simultaneous quadratic twists.

For $p = 3, 5$ we have $X_E(p,k) \cong \mathbb{P}^1$ and so there are infinitely many elliptic curves p-congruent to a given elliptic curve. Explicit formulae for these families of elliptic curves are given in [RS] in the direct case, and in [F1, F2] in the skew case. For $p \geq 7$ the curves $X_E(p,k)$ have genus at least 3, and so by Faltings' theorem there are only finitely many elliptic curves p-congruent to a given elliptic curve. Kraus and Oesterlé [KO] gave the example of the directly 7-congruent elliptic curves $152a1$ and $7448e1$. This was extended to infinitely many examples by Halberstadt and Kraus [HK], who also gave an equation for $X_E(7,1)$. A modification of their method, due to Poonen, Schaefer and Stoll [PSS], gives an equation for $X_E(7,3)$, and from this we were able to exhibit in [F3] infinitely many non-trivial pairs of skew 7-congruent elliptic curves.

Kani and Schanz [KS] described the geometry of the surfaces $Z(n,k)$, in particular showing that $Z(11,1)$ is an elliptic surface of Kodaira dimension 1. This work was extended by Kani and Rizzo [KR], who showed there are infinitely many non-trivial pairs of directly 11-congruent elliptic curves. We gave an alternative more explicit proof of this fact in [F3], and determined a Weierstrass equation for the elliptic surface $Z(11,1)$ in [F4]. Kumar [K, Theorem 21] computed an equation for $Z(11,2)$, and although not noted in his paper, the rational curve on this surface given by $rs - r + s^2 - s + 1 = 0$ gives rise to infinitely many non-trivial pairs of skew 11-congruent elliptic curves.

Examples of non-trivial 13-congruent elliptic curves have been known for some time. For example, the pair $52a1$ and $988b1$ appears in [FM, Table 5.3]. Since the first of these curves admits a rational 2-isogeny, this gives an example of both a direct and a skew 13-congruence. Prior to our work the only known examples of non-trivial 13-congruences were for pairs of elliptic curves that are both in the range of Cremona's tables (or simultaneous quadratic twists of such examples). In this paper, we show that there are infinitely many non-trivial pairs of 13-congruent elliptic curves, both in the direct and skew cases.

The only known example of a p-congruence for $p > 13$ is the pair of skew 17-congruent elliptic curves $3675b1$ and $47775b1$. This example was originally found by Cremona, and is explicitly recorded in [Bi, CF, F3, FK]. The fact the congruence is skew follows from [KO, Proposition 2]. It is a conjecture of Frey and Mazur that there are no non-trivial pairs of p-congruent elliptic curves for p sufficiently large. On the basis of our work, and that in [CF], we might refine this conjecture by suggesting that the answer to question (i) is the set of primes $p \leq 17$, and the answer to question (ii) is the set of primes $p \leq 13$.

Another reason why the case $n = 13$ is interesting, is that according to Kani and Schanz [KS, Theorem 4] it is the smallest value of n for which all the surfaces $Z(n,k)$ are of general type.

In Section 2 we state our main results by giving equations for $X_E(13,k)$ and $Z(13,k)$ for $k=1,2$. We also describe some of the curves of small genus we found on the surfaces $Z(13,k)$, including the ones giving rise to our infinite families of non-trivial pairs of 13-congruent elliptic curves.

To compute equations for $X_E(13,k)$ we follow the invariant-theoretic method developed in [F3]. However we do more to explain the generality in which we can expect these methods to work. To compute the necessary twists we need to start with an embedding of $X(p)$ in projective space such that the group $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ acts linearly. In Section 4 we explain the reasons behind our choice of embedding (Klein's A-curve) in the case $p=13$. In Section 5 we start on the invariant theory proper, deriving equations first for $X(13)$, and then for its twists $X_E(13,1)$ and $X_E(13,2)$. One basic difficulty is that the invariant of smallest degree has degree 2, but since a quadratic form has infinite automorphism group, it cannot carry the information needed to specify our curve. This forced us to work with an invariant of degree 4. The twisted forms of this invariant are too large to sensibly include in the paper, but are available from [F5].

Having equations for $X_E(13,k)$ in principle gives us equations for $Z(13,k)$. However the equations obtained in this way are very complicated, and not useful for finding rational points or curves of small genus on the surfaces. For several smaller values of n, as described in [F4], we were able to find substitutions to simplify these equations. However this step defeated us in the case $n=13$. In Section 6 we instead develop a new approach for computing equations for $Z(n,k)$, not going via the equations for $X_E(n,k)$, but still using the invariant theory.

Since the surface $Z(n,k)$ parametrises pairs of elliptic curves, it comes with a standard involution that corresponds to swapping over the two elliptic curves. The method in Section 6 gives us equations for $Z(13,k)$ as a double cover of the plane, where the map to the plane quotients out by the standard involution. This is the same format as used by Kumar [K] when giving his equations for $Z(n,-1)$ for $n\leq 11$. In using this format we are relying on the fact that the quotient of $Z(n,k)$ by the standard involution is a rational surface. It would be interesting to determine how large n must become before this property fails.

In Section 8 we give some examples of pairs of non-trivial 13-congruent elliptic curves over $\mathbb{Q}$ and over $\mathbb{Q}(t)$. The examples over $\mathbb{Q}$ may be verified, independently of our work, by checking that the traces of Frobenius are congruent mod 13 for sufficiently many good primes p. The examples over $\mathbb{Q}(t)$ give rise, by specialising t, to the infinitely many examples over $\mathbb{Q}$ that are our main result.

All computer calculations in support of this work was carried out using Magma [BCP]. Some Magma files containing some details of the calculations are available from [F5]. We refer to elliptic curves by their labels in Cremona's tables [C]. We write K for a field of characteristic 0 and $\overline{K}$ for its algebraic closure.

2. Statement of results

2.1. **The curves $X_E(13,1)$ and $X_E(13,2)$.** The elliptic curves n-congruent with power k to a given elliptic curve E are parametrised by (the non-cuspidal points of) the smooth projective curve $X_E(n,k)$. We have computed equations for these curves in the case $n = 13$. In this section we give formulae first for $X(13)$, and then for $X_E(13,1)$ and $X_E(13,2)$, each as a curve of degree 42 in $\mathbb{P}^6$. Since the equations themselves would (in the latter two cases) take several pages to write out, we instead describe how they may be recovered from a set of 14 hyperplanes, equivalently a set of 14 points in the dual projective space $(\mathbb{P}^6)^\vee$. This description (which only uses linear algebra) does not however correspond to how we originally computed the equations.

In the case of $X(13)$ the 14 points are

$$(1) \qquad (1:0:\ldots:0) \quad \text{and} \quad (1:\zeta^k:\zeta^{3k}:\zeta^{4k}:\zeta^{9k}:\zeta^{10k}:\zeta^{12k})$$

where $\zeta = e^{2\pi i/13}$ and $0 \le k \le 12$.

Theorem 2.1. *Let U be the 14-dimensional space of quadratic forms vanishing at the 14 points (1). Let $U^\perp$ be the 14-dimensional space of quadratic forms annihilated by*

$$\left\{ f\left(\frac{\partial}{\partial x_1},\ldots,\frac{\partial}{\partial x_7}\right) : f \in U \right\}.$$

Let $V \subset U^\perp$ be the 13-dimensional subspace spanned by the support of all linear syzygies, i.e. the span of the set

$$\left\{ \sum_{i=1}^7 \lambda_i f_i \;\middle|\; \lambda_i \in \{0,1\}, f_i \in U^\perp \text{ and } \sum_{i=1}^7 x_i f_i = 0 \right\}.$$

Let W be the 7-dimensional space of cubic forms whose partial derivatives belong to V. Then W defines the union of $X(13) \subset \mathbb{P}^6$ and 42 lines.

Our equations for $X_E(13,1)$ and $X_E(13,2)$ are obtained from those for $X(13)$ by twisting, that is, by making a change of coordinates on $\mathbb{P}^6$ defined over $\overline{K}$. To describe the points that take the place of (1), we let t be a coordinate on $X_0(13) \cong \mathbb{P}^1$ chosen (following Fricke) so that the j-map is given by

$$j = (t^2+5t+13)(t^4+7t^3+20t^2+19t+1)^3/t.$$

It is easy to write down an elliptic curve with this j-invariant. For example, we may take the elliptic curve $y^2 = x^3 - 27c_4(t)x - 54c_6(t)$ where

$$c_4(t) = (t^2+5t+13)(t^2+6t+13)(t^4+7t^3+20t^2+19t+1),$$
$$c_6(t) = (t^2+5t+13)(t^2+6t+13)^2(t^6+10t^5+46t^4+108t^3+122t^2+38t-1).$$

We define polynomials $f_1, \ldots, f_7$ and $g_1, \ldots, g_7$ by

$$f_1(s,t) = 1,$$
$$f_2(s,t) = -(t+1),$$
$$f_3(s,t) = 3s(t+2)(t^2+5t+13)(t^2+6t+13),$$
$$f_4(s,t) = -9s(t+1)(t^2+5t+13)(t^2+6t+13),$$
$$f_5(s,t) = 108s^2(t^2+5t+13)(t^2+6t+13)(t^3+5t^2+10t+2) + 27s^2(t+3)c_4(t),$$
$$f_6(s,t) = 162s^2(t^2+5t+13)(t^2+6t+13)(t^3+6t^2+14t+7) + 27s^2(t+4)c_4(t),$$
$$f_7(s,t) = 11664s^3(t+1)(t^2+5t+13)(t^2+6t+13)^2 + 54s^2c_4(t)f_4(s,t),$$

and

$$g_1(s,t) = 2,$$
$$g_2(s,t) = 2(t+1),$$
$$g_3(s,t) = 3s(t^2+6t+13)(t^3+4t^2+8t-1),$$
$$g_4(s,t) = 12s(t^2+6t+13)(t^2+3t+5),$$
$$g_5(s,t) = 6s(t^2+6t+13)(t^3+8t^2+20t+7),$$
$$g_6(s,t) = 108s^2(t+1)^2(t^2+5t+13)(t^2+6t+13) - 9s^2(t+3)c_4(t),$$
$$g_7(s,t) = -216s^2(t-1)(t^2+5t+13)(t^2+6t+13) - 18s^2(t+2)c_4(t).$$

Theorem 2.2. *Let E/K be the elliptic curve $y^2 = x^3+ax+b$. Let U_1, respectively U_2, be the space of quadratic forms vanishing at*

$$(f_1(s,t) : \ldots : f_7(s,t)), \quad \textit{respectively} \quad (g_1(s,t) : \ldots : g_7(s,t)),$$

for all $s,t \in \overline{K}$ satisfying $a = -27s^2c_4(t)$ and $b = -54s^3c_6(t)$. Let W_k be the space of cubic forms constructed from U_k by the procedure in Theorem 2.1. Then W_k defines the union of $X_E(13,k) \subset \mathbb{P}^6$ and 42 lines, where the latter are not in general defined over K.

The cubic forms in Theorem 2.2, as polynomials with coefficients in $\mathbb{Z}[a,b]$, are available from [F5]. As described in Sections 5.2 and 5.3, we have also found equations that define the curve $X_E(13,k)$ exactly, and define the j-map $X_E(13,k) \to \mathbb{P}^1$. It would be possible to simplify the $f_i(s,t)$ and $g_i(s,t)$ by making a change of coordinates on $\mathbb{P}^6$. However, we made our choice of co-ordinates with the aim of simplifying the cubic forms.

Remark 2.3. If a and b have weights 2 and 3, and $x_1, \ldots, x_7$ have weights $3,3,2,2,1,1,0$, then the cubic forms in the case $k = 1$ are homogeneous with weights $6,7,7,8,8,9,9$. Likewise, if $x_1, \ldots, x_7$ have weights $2,2,1,1,1,0,0$, then the cubic forms in the case $k = 2$ have weights $4,5,5,6,6,6,7$. These gradings reflect the fact that $X_E(13,k)$ only depends on E up to quadratic twist.

2.2. **The surfaces $Z(13,1)$ and $Z(13,2)$.** The surface $Z(n,k)$ parametrises pairs of elliptic curves E and E' that are n-congruent with power k, up to simultaneous quadratic twist. We have computed equations for these surfaces in the case $n = 13$.

Theorem 2.4. *(i) The surface $Z(13,1)$ is birational over $\mathbb{Q}$ to the surface with affine equation $y^2 + h_1(r,s)y = g_1(r,s)$ where*

$$\begin{aligned} h_1(r,s) &= s^4 + (2r^2 - 5r + 7)s^3 + (r^4 - 3r^3 - 14r^2 + r + 16)s^2 \\ &\quad + r^2(2r^3 - 5r^2 + 15r + 27)s + r^4(r^2 - 1), \\ g_1(r,s) &= 4(7r - 8)s^6 + 22(r - 2)s^5 - (28r^5 + 24r^4 - 2r^3 - 39r^2 + 2r + 68)s^4 \\ &\quad + r^2(84r^3 + 233r^2 - 116r - 223)s^3 - r^4(20r^2 + 181r + 181)s^2 \\ &\quad - 4r^6(r - 1)(7r + 3)s. \end{aligned}$$

(ii) The surface $Z(13,2)$ is birational over $\mathbb{Q}$ to the surface with affine equation $y^2 + h_2(r,s)y = g_2(r,s)$ where

$$\begin{aligned} h_2(r,s) &= r^3s^4 + r(2r^3 + 7r^2 + 1)s^3 + (r^5 + 7r^4 + 9r^3 + r^2 + 1)s^2 \\ &\quad + 2(r^3 + 2r + 1)s + r + 1, \\ g_2(r,s) &= 2r^4(5r + 4)s^7 + r^3(19r^3 + 48r^2 + 33r + 22)s^6 \\ &\quad + r^2(8r^5 + 40r^4 + 79r^3 + 82r^2 + 47r + 21)s^5 \\ &\quad - r(r^7 - 29r^5 - 91r^4 - 75r^3 - 53r^2 - 34r - 7)s^4 \\ &\quad + r(6r^6 + 35r^5 + 50r^4 + 37r^3 + 42r^2 + 22r + 10)s^3 \\ &\quad + r(14r^4 + 33r^3 + 30r^2 + 14r + 1)s^2 + r^2(10r + 13)s + 2r. \end{aligned}$$

(iii) Let $k = 1$ or 2. Let $j, j' : Z(13,k) \to \mathbb{P}^1$ be the maps giving the j-invariants of the elliptic curves E and E'. We have computed polynomials $A_k, B_k, D_k \in \mathbb{Z}[r,s]$ such that $jj' = A_k^3/D_k$ and $(j - 1728)(j' - 1728) = B_k^2/D_k$. The polynomials A_k and B_k are available from [F5]. *The D_k are given by*

$$\begin{aligned} D_1(r,s) &= s^5(r + s - 1)^4(r^2 + s - 1)^2(r^4 + r^3s - r^3 + rs^2 - rs - s^2 + s)^{13}, \\ D_2(r,s) &= -r^6(r^2 + rs + r + 1)^3(r^3s + r^2s^2 + 2r^2s + rs^2 + rs + r + s)^{13}. \end{aligned}$$

Remark 2.5. Let $k = 1$ or 2. By completing the square, the first two parts of Theorem 2.4 are equivalent to the statement that $Z(13,k)$ is birational to the surface $y^2 = F_k(r,s,1)$ where F_k is the homogeneous polynomial of degree $10 + 2k$ satisfying $F_k(r,s,1) = h_k(r,s)^2 + 4g_k(r,s)$.

According to Kani and Schanz [KS], the surfaces $Z(13,k)$ are of general type, and so by the Bombieri-Lang conjecture (see for example [HS]) are expected to contain only finitely many curves of genus 0 or 1.

On $Z(13,1)$ there are genus 0 curves given by the vanishing of s, $r+s-1$, r^2+s-1, r and $r+s$. The first three of these are factors of D_1, and so do not correspond to any families of elliptic curves. The last two define copies of the modular curves $X_0(10)$ and $X_0(25)$. Remarkably we found a further pair of genus 0 curves given by

$$r^5+r^4s-3r^4-r^3s+2r^2s^2-4r^2s-2rs^2+s^3-4s^2=0.$$

From this we obtain the infinite family of directly 13-congruent elliptic curves presented in Example 8.5. There are also genus 1 curves given by the vanishing of r^2+s, $r^2+rs-r-s+1$ and r^2+rs-s. These are copies of $X_0(m)$ for $m=27,36$ and 49.

On $Z(13,2)$ there are genus 0 curves given by the vanishing of r, $r^2+rs+r+1$, s and $r^2s+rs^2+rs+2s^2-2s+1$. The first two are factors of D_2, the third is a copy of $X_0(18)$, and from the fourth we obtain the infinite family of skew 13-congruent elliptic curves presented in Example 8.6. There are also genus 1 curves given by the vanishing of $r+1$, $s-1$, $rs+1$, $r^2s+2rs+1$ and $r^2s+rs+1$. These are copies of $X_0(m)$ for $m=19,20,21,24$ and 32. A further genus 1 curve is given by

$$r^3s+r^2s^2+3r^2s+4rs+r+2=0.$$

This is an elliptic curve of rank 2 with Cremona label $267632f1$ and Weierstrass equation $y^2=x^3-515x-4494$. It parametrises another infinite family of non-trivial pairs of skew 13-congruent elliptic curves.

It would be interesting to determine whether there are any more curves of genus 0 or 1 on the surfaces $y^2=F_k(r,s,1)$.

2.3. **Baran's modular curve.** For $k=1,2$ we have written $Z(13,k)$ as a double cover of $\mathbb{P}^2$ ramified over the curve $C_k=\{F_k=0\}$. A rational point on C_k corresponds to an elliptic curve that is 13-congruent to itself in a non-trivial way. Such a congruence is only possible if the mod 13 Galois representation of the elliptic curve is not surjective. More specifically, arguing as in [Ha], we see that C_1 and C_2 are copies of the modular curves $X_{\mathrm{s}}^+(13)$ and $X_{\mathrm{ns}}^+(13)$ associated to the normaliser of a split or non-split Cartan subgroup of level 13.

These curves were first computed by Baran [Ba], who also discovered the surprising fact, specific to level 13, that the two curves are isomorphic. We were able to verify using Magma that our singular curves C_1 and C_2 (of degrees 12 and 14) are both birational to the smooth plane quartic

$$C=\{(y+z)x^3-(2y^2+yz)x^2+(y^3-y^2z+2yz^2-z^3)x-(2y^2z^2-3yz^3)=0\}\subset\mathbb{P}^2$$

found by Baran. Using Theorem 2.4(iii) we were also able to recover the two different moduli interpretations of this curve, as given in [Ba, Appendix A]. We remark that the determination of all $\mathbb{Q}$-rational points on C (and hence also on C_1 and C_2) was recently completed in [B+].

We describe further modular curves on the surfaces $Z(13,k)$ in Section 7.

3. Twists and quotients

In this section we recall the definition of $X(n)$ over a non-algebraically closed field, and explain how in principle $X_E(n,k)$ may be described as a twist of $X(n)$. We also describe $Z(n,k)$ as a quotient of $X(n)\times X(n)$. We write ζ_n for a primitive nth root of unity, and μ_n for the group of all nth roots unity.

Let $n \geq 3$ be an integer. The modular curve $X(n)$ is the smooth projective curve birational to $Y(n)$, where $Y(n)$ is the modular curve parametrising the pairs (E,ϕ) where E is an elliptic curve and $\phi : E[n] \to \mu_n \times \mathbb{Z}/n\mathbb{Z}$ is a symplectic isomorphism. By symplectic we mean that the Weil pairing on $E[n]$ agrees with the standard pairing $((\zeta,c),(\xi,d)) \mapsto \zeta^d\xi^{-c}$ on $\mu_n \times \mathbb{Z}/n\mathbb{Z}$. We note that, with this definition, $X(n)$ is both defined over $\mathbb{Q}$ and geometrically irreducible.

Let Γ be the group of symplectic automorphisms of $\mu_n \times \mathbb{Z}/n\mathbb{Z}$. As a group this is a copy of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, but with Galois action given by

$$\sigma(\gamma) = \begin{pmatrix} \chi(\sigma) & 0 \\ 0 & 1 \end{pmatrix} \gamma \begin{pmatrix} \chi(\sigma)^{-1} & 0 \\ 0 & 1 \end{pmatrix} \tag{2}$$

where χ is the mod n cyclotomic character. There is an action of Γ on $X(n)$ given by $\gamma : (E,\phi) \mapsto (E,\gamma\phi)$. We suppose that

(i) we have embedded $X(n) \subset \mathbb{P}^{N-1}$, and
(ii) the action of Γ is given by a Galois equivariant group homomorphism

$$\rho : \Gamma \to \mathrm{GL}_N(\mathbb{Q}(\zeta_n)).$$

The following is a variant of [F3, Lemma 3.2]. We write σ_k for the automorphism of $\mathbb{Q}(\zeta_n)$ given by $\zeta_n \mapsto \zeta_n^k$. We also write $\propto$ for equality in PGL_N.

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

$$\sigma(h)h^{-1} \propto \sigma_k\rho(\sigma(\phi)\phi^{-1}) \tag{3}$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then $X_E(n,k) \subset \mathbb{P}^{N-1}$ is the twist of $X(n) \subset \mathbb{P}^{N-1}$ given by $X_E(n,k) \cong X(n)$; $\mathbf{x} \mapsto h\mathbf{x}$.

Proof. Let $\varepsilon_k : \mu_n \times \mathbb{Z}/n\mathbb{Z} \to \mu_n \times \mathbb{Z}/n\mathbb{Z}$ be the map sending $(\zeta,b) \mapsto (\zeta^k,b)$. The non-cuspidal points of $X_E(n,k)$ correspond to pairs (F,ψ) where F is an elliptic curve and $\psi : F[n] \to E[n]$ is an isomorphism that raises the Weil pairing to the power k^{-1}. (In fact we could take the power to be km^2 for any $m \in (\mathbb{Z}/n\mathbb{Z})^\times$, but the choice here is convenient for the definition of α.) Let $\alpha : X_E(n,k) \to X(n)$ be given by $(F,\psi) \mapsto (F,\varepsilon_k\phi\psi)$. Then

$$\sigma(\alpha)\alpha^{-1} \propto \rho(\sigma(\varepsilon_k\phi)(\varepsilon_k\phi)^{-1}) = \rho(\varepsilon_k\sigma(\phi)\phi^{-1}\varepsilon_k^{-1}) = \sigma_k\rho(\sigma(\phi)\phi^{-1}), \tag{4}$$

where for the last two equalities we have used (2) and the fact that both ε_k and ρ are Galois equivariant.

Now let $X' = \{\mathbf{x} \in \mathbb{P}^{N-1} : h\mathbf{x} \in X(n)\}$. Since $\sigma(h)h^{-1}$ is an automorphism of $X(n)$ we see that X' is defined over K. By (3) and (4) the curves $X_E(n,k)$ and X' are twists of $X(n)$ by the same cocycle, and are therefore isomorphic over K. □

The following description of $Z(n,k)$ as a quotient of $X(n) \times X(n)$ is the starting point of [KS]. We revisit this result since we wish to be sure that it works over a non-algebraically closed field.

Lemma 3.2. *The surface $Z(n,k)$ is birational to the quotient of $X(n) \times X(n)$ by the action of Γ given by $\gamma \mapsto (\rho(\gamma), \sigma_k\rho(\gamma))$.*

Proof. There is a Galois equivariant map $X(n) \times X(n) \to Z(n,k)$ given by

$$((E_1, \phi_1), (E_2, \phi_2)) \mapsto (E_1, E_2, \phi_2^{-1}\varepsilon_k\phi_1).$$

where ε_k is as in the proof of Lemma 3.1. If we act by $\gamma \in \Gamma$ then ϕ_1 and ϕ_2 become $\gamma\phi_1$ and $\varepsilon_k\gamma\varepsilon_k^{-1}\phi_2$. This leaves $\phi_2^{-1}\varepsilon_k\phi_1$ unchanged. Conversely, any pair of points in $Y(n) \times Y(n)$ with the same image in $Z(n,k)$ are related in this way. □

4. The modular curve $X(p)$

In this section we explain how (in the case $n = p$ is a prime) we may arrange that the assumptions (i) and (ii) in Section 3 are satisfied. We also describe the ring of invariants that arises in this context.

4.1. **Group actions on curves.** Let X be a smooth projective curve over $\mathbb{C}$, and let G be a finite group of automorphisms of X. Let G act trivially on $\mathbb{C}^\times$ and on $\mathbb{C}(X)^\times$ by $\sigma : f \mapsto f \circ \sigma^{-1}$. Splitting the exact sequence of G-modules

$$0 \to \mathbb{C}^\times \to \mathbb{C}(X)^\times \to \operatorname{Div} X \to \operatorname{Pic} X \to 0$$

into short exact sequences, and taking group cohomology gives a diagram

$$\begin{array}{ccccc} & & & & H^1(G, \mathbb{C}(X)^\times) \\ & & & & \downarrow \\ (\operatorname{Div} X)^G & \longrightarrow & (\operatorname{Pic} X)^G & \xrightarrow{\delta} & H^1(G, \mathbb{C}(X)^\times/\mathbb{C}^\times) \\ & & & & \downarrow \Delta \\ & & & & H^2(G, \mathbb{C}^\times) \end{array}$$

Let $\Upsilon : (\operatorname{Pic} X)^G \to H^2(G, \mathbb{C}^\times)$ be the composite of the connecting maps δ and Δ. Since G acts faithfully on X, we have $H^1(G, \mathbb{C}(X)^\times) = 0$ by Hilbert's theorem 90.

We thus obtain an exact sequence

$$0 \longrightarrow \frac{(\operatorname{Div} X)^G}{\sim} \longrightarrow (\operatorname{Pic} X)^G \xrightarrow{\Upsilon} H^2(G, \mathbb{C}^\times). \tag{5}$$

There is an alternative description of Υ in terms of theta groups. For $D \in \operatorname{Div} X$ representing an element of $(\operatorname{Pic} X)^G$ we define the theta group

$$\Theta_D = \{(f, \sigma) : f \in \mathbb{C}(X)^\times, \sigma \in G \text{ such that } \operatorname{div}(f) = \sigma D - D\}$$

with group law

$$(f, \sigma) \circ (g, \tau) = (f \cdot \sigma(g), \sigma\tau). \tag{6}$$

This group sits naturally in an exact sequence $0 \to \mathbb{C}^\times \to \Theta_D \to G \to 0$. In other words, Θ_D is an extension of G by $\mathbb{C}^\times$.

Lemma 4.1. *If $[D] \in (\operatorname{Pic} X)^G$ then $\Upsilon(D)$ is the class of Θ_D in $H^2(G, \mathbb{C}^\times)$.*

Proof. For each $\sigma \in G$ we pick $f_\sigma \in \mathbb{C}(X)^\times$ with $\operatorname{div}(f_\sigma) = \sigma D - D$. The class of Θ_D in $H^2(G, \mathbb{C}^\times)$ is represented by the 2-cocycle ϕ satisfying

$$(f_\sigma, \sigma) \circ (f_\tau, \tau) = \phi(\sigma, \tau)(f_{\sigma\tau}, \sigma\tau). \tag{7}$$

Comparing (6) and (7) we find that $\phi(\sigma, \tau) = f_\sigma \cdot \sigma(f_\tau) \cdot f_{\sigma\tau}^{-1}$. By the formulae for the connecting maps in group cohomology, we see that the image of $[D]$ under δ is represented by $\sigma \mapsto f_\sigma$, and its image under Δ is represented by ϕ. □

Lemma 4.2. *If $[D] \in (\operatorname{Pic} X)^G$ and $H^0(X, \mathcal{O}(D))$ has dimension $n \geq 1$, then there is a natural action of G on the 1-dimensional subspaces of $H^0(X, \mathcal{O}(D))$ giving rise to a projective representation $\overline{\rho} : G \to \mathrm{PGL}_n(\mathbb{C})$. This lifts to a representation $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ if and only if $\Upsilon(D) = 0$.*

Proof. There is a linear action of Θ_D on $H^0(X, \mathcal{O}(D))$ via $(f, \sigma) : g \mapsto f \cdot \sigma(g)$. Picking a basis for $H^0(X, \mathcal{O}(D))$, this defines a representation $\pi : \Theta_D \to \mathrm{GL}_n(\mathbb{C})$. There is a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{C}^\times & \longrightarrow & \Theta_D & \longrightarrow & G & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \pi} & \swarrow & \downarrow{\scriptstyle \overline{\rho}} & & \\
0 & \longrightarrow & \mathbb{C}^\times & \longrightarrow & \mathrm{GL}_n(\mathbb{C}) & \longrightarrow & \mathrm{PGL}_n(\mathbb{C}) & \longrightarrow & 0
\end{array}$$

By Lemma 4.1 we have $\Upsilon(D) = 0$ if and only if the top row splits. If the top row splits then it is clear that $\overline{\rho}$ lifts to ρ (as indicated by the dotted arrow). Conversely if $\overline{\rho}$ lifts to ρ, then by a diagram chase each $\sigma \in G$ lifts uniquely to $x \in \Theta_D$ with $\pi(x) = \rho(\sigma)$, and the map $\sigma \mapsto x$ is a splitting of the top row. □

4.2. **The action of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ on $X(p)$.** We shall need the following standard group-theoretic facts.

Lemma 4.3. *Let $\mathcal{G} = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ where $p \geq 5$ is a prime. Then*

(i) *The groups $H^i(\mathcal{G}, \mathbb{C}^\times)$ are trivial for $i = 1, 2$.*
(ii) *Every projective representation of $\mathcal{G}$ lifts uniquely to a representation.*

Proof. (i) The group $\mathcal{G}$ is generated by elements $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ with $S^4 = T^p = (ST)^3 = I_2$. Therefore $H^1(\mathcal{G}, \mathbb{C}^\times) = \mathrm{Hom}(\mathcal{G}, \mathbb{C}^\times) = 0$. The vanishing of $H^2(\mathcal{G}, \mathbb{C}^\times)$ was proved by Schur, using the fact that every Sylow subgroup of $\mathcal{G}$ is either cyclic or a generalised quaternion group. See [G, Theorem 4.232] or [Hu, Chapter V, Satz 25.7].
(ii) If $\overline{\rho} : \mathcal{G} \to \mathrm{PGL}_n(\mathbb{C})$ is a projective representation then

$$\{(g, M) \in \mathcal{G} \times \mathrm{GL}_n(\mathbb{C}) : \overline{\rho}(g) \propto M\}$$

is an extension of $\mathcal{G}$ by $\mathbb{C}^\times$, and so corresponds to an element of $H^2(\mathcal{G}, \mathbb{C}^\times)$. Thus the vanishing of $H^2(\mathcal{G}, \mathbb{C}^\times)$ proves the existence of a lift, and the vanishing of $\mathrm{Hom}(\mathcal{G}, \mathbb{C}^\times)$ shows it is unique. □

Now let $X = X(p)$ where $p \geq 5$ is a prime. As a Riemann surface, it is the quotient of the extended upper half plane $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ by the action of $\Gamma(p) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$. There is an action of $G = \mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ on X with quotient the j-line. The quotient map is ramified over $j = 0, 1728, \infty$ with ramification indices 3, 2 and p. Thus, writing $\nu = (p^2 - 1)/24$, all but three G-orbits of points on X have size $|G| = 12p\nu$, and the remaining orbits have sizes 12ν, $4p\nu$ and $6p\nu$. It may be proved using the Hurwitz bound (see [AR, Theorem 20.40]) that G is the full automorphism group of X when $p \geq 7$.

The character table of $\mathcal{G} = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is described for example in [FH, §5.2]. The non-trivial representations of smallest degree are conjugate representations ϕ and ϕ' each of degree $m = (p-1)/2$, and conjugate representations ψ and ψ' each of degree $m+1$. Klein gave equations for $X(p)$ both as a curve of degree $(m-1)\nu$ in $\mathbb{P}^{m-1}$ with $\mathcal{G}$ acting via ϕ, and as a curve of degree $m\nu$ in $\mathbb{P}^m$ with $\mathcal{G}$ acting via ψ. Following the terminology in [AR], we call these the z-curve and the A-curve. For example, when $p = 7$ the z-curve is the Klein quartic.

Theorem 4.4 (Adler, Ramanan)**.** *The group $(\mathrm{Pic}\, X)^G$ is infinite cyclic, generated by a divisor class λ of degree $\nu = (p^2 - 1)/24$.*

Proof. This is [AR, Theorem 24.1]. The proof works by analysing the exact sequence (5). The authors first show that $(\mathrm{Div}\, X)^G/\sim$ is infinite cyclic, generated by a divisor class of degree $\gcd(12\nu, 4p\nu, 6p\nu) = 2\nu$. By Lemma 4.3(i) and the

Hochschild-Serre exact sequence

$$\mathrm{Hom}(\mathcal{G},\mathbb{C}^\times) \xrightarrow{\mathrm{res}} \mathrm{Hom}(\{\pm 1\},\mathbb{C}^\times) \longrightarrow H^2(G,\mathbb{C}^\times) \xrightarrow{\mathrm{inf}} H^2(\mathcal{G},\mathbb{C}^\times).$$

we have $H^2(G,\mathbb{C}^\times) \cong \mathbb{Z}/2\mathbb{Z}$. The proof is completed by constructing λ as the difference of the hyperplane sections for the z-curve and the A-curve. □

Applying the Riemann Hurwitz theorem to the j-map $X(p) \to \mathbb{P}^1$ shows that $X(p)$ has genus $(p-6)\nu + 1$. The canonical divisor is therefore $2(p-6)\lambda$.

4.3. **An abstract ring of invariants.** We introduce a ring that plays a central role in our calculations.

Theorem 4.5. *Let $R = \oplus_{d\geq 0} R_d = \oplus_{d\geq 0} H^0(X,\mathcal{O}(d\lambda))$ and $\mathcal{G} = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.*

(i) *There is a natural action of $\mathcal{G}$ on R where $-I_2$ acts as $(-1)^d$ on R_d.*
(ii) *The $\mathcal{G}$-invariant subring of R is generated by elements c_4, c_6 and D of degrees $4p$, $6p$ and 12.*
(iii) *We may scale c_4, c_6 and D so that $c_4^3 - c_6^2 = 1728D^p$ and the j-map $X \to \mathbb{P}^1$ is given by $j = c_4^3/D^p$.*

Proof. (i) Suppose that $R_d = H^0(X,\mathcal{O}(d\lambda))$ has dimension $n \geq 1$. Since λ is G-invariant, we obtain a projective representation $\overline{\rho} : G \to \mathrm{PGL}_n(\mathbb{C})$, and by Lemma 4.3(ii) this lifts uniquely to a representation $\rho : \mathcal{G} \to \mathrm{GL}_n(\mathbb{C})$. This gives the required action of $\mathcal{G}$ on R_d. It is clear that $\rho(-I_2) = \pm I_n$. Lemma 4.2 shows that the sign is + (i.e., the action factors via G) precisely when $\Upsilon(d\lambda) = 0$. However we saw in the proof of Theorem 4.4 that $\Upsilon(\lambda)$ is the non-trivial element of $H^2(G,\mathbb{C}^\times) \cong \mathbb{Z}/2\mathbb{Z}$. The action of $\mathcal{G}$ on R_d therefore factors via G precisely when d is even.
(ii) The fibres of the j-map above $0, 1728$ and ∞ are effective divisors in the classes of $4p\lambda$, $6p\lambda$ and 12λ. We let c_4, c_6 and D be the corresponding elements of R. Let $f \in R_d$ be a $\mathcal{G}$-invariant element. We show by induction on d that f belongs to the subring generated by c_4, c_6 and D. If $d \geq 1$ then f vanishes on the G-orbit of some point $P \in X$. If the orbit has size $4p\nu$, $6p\nu$ or 12ν then we divide through by c_4, c_6 or D, and apply the induction hypothesis. Otherwise the orbit has size $|G| = 12p\nu$. In this case we divide through by a linear combination of c_4^3 and c_6^2 chosen so that it vanishes at P.
(iii) Let $P \in X$ be a cusp, i.e., a point above $j = \infty$. Let f be a linear combination of c_4^3 and c_6^2 that vanishes at P. Since f vanishes at exactly $|G|$ points (counted with multiplicity) it cannot vanish on any orbits of size $|G|$. Therefore f vanishes only at the cusps, and so must be a scalar multiple of D^p. Scaling the invariants appropriately gives the relation as claimed. Finally, the formula offered for the j-map quotients out by the action of G, and has degree $|G|$. It must therefore

agree with the j-map up to composition with a Mobius map. However, since both maps send the zeros of c_4, c_6 and D to $j = 0, 1728$ and ∞, this Mobius map fixes three points, and is therefore the identity. □

In our earlier work [F3] on twists of $X(p)$ for $p = 7$ and 11, we mainly worked with the z-curve. In the case $p = 13$ the z-curve has degree 35 in $\mathbb{P}^5$ and the A-curve has degree 42 in $\mathbb{P}^6$. By Theorem 4.5 we have

$$\oplus_{d\geq 0} H^0(X, \mathcal{O}(5d\lambda))^{\mathcal{G}} = \mathbb{C}[D^5, Dc_6, D^4c_4, c_4c_6, D^3c_4^2],$$
$$\oplus_{d\geq 0} H^0(X, \mathcal{O}(6d\lambda))^{G} = \mathbb{C}[D, c_6]. \tag{8}$$

The ring of invariants is much simpler in the second of these two cases. We therefore decided to work with the A-curve in the case $p = 13$.

5. Equations for $X(13)$ and its twists

5.1. **Equations for the A-curve.** Let $\zeta = e^{2\pi i/13}$ and $\xi_k = \zeta^k + \zeta^{-k}$. Let $G \cong \mathrm{PSL}_2(\mathbb{Z}/13\mathbb{Z})$ be the subgroup of $\mathrm{SL}_7(\mathbb{C})$ generated by M_2, M_6 and M_{13} where

$$M_2 = \frac{1}{\sqrt{13}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & \xi_2 & \xi_4 & \xi_8 & \xi_3 & \xi_6 & \xi_1 \\ 2 & \xi_4 & \xi_8 & \xi_3 & \xi_6 & \xi_1 & \xi_2 \\ 2 & \xi_8 & \xi_3 & \xi_6 & \xi_1 & \xi_2 & \xi_4 \\ 2 & \xi_3 & \xi_6 & \xi_1 & \xi_2 & \xi_4 & \xi_8 \\ 2 & \xi_6 & \xi_1 & \xi_2 & \xi_4 & \xi_8 & \xi_3 \\ 2 & \xi_1 & \xi_2 & \xi_4 & \xi_8 & \xi_3 & \xi_6 \end{pmatrix}, \quad M_6 = - \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

and $M_{13} = \mathrm{Diag}(1, \zeta, \zeta^4, \zeta^3, \zeta^{12}, \zeta^9, \zeta^{10})$. We write $\mathbb{C}[x_0, \ldots, x_6]_d$ for the space of homogeneous polynomials of degree d.

Definition 5.1. An *invariant* of degree d is a polynomial $I \in \mathbb{C}[x_0, \ldots, x_6]_d$ satisfying $I \circ g = I$ for all $g \in G$.

The invariants of smallest degree are Q and F given by

$$Q = x_0^2 + x_1x_4 + x_2x_5 + x_3x_6,$$
$$F = 2x_0^4 + 6x_0(x_1x_3x_5 + x_2x_4x_6) + 3(x_1x_2x_4x_5 + x_1x_3x_4x_6 + x_2x_3x_5x_6) + x_1x_2^3 + x_2x_3^3 + x_3x_4^3 + x_4x_5^3 + x_5x_6^3 + x_6x_1^3.$$

We use these invariants to give equations for $X(13)$ as a curve of degree 42 in $\mathbb{P}^6$, defined over $\mathbb{Q}$. For f and g homogeneous forms in $x_0, \ldots, x_6$ we put

$$\langle f, g\rangle = \mathrm{trace}(H(f)H(Q)^{-1}H(g)H(Q)^{-1}) \tag{9}$$

where H denotes the Hessian matrix, that is, the 7×7 matrix of second partial derivatives. We prove the following refinement of Theorem 2.1.

Theorem 5.2. *Let Q and F be the invariants defined above.*

(i) *The vector space W of cubic forms f satisfying $\langle f, F - 3Q^2 \rangle = 0$ has dimension 7. Moreover $F - 3Q^2$ is, up to scalars, the unique quartic form satisfying $\langle f, F - 3Q^2 \rangle = 0$ for all $f \in W$.*

(ii) *Let U be the vector space of quadratic forms vanishing on the G-orbit of $\{x_0 = 0\}$ in $(\mathbb{P}^6)^\vee$. Then W is the space of cubic forms constructed from U by the procedure in Theorem 2.1.*

(iii) *If W has basis $f_0, \ldots, f_6$ then*

$$X(13) \cong \{f_0 = \ldots = f_6 = F + Q^2 = 0\} \subset \mathbb{P}^6.$$

This is a curve of degree 42, and the 84 cusps are cut out by the quadratic form Q. The cubic forms $f_0, \ldots, f_6$ are not sufficient to define the curve, but rather define the union of the curve and 42 lines. The 42 lines each pass through two cusps, and may be divided into 14 sets of 3, where each set of 3 lines spans one of the hyperplanes in (ii).

Proof. The first two parts are checked by linear algebra. The space of cubic forms W has basis $f_0, \ldots, f_6$ where

$$f_0 = -2x_0^3 + x_0(x_1x_4 + x_2x_5 + x_3x_6) + x_1x_3x_5 + x_2x_4x_6,$$
$$f_1 = x_0x_1^2 + 2x_0x_3x_4 + 2x_1x_2x_6 + x_2x_4^2 + x_5x_3^2 + x_6x_5^2,$$

and the remaining f_i are obtained from f_1 by the action of M_6, i.e., by cyclically permuting the subscripts $1, 2, \ldots, 6$.

Let $a_1, \ldots, a_6$ be coordinates on $\mathbb{P}^5$. We write $a_0 = 0$, $a_{-i} = -a_i$ and agree to read all subscripts mod 13. According to [F3, Section 2], the z-curve for $X(13)$ is defined by the 4 by 4 Pfaffians of the 13 by 13 skew symmetric matrix $(a_{i-j}a_{i+j})$. According to [AR, §51], the A-curve is the image of the z-curve via the map

$$(x_0 : x_1 : \ldots : x_6) = \left(1 : \frac{a_2}{a_1} : \frac{a_4}{a_2} : \frac{a_8}{a_4} : \frac{a_3}{a_8} : \frac{a_6}{a_3} : \frac{a_{12}}{a_6}\right).$$

A calculation, performed using Magma [BCP], shows that the A-curve is defined by the vanishing of $f_0, \ldots, f_6$ and $F + Q^2$. As we remark in the proof of the next lemma, further equations are needed to generate the homogeneous ideal. We also checked using Magma that this curve has degree 42, and that it meets the hypersurface defined by Q in 84 distinct points. This set of points is preserved by the action of $G \cong \mathrm{PSL}_2(\mathbb{Z}/13\mathbb{Z})$, and so must be the set of cusps on $X(13)$.

If we write $P_0 = (1 : 0 \ldots : 0)$, $P_1 = (0 : 1 : 0 : \ldots : 0)$, etc, then $P_1, P_2, \ldots, P_6$ are cusps, and the cubics vanish on the lines P_1P_4, P_2P_5 and P_3P_6. These lines belong to a single G-orbit of size 42. Another calculation using Magma shows that the cubics define a curve of degree 84, which must therefore be the union of $X(13)$ and the 42 lines. □

Some care must be taken in working with the above model for $X(13)$, since it is not projectively normal. In other words, the rings S and S' in the following lemma are not the same.

Lemma 5.3. *Let $X = X(13) \subset \mathbb{P}^6$ be as in Theorem 5.2. Let $S = \oplus_{d\geq 0} S_d$ be its homogeneous coordinate ring, and let $S' = \oplus_{d\geq 0} H^0(X, \mathcal{O}_X(d))$. Then*

$$\sum_{d\geq 0} (\dim S_d)t^d = 1 + 7t + 28t^2 + 77t^3 + 119t^4 + \ldots$$
$$\sum_{d\geq 0} (\dim S'_d)t^d = 1 + 7t + 35t^2 + 77t^3 + 119t^4 + \ldots$$

and $\dim S_d = \dim S'_d = 42d - 49$ for all $d \geq 3$.

Proof. Using the Gröbner basis machinery in Magma [BCP] we were able to compute 42 quartic forms that together with the 7 cubic forms generate the homogeneous ideal of X. From this it is easy to compute $\dim S_d$ for any given d. In particular we verified the values recorded in the statement of the lemma for each $d \leq 4$. On the other hand, since X has degree 42 and genus 50 it follows by Riemann-Roch that $\dim S'_d = 42d - 49$ for all $d \geq 3$.

Let $T = \oplus_d T_d$ be the homogeneous coordinate ring of the set of 84 cusps. Again by computer algebra we find

$$\sum_{d\geq 0} (\dim T_d)t^d = 1 + 7t + 27t^2 + 70t^3 + 84t^4 + \ldots$$

Therefore $\dim T_d = 84$ for all $d \geq 4$. We show by induction on d that the inclusion $S_d \subset S'_d$ is an equality for all $d \geq 3$. We have already checked this for $d = 3, 4$. So let $f \in S'_d$ with $d \geq 5$. Since $\dim T_d = 84$ we may reduce to the case where f vanishes at the cusps. But then applying the induction hypothesis to $f/Q \in S'_{d-2}$ gives the result. Finally, by identifying S'_d with the subspace of S'_{d+2} vanishing at the cusps, we compute

$$\dim S'_1 = \dim S_3 - \dim T_3 = 7,$$
$$\dim S'_2 = \dim S_4 - \dim T_4 = 35.$$ □

Remark 5.4. We have shown that $\dim S_1' = 7$ and therefore $X(13) \subset \mathbb{P}^6$ is embedded by a complete linear system. This is a special case of the "WYSIWYG hypothesis" in [AR].

Definition 5.5. A *covariant* of degree d is a column vector $\mathbf{v}$ of polynomials in $\mathbb{C}[x_0, \dots, x_6]_d$ 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

$$\nabla_Q I = H(Q)^{-1} \begin{pmatrix} \partial I/\partial x_0 \\ \vdots \\ \partial I/\partial x_6 \end{pmatrix}.$$

On the other hand if $\mathbf{v}$ and $\mathbf{w}$ are covariants of degrees d and e then

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

is an invariant of degree $d+e$. We may also think of covariants as G-equivariant polynomial maps $\mathbb{C}^7 \to \mathbb{C}^7$. Thus 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.

It is easy to compute the dimensions of the spaces of invariants and covariants of any given degree d from the character table of G. We may also solve for the invariants and covariants of degree d by linear algebra over $\mathbb{Q}(\zeta)$, at least if d is not too large.

Remark 5.6. A standard trick for computing invariants is to start with an arbitrary polynomial f and apply the operator $f \mapsto \frac{1}{|G|} \sum_{g \in G} f \circ g$. An efficient way to organise this calculation, which will become important in Section 6, is the following. Let $\pi : f \mapsto \frac{1}{13} \sum_{i=0}^{12} f \circ M_{13}^i$ be the projection map that sends a monomial fixed by M_{13} to itself, and all other monomials to zero. Then starting with a monomial in the image of π we apply the operators $f \mapsto \sum_{i=0}^{5} f \circ M_6^i$ and $f \mapsto f + 13\pi(f \circ M_2)$.

For our work in Sections 5.2 and 5.3, it is important that we find ways of constructing invariants and covariants from previously known examples in a basis-free way. Another consideration is that it would be overkill for us to completely classify the invariants and covariants, as we are only interested in them modulo the equations defining the curve $X = X(13)$.

Writing ψ for the standard representation of $G \subset \mathrm{SL}_7(\mathbb{C})$, we find that $\wedge^3\psi$ contains a copy of the trivial representation. The corresponding G-invariant alternating form is

$$\Phi = (x_0 \wedge x_1 \wedge x_4) - (x_0 \wedge x_2 \wedge x_5) + (x_0 \wedge x_3 \wedge x_6) + (x_1 \wedge x_3 \wedge x_5) - (x_2 \wedge x_4 \wedge x_6). \tag{10}$$

Again let $\langle\ ,\ \rangle$ be as defined in (9).

Lemma 5.7. *There is a 7×7 alternating matrix N of linear forms in $\mathbb{C}[x_0,\dots,x_6]$, unique up to an overall scaling, such that*

$$\big\langle (N\nabla_Q F)_i, \frac{\partial F}{\partial x_i}\big\rangle = 0$$

for all $0\le i\le 6$.

Proof. This is checked by linear algebra. We find that

$$N = \begin{pmatrix} 0 & x_4 & -x_5 & x_6 & -x_1 & x_2 & -x_3 \\ -x_4 & 0 & 0 & x_5 & x_0 & -x_3 & 0 \\ x_5 & 0 & 0 & 0 & -x_6 & -x_0 & x_4 \\ -x_6 & -x_5 & 0 & 0 & 0 & x_1 & x_0 \\ x_1 & -x_0 & x_6 & 0 & 0 & 0 & -x_2 \\ -x_2 & x_3 & x_0 & -x_1 & 0 & 0 & 0 \\ x_3 & 0 & -x_4 & -x_0 & x_2 & 0 & 0 \end{pmatrix}. \tag{11}$$

In a more succinct notation, we have $N=(N_{ij})$ where $N_{ij}=(\frac{\partial}{\partial x_i}\wedge\frac{\partial}{\partial x_j})\Phi$. □

We define covariants $\mathbf{v}_3=\nabla_Q F$ and $\mathbf{v}_4 = H(Q)^{-1}N\mathbf{v}_3$, where N is given by (11). Then $\mathbf{v}_9=\mathbf{v}_3\circ\mathbf{v}_3$ is a covariant of degree 9, and $c_6=\mathbf{v}_4\cdot\mathbf{v}_9$ is an invariant of degree 13. Our next theorem shows that although the rings S and S' in Lemma 5.3 are different, their G-invariant subrings are the same.

Theorem 5.8. *Let S be the coordinate ring of $X\subset\mathbb{P}^6$. Then $S^G=\mathbb{C}[Q,c_6]$ and the j-map $X\to\mathbb{P}^1$ is given by $j=1728-c_6^2/Q^{13}$.*

Proof. We find that $c_6(0,1,0,0,0,0,0)=-1$, and so c_6 does not vanish identically on X. Since $X\subset\mathbb{P}^6$ is the A-curve, it has hyperplane section 6λ. Therefore S^G is a subring of

$$\oplus_{d\ge 0}H^0(X,\mathcal{O}(6d\lambda))^G.$$

By Theorem 4.5, or more specifically (8), the latter is a polynomial ring in two variables, generated in degrees 2 and 13. Since we have constructed invariants Q and c_6 of these degrees, and these invariants do not vanish on X, this proves the first part of the theorem.

By Theorem 4.5(iii) we have $j-1728=\xi c_6^2/Q^{13}$ for some constant ξ. Let ω be a primitive cube root of unity, and put $\alpha=\sqrt{-1+3\omega}$. The point

$$(-2:\omega+\alpha:\omega-\alpha:\omega+\alpha:\omega-\alpha:\omega+\alpha:\omega-\alpha)\in X$$

is fixed by $M_6^2\in G$ of order 3, and so lies above $j=0$. The function c_6^2/Q^{13} takes the value 1728 at this point. Therefore $\xi=-1$. □

For later use (when applying Lemma 6.2) we also record a point on X above $j = 1728$. Let $i = \sqrt{-1}$ and let β be a root of $x^3 - (i+1)x^2 - x + i = 0$. Let σ be the automorphism of $\mathbb{Q}(\beta)$ given by $\beta \mapsto \beta^2 - \beta$. Then the point

$$(1 : \beta : \sigma(\beta) : \sigma^2(\beta) : \beta : \sigma(\beta) : \sigma^2(\beta)) \in X$$

is fixed by $M_6^3 \in G$ of order 2, and so lies above $j = 1728$.

5.2. **Equations for $X_E(13,1)$.** We compute equations for $X_E(13,1)$ from those for $X = X(13)$ in Theorem 5.2 by making a change of coordinates. For this we use the 7×7 matrix formed from the following 7 covariants. As before, the subscripts indicate the degrees of the covariants.

$$\begin{aligned}
&\mathbf{v}_1 = (x_0, x_1, \ldots, x_6)^T && \mathbf{v}_{10} = \operatorname{coeff}(\mathbf{v}_4 \circ (\mathbf{v}_1 + t\mathbf{v}_3), t^3)\\
&\mathbf{v}_3 = \nabla_Q F && \mathbf{v}_{12} = \mathbf{v}_3 \circ \mathbf{v}_4\\
&\mathbf{v}_4 = H(Q)^{-1} N \mathbf{v}_3 && \mathbf{v}_{13} = \operatorname{coeff}(\mathbf{v}_4 \circ (\mathbf{v}_1 + t\mathbf{v}_4), t^3)\\
&\mathbf{v}_9 = \mathbf{v}_3 \circ \mathbf{v}_3
\end{aligned}$$

Lemma 5.9. *We have*

$$\det(\mathbf{v}_1, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_9, \mathbf{v}_{10}, \mathbf{v}_{12}, \mathbf{v}_{13}) = (c_6^2 - 1728Q^{13})^2 \mod I(X).$$

Proof. The left hand side is an invariant of degree 52, and so by Theorem 5.8 is a linear combination of Q^{26}, $Q^{13}c_6^2$ and c_6^4. We may determine the correct linear combination by evaluating each side at some random points on X. We initially did this by working mod p for some moderately sized prime p. To verify the answer in characteristic 0, we used the point on X defined over a degree 20 number field given by $(1 : 1 : \gamma : \ldots)$ where γ is a root of

$$\begin{aligned}
x^{20} + 5x^{17} - 7x^{16} + 2x^{15} + 10x^{14} + x^{13} + 5x^{12} + 4x^{11} - 21x^{10}\\
+ 19x^9 + 10x^8 + 3x^7 + 8x^6 - 17x^5 + 5x^3 + 2x^2 + 1 = 0.
\end{aligned}$$

□

We now twist the invariants Q and F. Specifically we put

$$\begin{aligned}
\mathcal{Q}(y_1, \ldots, y_7) &= Q(y_1\mathbf{v}_1 + y_2\mathbf{v}_3 + y_3\mathbf{v}_4 + y_4\mathbf{v}_9 + y_5\mathbf{v}_{10} + y_6\mathbf{v}_{12} + y_7\mathbf{v}_{13})\\
\mathcal{F}(y_1, \ldots, y_7) &= F(y_1\mathbf{v}_1 + y_2\mathbf{v}_3 + y_3\mathbf{v}_4 + y_4\mathbf{v}_9 + y_5\mathbf{v}_{10} + y_6\mathbf{v}_{12} + y_7\mathbf{v}_{13})
\end{aligned}$$

Each of the coefficients of these forms is an invariant, and so working modulo $I(X)$ may be written as a polynomial in Q and c_6. By a series of computations similar

to the proof of Lemma 5.9 we find that

$$\begin{aligned}\mathcal{Q}(y_1,\dots,y_7) = {} & Qy_1^2 - 4Q^2y_1y_2 + 44Q^5y_1y_4 + c_6y_1y_6 - 36Q^7y_1y_7 - 2Q^3y_2^2 \\ & - 124Q^6y_2y_4 - c_6y_2y_5 + 300Q^8y_2y_7 + 6Q^4y_3^2 + c_6y_3y_4 + 324Q^7y_3y_5 \\ & - 12Q^8y_3y_6 - 2Q^2c_6y_3y_7 + 502Q^9y_4^2 + 24Q^3c_6y_4y_5 + 27Q^4c_6y_4y_6 \\ & - 396Q^{11}y_4y_7 + 4302Q^{10}y_5^2 - 36Q^{11}y_5y_6 - 35Q^5c_6y_5y_7 + 150Q^{12}y_6^2 \\ & - 54Q^6c_6y_6y_7 - (3282Q^{13} - c_6^2)y_7^2.\end{aligned}$$

The coefficient of y_1^2 is $\mathbf{v}_1 \cdot \mathbf{v}_1 = Q$, and the coefficient of y_3y_4 is $\mathbf{v}_4 \cdot \mathbf{v}_9 = c_6$, which is how we defined c_6 in the last section. We note that several of the coefficients were forced to be zero by the fact there are no monomials in Q and c_6 of the appropriate degree. In a similar way we compute

$$\begin{aligned}\mathcal{F}(y_1,\dots,y_7) = {} & -Q^2y_1^4 - 4Q^3y_1^3y_2 - 124Q^6y_1^3y_4 - c_6y_1^3y_5 + 300Q^8y_1^3y_7 \\ & - 6Q^4y_1^2y_2^2 - 372Q^7y_1^2y_2y_4 - 3Qc_6y_1^2y_2y_5 + 900Q^9y_1^2y_2y_7 + 18Q^5y_1^2y_3^2 \\ & + \ldots + (307161Q^{19}c_6 - 32Q^6c_6^3)y_6y_7^3 - (24003375Q^{26} + 408Q^{13}c_6^2 - 2c_6^4)y_7^4.\end{aligned}$$

We now make a change of coordinates to simplify $\mathcal{Q}$ and $\mathcal{F}$, and so that we obtain correct formulae in the case $j(E) = 0$. We put $c_6 = -864b$ and substitute

$$\begin{aligned}y_1 &= 16Q^6(12a^2(x_1 + 2x_2) + 18abx_3 + 14(4a^3 + 27b^2)x_5 + 81b^2x_6), \\ y_2 &= 2Q^5(96a^2x_2 - 144ab(x_3 - 3x_4) + (48a^3 - 324b^2)x_5 \\ &\qquad + (52a^3 - 297b^2)x_6 - 864a^2bx_7), \\ y_3 &= Q^{11}(2a(x_3 - 56x_4) + 3b(44x_5 + 3x_6) + 176a^2x_7), \\ y_4 &= -4Q^2(4a^3 + 27b^2)(2x_5 - x_6), \\ y_5 &= 2Q^8(2ax_4 - 3bx_5 - 4a^2x_7), \\ y_6 &= Q^7(2a(x_3 - 2x_4) + 3b(2x_5 + 3x_6) + 8a^2x_7), \\ y_7 &= 2(4a^3 + 27b^2)x_6.\end{aligned}$$

This transformation has determinant $-2^{23}3^3a^8Q^{39}(4a^3 + 27b^2)^2$. Dividing $\mathcal{Q}$ and $\mathcal{F}$ by $2^{16}3^2a^4(4a^3 + 27b^2)$ and $2^{32}3^4a^8(4a^3 + 27b^2)^2$, and eliminating Q by the rule $Q^{13} = 16(4a^3 + 27b^2)$, we obtain

$$\begin{aligned}\mathcal{Q}(x_1,\dots,x_7) = {} & x_1^2 - 6x_2^2 + ax_3^2 + 9bx_3x_6 - 6ax_4^2 + 18bx_4x_5 + 24a^2x_4x_7 \\ & + 2a^2x_5^2 - 36abx_5x_7 - 3a^2x_6^2 + 162b^2x_7^2,\end{aligned}$$

and

$$\begin{aligned}\mathcal{F}(x_1,\dots,x_7) = {} & -x_1^4 - 12x_1^3x_2 - 54x_1^2x_2^2 - 18ax_1^2x_4^2 + 54bx_1^2x_4x_5 \\ & + 72a^2x_1^2x_4x_7 + 6a^2x_1^2x_5^2 - 108abx_1^2x_5x_7 + 486b^2x_1^2x_7^2 - 60x_1x_2^3 \\ & + \ldots - 432ab(4a^3 - 27b^2)x_6x_7^3 - 3(8a^3 - 27b^2)(40a^3 - 27b^2)x_7^4.\end{aligned}$$

These polynomials $\mathcal{Q}$ and $\mathcal{F}$ have weights 6 and 12 with respect to the grading in Remark 2.3.

For f and g homogeneous polynomials in $x_1, \dots, x_7$ we define

$$\langle f, g \rangle = \operatorname{trace}(H(f)H(\mathcal{Q})^{-1}H(g)H(\mathcal{Q})^{-1}).$$

The proof of the next theorem is similar to that of [F3, Lemmas 3.7 and 3.12].

Theorem 5.10. *Let E/K be the elliptic curve $y^2 = x^3 + ax + b$. Let $f_1, \dots, f_7$ be a basis for the space of cubic forms f satisfying $\langle f, \mathcal{F} - 3\mathcal{Q}^2 \rangle = 0$. Then*

$$X_E(13,1) \cong \{f_1 = \dots = f_7 = \mathcal{F} + \mathcal{Q}^2 = 0\} \subset \mathbb{P}^6.$$

Proof. We assume that $j(E) \neq 0, 1728$, equivalently $ab \neq 0$, leaving the remaining cases to Section 5.4. Let $(x_0 : \dots : x_6)$ be a $\overline{K}$-point on $X(13)$ corresponding to (E, ϕ) for some choice of symplectic isomorphism $\phi : E[13] \to \mu_{13} \times \mathbb{Z}/13\mathbb{Z}$. By Theorem 5.8, and the formula $j(E) = 1728(4a^3)/(4a^3 + 27b^2)$, we may scale $(x_0, \dots, x_6)$ to satisfy $Q(x_0, \dots, x_6)^{13} = 16(4a^3 + 27b^2)$ and

$$c_6(x_0, \dots, x_6) = -864b. \tag{12}$$

Let h be the 7×7 matrix formed by evaluating the covariants

$$Q^6\mathbf{v}_1,\ Q^5\mathbf{v}_3,\ Q^{11}\mathbf{v}_4,\ Q^2\mathbf{v}_9,\ Q^8\mathbf{v}_{10},\ Q^7\mathbf{v}_{12},\ \mathbf{v}_{13} \tag{13}$$

at $(x_0, \dots, x_6)$. By Lemma 5.9 and our assumption $a \neq 0$ this matrix is non-singular. Let $\rho : \mathrm{SL}_2(\mathbb{Z}/13\mathbb{Z}) \to \mathrm{GL}_7(\overline{K})$ describe the action of $\mathrm{PSL}_2(\mathbb{Z}/13\mathbb{Z})$ on $X(13)$. We claim that

$$\sigma(h)h^{-1} \propto \rho(\sigma(\phi)\phi^{-1}) \tag{14}$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Let $\xi_\sigma = \sigma(\phi)\phi^{-1} \in \mathrm{SL}_2(\mathbb{Z}/13\mathbb{Z})$. Since $(\sigma(x_0) : \dots : \sigma(x_6))$ corresponds to $(E, \sigma(\phi))$ we have

$$\begin{pmatrix} \sigma(x_0) \\ \vdots \\ \sigma(x_6) \end{pmatrix} = \lambda_\sigma \rho(\xi_\sigma) \begin{pmatrix} x_0 \\ \vdots \\ x_6 \end{pmatrix} \tag{15}$$

for some $\lambda_\sigma \in \overline{K}^\times$. Then since c_6 is an invariant of degree 13 we have

$$\sigma(c_6(x_0, \dots, x_6)) = \lambda_\sigma^{13} c_6(x_0, \dots, x_6).$$

By (12) and our assumption $b \neq 0$, it follows that λ_σ is a 13th root of unity. Since the covariants (13) all have degree a multiple of 13, our claim (14) now follows from (15) and the definition of a covariant (see Definition 5.5).

Finally, Lemma 3.1 shows that $X_E(13,1) \subset \mathbb{P}^6$ is obtained from $X(13) \subset \mathbb{P}^6$ by making the change of coordinates given by h, and Theorem 5.2 shows how we may recover equations for the curve from $\mathcal{Q}$ and $\mathcal{F}$. □

The cubic forms $f_1, \ldots, f_7$, as polynomials with coefficients in $\mathbb{Z}[a,b]$, are available from [F5]. Alternatively, they may be computed from the description given in Section 2.1.

Next we compute the j-map $X_E(13,1) \to \mathbb{P}^1$. Revisiting Lemma 5.7 with $\mathcal{Q}$ and $\mathcal{F}$ in place of Q and F we obtain a skew symmetric matrix $\mathcal{N}$ given by $\mathcal{N}_{ij} = (\frac{\partial}{\partial x_i} \wedge \frac{\partial}{\partial x_j})\Phi$ where

$$\begin{aligned}\Phi &= 12(x_1 \wedge x_2 \wedge x_7) - 2(x_1 \wedge x_3 \wedge x_5) - 3(x_1 \wedge x_3 \wedge x_6) + 6(x_1 \wedge x_4 \wedge x_5)\\ &+ 6(x_1 \wedge x_4 \wedge x_6) + 12a(x_1 \wedge x_5 \wedge x_7) + 12a(x_1 \wedge x_6 \wedge x_7) - 6(x_2 \wedge x_3 \wedge x_5)\\ &- 6(x_2 \wedge x_3 \wedge x_6) + 12(x_2 \wedge x_4 \wedge x_5) + 18(x_2 \wedge x_4 \wedge x_6) + 24a(x_2 \wedge x_5 \wedge x_7)\\ &+ 36a(x_2 \wedge x_6 \wedge x_7) - 12a(x_3 \wedge x_4 \wedge x_7) + 18b(x_3 \wedge x_5 \wedge x_7) + 54b(x_4 \wedge x_6 \wedge x_7)\\ &+ 12a^2(x_5 \wedge x_6 \wedge x_7).\end{aligned}$$

We put $\mathfrak{v}_3 = \nabla_{\mathcal{Q}} \mathcal{F}$, $\mathfrak{v}_4 = H(\mathcal{Q})^{-1}\mathcal{N}\mathfrak{v}_3$, $\mathfrak{v}_9 = \mathfrak{v}_3 \circ \mathfrak{v}_3$ and $\mathfrak{c}_6 = \mathrm{coeff}(\mathcal{Q}(\mathfrak{v}_4 + t\mathfrak{v}_9), t)$. The map $j : X_E(13,1) \to \mathbb{P}^1$ satisfies $j - 1728 = \xi\mathfrak{c}_6^2/\mathcal{Q}^{13}$ for some constant ξ. Evaluating at the tautological point $(1:0:\ldots:0) \in X_E(13,1)$ we find

$$\mathcal{Q}(1,0,\ldots,0) = 1 \quad \text{and} \quad \mathfrak{c}_6(1,0,\ldots,0) = -216b/(4a^3+27b^2).$$

Since $j(E) = 1728(4a^3)/(4a^3+27b^2)$ it follows that $\xi = -(4a^3+27b^2)$ and so

$$j = 1728 - \frac{(4a^3+27b^2)\mathfrak{c}_6^2}{\mathcal{Q}^{13}}.$$

Remark 5.11. (i) The quadratic form $\mathcal{Q}$ may be recovered from Φ as the GCD of the 6×6 Pfaffians of $\mathcal{N}$ where $\mathcal{N}_{ij} = (\frac{\partial}{\partial x_i} \wedge \frac{\partial}{\partial x_j})\Phi$.
(ii) We may simplify $\mathcal{Q}$ and Φ by making the further change of coordinates

$$\begin{aligned}x_1 &= -au_1 - a^2u_2 + 9bu_3 + 9bu_4 - (3/2)bu_5 - 3au_6 + 2a^2u_7,\\ x_2 &= (1/2)au_1 + (1/3)a^2u_2 - (9/2)bu_3 - 3bu_4 + (3/4)bu_5 + au_6 - a^2u_7,\end{aligned}$$

$x_3 = 3bu_2 + 2au_4$, $x_4 = 2au_3 - 3bu_7$, $x_5 = -(1/2)u_1 - au_7$, $x_6 = -(1/3)au_2 + u_6$, $x_7 = (1/2)u_3 + (1/12)u_5$. Then $\mathcal{Q} = u_1u_7 + u_2u_6 + u_3u_5 + u_4^2$ and

$$\Phi = (u_1 \wedge u_2 \wedge u_3) + (u_1 \wedge u_4 \wedge u_7) + (u_2 \wedge u_4 \wedge u_6) + (u_3 \wedge u_4 \wedge u_5) + (u_5 \wedge u_6 \wedge u_7). \tag{16}$$

In particular these expressions do not depend on a and b. Unfortunately, this change of coordinates makes $\mathcal{F}$ more complicated.
(iii) The alternating forms (10) and (16) differ by a relabelling of the variables.

In computing our equations for $X_E(13,1)$ from those for $X(13)$ we have therefore twisted by a cocycle taking values in the stabiliser of Φ. According to [FH, Proposition 22.12] this stabiliser is the 14-dimensional exceptional Lie group G_2.

5.3. **Equations for $X_E(13,2)$.** Let $G \cong \mathrm{PSL}_2(\mathbb{Z}/13\mathbb{Z})$ be the subgroup of $\mathrm{SL}_7(\mathbb{C})$ defined in Section 5.1. We write $g \mapsto \widetilde{g}$ for the automorphism of G induced by $\zeta \mapsto \zeta^2$.

Definition 5.12. A *skew covariant* of degree d is a column vector $\mathbf{w}$ of polynomials in $\mathbb{C}[x_0,\dots,x_6]_d$ satisfying $\mathbf{w} \circ g = \widetilde{g}\mathbf{w}$ for all $g \in G$.

Our first example of a skew covariant is $\mathbf{w}_3 = (f_0, f_1, \dots, f_6)^T$ where the f_i are the cubic polynomials vanishing on $X(13)$, as defined in the proof of Theorem 5.2. Let $\mathbf{w}_4 = (g_0, g_1, \dots, g_6)^T$ be the skew covariant of degree 4 where

$$\begin{aligned} g_0 &= 4x_0(x_1x_3x_5 - x_2x_4x_6) + x_1x_2^3 - x_2x_3^3 + x_3x_4^3 - x_4x_5^3 + x_5x_6^3 - x_6x_1^3, \\ g_1 &= 4x_0^2x_1^2 - 4x_0^2x_3x_4 + 4x_0x_1x_2x_6 - 2x_0x_3^2x_5 - 2x_0x_5^2x_6 - x_1^3x_4 + x_1^2x_2x_5 \\ &\quad - 2x_1x_3x_4^2 - x_1x_5^3 - x_2^3x_3 - 2x_2^2x_6^2 + 4x_2x_3x_4x_5 + x_3^2x_4x_6 + x_4x_5x_6^2, \end{aligned}$$

and the remaining g_i are obtained from g_1 by the action of M_6, i.e. by cyclically permuting the subscripts $1,2,\dots,6$ and alternating the signs. We note that the polynomials $g_0, g_1, \dots, g_6$ vanish at the cusps of $X(13)$, but do not vanish identically on $X(13)$, and are not divisible by Q. They therefore account for the discrepancy (in degree 2) between the rings S and S' in Lemma 5.3.

We construct further skew covariants by precomposing with a covariant.

$$\begin{aligned} \mathbf{w}_5 &= \mathrm{coeff}(\mathbf{w}_3 \circ (\mathbf{v}_1 + t\mathbf{v}_3), t) & \mathbf{w}_8 &= \mathrm{coeff}(\mathbf{w}_4 \circ (\mathbf{v}_1 + t\mathbf{v}_3), t^2) \\ \mathbf{w}_6 &= \mathrm{coeff}(\mathbf{w}_4 \circ (\mathbf{v}_1 + t\mathbf{v}_3), t) & \mathbf{w}_{11} &= \mathrm{coeff}(\mathbf{w}_5 \circ (\mathbf{v}_1 + t\mathbf{v}_3), t^3) \\ \mathbf{w}_7 &= \mathrm{coeff}(\mathbf{w}_3 \circ (\mathbf{v}_1 + t\mathbf{v}_3), t^2) & \mathbf{w}_{13} &= \mathrm{coeff}(\mathbf{w}_5 \circ (\mathbf{v}_1 + t\mathbf{v}_3), t^4) \end{aligned}$$

Lemma 5.13. *We have*

$$\det(\mathbf{w}_4, \mathbf{w}_5, \mathbf{w}_6, \mathbf{w}_7, \mathbf{w}_8, \mathbf{w}_{11}, \mathbf{w}_{13}) = 2Q(c_6^2 - 1728Q^{13})^2 \mod I(X).$$

Proof. The proof is similar to that of Lemma 5.9. The factor Q on the right hand side arises since the entries of $\mathbf{w}_4$ vanish at the cusps. □

We now twist the invariants Q and F. Specifically we put

$$\begin{aligned} \mathcal{Q}(y_1,\dots,y_7) &= Q(y_1\mathbf{w}_4 + y_2\mathbf{w}_5 + y_3\mathbf{w}_6 + y_4\mathbf{w}_7 + y_5\mathbf{w}_8 + y_6\mathbf{w}_{11} + y_7\mathbf{w}_{13}) \\ \mathcal{F}(y_1,\dots,y_7) &= F(y_1\mathbf{w}_4 + y_2\mathbf{w}_5 + y_3\mathbf{w}_6 + y_4\mathbf{w}_7 + y_5\mathbf{w}_8 + y_6\mathbf{w}_{11} + y_7\mathbf{w}_{13}) \end{aligned}$$

Each of the coefficients of these forms is an invariant, and so working modulo $I(X)$ may be written as a polynomial in Q and c_6. By a series of computations similar

to the proof of Lemma 5.9 we find that

$$\begin{aligned}\mathcal{Q}(y_1,\dots,y_7) &= 2Q^4y_1^2 + 16Q^5y_1y_3 - 72Q^6y_1y_5 + Qc_6y_1y_6 + 6Q^5y_2^2\\ &\quad - 2c_6y_2y_5 - 864Q^8y_2y_6 + 1932Q^9y_2y_7 - 4Q^6y_3^2 + c_6y_3y_4 - 72Q^7y_3y_5\\ &\quad - 20Q^2c_6y_3y_6 - 42Q^3c_6y_3y_7 - 12Q^7y_4^2 - 3Qc_6y_4y_5 + 576Q^9y_4y_6\\ &\quad + 1008Q^{10}y_4y_7 + 612Q^8y_5^2 + 198Q^3c_6y_5y_6 - 196Q^4c_6y_5y_7\\ &\quad + 24408Q^{11}y_6^2 - 163296Q^{12}y_6y_7 + (132630Q^{13} + c_6^2)y_7^2,\end{aligned}$$

and

$$\begin{aligned}\mathcal{F}(y_1,\dots,y_7) &= 5Q^8y_1^4 + 8Q^9y_1^3y_3 + Q^3c_6y_1^3y_4 - 144Q^{10}y_1^3y_5 - 19Q^5c_6y_1^3y_6\\ &\quad - 42Q^6c_6y_1^3y_7 + 54Q^9y_1^2y_2^2 - 6Q^3c_6y_1^2y_2y_3 + 144Q^{10}y_1^2y_2y_4\\ &\quad + \ldots + (88642532225Q^{26} - 1969502Q^{13}c_6^2 + 2c_6^4)y_7^4.\end{aligned}$$

We put $c_6 = -864b$ and substitute

$$\begin{aligned}y_1 &= 6Q^{11}(36bx_1 + 90bx_2 - 2a^2(5x_3 + 8x_4 + 2x_5) - 9abx_6 + 42abx_7),\\ y_2 &= 4Q^4(4a^3 + 27b^2)(1347x_1 - 936x_2 - 317ax_6 - 185ax_7),\\ y_3 &= 3Q^{10}(36bx_1 - 18bx_2 + 2a^2(x_3 - 8x_4 - 14x_5) + 9abx_6 + 6abx_7),\\ y_4 &= 24Q^3(4a^3 + 27b^2)(21x_1 - 36x_2 - ax_6 + 9ax_7),\\ y_5 &= 3Q^9(18bx_2 - 2a^2(x_3 + 2x_5) + 3abx_6 + 6abx_7),\\ y_6 &= 8Q(4a^3 + 27b^2)(6x_1 - 6x_2 - ax_6),\\ y_7 &= -4(4a^3 + 27b^2)(3x_1 - ax_6 - ax_7).\end{aligned}$$

This transformation has determinant $2^{26}3^8a^8Q^{38}(4a^3 + 27b^2)^4$. Dividing $\mathcal{Q}$ and $\mathcal{F}$ by $2^{18}3^4a^4(4a^3 + 27b^2)^2$ and $2^{32}3^8a^8(4a^3 + 27b^2)^3$, and eliminating Q by the rule $Q^{13} = 16(4a^3 + 27b^2)$, we obtain

$$\mathcal{Q}(x_1,\dots,x_7) = x_1x_7 + x_2x_6 + x_3x_5 + x_4^2,$$

and

$$\begin{aligned}\mathcal{F}(x_1,\dots,x_7) &= 48ax_1^3x_2 + 36bx_1^3x_3 + 72bx_1^3x_5 + 8a^2x_1^3x_6 + 16a^2x_1^3x_7\\ &\quad - 144ax_1^2x_2^2 - 216bx_1^2x_2x_3 + 432bx_1^2x_2x_4 + 432bx_1^2x_2x_5 - 48a^2x_1^2x_2x_7\\ &\quad + \ldots + 12a^2(a^3 + 9b^2)x_6^2x_7^2 + 56a^2(a^3 + 7b^2)x_6x_7^3 + 16a^2(3a^3 + 20b^2)x_7^4.\end{aligned}$$

These polynomials $\mathcal{Q}$ and $\mathcal{F}$ have weights 2 and 10 with respect to the grading in Remark 2.3.

For f and g homogeneous polynomials in $x_1,\dots,x_7$ we define

$$\langle f, g\rangle = \mathrm{trace}(H(f)H(\mathcal{Q})^{-1}H(g)H(\mathcal{Q})^{-1}).$$

Theorem 5.14. *Let E/K be the elliptic curve $y^2 = x^3 + ax + b$. Let $f_1, \ldots, f_7$ be a basis for the space of cubic forms f satisfying $\langle f, \mathcal{F} - 48(4a^3 + 27b^2)\mathcal{Q}^2\rangle = 0$. Then*

$$X_E(13,2) \cong \{f_1 = \ldots = f_7 = \mathcal{F} + 16(4a^3 + 27b^2)\mathcal{Q}^2 = 0\} \subset \mathbb{P}^6.$$

Proof. The proof is similar to that of Theorem 5.10, except that we now form the matrix h by evaluating the skew covariants

$$Q^{11}\mathbf{w}_4,\ Q^4\mathbf{w}_5,\ Q^{10}\mathbf{w}_6,\ Q^3\mathbf{w}_7,\ Q^9\mathbf{w}_8,\ Q\mathbf{w}_{11},\ \mathbf{w}_{13}$$

and show using the definition of a skew covariant (see Definition 5.12) that

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

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

Again the cubic forms $f_1, \ldots, f_7$, as polynomials with coefficients in $\mathbb{Z}[a,b]$, are available from [F5]. Alternatively, they may be computed from the description given in Section 2.1.

Next we compute the j-map $X_E(13,2) \to \mathbb{P}^1$. Revisiting Lemma 5.7 with $\mathcal{Q}$ and $\mathcal{F}$ in place of Q and F we obtain a skew symmetric matrix $\mathcal{N}$ given by $\mathcal{N}_{ij} = (\frac{\partial}{\partial x_i} \wedge \frac{\partial}{\partial x_j})\Phi$ where

$$\Phi = (x_1 \wedge x_4 \wedge x_7) - (x_1 \wedge x_5 \wedge x_6) - (x_2 \wedge x_3 \wedge x_7) - (x_2 \wedge x_4 \wedge x_6) - (x_3 \wedge x_4 \wedge x_5).$$

We put $\mathfrak{v}_3 = \nabla_{\mathcal{Q}}\mathcal{F}$, $\mathfrak{v}_4 = H(\mathcal{Q})^{-1}\mathcal{N}\mathfrak{v}_3$, $\mathfrak{v}_9 = \mathfrak{v}_3 \circ \mathfrak{v}_3$ and $\mathfrak{c}_6 = \mathrm{coeff}(\mathcal{Q}(\mathfrak{v}_4 + t\mathfrak{v}_9), t)$. The map $j : X_E(13,2) \to \mathbb{P}^1$ satisfies $j - 1728 = \xi\mathfrak{c}_6^2/\mathcal{Q}^{13}$ for some constant ξ. In principle we could compute ξ by carefully keeping track of all the changes of coordinates and rescalings described above, but in practice it is simpler to look at some numerical examples. We find that

$$j = 1728 - \frac{\mathfrak{c}_6^2}{2^{40}(4a^3 + 27b^2)^{10}\mathcal{Q}^{13}}.$$

Remark 5.15. We have arranged that the forms $\mathcal{Q}$ and Φ do not depend on a and b, and indeed, up to a relabelling of the variables, are the same as the forms we started with. Therefore, exactly as in Remark 5.11, we have twisted by a cocycle taking values in G_2.

5.4. **The cases $j(E) = 0, 1728$.** We have shown that the equations for $X_E(13,1)$ and $X_E(13,2)$ in Theorems 5.10 and 5.14 are correct for all elliptic curves E with $j(E) \neq 0, 1728$. We now remove this restriction. The first step is to show that if the theorems are correct for some elliptic curve E then they are correct for any 2-isogenous elliptic curve F.

Let E be the elliptic curve $y^2 = x^3 + ax + b$, and let F be the elliptic curve $y^2 = x^3 + Ax + B$ where $A = -15\theta^2 - 4a$, $B = 14a\theta + 22b$ and θ is a root of

$x^3 + ax + b = 0$. If we put $c = 3\theta$ and $d = 3\theta^2 + a$ then E is isomorphic to $y^2 = x(x^2 + cx + d)$ and F is isomorphic to $y^2 = x((x-c)^2 - 4d)$. In particular E and F are 2-isogenous.

Starting from the equations in Theorems 5.10 and 5.14, we find there is an isomorphism $X_E(13,1) \cong X_F(13,2)$ given by $(x_1 : \ldots : x_7) \mapsto (x_1' : \ldots : x_7')$ where

$$\begin{aligned}
x_1' &= (14\theta^2 + 8a)x_1 + 32\theta^2 x_2 - (3a\theta - 25b)x_3 + (38a\theta - 18b)x_4 - (18a\theta^2 \\
&\quad + 30b\theta + 16a^2)x_5 - (11a\theta^2 - 3b\theta + 24a^2)x_6 + (144b\theta^2 - 44a^2\theta + 132ab)x_7, \\
x_2' &= (14\theta^2 + 8a)x_2 + (3a\theta + 7b)x_3 + (11a\theta + 15b)x_4 - (17a\theta^2 - 9b\theta + 8a^2)x_5 \\
&\quad - (5a\theta^2 - 21b\theta + 8a^2)x_6 + (144b\theta^2 + 10a^2\theta + 66ab)x_7, \\
x_3' &= 8\theta x_1 + 8\theta x_2 + 8\theta^2 x_3 + (30\theta^2 + 24a)x_4 + (10a\theta - 6b)x_5 - (8a\theta + 24b)x_6 \\
&\quad + (12a\theta^2 - 108b\theta)x_7, \\
x_4' &= 4\theta x_1 + 8\theta x_2 + (5\theta^2 + 4a)x_3 - (5a\theta - 3b)x_6, \\
x_5' &= -4\theta x_1 - 12\theta x_2 + (3\theta^2 - 4a)x_4 + (a\theta + 9b)x_5 + (6a\theta^2 - 18b\theta + 16a^2)x_7, \\
x_6' &= -4x_1 - 12x_2 + 6\theta x_4 - (6\theta^2 + 4a)x_5 - 12a\theta x_7, \\
x_7' &= 2x_1 + 4x_2 + \theta x_3 + (3\theta^2 + 2a)x_6.
\end{aligned}$$

The determinant of this transformation is $-2^{10}3^2d^3(c^2 - 4d)^5$, and so in particular is non-zero.

Let $E_{a,b}$ be the elliptic curve $y^2 = x^3 + ax + b$. Since $E_{1,0}$ is 2-power isogenous to $y^2 = x^3 - 44x + 112$ and $E_{0,1}$ is 2-isogenous to $y^2 = x^3 - 15x + 22$, it follows that Theorems 5.10 and 5.14 hold for the elliptic curves $E_{1,0}$ and $E_{0,1}$. It remains to show that if these results hold for some elliptic curve with $j = 0, 1728$ then they hold for all such curves.

The non-cuspidal points of $X_E(p,k)$ correspond to pairs (F, ψ), where F is an elliptic curve and $\psi : F[p] \to E[p]$ is a isomorphism that raises the Weil pairing to the power k. We write $\mathrm{SL}(E[p])$ for the group of automorphisms of $E[p]$ that respect the Weil pairing. Then $\mathrm{SL}(E[p])$ acts on $X_E(p,k)$ via $\gamma : (F, \psi) \mapsto (F, \gamma\psi)$. There is therefore a group homomorphism

$$\pi_E : \mathrm{Aut}(E)/\{\pm 1\} \to \mathrm{SL}(E[p])/\{\pm 1\} \to \mathrm{Aut}(X_E(p,k)). \tag{17}$$

Lemma 5.16. *Let E and E' be elliptic curves defined over K and $\alpha : E' \to E$ an isomorphism defined over $\overline{K}$. Then there is an isomorphism $\beta : X_{E'}(p,k) \to X_E(p,k)$ defined over $\overline{K}$ satisfying*

$$\sigma(\beta)\beta^{-1} = \pi_E(\sigma(\alpha)\alpha^{-1})$$

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

Proof. Let $\beta : X_{E'}(p,k) \to X_E(p,k)$ be the isomorphism given on non-cuspidal points by $(F,\psi) \mapsto (F,\alpha\psi)$. Then $\sigma(\beta)\beta^{-1}$ maps $(F,\psi) \mapsto (F,\sigma(\alpha)\alpha^{-1}\psi)$, and is therefore equal to $\pi_E(\sigma(\alpha)\alpha^{-1})$. □

Proof of Theorem 5.10 for $j = 1728$. We have already shown that the theorem holds for $E = E_{1,0}$. We now prove it for $E' = E_{a,0}$. We identify $\mathrm{Aut}(E) = \mu_4$ via $\zeta : (x,y) \mapsto (\zeta^{-2}x, \zeta^{-3}y)$. Let $\alpha : E' \to E$ be the isomorphism given by $(x,y) \mapsto (a^{-1/2}x, a^{-3/4}y)$. Then

$$\sigma(\alpha)\alpha^{-1} = \frac{\sigma(a^{1/4})}{a^{1/4}}. \tag{18}$$

Let $X, X_a \subset \mathbb{P}^6$ be the models claimed for $X_E(13,1)$ and $X_{E'}(13,1)$ in Theorem 5.10. We have already shown that $X \cong X_E(13,1)$. From the grading in Remark 2.3 we construct an isomorphism $\beta : X_a \to X$ given by

$$(x_1 : \ldots : x_7) \mapsto (x_1 : x_2 : a^{1/2}x_3 : a^{1/2}x_4 : ax_5 : ax_6 : a^{3/2}x_7).$$

Then

$$\sigma(\beta)\beta^{-1} = \begin{cases} 1 & \text{if } \sigma(a^{1/2}) = a^{1/2} \\ \iota & \text{if } \sigma(a^{1/2}) = -a^{1/2} \end{cases} \tag{19}$$

where

$$\iota : (x_1 : \ldots : x_7) \mapsto (x_1 : x_2 : -x_3 : -x_4 : x_5 : x_6 : -x_7).$$

If $\sigma(\beta)\beta^{-1} = \pi_E(\sigma(\alpha)\alpha^{-1})$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ then we see by Lemma 5.16 that X_a and $X_{E'}(13,1)$ are twists of $X = X_E(13,1)$ by the same cocycle, and are therefore isomorphic over K. Comparing (18) and (19), it remains to show that π_E sends $\zeta_4 \mapsto \iota$. More generally, we claim that ι is the unique involution of $X_E(13,1)$ defined over $\mathbb{Q}(i)$. By [AR, Theorem 20.40] the second map in (17) is an isomorphism. This reduces our claim to one about $\mathrm{SL}(E[13])/\{\pm 1\}$. It may be checked, for example by consulting the LMFDB [L], that the mod 13 Galois representation attached to $E/\mathbb{Q}(i)$ has image a split Cartan subgroup, i.e., the subgroup C of diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}/13\mathbb{Z})$. But then the group

$$\{h \in \mathrm{SL}_2(\mathbb{Z}/13\mathbb{Z}) : ghg^{-1} = \pm h \text{ for all } g \in C\}/\{\pm 1\}$$

is cyclic of order 6, and so contains a unique element of order 2. □

Proof of Theorem 5.10 for $j = 0$. We have already shown that the theorem holds for $E = E_{0,1}$. We now prove it for $E' = E_{0,b}$. We identify $\mathrm{Aut}(E) = \mu_6$ via $\zeta : (x,y) \mapsto (\zeta^{-2}x, \zeta^{-3}y)$. Let $\alpha : E' \to E$ be the isomorphism given by $(x,y) \mapsto (b^{-1/3}x, b^{-2/3}y)$. Then

$$\sigma(\alpha)\alpha^{-1} = \frac{\sigma(b^{1/6})}{b^{1/6}}.$$

Let $X, X_b \subset \mathbb{P}^6$ be the models claimed for $X_E(13,1)$ and $X_{E'}(13,1)$ in Theorem 5.10. We have already shown that $X \cong X_E(13,1)$. From the grading in Remark 2.3 we construct an isomorphism $\beta : X_b \to X$ given by

$$(x_1 : \ldots : x_7) \mapsto (x_1 : x_2 : b^{1/3}x_3 : b^{1/3}x_4 : b^{2/3}x_5 : b^{2/3}x_6 : bx_7).$$

Then

$$\sigma(\beta)\beta^{-1} = \begin{cases} 1 & \text{if } \sigma(b^{1/3}) = b^{1/3} \\ \varepsilon & \text{if } \sigma(b^{1/3}) = \zeta_3 b^{1/3} \\ \varepsilon^2 & \text{if } \sigma(b^{1/3}) = \zeta_3^2 b^{1/3} \end{cases}$$

where

$$\varepsilon : (x_1 : \ldots : x_7) \mapsto (x_1 : x_2 : \zeta_3 x_3 : \zeta_3 x_4 : \zeta_3^2 x_5 : \zeta_3^2 x_6 : x_7).$$

Arguing as in the proof with $j = 1728$, it remains to show that the map π_E sends $\zeta_6 \mapsto \varepsilon$. We find that ε and ε^2 are the only order 3 automorphisms of $X_E(13,1)$ defined over $\mathbb{Q}(\zeta_3)$. Therefore $X_{E'}(13,1)$ is isomorphic to X_b or $X_{1/b}$. To rule out the latter we take $b = 2$ and consider the 3-isogenous elliptic curves $E' : y^2 = x^3 + 2$ and $F : y^2 = x^3 - 120x + 506$. Since 3 is a quadratic residue mod 13 we have $X_{E'}(13,1) \cong X_F(13,1)$. However the curves $X_{1/2}$ and $X_F(13,1)$ are not isomorphic, since they have a different number of points mod 19. □

The proof of Theorem 5.14 in the cases $j = 0, 1728$ is similar.

6. Modular diagonal quotient surfaces

In this section we prove Theorem 2.4.

6.1. **Equations for $Z(13,1)$.** Let $X = X(13) \subset \mathbb{P}^6$ be the A-curve as defined in Section 5.1. By Lemma 3.2 the surface $Z(13,1)$ is birational to the quotient of $X \times X \subset \mathbb{P}^6 \times \mathbb{P}^6$ by the diagonal action of $G \cong \mathrm{PSL}_2(\mathbb{Z}/13\mathbb{Z})$. We write $x_0, \ldots, x_6$ and $y_0, \ldots, y_6$ for our coordinates on the first and second copies of $\mathbb{P}^6$.

Definition 6.1. A *bi-invariant* of degree (m,n) is a polynomial in $x_0, \ldots, x_6$ and $y_0, \ldots, y_6$, 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 obtain equations for $Z(13,1)$ by computing generators and relations for the ring of bi-invariants mod $I(X \times X)$. In practice we only compute some of the generators and some of the relations, and then explain why these are sufficient.

At the start of Section 5.1 we defined invariants Q and F of degrees 2 and 4. We write Q_{20} and F_{40} for these same polynomials viewed as bi-invariants of degrees $(2,0)$ and $(4,0)$. More generally we define bi-invariants Q_{ij} and F_{ij} by the rules

$$Q(\lambda x_0 + \mu y_0, \ldots, \lambda x_6 + \mu y_6) = \lambda^2 Q_{20} + \lambda\mu Q_{11} + \mu^2 Q_{02}$$
$$F(\lambda x_0 + \mu y_0, \ldots, \lambda x_6 + \mu y_6) = \lambda^4 F_{40} + \lambda^3\mu F_{31} + \ldots + \mu^4 F_{04}$$

where the subscripts indicate the degree.

The dimension of the space of bi-invariants of degree (m, n) may be computed from the character table for G. For some small values of m and n these dimensions are as follows.

	0	1	2	3	4	5	6	7	8	9	10
0	1	0	1	0	2	0	4	1	7	3	14
1	0	1	0	2	1	5	5	14	17	37	48
2	1	0	3	1	10	9	32	38	90	118	226
3	0	2	1	10	14	41	67	142	222	402	602
4	2	1	10	14	51	82	198	316	610	938	1592
5	0	5	9	41	82	206	377	746	1244	2152	3346

To compute the bi-invariants of a given degree we use the efficient averaging method described in Remark 5.6.

To find relations between the bi-invariants modulo $I(X \times X)$ we initially worked mod p for some moderately sized prime p, employing the heuristic that a polynomial vanishing at many $\mathbb{F}_p$-points on $X \times X$ is likely to vanish on the whole surface. One way to establish these relations rigorously would be to employ the Gröbner basis machinery in Magma. However this proved too slow in all but the simplest cases. We instead used the following lemma, which is an easy consequence of Bezout's theorem.

Lemma 6.2. *Let I be a bihomogeneous form of degree (m, n) with $m, n \leq 23$. 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. We fix $P_0 \in X$ with $j(P_0) \in \{0, 1728, \infty\}$, and let $f(Q) = I(P_0, Q)$. The hypersurface $\{f = 0\} \subset \mathbb{P}^6$ meets X in at least $84 + 364 + 546 > 42 \times 23$ points. Since X has degree 42 and f has degree $n \leq 23$ it follows by Bezout's theorem that f vanishes identically on X. Therefore I vanishes on $\{P_0\} \times X$. We now fix any $Q_0 \in X$. Applying the same argument to $g(P) = I(P, Q_0)$, and using that $m \leq 23$, shows that I vanishes on $X \times X$. □

We note that if the bihomogeneous form in Lemma 6.2 is a bi-invariant (or a skew bi-invariant, as defined in the next section) then this significantly reduces the amount of work needed to check the hypotheses of the lemma.

If I is a bi-invariant of degree (m, n) then we write I' for the bi-invariant of degree (n, m) obtained by switching the x's and y's. A bi-invariant of degree (m, m) is *symmetric* if $I' = I$, and *anti-symmetric* if $I' = -I$.

The vector space of bi-invariants of degree $(3, 3)$ has dimension 10, and the subspace of symmetric bi-invariants has dimension 9. Making a good choice of

basis for this space significantly simplifies the calculations that follow. To specify our choice of basis $z_1, \ldots, z_9$, we let $m_1, \ldots, m_{10}$ be the monomials

$$x_2^3y_0^2y_1,\ x_1x_4^2y_0^2y_1,\ x_2^2x_3y_0y_1^2,\ x_3x_4x_5y_0y_1^2,\ x_2x_3^2y_1^3,$$
$$x_4^3y_1^3,\ x_0^2x_6y_1^3,\ x_1x_4x_6y_1^3,\ x_2x_5x_6y_1^3,\ x_3x_6^2y_1^3,$$

and then record the coefficients of these monomials in a table.

	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}
z_1	1	−2	−2	4	0	1	1	1	−1	0
z_2	−2	0	4	−2	−1	−1	−2	−1	1	0
z_3	0	−3	0	1	−1	0	0	0	0	0
z_4	0	0	−2	0	0	0	0	0	−1	0
z_5	1	0	−3	0	0	0	1	0	−1	0
z_6	1	−1	−3	0	0	0	1	0	−1	0
z_7	1	−1	−2	4	0	0	1	1	−1	0
z_8	0	−4	2	0	−1	0	0	0	1	−1
z_9	0	0	1	2	0	0	0	0	0	0

Some of these bi-invariants may also be described in terms of the Q_{ij} and F_{ij}. Specifically we have

$$Q_{11}^3 = z_1 + z_5 - z_6 - z_7, \tag{20}$$

$$\begin{aligned} Q_{11}Q_{20}Q_{02} &= z_5 - z_6, \\ Q_{11}F_{22} &= -3(z_6 - z_7 + z_9), \\ Q_{20}F_{13} + Q_{02}F_{31} &= z_1 + z_2 - 4z_4 + z_6 + z_7 - z_8 - 3z_9. \end{aligned} \tag{21}$$

We find using Lemma 6.2 that z_9 and the following 9 quadratic forms in $z_1, \ldots, z_8$ vanish identically on $X \times X$.

$$\begin{aligned} &z_1z_4 - z_3z_5, && z_1z_7 - z_1z_8 + z_2z_7 - z_4z_6 + z_5z_7, \\ &z_1z_6 - z_3z_7, && z_1(z_1 + z_2 - z_3 - z_4 + z_5 - z_7) - z_2z_6 + z_3z_6, \\ &z_4z_7 - z_5z_6, && z_4(z_1 + z_2 - z_3 - z_4 + z_5) - z_3z_8, \\ &z_1^2 + z_1z_2 - z_2z_4, && z_5(z_1 + z_2 - z_3 - z_4 + z_5) - z_1z_8, \\ & && z_8(z_1 + z_5 - z_6 - z_7) - z_5z_7. \end{aligned}$$

These quadratic forms define a rational surface $\Sigma \subset \mathbb{P}^7$. Indeed, the map $\Sigma \to \mathbb{P}^2$ given by projection onto the first 3 coordinates, is a birational map with inverse

$$\begin{aligned} (z_1, \ldots, z_8) = (r, s, 1, r(r+s)/s, r^2(r+s)/s, rf(r,s)/(s(r^2+s-1)), \\ r^2f(r,s)/(s(r^2+s-1)), r(r+s)f(r,s)/s^2) \end{aligned} \tag{22}$$

where $f(r,s) = r^3 + r^2 s - r^2 + s^2 - s$.

The space of anti-symmetric bi-invariants of degree $(3,3)$ is 1-dimensional, spanned by $w = Q_{20}F_{13} - Q_{02}F_{31}$. We write $Z(13,1)$ as a double cover of Σ by finding an expression for w^2 in terms of $z_1, \ldots, z_8$. Specifically, working mod $I(X \times X)$, we find the relation $w^2 + 64(Q_{20}Q_{02})^3 = g(z_1, \ldots, z_8)$ where

$$\begin{aligned} g(z_1,\ldots,z_8) &= z_1z_2 + z_2^2 - 48z_2z_3 + 48z_2z_5 + 126z_2z_6 - 48z_2z_7 - 2z_2z_8 \\ &\quad + 48z_3^2 - 7z_3z_4 - 57z_3z_5 - 108z_3z_6 + 126z_3z_7 + 21z_3z_8 + z_4^2 - 41z_4z_5 \\ &\quad - 26z_4z_6 + 8z_4z_8 + 104z_5^2 - 60z_5z_6 - 106z_5z_7 + 120z_5z_8 + 37z_6^2 - 10z_6z_7 \\ &\quad - 158z_6z_8 + z_7^2 - 70z_7z_8 + z_8^2. \end{aligned}$$

It follows by (20), (21) and (22) that

$$w^2 = ((r-1)/(s^2(r^2+s-1)))^2 F_1(r,s,1)$$

where F_1 is the polynomial defined in Remark 2.5. The bi-invariants therefore define a rational map from $Z(13,1)$ to the surface $y^2 = F_1(r,s,1)$. We show in Remark 6.3 below that this map has degree 1.

We now compute the maps j and j' giving the moduli interpretation of $Z(13,1)$. To do this we need some more bi-invariants, and some more relations. If $\mathbf{v}$ is a covariant of degree m (see Definition 5.5) and $\mathbf{y} = (y_0, \ldots, y_6)^T$ then $\mathbf{y}^T H(Q)\mathbf{v}$ is a bi-invariant of degree $(m,1)$. Applying this construction to $\mathbf{v}_4$ as defined in Section 5.2 gives a bi-invariant I_{41}. We put $I_{32} = (\sum y_i \frac{\partial}{\partial x_i})I_{41}$ and $I_{23} = I'_{32}$. Let c_6 be the invariant of degree 13 defined at the end of Section 5.1, now viewed as a bi-invariant of degree $(13,0)$. Then c'_6 has degree $(0,13)$. Let $\alpha = Q_{20}I_{23}^2$, $\alpha' = Q_{02}I_{32}^2$, $\beta = Q_{02}^6 I_{23}c_6$, $\beta' = Q_{20}^6 I_{32}c'_6$ and $\gamma = (Q_{20}Q_{02})^3$. Working mod $I(X \times X)$ we find some relations

$$\begin{aligned} f_1(\alpha+\alpha') &= f_3, & Q_{11}I_{32}I_{23} &= g_2, \\ f_2(\beta+\beta') &= f_7, & h_2c_6c'_6 &= Q_{11}(\ell_6 + \ell_4\gamma + \ell_2\gamma^2 - 64\gamma^3), \end{aligned}$$

where each f_i, g_i, h_i, ℓ_i is a homogeneous polynomial of degree i in $z_1, \ldots, z_8$. These polynomials are available from [F5]. The relations were checked using Lemma 6.2. Using (20), (21) and (22) we may then write the coefficients of the quadratics $(Y-\alpha)(Y-\alpha')$ and $(Y-\beta)(Y-\beta')$ as rational functions in r and s. The discriminant of each quadratic is equal to $F_1(r,s,1)$ times a square. Moreover, by Theorem 5.8 we have $j = 1728 - \beta^2/(\alpha\gamma^4)$, which we may then write as an element of $\mathbb{Q}(r, s, \sqrt{F_1(r,s,1)})$. The final expressions for j and j' are too complicated to record here, but take the form specified in Theorem 2.4, and are available from [F5].

Remark 6.3. We have constructed rational maps

$$X \times X \longrightarrow Z(13,1) \longrightarrow \{y^2 = F_1(r,s,1)\} \xrightarrow{(j,j')} \mathbb{P}^1 \times \mathbb{P}^1. \tag{23}$$

The composite corresponds to a Galois extension of function fields, with Galois group $G \times G$. Since $G \cong \mathrm{PSL}_2(\mathbb{Z}/13\mathbb{Z})$ 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 (23) 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 $Q_{11}^2/(Q_{20}Q_{02})$ on $X \times X$ is not $G \times G$-invariant. In fact, it is not even $\langle M_6 \rangle \times \langle M_6 \rangle$-invariant. Therefore $Z(13,1)$ is birational to $\{y^2 = F_1(r,s,1)\}$, and this completes the proof of Theorem 2.4 in the case $k = 1$.

6.2. **Equations for $Z(13,2)$.** The calculations here are similar to those in the last section. The main difference is that we modify the definition of a bi-invariant. As in Section 5.3 we write $g \mapsto \widetilde{g}$ for the automorphism of G induced by $\zeta \mapsto \zeta^2$.

Definition 6.4. A *skew bi-invariant* of degree (m,n) is a polynomial in $x_0, \ldots, x_6$ and $y_0, \ldots, y_6$, that is homogeneous of degrees m and n in the two sets of variables, and is invariant under the action of G via $g : (x,y) \mapsto (gx, \widetilde{g}y)$.

The polynomials Q_{20} and Q_{02} defined in Section 6.1 are skew bi-invariants, but Q_{11} is not. The dimension of the space of skew bi-invariants of degree (m,n) may again be computed from the character table for G. For some small values of m and n these dimensions are as follows.

	0	1	2	3	4	5	6	7	8	9	10
0	1	0	1	0	2	0	4	1	7	3	14
1	0	0	0	1	1	4	5	14	17	37	48
2	1	0	3	1	10	9	32	38	90	118	226
3	0	1	1	9	14	40	67	142	222	402	602
4	2	1	10	14	51	82	198	316	610	938	1592
5	0	4	9	40	82	205	377	746	1244	2152	3346

In particular the spaces of skew bi-invariants of degrees $(2,2)$ and $(3,3)$ have dimensions 3 and 9. The first of these spaces has basis t_1, t_2, t_3 where

$$t_1 = 2x_0^2y_0^2 + x_4^2y_0y_1 + \ldots$$
$$t_2 = (x_0^2 - x_1x_4 - x_2x_5 - x_3x_6)y_0^2 + x_4^2y_0y_1 + \ldots$$
$$t_3 = (-5x_0^2 + x_1x_4 + x_2x_5 + x_3x_6)y_0^2 - (x_4^2 + 2x_1x_6)y_0y_1 + \ldots.$$

To specify the first 5 polynomials in the basis $u_1, \ldots, u_9$ we chose for the space of skew bi-invariants of degree $(3,3)$, we let $m_1, \ldots, m_9$ be the monomials

$$x_2^2x_3y_0^2y_1,\ x_1x_2^2y_0y_1^2,\ x_3^3y_0y_1^2,\ x_0^2x_5y_0y_1^2,\ x_1x_3^2y_1^3,\ x_2^2x_4y_1^3,\ x_4^2x_5y_1^3,\ x_1x_5x_6y_1^3,\ x_0x_6^2y_1^3,$$

and then record the coefficients of these monomials in a table

	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9
u_1	0	-2	0	0	-1	0	0	-1	0
u_2	-3	1	0	-1	0	0	0	1	0
u_3	0	2	0	0	1	0	1	2	0
u_4	-1	1	0	1	0	0	0	0	0
u_5	-1	-2	-1	-3	0	0	0	0	1

Amongst other relations, we found that $u_6, \dots, u_9$ and the following polynomials vanish identically on $X \times X$.

$$u_3u_4 - u_1u_5, \qquad u_2^3 - u_1u_2u_3 - 2u_2^2u_3 - u_2^2u_4 + u_1u_3u_4 + u_2u_3u_4 - u_2u_3u_5,$$
$$t_2u_4 - t_3u_1, \qquad t_1u_1(u_2 - u_3) - t_2(u_1u_2 - u_1u_4 + u_2u_3 + u_2u_5),$$
$$t_1t_2^2 - u_1u_3.$$

The first two relations define a rational surface $\Sigma \subset \mathbb{P}^4$, parametrised by

$$(u_1, \dots, u_5) = (r, 1, -rs, f(r,s), -sf(r,s))$$

where $f(r,s) = (r^2s + 2rs + 1)/(r^2s + rs^2 + rs + 1)$. The other three show that

$$(t_1, t_2, t_3) = (-s(r^2 + rs + r + 1)/\tau, r(r^2s + rs^2 + rs + 1)/\tau, (r^2s + 2rs + 1)/\tau)$$

where $\tau^3 = (r^2 + rs + r + 1)(r^2s + rs^2 + rs + 1)^2$.

For I a skew bi-invariant we write I' for the skew bi-invariant obtained as

$$I'(x;y) = I(y; -x_0, -x_2, -x_3, -x_4, -x_5, -x_6, -x_1).$$

It may be checked that $I'' = I$. The space of skew bi-invariants of degree $(3,2)$ is spanned by $I_{32} = 12(x_1x_3x_5 - x_2x_4x_6)y_0^2 + \dots$ and the space of skew bi-invariants of degree $(4,1)$ is spanned by $I_{41} = \mathbf{y}^T H(Q)\mathbf{w}_4$ where $\mathbf{w}_4$ is the skew covariant defined in Section 5.3. We put $I_{23} = I'_{32}$ and $I_{14} = I'_{41}$. Let $\alpha = Q_{20}^3 I_{14}^2$, $\alpha' = Q_{02}^3 I_{41}^2$, $\beta = Q_{02}^5 I_{14} c_6$, $\beta' = Q_{20}^5 I_{41} c_6'$ and $\gamma = I_{32}I_{23}$. Working mod $I(X \times X)$ we find some relations

$$\begin{aligned}
Q_{20}Q_{02} &= t_1 - t_2, \\
I_{41}I_{14} &= (t_1 - t_2)(u_1 + u_2 - 3u_3 - u_4), \\
u_1(u_1 + u_3)\gamma &= f_{11}, \\
t_3(t_1 + t_3)(\alpha + \alpha') &= f_{12}, \\
4(t_1^2t_3 + u_4u_5)(\beta + \beta') &= f_{20} + f_{15}\gamma + f_{10}\gamma^2 + f_5\gamma^3, \\
g_{10}c_6c_6' &= f_{23} + f_{18}\gamma + f_{13}\gamma^2 + f_8\gamma^3,
\end{aligned}$$

where each f_i, g_i is a polynomial of weighted degree i in $t_1, t_2, t_3, u_1, \dots, u_5$, where the t's have weight 2 and the u's have weight 3. These polynomials are available

from [F5]. The relations were checked using Lemma 6.2. Using these relations, and the above parametrisation of Σ, we may write the coefficients of the quadratics $(Y-\alpha\tau)(Y-\alpha'\tau)$ and $(Y-\beta\tau)(Y-\beta'\tau)$ as rational functions in r and s. The discriminant of each quadratic is equal to $F_2(r,s,1)$ times a square, where F_2 is the polynomial defined in Remark 2.5. The skew bi-invariants therefore define a rational map from $Z(13,2)$ to the surface $\{y^2=F_2(r,s,1)\}$. Adapting the argument in Remark 6.3 shows that this map has degree 1. Moreover by Theorem 5.8 we have $j=1728-\beta^2/(\alpha(Q_{20}Q_{02})^{10})$, which we may then rewrite as an element of $\mathbb{Q}(r,s,\sqrt{F_2(r,s,1)})$. This gives the moduli interpretation, and so completes the proof of Theorem 2.4 in the case $k=2$.

7. Modular curves on $Z(13,1)$ and $Z(13,2)$

Following on from Sections 2.2 and 2.3 we describe some more modular curves on the surfaces $Z(13,1)$ and $Z(13,2)$.

Let $m\geq 2$ be an integer coprime to 13. Then any pair of m-isogenous elliptic curves are 13-congruent with power k, where $k=1$ if m is a quadratic residue mod 13, and $k=2$ otherwise. There is therefore a copy of the modular curve $X_0(m)$ on the surface $Z(13,k)$. In Table 1 we explicitly identify these curves in all cases where the genus g of $X_0(m)$ is 0 or 1. The polynomials F_1 and F_2 were defined in Remark 2.5.

In compiling Table 1 we used the `SmallModularCurve` database in Magma to check the moduli interpretations. For example, the entry with $m=10$ shows that $Z(13,1)$ contains a curve isomorphic to $y^2=t^2+16t-16$. We parametrise this curve by putting $t=-(T^2+8T+20)/T$, and find by Theorem 2.4(iii) that

$$X^2-(j+j')X+jj'=\big(X-j_{10}(T)\big)\big(X-j_{10}(20/T)\big)$$

where

$$j_{10}(T)=\frac{(T(T+4)^5+16T+80)^3}{T(T+4)^5(T+5)^2}$$

is the j-map on $X_0(10)$.

To find many of these curves it was necessary to blow up the surfaces in Theorem 2.4. For example, the entry with $m=15$ shows that when we blow up our model for $Z(13,2)$ at $(r:s:1)=(1:-1:0)$ we obtain a curve isomorphic to $y^2=(t^2+t-1)(t^2+13t+11)$. Putting this elliptic curve in Weierstrass form we find it has Cremona label $15a1$, and is therefore isomorphic to $X_0(15)$.

The surfaces $Z(13,1)$ and $Z(13,2)$ also contain modular curves of level 13. For example, the factors of D_1 and D_2 (as defined in Theorem 2.4(iii)) appearing with multiplicity 13, say δ_1 and δ_2, each define a copy of the genus 2 curve $X_1(13)$. In fact it is a general phenomenon, exploited in [KS], that $Z(n,k)$ contains copies of $X_1(n)$ above $j=\infty$ and $j'=\infty$.

TABLE 1. Copies of $X_0(m)$ on $Z(13,1)$ or $Z(13,2)$

m	g	Formula specifying a curve on (a blow up of) $y^2 = F_k(r,s,1)$
2	0	$F_2(4, -3-\varepsilon^2+t\varepsilon^4, -2+2\varepsilon) = 2^{18}(4t+1)\varepsilon^4 + O(\varepsilon^5)$
3	0	$F_1(1, 1+\varepsilon+t\varepsilon^3, 2+\varepsilon) = 16(54t+1)\varepsilon^4 + O(\varepsilon^5)$
4	0	$F_1(1, t\varepsilon^2, -1+\varepsilon) = 4(32t+1)\varepsilon^2 + O(\varepsilon^3)$
5	0	$F_2(t\varepsilon^2, 1, -1+\varepsilon) = -(16t^2+44t-1)\varepsilon^4 + O(\varepsilon^5)$
6	0	$F_2(\varepsilon^3, t, \varepsilon^2) = t^6(t^2+34t+1)\varepsilon^{18} + O(\varepsilon^{19})$
7	0	$F_2(1, -1+t\varepsilon^2+t\varepsilon^3, -1+t\varepsilon^2) = t^4(t+1)(t-27)\varepsilon^{12} + O(\varepsilon^{13})$
8	0	$F_2(\varepsilon^2-\varepsilon^3-t\varepsilon^4, -1, -\varepsilon) = (t^2+28t+68)\varepsilon^{14} + O(\varepsilon^{15})$
9	0	$F_1(\varepsilon, 1-\varepsilon^2+t\varepsilon^3, 1) = (t^2-18t-27)\varepsilon^6 + O(\varepsilon^7)$
10	0	$F_1(0, t, 1) = t^4(t-1)^2(t^2+16t-16)$
11	1	$F_2(1, -\varepsilon^3+\varepsilon^4+t\varepsilon^5, \varepsilon) = (t+2)(t^3-14t^2-12t-4)\varepsilon^{20} + O(\varepsilon^{21})$
12	0	$F_1(1, -1+t\varepsilon, \varepsilon) = t^2(t^2+14t+1)\varepsilon^4 + O(\varepsilon^5)$
14	1	$F_1(\varepsilon, 1, -\varepsilon^2+t\varepsilon^3) = (t^4+14t^3+19t^2+14t+1)\varepsilon^{12} + O(\varepsilon^{13})$
15	1	$F_2(1, -1+t\varepsilon, \varepsilon) = (t^2+t-1)(t^2+13t+11)\varepsilon^4 + O(\varepsilon^5)$
16	0	$F_1(1, \varepsilon, 1+t\varepsilon) = (4t^2+4t-7)\varepsilon^2 + O(\varepsilon^3)$
17	1	$F_1(t\varepsilon, \varepsilon^2, t) = t^8(t^4-6t^3-27t^2-28t-16)\varepsilon^8 + O(\varepsilon^9)$
18	0	$F_2(t, 0, 1) = t^2+10t+1$
19	1	$F_2(-1, t, 1) = (t-1)^4(t-2)(t^3+10t^2+12t+4)$
20	1	$F_2(t, 1, 1) = (t+1)^6(t^4+12t^3+28t^2+32t+16)$
21	1	$F_2(1, -t^2, t) = t^8(t+1)^4(t^4+6t^3-17t^2+6t+1)$
24	1	$F_2(t^3+2t^2, -1, t^2+2t) = t^{10}(t+1)^6(t+2)^6(t^4-4t^3-16t^2-8t+4)$
25	0	$F_1(t, -t, 1) = t^4(t^2+4t-16)$
27	1	$F_1(t, t^2, -1) = t^8(t+2)(t^3-6t^2-4)$
32	1	$F_2(t+1, -t^3, t^2+t) = t^{20}(t+1)^6(4t^4-12t^2-16t-7)$
36	1	$F_1(t+1, -t^2-t-1, -t^2-t) = t^{12}(t+1)^4(4t^4+8t^3+12t^2+8t+1)$
49	1	$F_1(t, -t^2, t-1) = t^8(t-2)^2(t-1)^4(t+1)^2(t^4-6t^3+3t^2+18t-19)$

Setting $j = j'$ in Theorem 2.4 give a curve whose irreducible components are modular curves of level 13. This gives a convenient way of computing the double covers $X_{\mathrm{s}}(13) \to X_{\mathrm{s}}^+(13)$ and $X_{\mathrm{ns}}(13) \to X_{\mathrm{ns}}^+(13)$, as were recently computed by another method in [DMS]. The details are as follows. Recall that in Theorem 2.4 we wrote $Z(13,k)$ as a double cover of $\mathbb{P}^2$. We also wrote $j+j'$ and jj' as

rational functions in r and s. We now put $r = x/z$ and $s = y/z$, and factor the numerator and denominator of $(j - j')^2$ into irreducible polynomials in $\mathbb{Q}[x, y, z]$. Let $\Delta_k(x, y, z) = z^4\delta_k(x/z, y/z)$. In the cases $k = 1$ and $k = 2$ we obtain

$$(j - j')^2 = \frac{F_1(G_1G_2H_1H_2H_3M)^2}{y^8z^8(x + y - z)^6(x^2 + yz - z^2)^2\Delta_1^{26}}$$

and

$$(j - j')^2 = \frac{F_2(G_3G_4G_5H_4H_5H_6)^2}{x^{10}z^{10}(x^2 + xy + xz + z^2)^4\Delta_2^{26}}$$

where

- F_1 and F_2 are as in Remark 2.5. As noted in Section 2.3, they define copies of $X_{\mathrm{s}}^+(13)$ and $X_{\mathrm{ns}}^+(13)$.
- $G_1, \dots, G_5$ have degrees $8, 11, 9, 10, 11$. Each defines a copy of $X_{\mathrm{s}}^+(13)$ with inverse image in $Z(13, k)$ a copy of $X_{\mathrm{s}}(13)$.
- $H_1, \dots, H_6$ have degrees $8, 11, 13, 7, 10, 12$. Each defines a copy of $X_{\mathrm{ns}}^+(13)$ with inverse image in $Z(13, k)$ a copy of $X_{\mathrm{ns}}(13)$.
- M has degree 8, but factors as the product of two quartics defined over $\mathbb{Q}(\zeta_{13})$. Each factor defines a curve whose inverse image in $Z(13, 1)$ is a copy of $X_1(13)$, but with a non-standard moduli interpretation.

There is a group-theoretic explanation for the factorisations of these numerators. In the case $k = 1$ we let $\mathrm{PSL}_2(\mathbb{Z}/13\mathbb{Z})$ act on its non-trivial elements by conjugation, and find that there are 8 orbits, with stabilisers conjugate to (in an obvious notation)

$$C_{\mathrm{s}}^+, C_{\mathrm{s}}, C_{\mathrm{s}}, C_{\mathrm{ns}}, C_{\mathrm{ns}}, C_{\mathrm{ns}}, B, B.$$

In the case $k = 2$ we let $\mathrm{PSL}_2(\mathbb{Z}/13\mathbb{Z})$ acts by conjugation on the elements in $\mathrm{PGL}_2(\mathbb{Z}/13\mathbb{Z})$ whose determinant is not a square, and find that there are 7 orbits, with stabilisers conjugate to

$$C_{\mathrm{ns}}^+, C_{\mathrm{s}}, C_{\mathrm{s}}, C_{\mathrm{s}}, C_{\mathrm{ns}}, C_{\mathrm{ns}}, C_{\mathrm{ns}}.$$

8. Examples

8.1. **Examples over $\mathbb{Q}$.** We use our results, as presented in Section 2, to exhibit some non-trivial pairs of 13-congruent elliptic curves over $\mathbb{Q}$.

Example 8.1. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - 4x - 3$, labelled 52a2 in Cremona's tables.[1] Taking $a = -4$ and $b = -3$ we find on $X_E(13, 1)$ the point

$$(-30 : 23 : -72 : -16 : 0 : 16 : 1)$$

mapping to $j = -2^8 \cdot 3^3 \cdot 151^3 \cdot 2399^3/(13 \cdot 19^{13})$. This is the j-invariant of the elliptic curve $E'/\mathbb{Q}$ with Cremona label 988b1. Therefore E is directly 13-congruent to

[1] Confusingly, the numbering of the elliptic curves in the isogeny class $52a$ is different in Cremona's tables and in the LMFDB.

the quadratic twist of E' by some square-free integer d. Comparing a few traces of Frobenius shows that $d = 1$.

Example 8.2. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + x - 10$, labelled 52a1 in Cremona's tables. Taking $a = 1$ and $b = -10$ we find on $X_E(13, 2)$ the points

$$(9 : 0 : 4 : 2 : -2 : 2 : -1), \qquad (134 : -45 : 134 : 44 : 5 : -18 : 4),$$

mapping to $j = 2^{14} \cdot 3^3/13$ and $-2^8 \cdot 3^3 \cdot 151^3 \cdot 2399^3/(13 \cdot 19^{13})$. These correspond to the elliptic curves 52a2 and 988b1 that are each skew 13-congruent to E.

In Theorem 2.4 we gave equations for the surfaces $Z(13, 1)$ and $Z(13, 2)$, each as a double cover of $\mathbb{P}^2$. We use these formulae to exhibit some non-trivial pairs of 13-congruent elliptic curves over $\mathbb{Q}$, where both curves are beyond the range of Cremona's tables.

Example 8.3. There is a $\mathbb{Q}$-rational point on the surface $Z(13, 1)$ above $(r : s : 1) = (4 : 5 : 3)$. This maps to the pair of j-invariants

$$j = \frac{-257^3 \cdot 811^3}{2^2 \cdot 3^{12} \cdot 5^4 \cdot 11} \qquad \text{and} \qquad j' = \frac{-441851363^3}{2^5 \cdot 3 \cdot 5 \cdot 11 \cdot 23^{13}}.$$

These are the j-invariants of a pair of directly 13-congruent elliptic curves

$$E: \quad y^2 + xy + y = x^3 - 464619x - 122105558$$
$$E': \quad y^2 + xy + y = x^3 - 11276810818409x + 14959107699948354572$$

with conductors $N = 3778170 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 107^2$ and $N' = 86897910 = 23N$.

Example 8.4. There is a $\mathbb{Q}$-rational point on the surface $Z(13, 2)$ above $(r : s : 1) = (2 : -9 : 6)$. This maps to the pair of j-invariants

$$j = \frac{29^3 \cdot 61^3 \cdot 103}{2^{19} \cdot 3^7 \cdot 17} \qquad \text{and} \qquad j' = \frac{13^3 \cdot 103^2 \cdot 270539^3}{2 \cdot 3^3 \cdot 17^2 \cdot 19^{13}}.$$

These are the j-invariants of a pair of skew 13-congruent elliptic curves

$$E: \quad y^2 + xy = x^3 + 3796x - 685680$$
$$E': \quad y^2 + xy = x^3 + 8246713256941x + 11003401358367836019$$

with conductors $N = 1082118 = 2 \cdot 3 \cdot 17 \cdot 103^2$ and $N' = 20560242 = 19N$.

8.2. **Examples over $\mathbb{Q}(t)$.** The following pairs of 13-congruent elliptic curves over $\mathbb{Q}(t)$ were found as described in Section 2.2. By specialising t they give rise to infinitely many non-trivial pairs of 13-congruent elliptic curves over $\mathbb{Q}$.

Example 8.5. Let $E/\mathbb{Q}(t)$ be the elliptic curve

$$E: \quad y^2 = x^3 - 3p^2qf_1x + 2p^2q^2f_2,$$

where $p(t) = t^2 - 3t - 1$, $q(t) = t^3 - 2t^2 - 3t - 8$, and

$$\begin{aligned} f_1(t) &= t^7 + 4t^6 + 8t^5 + 6t^4 - 8t^3 - 24t^2 - 27t - 8, \\ f_2(t) &= t^{11} + 4t^{10} + 5t^9 - 12t^8 - 63t^7 - 124t^6 - 137t^5 - 80t^4 - 61t^3 - 72t^2 \\ &\quad - 153t + 8. \end{aligned}$$

Taking $a = -3p^2qf_1$ and $b = 2p^2q^2f_2$, we find on $X_E(13,1)$ the point

$$\begin{aligned} &(2592t(t+1)(t^2+2t+3)p^2qr^2 : -432t^2(2t^2+3t+7)p^2qr^2 \\ &\qquad : -72(t^3+2t^2+4t-1)p^2qr : 72p^2qr \\ &\qquad : -6(t^6-3t^4-11t^3-14t^2-5t-4)p : -24(t-1)pr : t-1) \end{aligned}$$

where $r(t) = t^3+t^2+2t-1$. This point maps to $j' = pg_1^3/(rd) = 1728+(qg_2^2)/(rd)$ where

$$\begin{aligned} g_1(t) &= t^{31} + 23t^{30} + 270t^{29} + 2379t^{28} + 17607t^{27} + 110676t^{26} + 586710t^{25} \\ &\quad + 2624262t^{24} + 9977316t^{23} + 32555542t^{22} + 92002244t^{21} + 226872066t^{20} \\ &\quad + 490871649t^{19} + 935166681t^{18} + 1571157252t^{17} + 2326844467t^{16} \\ &\quad + 3029704865t^{15} + 3450459162t^{14} + 3407984048t^{13} + 2880044002t^{12} \\ &\quad + 2037108963t^{11} + 1159162859t^{10} + 486247810t^9 + 109783239t^8 \\ &\quad - 25731445t^7 - 37205624t^6 - 17036352t^5 - 3782272t^4 - 99968t^3 \\ &\quad + 90624t^2 + 50176t + 8192, \\ g_2(t) &= t^{46} + 34t^{45} + 586t^{44} + \ldots - 10680320t^2 - 2752512t - 262144, \\ d(t) &= t^4(t+2)^3(t^4+4t^3+9t^2+11t+8)(t^6+4t^5+9t^4+8t^3+2t^2-9t-6)^{13}. \end{aligned}$$

This is the j-invariant of an elliptic curve directly 13-congruent to E. (Notice that the full formula for g_2 may be recovered from the equality of two expressions we gave for j'.) Specialising t and comparing traces of Frobenius, we find that the correct quadratic twist is

$$E': \quad y^2 = x^3 - 3p^3q^3g_1x + 2p^4q^5g_2.$$

In Table 2 we record some pairs of 13-congruent elliptic curves over $\mathbb{Q}$, obtained by specialising the parameter t in Example 8.5. In each case we have taken simultaneous quadratic twists so that E has conductor as small as possible. Only the first 2 pairs of elliptic curves in Table 2 are isogenous (via an isogeny of the degree indicated). Example 8.5 therefore shows that there are infinitely many non-trivial pairs of directly 13-congruent elliptic curves over $\mathbb{Q}$.

TABLE 2. Pairs of directly 13-congruent elliptic curves

t	E	E'	deg	t	E	E'
1	$11a3$	$11a2$	25	$1/4$	$7707798*$	$27925352154*$
-1	$768h1$	$768h4$	10	-3	$15211515*$	$1566786045*$
4	$13688b1$	$8363368*$		$8/5$	$46427580*$	$5448415795740*$
2	$27930s1$	$27930r1$		3	$48963840*$	$42941287680*$
-4	$80408l1$	$8282024*$		5	$147656145*$	$1624217595*$
$-1/2$	$83030b1$	$913330*$		$7/2$	$192105606*$	$23030964786522*$
$-1/3$	$271545f1$	$589524195*$		$5/2$	$774703710*$	$6034167197190*$
$1/2$	$5429670*$	$320350530*$		7	$1040014080*$	$24181367374080*$

Example 8.6. Let $E/\mathbb{Q}(t)$ be the elliptic curve

$$E: \quad y^2 = x^3 - 3pq^2 f_1 x + 2pq^2 f_2.$$

where $p(t) = t^2 + t + 1$, $q(t) = 5t^2 + 8t + 11$, and

$$f_1(t) = t^4 - 13t^3 - 4t^2 - 5t + 1,$$
$$f_2(t) = 59t^9 + 183t^8 + 477t^7 + 315t^6 + 54t^5 - 570t^4 - 499t^3 - 429t^2 - 123t - 43.$$

Taking $a = -3pq^2 f_1$ and $b = 2pq^2 f_2$, we find on $X_E(13, 2)$ the point

$$(-2pqr_1 : pqr_2 : 2r_3 : -24(t+1)^2(t^2+1)^2 : tr_4 : 2t : 0)$$

where

$$r_1(t) = 29t^7 + 15t^6 + 7t^5 - 32t^4 + 89t^3 + 73t^2 + 83t + 24,$$
$$r_2(t) = 55t^7 + 117t^6 + 269t^5 + 356t^4 + 211t^3 + 179t^2 + 25t + 36,$$
$$r_3(t) = t^6 - 14t^5 - 43t^4 - 85t^3 - 106t^2 - 53t - 36,$$
$$r_4(t) = 13t^5 + 34t^4 + 17t^3 + 11t^2 - 22t - 5.$$

This point maps to $j' = pqg_1^3/d = 1728 - g_2^2/d$ where

$$g_1(t) = 211t^{14} + 665t^{13} + 1079t^{12} + 414t^{11} - 1754t^{10} - 5658t^9 - 9756t^8 - 12536t^7 - 12796t^6 - 10606t^5 - 7358t^4 - 4030t^3 - 1831t^2 - 553t - 131,$$
$$g_2(t) = 3107t^{23} + 45563t^{22} + 257591t^{21} + \ldots + 35789t + 4973,$$
$$d(t) = (t+1)(t^2+1)(2t^2+t+1)^2(2t^3+2t^2+3t+1)^{13}.$$

This is the j-invariant of an elliptic curve skew 13-congruent to E. Specialising t and comparing traces of Frobenius, we find that the correct quadratic twist is

$$E' : \quad y^2 = x^3 + 3pq^3g_1x + 2pq^4g_2.$$

In Table 3 we record some pairs of 13-congruent elliptic curves over $\mathbb{Q}$, obtained by specialising the parameter t in Example 8.6. In each case we have taken simultaneous quadratic twists so that E has conductor as small as possible. Only the first 3 pairs of elliptic curves in Table 3 are isogenous (via an isogeny of the degree indicated). Example 8.6 therefore shows that there are infinitely many non-trivial pairs of skew 13-congruent elliptic curves over $\mathbb{Q}$.

TABLE 3. Pairs of skew 13-congruent elliptic curves

T	E_1	E_2	deg	T	E_1	E_2
0	$121c1$	$121c2$	11	3	$185900a1$	$7621900*$
1	$162c1$	$162c4$	21	-7	$255162e1$	$4848078*$
$-1/3$	$1225h1$	$1225h2$	37	$1/2$	$1242150*$	$1242150*$
-3	$1960i1$	$21560l1$		$1/7$	$1695978*$	$429082434*$
-2	$14175k1$	$184275o1$		$-3/2$	$2141594*$	$49256662*$
$1/3$	$23660f1$	$733460*$		$-3/5$	$2147950*$	$2147950*$
$-3/4$	$92950q1$	$2881450*$		-5	$4746924*$	$507920868*$
$-1/2$	$98010s1$	$98010t1$		$1/5$	$7495800*$	$397277400*$

8.3. **Tables.** In Tables 4 and 5 we list some $\mathbb{Q}$-rational points on $Z(13,1)$ and $Z(13,2)$ that do not lie on any of the curves of genus 0 or 1 in Section 2.2. In Table 6 we list some pairs of 13-congruent elliptic curves over $\mathbb{Q}$ with small conductor. We have 3 methods for finding such examples

- We sort Cremona's tables by traces of Frobenius mod 13 and look for matches. This method is described more fully in [CF].
- We loop over all elliptic curves E in Cremona's tables (ignoring quadratic twists of earlier curves) and search for rational points on $X_E(13,1)$ and $X_E(13,2)$. In many cases the second elliptic curve is beyond the range of Cremona's tables.
- We search for rational points on $Z(13,1)$ and $Z(13,2)$. This can give examples where both curves are beyond the range of Cremona's tables.

Elliptic curves are specified either by their Cremona label, or by writing $N*$ where N is the conductor of the elliptic curve. In the latter case Weierstrass equations are available from [F5]. We do not list examples that could be deduced from earlier entries by swapping over the curves, by using an isogeny of degree

TABLE 4. Known rational points on $Z(13,1)$

$(2,1,-3)$	$(15,-63,4)$	$(104,-481,64)$	$(-5110,5329,1176)$
$(-3,4,3)$	$(60,-65,16)$	$(680,-175,289)$	$(6552,-1352,2835)$
$(-2,5,4)$	$(30,68,63)$	$(630,685,-324)$	$(-6920,8477,4800)$
$(4,5,3)$	$(21,-1,98)$	$(440,-48,1085)$	$(2470,9025,7436)$
$(3,1,-6)$	$(-51,136,111)$	$(495,81,-1144)$	$(-4389,9386,9702)$
$(-6,11,9)$	$(-78,172,169)$	$(442,1224,1183)$	$(7259,1525,9996)$
$(-12,16,9)$	$(39,169,180)$	$(1430,-1469,225)$	$(3105,13225,994)$
$(14,4,-21)$	$(-56,256,245)$	$(280,-1656,49)$	$(13340,4205,-5819)$
$(-5,23,6)$	$(-17,289,20)$	$(-1326,2312,1521)$	$(10540,289,-26908)$
$(-15,25,18)$	$(95,-7,418)$	$(3540,-3481,144)$	$(-34086,34385,3249)$
$(38,7,12)$	$(455,169,294)$	$(1309,-3757,588)$	$(8015,58166,-833)$
$(15,-40,9)$	$(476,289,240)$	$(4144,-999,2695)$	$(-220836,913936,859705)$

TABLE 5. Known rational points on $Z(13,2)$

$(1,6,2)$	$(-9,40,30)$	$(-1176,1331,231)$	$(7546,1350,-735)$
$(-8,5,4)$	$(-40,27,24)$	$(1445,-216,510)$	$(-1682,1331,11484)$
$(1,-8,6)$	$(17,-56,34)$	$(-532,2197,1235)$	$(4563,12167,13455)$
$(8,-1,4)$	$(15,-64,20)$	$(63,2560,120)$	$(14175,-1331,4389)$
$(2,-9,6)$	$(-49,64,140)$	$(-1989,2744,2730)$	$(1156,-15625,5525)$
$(1,-7,9)$	$(175,32,140)$	$(2975,1,-255)$	$(13248,-42875,21840)$
$(11,-8,22)$	$(-64,343,280)$	$(925,-2662,4070)$	$(-78352,54925,21580)$
$(5,-24,14)$	$(153,343,-105)$	$(175,-4608,3080)$	$(25205,-98304,47712)$
$(27,-1,12)$	$(-363,250,165)$	$(1007,-4913,2584)$	$(-159367,109744,81016)$
$(-8,27,12)$	$(790,-343,1106)$	$(-845,4968,1482)$	
$(-20,27,30)$	$(-1107,824,246)$	$(-5635,6859,1995)$	

coprime to 13, or by taking simultaneous quadratic twists. We specify whether the 13-congruence is direct ($k=1$) or skew ($k=2$). The entries in bold are examples coming from the infinite families in Examples 8.5 and 8.6.

The examples where both E and E' are within the range of Cremona's tables were independently found by Cremona and Freitas. Indeed, there are 18 such pairs

TABLE 6. Pairs of 13-congruent elliptic curves

k	E	E'	k	E	E'
2	$52a1$	$988b1$	1	**271545f1**	**589524195**$*$
1	$345b1$	$10005m1$	2	$314330i1$	$314330j1$
2	$735c1$	$9555h1$	2	1082118$*$	20560242$*$
1	$1190a1$	$265370d1$	2	1137150$*$	76189050$*$
1	$1274h1$	$21658t1$	2	**1242150**$*$	**1242150**$*$
1	$1445b1$	$10115e1$	1	1296924$*$	1437132$*$
2	**1960i1**	**21560l1**	2	1425720$*$	1425720$*$
1	$3990ba1$	$43890cu1$	2	**1695978**$*$	**429082434**$*$
2	$4719b1$	$33033k1$	2	**2141594**$*$	**49256662**$*$
2	$5070j1$	$35490bg1$	2	**2147950**$*$	**2147950**$*$
1	$11638o1$	$151294h1$	2	2164218$*$	413365638$*$
2	$12274c1$	$135014s1$	2	2228037$*$	69069147$*$
1	**13688b1**	**8363368**$*$	1	2428110$*$	31565430$*$
2	**14175k1**	**184275o1**	2	3647770$*$	69307630$*$
1	$20184i1$	$20184j1$	1	3778170$*$	86897910$*$
2	**23660f1**	**733460**$*$	1	3944850$*$	3944850$*$
1	**27930s1**	**27930r1**	2	4083510$*$	730948290$*$
2	$29970f1$	4705290$*$	2	**4746924**$*$	**507920868**$*$
2	$69230m1$	761530$*$	1	**5429670**$*$	**320350530**$*$
1	**80408l1**	**8282024**$*$	2	**7495800**$*$	**397277400**$*$
1	**83030b1**	**913330**$*$	1	**7707798**$*$	**27925352154**$*$
2	**92950q1**	**2881450**$*$	2	10052196$*$	3608738364$*$
1	$95370cl1$	$95370cm1$	1	**15211515**$*$	**1566786045**$*$
2	**98010s1**	**98010t1**	2	15893150$*$	842336950$*$
2	$162266e1$	17686994$*$	2	**16207776**$*$	**1183167648**$*$
2	$177735a1$	1955085$*$	2	**17859765**$*$	**553652715**$*$
2	**185900a1**	**7621900**$*$	1	21140427$*$	264234197073$*$
2	$237538k1$	23041186$*$	1	21219400$*$	233413400$*$
2	**255162e1**	**4848078**$*$	2	21997290$*$	285964770$*$

in Table 6 which, together with the 3 elliptic curves (52a2, 735c2, 1190a2) isogenous to those already in the table, gives the 39 examples in [CF, Section 3.7]. In addition the pair of curves with conductor $1242150 = 2 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 13^2$ was independently found by Best and Matschke [Be], in connection with their work tabulating elliptic curves with good reduction outside $\{2, 3, 5, 7, 11, 13\}$.

Appendix A. Elliptic curves whose 13-torsion subgroups have isomorphic semi-simplifications

If elliptic curves E_1 and E_2 over $\mathbb{Q}$ are 13-congruent then their traces of Frobenius are congruent mod 13 at all primes of good reduction. The converse is also true provided that the elliptic curves E_1 and E_2 do not admit a rational 13-isogeny. Otherwise, the Chebotarev density theorem and Brauer Nesbitt theorem only give that $E_1[13]$ and $E_2[13]$ have isomorphic semi-simplifications.

Theorem A.1. *There are infinitely many pairs of elliptic curves E_1 and E_2 over $\mathbb{Q}$, each admitting a rational 13-isogeny, such that $E_1[13]$ and $E_2[13]$ have isomorphic semi-simplifications. Moreover these examples correspond to infinitely many pairs of j-invariants.*

We prove the theorem by finding pairs of 13-isogenies whose kernels are isomorphic as Galois modules. It then follows by properties of the Weil pairing that the 13-torsion subgroups have isomorphic semi-simplifications. After we had completed the proof of Theorem A.1 we discovered that essentially the same proof was given by N. Elkies in 2013 in response to a question asked by S. Keil at

`https://mathoverflow.net/questions/129818/elliptic-curves-over-qq-with-identical-13-isogeny`

Our motivation for considering Theorem A.1 is the following question of N. Freitas, to which we still do not know an answer.

Question A.2 (Freitas)**.** *Are there any pairs of 13-congruent elliptic curves over $\mathbb{Q}$ where one (and hence both) of these curves admits a rational 13-isogeny?*

Proof of Theorem A.1. Let t be the coordinate on $X_0(13) \cong \mathbb{P}^1$ specified in Section 2.1, and let $s = t + 4$. The modular curve $X_1(13)$ is the genus 2 curve

$$y^2 = (x^3 - 3x + 1)^2 - 2(x^3 - 3x + 1)x(x - 1) + 5x^2(x - 1)^2$$

with automorphism group $G \cong C_6$ generated by $x \mapsto 1/(1 - x)$ and $y \mapsto -y$. The forgetful map $\pi : X_1(13) \to X_0(13)$ quotients out by this action, and is given by

$$(x, y) \mapsto s = \frac{x^3 - 3x + 1}{x(x - 1)} = x + \frac{1}{1 - x} + \frac{x - 1}{x}.$$

We claim that the quotient of $X_1(13) \times X_1(13)$ by the diagonal action of G is birational to the surface $\Sigma = \{Y^2 = f(T^3 - 3T + 1, T(T-1); X)\} \subset \mathbb{A}^3$ where

$$f(\lambda, \mu; X) = (X^2 - 2X + 5)\big((\lambda^2 - 2\lambda\mu + 5\mu^2)X^2 - 2(\lambda^2 + \lambda\mu + 6\mu^2)X + (5\lambda^2 - 12\lambda\mu + 72\mu^2)\big).$$

Indeed, G acts on the fibres of the map $\alpha : X_1(13) \times X_1(13) \to \Sigma$ given by $((x_1, y_1), (x_2, y_2)) \mapsto (T, X, Y)$ where

$$T = \frac{x_1x_2 - x_1 + 1}{x_2 - x_1}, \quad X = \frac{x_2^3 - 3x_2 + 1}{x_2(x_2 - 1)}, \quad Y = \frac{(X^2 - 3X + 9)y_1y_2}{(x_1 - x_2)^3}.$$

Moreover, if we define $\beta : \Sigma \to X_0(13) \times X_0(13)$ by

$$(T, X, Y) \mapsto (s_1, s_2) = \left(\frac{(T^3 - 3T + 1)X - 9T(T-1)}{T(T-1)X + (T^3 - 3T^2 + 1)}, X\right).$$

then there is a commutative diagram

$$\begin{array}{ccc} X_1(13) \times X_1(13) & \xrightarrow{(\pi,\pi)} & X_0(13) \times X_0(13) \\ & {\scriptstyle\alpha}\searrow \quad \nearrow{\scriptstyle\beta} & \\ & \Sigma & \end{array}$$

The surface Σ parametrises pairs of 13-isogenies together with a choice of isomorphism between their kernels. It has infinitely many rational points, since there is a genus 1 fibration given by $(T, X, Y) \mapsto T$, and it easy to exhibit a fibre (e.g. $T = -2$) that is an elliptic curve of positive rank. □

Example A.3. The rational point $(T, X, Y) = (17/33, 1, 126340/33^3)$ on Σ corresponds to the elliptic curves

$$\begin{aligned} E_1 :&\quad y^2 + y = x^3 - x^2 - 2x - 1, \\ E_2 :&\quad y^2 + y = x^3 - x^2 - 1424883795842044404862x \\ &\qquad - 20702237422068075268318817670099, \end{aligned}$$

with discriminants $\Delta(E_1) = -3 \cdot 7^2$ and $\Delta(E_2) = 3 \cdot 7^2 \cdot 13^{13} \cdot 251^{13} \cdot 17681$. By construction $E_1[13]$ and $E_2[13]$ have isomorphic semi-simplifications. However E_1 and E_2 are not 13-congruent, as may be seen from the fact that $p = 17681$ ramifies in $\mathbb{Q}(E_2[13])/\mathbb{Q}$ but not in $\mathbb{Q}(E_1[13])/\mathbb{Q}$.

Remark A.4. The surface Σ also has a genus 2 fibration given by $(T, X, Y) \mapsto X$. The fibres are twists of $X_1(13)$ parametrising 13-isogenies with a given Galois action on the kernel.

References

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

[B+] J. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman and J. Vonk, Explicit Chabauty-Kim for the split Cartan modular curve of level 13, *Ann. of Math.* (2) **189** (2019), no. 3, 885–944.

[Ba] B. Baran, An exceptional isomorphism between modular curves of level 13, *J. Number Theory* **145** (2014), 273–300.

[Be] A. Best, personal communication, October 2019.

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

[BCP] 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/`

[C] J.E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1997. See also `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, preprint, 2019, `arXiv:1910.12290[math.NT]`

[DMS] V. Dose, P. Mercuri and C. Stirpe, Double covers of Cartan modular curves, *J. Number Theory* **195** (2019), 96–114.

[F1] T.A. Fisher, The Hessian of a genus one curve, *Proc. Lond. Math. Soc.* (3) **104** (2012) 613-648.

[F2] T.A. Fisher, Invariant theory for the elliptic normal quintic, I. Twists of $X(5)$, *Math. Ann.* **356** (2013), no. 2, 589-616.

[F3] T.A. Fisher, On families of 7- and 11-congruent elliptic curves, *LMS J. Comput. Math.* **17** (2014), no. 1, 536–564.

[F4] T.A. Fisher, Explicit moduli spaces for congruences of elliptic curves, to appear in *Math. Zeit.*, `arXiv:1804.10195[math.NT]`

[F5] T.A. Fisher, On families of 13-congruent elliptic curves, *Magma files accompany this article*, `https://www.dpmms.cam.ac.uk/~taf1000/papers/congr13.html`

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

[FM] G. Frey and M. Müller, Arithmetic of modular curves and applications, in *Algorithmic algebra and number theory*, B.H. Matzat, G.-M. Greuel and G. Hiss (eds.), (Heidelberg, 1997), Springer, Berlin, 1999.

[FH] W. Fulton and J. Harris, *Representation theory, A first course*, Graduate Texts in Mathematics **129**, Springer-Verlag, New York, 1991.

[G] D. Gorenstein, *Finite simple groups, An introduction to their classification*, Plenum Publishing Corp., New York, 1982.

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

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

[HS] M. Hindry and J.H. Silverman, *Diophantine geometry. An introduction*, Graduate Texts in Mathematics **201**, Springer-Verlag, New York, 2000.

[Hu] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band **134**, Springer-Verlag, Berlin-New York 1967.

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

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

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

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

[L] The LMFDB Collaboration, The L-functions and Modular Forms Database, `http://www.lmfdb.org`, 2019, [Online; accessed 18 December 2019].

[PSS] B. Poonen, E.F. Schaefer and M. Stoll, Twists of $X(7)$ and primitive solutions to $x^2+y^3 = z^7$, *Duke Math. J.* **137** (2007), no. 1, 103–158.

[RS] 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.

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

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