ON 12-CONGRUENCES OF ELLIPTIC CURVES

SAM FRENGLEY

Abstract. We construct infinite families of pairs of (geometrically non-isogenous) elliptic curves defined over \( \mathbb{Q} \) with 12-torsion subgroups that are isomorphic as Galois modules. This extends previous work of Chen [5] and Fisher [13] where it is assumed that the underlying isomorphism of 12-torsion subgroups respects the Weil pairing. Our approach is to compute explicit birational models for the modular diagonal quotient surfaces which parametrise such pairs of elliptic curves.

A key ingredient in the proof is to construct simple (algebraic) conditions for the 2, 3, or 4-torsion subgroups of a pair of elliptic curves to be isomorphic as Galois modules. These conditions are given in terms of the \( j \)-invariants of the pair of elliptic curves.

1. Introduction

Let \( N \geq 1 \) be an integer, \( K \) be a perfect field of characteristic coprime to \( N \), and \( G_K := \text{Gal}(\overline{K}/K) \) be the absolute Galois group of \( K \). Let \( E/K \) and \( E'/K \) be elliptic curves and let \( E[N] \) and \( E'[N] \) be their \( N \)-torsion subgroups.

We say that \( E \) and \( E' \) are \( N \)-congruent (or \( N \)-congruent over \( K \)) if there exists a \( G_K \)-equivariant isomorphism \( \phi: E[N] \rightarrow E'[N] \). In this case the isomorphism \( \phi \) is said to be an \( N \)-congruence.

Frey and Mazur conjectured that there exists a constant \( C_0 > 1 \) such that for any \( N \geq C_0 \) there are no pairs of non-isogenous \( N \)-congruent elliptic curves over \( \mathbb{Q} \). It is necessary to exclude isogenies since for each integer \( m \) coprime to \( N \) the restriction of an \( m \)-isogeny to \( E[N] \) is an \( N \)-congruence.

Note that if \( \phi: E[N] \rightarrow E'[N] \) is an \( N \)-congruence then there exists an element \( r \in (\mathbb{Z}/N\mathbb{Z})^\times \) such that for all \( P,Q \in E[N] \) we have
\[
e_{E,N}(P,Q) = e_{E',N}(\phi(P),\phi(Q))^r
\]
where \( e_{E,N} \) and \( e_{E',N} \) denote the Weil pairings on \( E \) and \( E' \) respectively. In this case we say that \( \phi \) is an \((N,r)\)-congruence or an \( N \)-congruence with power \( r \). For each integer \( m \) coprime to \( N \) composing \( \phi \) with multiplication by \( m \) changes the power of \( \phi \) by a factor of \( m^2 \), so we consider the power of \( \phi \) only up to multiplication by a square in \((\mathbb{Z}/N\mathbb{Z})^\times\).

We are concerned with the following question: for which pairs \((N,r)\) do there exist examples (or infinite families of examples) of pairs of non-isogenous \((N,r)\)-congruent elliptic curves over \( \mathbb{Q} \)?

In the case when \( N = p \) is a prime number, infinite families of geometrically non-isogenous \((p,r)\)-congruent elliptic curves over \( \mathbb{Q} \) have been found for every power \( r \) when \( p \leq 13 \) (see Table 1). A pair of non-isogenous \((17,3)\)-congruent elliptic curves appearing in the LMFDB [27] has been found by Cremona (see [2], [8], or [10]). Fisher [13] also found a pair of non-isogenous \((17,1)\)-congruent elliptic curves over \( \mathbb{Q} \), and has conjectured that these are the only 17-congruences over \( \mathbb{Q} \). Moreover Fisher conjectured that there exist no pairs of non-isogenous, \( p \)-congruent, elliptic curves over \( \mathbb{Q} \) for \( p \geq 19 \) (see [13] Conjecture 1.1).

For composite \( N \) infinite families of geometrically non-isogenous \((N,r)\)-congruent elliptic curves have been found for every power \( r \) when \( N \leq 10 \) and for \((N,r) = (12,1)\) (see Table 1).

On the other hand in [10] we found examples of elliptic curves over \( \mathbb{Q} \) admitting an \( N \)-congruence with a (non-isogenous) quadratic twist for each even \( N \leq 24 \), \( N = 28, 30, 32, 36 \), and 48. These examples arise in infinite families except in the cases when \( N = 30, 32, \) or 48. When \( N = 12 \) we showed that there are infinite families of elliptic curves admitting \((12,7)\) and \((12,11)\)-congruences with a (non-isogenous) quadratic twist. However, in these examples the elliptic curves in question are geometrically isogenous and their mod 12 Galois representations are not surjective.

Date: September 14, 2023.
For any $N \geq 2$ and $r \in (\mathbb{Z}/N\mathbb{Z})^\times$ let $Z(N, r)$ be the (coarse) moduli space which parametrises triples $(E, E', \phi)$ where $E$ and $E'$ are elliptic curves (defined up to simultaneous quadratic twist) and $\phi: E[N] \to E'[N]$ is an $(N, r)$-congruence (defined up to composition with an automorphism of $E$ or $E'$). Following Kani–Schanz [19] we call $Z(N, r)$ a modular diagonal quotient surface. The surface $Z(N, r)$ is naturally equipped with an involution which reverses the roles of $E$ and $E'$. We write $W(N, r)$ for the quotient of $Z(N, r)$ by this involution.

The main contribution of this article is to give explicit equations for the surfaces $Z(12, r)$ for each $r \in (\mathbb{Z}/12\mathbb{Z})^\times$. We use these equations to find infinite families of $(12, r)$-congruent elliptic curves which are not geometrically isogenous.

The surface $Z(12, 1)$ is an elliptic K3 surface and models were computed by Chen and Fisher (see Chapter 7 and [13]) using equations for the twist $X_1^0(12)$ of $X(12)$ which parametrises elliptic curves which are $(12, 1)$-congruent to $E$ (see Section 2). Chen [6, Chapter 7.4] also computed equations for the twist $X_1^0(12)$ and it may be possible to compute a simple birational model for $Z(12, 7)$ using these. Using different techniques we prove:

**Theorem 1.1.** Each of the surfaces $W(12, r)$ are rational and the surfaces $Z(12, r)$ are birational over $\mathbb{Q}$ to the affine surfaces

$$z^2 = F_{12, r}(u, v)$$

where $F_{12, r}(u, v) \in \mathbb{Q}[u, v]$ are the polynomials

- $F_{12, 1}(u, v) = -4u^4 - 2(2v^2 + 3)u^3 - (v^4 - 13v^2 + 3)u^2 + 2(5v^4 + 9v^2)u + 6v^4 - 6v^2 + 9v^2$,
- $F_{12, 5}(u, v) = v^2u^8 + 4v^2u^7 + (-4v^4 - 20v^2 + 4)u^6 + (-12v^4 - 32v^2 - 8)u^5 + (6v^6 + 44v^4 + 160v^2 - 76)v^4 + (12v^6 + 64v^4 - 64v^2 + 352)v^3 + (-4v^8 - 28v^6 - 204v^4 - 232v^2 - 592)u^2 + (-4v^8 - 32v^6 + 72v^4 - 224v^2 + 448)v + u^{10} + 4v^8 + 40v^6 + 52v^4 - 32v^2 - 128$,
- $F_{12, 7}(u, v) = -((u - 1)(u^2 + 1)u + v^2 - 1)(u^4 + 6u^2 + 3 + (-2v^2 + 12)u^2 + (-6v^2 + 8)u + v^4 - v^2)$,
- $F_{12, 11}(u, v) = -(u + 1)((v^4 + 6v^2 + 1)u - 7v^4 - 2v^2 + 1)(v^4u^4 + 8v^4u^3 + (-9v^6 + 24v^4 + 11v^2)u^2 + (-54v^6 - 36v^4 - 6v^2)u + 27v^8 + 27v^6 + 9v^4 - v^2 - 1)$.

Moreover the double covers $Z(12, r) \to W(12, r)$ are given by $(u, v, z) \to (u, v)$.

The maps $Z(12, r) \to X(1) \times X(1)$ which give the moduli interpretations for the surfaces $Z(12, r)$ are too complicated to reproduce here but may be recovered from the computations in Section 5. We record them in the electronic data corresponding to this article [17].
Remark 1.2. Note that the polynomials $F_{12,r}(u,v)$ contain only even powers of $v$. In Section 4 we will show that $Z(12,r)$ is a double cover of a surface $Z^{+}(12,r)$. This double cover is the quotient by the involution $v \mapsto -v$.

Remark 1.3. The model for the surface $Z(12,1)$ given in Theorem 1.1 admits a genus 1 fibration over the $t$-line given by $y^2 = F_{12,1}(x,t)$ (in fact, this fibration is elliptic, see Example 6.3).

Since the surfaces $Z(12,r)$ are of general type when $r \neq 1$ they cannot admit genus 1 fibrations. However, they do admit genus 2 fibrations over the $t$-line which are given by $y^2 = F_{12,5}(x,t)$, $y^2 = F_{12,7}(x,t)$, and $y^2 = F_{12,11}(x,t)$ respectively.

It is possible to find pairs of 12-congruent elliptic curves by sieving for examples where both $E$ and $E'$ are contained in the LMFDB [27] (as described in [8] Section 3). The power of these congruences may be determined using the equations of Rubin, Silverberg, and Fisher [9, 34, 36, 39] for $X_E^r(N)$ when $N = 3$ and 4. For example the pairs of elliptic curves with LMFDB labels (55, a1, 1045, b1), (60450, cx2, 60450, cv2), and (735, d2, 24255, bh1) are not geometrically isogenous and are (12, 1), (12, 5), and (12, 7)-congruent respectively.

On the other hand we were not able to find any examples of (12, 11)-congruences between geometrically non-isogenous curves in the LMFDB. The rational point $\left( \frac{-19}{3}, \frac{7844488}{27} \right)$ on the model for $Z(12,11)$ in Theorem 1.1 gives rise to the pair of geometrically non-isogenous (12, 11)-congruent elliptic curves

\[ E : y^2 + xy = x^3 - 21666120x - 57035036608, \]
\[ E' : y^2 + xy = x^3 + 398520965x + 166506419482597 \]

which have conductor 4976690. Moreover, among pairs of geometrically non-isogenous (12, 11)-congruent elliptic curves which we found, these curves have the smallest conductor (see Section 6.3).

By exhibiting a rational curve on the elliptic K3 surface $Z(12,1)$ Chen found an infinite family of (12, 1)-congruent elliptic curves over $\mathbb{Q}$ [5 Proposition 1.7.11]. Fisher gave a fibration with a section of infinite order, thus giving an infinite family of (12, 1)-congruent elliptic curves over $\mathbb{Q}(t)$ [13 Corollary 1.3].

In contrast Kani–Schanz [19] showed that when $r \neq 1$ the surfaces $Z(12,r)$ are of general type. In this case we expect (by the Bombieri–Lang conjecture) that there are at most finitely many curves of geometric genus 0 or 1 on $Z(12,r)$.

By finding curves of genus 0 or 1 on the models for $Z(12,r)$ in Theorem 1.1 we deduce:

**Theorem 1.4.** For each $r \in (\mathbb{Z}/12\mathbb{Z})^\times$ there are infinitely many pairs of $j$-invariants of $(12,r)$-congruent elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ which are not geometrically isogenous.

Moreover there are infinite subfamilies such that the mod 12 Galois representation attached to $E/\mathbb{Q}$ (and $E'/\mathbb{Q}$) is surjective.

Remark 1.5. Since a pair of elliptic curves are $(12,r)$-congruent if and only if they are both $(3,r)$ and $(4,r)$-congruent, the families of elliptic curves in Theorem 1.4 may be checked using known formulae for the twists $X_E^r(N)$ when $N = 3, 4$. Such equations have been computed by Rubin and Silverberg [34, 36, 39] when $r = 1$, and by Fisher [9] for each $r$.

1.1. **Outline of the paper.** In Section 2 we give background on the invariant theory of the modular curve $X(N)$ when $N \leq 4$ following Klein [22] and Fisher [9]. We describe $Z(N,r)$ as a quotient of $X(N) \times X(N)$ following Kani and Schanz [19].

In Section 3 we use invariant theoretic techniques to find simple (symmetric) conditions for a pair of elliptic curves to be 2, 3, or 4-congruent (note that our condition for 2-congruence was already proved by Fisher, see [13 Lemma 3.5]).

We describe the relationship between the surface $Z(N_1N_2,r)$ and the fibre product $Z(N_1,r) \times_{Z(1)} Z(N_2,r)$ when $N_1$ and $N_2$ are coprime integers in Section 4. We employ this description to compute explicit models for the surfaces $Z(12,r)$ and prove Theorem 1.1 in Section 5.

Finally in Section 6 we find “interesting” curves on the surfaces $Z(12,r)$. We prove Theorem 1.4 in Section 6.4 by finding curves with infinitely many rational points (and which do not arise as Hecke correspondences) on the models for $Z(12,r)$ in Theorem 1.1. More precisely we give explicit examples of pairs of geometrically non-isogenous $(12,r)$-congruent elliptic curves which are defined over $\mathbb{Q}(t)$ when $r = 1, 7,$ and
11 (see Examples 6.3, 6.5, and 6.6). When \( r = 5 \) we give a family defined over \( \mathbb{Q}(C) \) where \( C/\mathbb{Q} \) is an elliptic curve of rank 1 (see Example 6.4).

1.2. Acknowledgements. I would like to thank my supervisor Tom Fisher for suggesting this topic and for many insightful conversations and comments on earlier versions of this article. I would also like to express my gratitude to Jef Laga and the anonymous referee for several comments on earlier versions of this paper and to Noah Porcelli, Tony Scholl, and Alice Silverberg for useful discussions and suggestions. I am grateful to the Woolf Fisher and Cambridge Trusts for their financial support.

2. The modular curve \( X(N) \) and the surface \( Z(N, r) \)

Let \( N \geq 1 \) be an integer, and let \( K \) be a field of characteristic coprime to \( 6N \).

Consider the \( G_K \)-module \( \mu_N \times \mathbb{Z}/N\mathbb{Z} \) endowed with the structure of symplectic abelian group via the pairing \( \langle (\zeta, c), (\xi, d) \rangle = \zeta^d \xi^{-c} \). Let \( \Gamma_N \) denote the group of symplectic automorphisms of \( \mu_N \times \mathbb{Z}/N\mathbb{Z} \), and note that \( \Gamma_N \) is isomorphic to \( \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) \) as an abstract group.

Let \( Y(N)/K \) be the (non-compact) modular curve of full level \( N \). For each field \( L/K \), the \( L \)-rational points on \( Y(N) \) parametrise pairs \( (E/L, \iota) \) where \( E/L \) is an elliptic curve and \( \iota: E[N] \to \mu_N \times \mathbb{Z}/N\mathbb{Z} \) is a \( G_L \)-equivariant isomorphism which is symplectic with respect to the Weil pairing on \( E[N] \). Recall that when \( N = 1, 2 \) the moduli space \( Y(N) \) is coarse, and the pair \( (E/L, \iota) \) is only determined up to twist.

An element \( g \in \Gamma_N \) acts on \( Y(N) \) via \( (E, \iota) \mapsto (E, g\iota) \) and this action extends uniquely to an automorphism of \( X(N) \). Elements \( g, g' \in \Gamma_N \) induce the same action on \( X(N) \) if and only if they differ by an automorphism of \( E \). In particular, this action descends to an action of \( \Gamma_N/\{\pm 1\} \).

2.1. The Twist \( X_E^r(N) \). Let \( E/K \) be an elliptic curve and \( r \) be an integer coprime to \( N \). Consider a \( \mathbb{R} \)-isomorphism \( \iota_r: E[N] \to \mu_N \times \mathbb{Z}/N\mathbb{Z} \) such that \( e_N(P, Q)^r = \langle \iota_r(P), \iota_r(Q) \rangle \). By the twisting principle \( \iota_r \) gives rise to a Galois cohomology class \( [\iota_r] \in H^1(K, \Gamma_N) \).

The \( G_K \)-equivariant homomorphism \( \Gamma_N \to \text{Aut}(X(N)_{\mathbb{R}}) \) induces a map on Galois cohomology \( H^1(K, \Gamma_N) \to H^1(K, \text{Aut}(X(N)_{\mathbb{R}})) \). Again by the twisting principle we may associate to the image of \( [\iota_r] \) a twist \( X_E^r(N)/K \) of \( X(N) \).

For each field \( L/K \), the \( L \)-rational points on the curve \( X_E^r(N) \) parametrise pairs \( (E'/L, \phi) \) where \( \phi: E[N] \to E'[N] \) is an \((N, r)\)-congruence.

2.2. The Surface \( Z(N, r) \). Recall that for each \( N \geq 2 \) and \( r \in (\mathbb{Z}/N\mathbb{Z})^\times \) we let \( Z(N, r)/K \) be the (coarse) moduli space of triples \( (E, E', \phi) \) where \( E/K \) and \( E'/K \) are elliptic curves (defined up to simultaneous quadratic twist) and \( \phi: E[N] \to E'[N] \) is an \((N, r)\)-congruence. Further recall that we write \( W(N, r) \) for the quotient of \( Z(N, r) \) by the involution swapping the roles of \( j \) and \( j' \). It will be useful for us to note that \( W(1) \) is birational to \( \mathbb{A}^2 \) and that we may take the quotient \( Z(1) \to W(1) \) to be given by \( (j, j') \mapsto (jj', (j - 1728)(j' - 1728)) \).

We then have a commutative diagram:

\[
\begin{array}{ccc}
Z(N, r) & \longrightarrow & W(N, r) \\
\downarrow & & \downarrow \\
Z(1) & \longrightarrow & W(1)
\end{array}
\]

Define the group \( \Delta_r \) to be the subgroup \( \{(g, \varepsilon_r(g)) : g \in \Gamma_N\} \subset \Gamma_N \times \Gamma_N \), where \( \varepsilon_r \) denotes conjugation by the matrix \( \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \).

The following lemma is due to Kani–Schanz [19] and Fisher [12] Lemma 3.2.

**Lemma 2.1** ([12] Lemma 3.2), [19]. The surface \( Z(N, r) \) is birational over \( K \) to the quotient of \( X(N) \times X(N) \) by \( \Delta_r \).
2.3. The Action of \( \Gamma_N \) on \( X(N) \). We briefly describe the invariant theory of the modular curves \( X(N) \) when \( N = 2, 3, \) and \( 4 \). In these cases the invariant theory of \( X(N) \) has been extensively studied, dating back to Klein [22]. We follow the more modern treatment of Fisher [9, Sections 3–4].

For \( N = 2,3,4 \) we identify the modular curve \( X(N) \) with \( \mathbb{P}^1 \). We define the (finite) subgroups \( G_N \subset \text{GL}_2(\mathbb{K}) \) to be the subgroups generated by

\[
N = 2 : \begin{pmatrix} 1/2 & 1/16 \\ 12 & -1/2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\]

\[
N = 3 : \begin{pmatrix} 1/3 \sqrt{-3} & 1 \\ 6 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\]

\[
N = 4 : \begin{pmatrix} 1/2 \sqrt{-2} & 1 \\ 2 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\]

where \( \zeta_N \in \mathbb{K} \) is a primitive \( N^{\text{th}} \) root of unity.

By mapping the generators \( \begin{pmatrix} \frac{1}{2} & 0 \\ 1 & 1 \end{pmatrix} \) and \( \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) of \( \Gamma_N \) to the above generators of (the projective image of) \( G_N \), we obtain a \( G_K \)-equivariant homomorphism \( \rho : \Gamma_N \to \text{PGL}_2(\mathbb{K}) \) giving the action of \( \Gamma_N \) on \( X(N) \).

Let \( G_N \) be the commutator subgroup of \( G_N \). It is a classical theorem of Klein that for each \( N = 2,3,4 \) the invariant ring \( K[x_0, x_1]^{G_N} \) is generated by invariants \( c_4, c_6 \), and \( D \) of weights \( 4N, 6N \), and 12 subject only to the relation \( c_4 - c_6^3 = 1728D^N \) (see [9, Theorem 3.3]). Explicitly we take

\[
N = 2 : \quad D = x_0(64x_0^3 - x_1^2) \quad c_4 = 192x_0^2 + x_1^2 \quad c_6 = x_1(576x_0^2 - x_1^2)
\]

\[
N = 3 : \quad D = -x_0(27x_0^3 + x_1^3) \quad c_4 = -x_1(216x_0^3 - x_1^3) \quad c_6 = 5832x_0^6 - 540x_0^3x_1^3 - x_1^6
\]

\[
N = 4 : \quad D = x_0x_1(16x_0^4 - x_1^4) \quad c_4 = 256x_0^8 + 224x_0^4x_1^4 + x_1^8 \quad c_6 = 4096x_0^{12} - 8448x_0^8x_1^4 - 528x_0^4x_1^8 + x_1^{12}
\]

Moreover, by considering ramification points it can be shown that the map \( X(N) \to X(1) \) given by \( j = c_4^3/D^N \) is the \( j \)-map (see [9, Lemma 4.4]).

With the models chosen above the forgetful map \( X(4) \to X(2) \) is given by \( [x_0 : x_1] \mapsto [-x_0^2x_1^2 : 16x_0^3 + x_1^3] \).

3. Symmetric equations for families of \( N \)-congruent elliptic curves

Several approaches have been applied to parametrising (universal) families of \( 2,3, \) and \( 4 \)-congruent elliptic curves.

Equations for \( X_N^4(N) \) when \( N = 2,3,4 \), and \( 5 \) were computed by Rubin and Silverberg (see [34, 36, 39]). Using a direct approach Lario–Rio computed equations for \( X_N^4(3) \) when \( r = 1 \) and \( 2 \) (see [26, Section 3]).

Fisher [9] described how when \( N = 2,3,4 \), and \( 5 \) the curve \( X_N^4(N) \) is related to the Hessian of a genus one model of degree \( N \), and hence computed explicit equations for \( X_N^4(N) \) using classical invariant theory. When \( N = 3 \) similar approaches have been employed in [11 and 25]. The former considers all powers, and the latter pays careful attention to the case when \( r = 1 \) and the characteristic of \( K \) is 2.

Kumar [24] (for every \( N \leq 11 \)) and Bröker–Howe–Lauter–Stevenhagen [3] (when \( N = 3 \)), and Bruin–Doerkse [4] (when \( N = 4 \)) have computed explicit equations for the surface \( Z(N, -1) \) using the description of \( Z(N, -1) \) as the moduli space of genus 2 curves with \( (N, N) \)-split Jacobians. The equations of Kumar and Bröker–Howe–Lauter–Stevenhagen are also symmetrical in \( E \) and \( E' \).

Our approach is to use Lemma [24] to compute models for the surfaces \( Z(N, r) \) for each \( (N, r) = (2,1) \), \( (3,1) \), \( (3,2) \), \( (4,1) \), and \( (4,3) \). An advantage of our approach is that by viewing \( E \) and \( E' \) symmetrically we are able to exploit natural factorisations of the maps \( Z(N, r) \to Z(1) = Y(1) \times Y(1) \) to provide simple conditions for \( E \) and \( E' \) to be 2, 3, or 4-congruent (see [8, 33]). Indeed, it is this observation which makes it practical for us to compute (birational) models for \( Z(12, r) \) via fibre products.

3.1. Computing quotients of \( X(N) \times X(N) \). We compute \( Z(N, r) \) from its description as a quotient of \( X(N) \times X(N) \) under the (twisted) diagonal action of \( \Gamma_N \). The method we describe has been successfully employed by Fisher to compute birational models for \( Z(13, r) \) and \( Z(17, r) \) (see [12] and [14]).
For each $N = 2, 3, 4$ let $\Delta_r \subset G_N \times G_N$ denote the preimage of $(\bar{\rho} \times \bar{\rho})(\Delta_r)$. Let $f(x_0, x_1, x'_0, x'_1)$ be a polynomial which is homogeneous of degrees $m$ and $m'$ in the two sets of variables.

**Definition 3.1.** We say that $f$ is an $r$–bi-invariant if $f$ is invariant under the action of $\Delta_r$ on the polynomial ring $\mathbb{K}[x_0, x_1, x'_0, x'_1]$. If $f(x_0, x_1, x'_0, x'_1) = f(x_0', x'_1, x_0, x_1)$ we say that $f$ is symmetric.

The action of $\Delta_r$ on $X(N) \times X(N)$ induces an action on $Y(N) \times Y(N) = \text{Spec } R$. By Lemma 2.1, the surface $Z(N, r)$ is birational to $\text{Spec } R^{\Delta_r}$. To compute a birational model for $Z(N, r)$ it is enough to compute generators and relations for the $K$-algebra $R^{\Delta_r}$, together with their relations with the rational functions $j$ and $j'$, where $j$ (respectively $j'$) is the rational function giving the $j$-invariant on each copy of $Y(N)$. Similarly if $S \subset R^{\Delta_r}$ is the subalgebra of elements invariant under the natural involution on $Y(N) \times Y(N)$, then $W(N, r)$ is birational to $\text{Spec } S$.

We do not attempt to fully describe the invariant ring $R^{\Delta_r}$. Instead we use the following observations:

If $A \subset K[x_0, x_1, x'_0, x'_1]$ is the subalgebra of $r$–bi-invariants, then the inclusion $Y(N) \times Y(N) \subset X(N) \times X(N)$ induces a rational map $Z(N, r) \dashrightarrow \text{Spec } R^{\Delta_r} \dashrightarrow \text{Proj } A$. Moreover if $B \subset A$ is the subalgebra of symmetric $r$–bi-invariants, then we have a rational map $W(N, r) \dashrightarrow \text{Spec } S \dashrightarrow \text{Proj } B$.

Consider non-zero $r$–bi-invariants $w_0, ..., w_k \in K[x_0, x_1, x'_0, x'_1]$ such that for each $i$ the $r$–bi-invariant $w_i$ is an element of the $K$-vector space of symmetric $r$–bi-invariants of homogeneous bi-degree $(m, m)$. Let $\varphi_{N, r}$ be the map $X(N) \times X(N) \dashrightarrow \mathbb{P}^k$ given by $([x_0 : x_1], [x'_0 : x'_1]) \mapsto [w_0 : ... : w_k]$. Since $w_0, ..., w_k$ are symmetric and invariant under the action of $\Delta_r$ we obtain a factorisation

$$X(N) \times X(N) \xrightarrow{\psi_{N, r}} W(N, r) \xrightarrow{\varphi_{N, r}} \text{im}(\varphi_{N, r}).$$

When $N = 2, 3, 4$ we will carefully choose symmetric $r$–bi-invariants $w_0, ..., w_k$ so that $\varphi_{N, r}$ is birational.

**3.2. Symmetric bi-invariants.** We now give choices of $r$–bi-invariants such that the map $\varphi_{N, r}$ is birational for each $N = 2, 3, 4$. We consider the action of $\Gamma_N$ on $X(N) \cong \mathbb{P}^1$ via the representation $\bar{\rho}$ in Section 2.3.

**Remark 3.2.** Note that in the case when $N = 4$ the actions of $\Gamma_1$ and $\Gamma_3$ on $K[x_0, x_1, x'_0, x'_1]$ have the same invariants. We therefore treat both cases simultaneously.

There is also an explanation for this phenomenon in terms of the moduli interpretation of $Z(4, r)$. Every elliptic curve $E/K$ is (4,3)-congruent with its quadratic twist by its discriminant (see [4] Corollary 7.4 or [16] Proposition 3.6 for a more general statement). In particular, if $E$ and $E'$ are (4,1)-congruent, then the quadratic twist of $E$ by its discriminant $E_{\Delta_r}(E)$ is (4,3)-congruent to $E'$. This induces an isomorphism $Z(4, 1) \cong Z(4, 3)$ which commutes with the $j$-invariant maps $Z(4, r) \to Z(1)$.

Recall the forms $D = D(x_0, x_1)$, $c_4 = c_4(x_0, x_1)$, and $c_6 = c_6(x_0, x_1)$ defined in Section 2.3. We let $D' = D(x'_0, x'_1)$, $c'_4 = c_4(x'_0, x'_1)$, and $c'_6 = c_6(x'_0, x'_1)$. The forgetful map $X(N) \times X(N) \to Z(1)$ is given by $([x_0 : x_1], [x'_0 : x'_1]) \mapsto (j, j')$ where $j = c'_4/D^4$ and $j' = c'_6/D^6$. We write $J = j/1728$ (similarly $J' = j'/1728$).

Additionally, we define the following $r$–bi-invariant forms:

$$(N, r) = (2, 1) : \quad I_{1,1} = 192x_0x'_0 + x_1x'_1,$$

$$(N, r) = (4, r) : \quad I_{2,2} = 16(x_0x'_1 - x_1x'_0)^2,$$

$$(N, r) = (3, 1) : \quad I_{2,2} = 3(54x_0^2x'_0^2 + x_0x_1x'_1^2 + x_1^2x'_0x'_1),$$

$$(N, r) = (3, 2) : \quad I_{2,2} = 18x_0x'_0 + x_1x'_1)^2.$$
the action of $H$ there are the relations:

$$H/\phi$$

Therefore the image of the map $\phi$ commutes, where the map $S$ is given by the rational functions $f, g, h$, and $(DD')^2$ are invariant under the action of $H \times H$. In particular, $w_0, w_1$ and $w_2$ are invariant under $H \times H$ and we have the relation $c_4' = 4w_0 - \frac{3}{2}w_1 - w_2$.

Using the equations for the forgetful map $X(4) \to X(2)$ given in Section 2.3 we see that the diagram

$$\begin{array}{ccc}
W(2,1) & \xrightarrow{\psi_{2,1}} & S(2,1) \\
\downarrow & & \downarrow \\
W(1) & & 
\end{array}$$

commutes, where the map $S(2,1) \to W(1)$ is given by the rational functions $J, J'$ and $(J-1)(J'-1)$ above.

### 3.2.2. Case $(N, r) = (4, r)$

We first note that the invariants $w_0, w_1, w_2, w_3$ satisfy the single relation

$$192w_0^2 - 96w_0w_1 + 128w_0w_3 + 48w_0w_2 - w_2^2 = 0.$$ 

Therefore the image of the map $\varphi_{4,r} : X(4) \times X(4) \to \mathbb{P}^3$ is the quadric surface $S(4, r) = \{192w_0^2 - 96w_0w_1 + 128w_0w_3 + 48w_0w_2 - w_2^2 = 0\}$.

Let $H = \ker(\text{SL}_2(\mathbb{Z}/4\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/2\mathbb{Z}))$, so that the forgetful map $X(4) \to X(2)$ is given by taking the quotient by the action of $H/\{\pm 1\}$. Note that the $r$–bi-invariants $I_{4,4}, c_4'c_4$, and $(DD')^2$ are invariant under the action of $H \times H$.

Using the equations for the forgetful map $X(4) \to X(2)$ given in Section 2.3 we see that the diagram

$$\begin{array}{ccc}
W(4, r) & \xrightarrow{\psi_{4,r}} & S(4, r) \\
\downarrow & & \downarrow \\
W(2,1) & \xrightarrow{\psi_{2,1}} & S(2,1) 
\end{array}$$

commutes, where the map $S(4, r) \to S(2,1)$ is given by $[w_0 : w_1 : w_2 : w_3] \mapsto [w_0 : w_1 : w_2^2 / w_3]$.

### 3.2.3. Case $(N, r) = (3, 1)$

The image of the rational map $\varphi_{3,1} : X(3) \times X(3) \to \mathbb{P}^3$ is the cubic surface $S(3, 1) = \{8w_0^2w_1 - 60w_0w_1w_2 + 12w_0w_1w_3 + 36w_0w_1w_3 - 9w_1^3 + 27w_2^2w_3 - 27w_1w_3^2 + 9w_3^3 = 0\}$. Additionally, there are the relations:

$$J = \frac{w_1(4w_0^2 - 192w_0w_1 + 12w_0w_2 + 72w_0w_3 - 603w_1^2 - 144w_1w_2 - 918w_1w_3 + 9w_2^2 + 108w_2w_3 + 351w_3^2)}{36w_3^2},$$

$$(J-1)(J'-1) = \frac{w_1w_2^2}{4w_3^3}. $$
We therefore have a commutative diagram

\[
\begin{array}{c}
W(3,1) \xrightarrow{\psi_{3.1}} S(3,1) \\
\downarrow \\
W(1)
\end{array}
\]

where the morphism \( S(3,1) \rightarrow W(1) \) is given by the rational functions \( JJ' \) and \((J - 1)(J' - 1)\) above.

3.2.4. Case \((N, r) = (3,2)\). Let \( S(3,2) = \mathbb{P}^2 \). The bi-invariants \( w_0, w_1, \) and \( w_2 \) are linearly independent, so the map \( \varphi_{3,2} : X(3) \times X(3) \rightarrow S(3,2) \) is surjective. We have the relations

\[
JJ' = \left( \frac{w_1}{w_2} \right)^3,
\]

\[
(J - 1)(J' - 1) = \frac{(w_0^2 - 3w_1^2 - 3w_1w_2 - 3w_2^2)^2}{4w_0^2(2w_0 + 3w_1 + 3w_2)}.
\]

Therefore there is a commutative diagram

\[
\begin{array}{c}
W(3,2) \xrightarrow{\psi_{3,2}} S(3,2) \\
\downarrow \\
W(1)
\end{array}
\]

where the map \( S(3,2) \rightarrow W(1) \) is given by the rational functions \( JJ' \) and \((J - 1)(J' - 1)\) above.

3.3. Symmetric conditions for 2, 3, and 4-congruences. We now prove Theorem 3.3. This provides a simple characterisation of 2, 3, and 4-congruent elliptic curves in terms of their \( j \)-invariants. It is important for our computations of the surfaces \( Z(12, r) \) that, unlike the equations of Fisher \cite{Fisher} and of Rubin and Silverberg \cite{RubinSilverberg1, RubinSilverberg2, RubinSilverberg3}, the conditions in Theorem 3.3 are symmetrical in the pair of congruent elliptic curves, \( E \) and \( E' \). This will be useful since we will be able to work with the surfaces \( W(12, r) \) which have simpler birational geometry.

The case when \( N = 2 \) appears in \cite[Lemma 3.5]{Silverberg} with a different (computational) proof using the equations for \( X_E^1(2) \). It is also possible to verify Theorem 3.3 using the equations of Fisher and of Rubin and Silverberg for \( X_E^1(N) \) (the necessary transformations are recorded in the electronic data \cite{Silverberg}). We opt for a more geometric approach which explains how we found these conditions.

**Theorem 3.3.** Let \( K \) be a field of characteristic not equal to 2 or 3. Let \( E/K \) and \( E'/K \) be elliptic curves with \( j \)-invariants \( j \) and \( j' \) respectively. Let \( c_4, c_6, \Delta \) and \( c_4', c_6', \Delta' \) be the \( c \)-invariants and discriminant of (a Weierstrass model of) \( E \) and \( E' \) respectively. Suppose that \( j, j' \notin \{0,1728\} \). Let \( J = j/1728 \) and \( J' = j'/1728 \).

Then we have the following:

(i) \( E \) and \( E' \) are 2-congruent if and only if there exist \( \alpha, \beta \in K \) such that

\[
\alpha^2 - (J - 1)(J' - 1) = 0,
\]

\[
\beta^3 - 3JJ'\beta - 2JJ'(\alpha + 1) = 0.
\]

(ii) If \( J \neq J' \) then \( E \) and \( E' \) are \((4, r)\)-congruent if and only if there exist \( \alpha, \beta, \gamma, \tau \in K \) such that \( \alpha \) and \( \beta \) satisfy the conditions of (i) and

\[
\gamma^4 - 6JJ'\beta^2 - 16(JJ')^2\gamma^2 + 3(JJ')^2(4JJ' - \beta^2) = 0,
\]

\[
\tau^2 = \begin{cases} 
3c_6c_6'\delta\alpha & \text{if } r \equiv 1 \pmod{4}, \\
3c_6c_6'\alpha & \text{if } r \equiv 3 \pmod{4} 
\end{cases}
\]

where \( \delta = 3(JJ' - (\alpha + 1)^2) \).
(iii) If $J \neq J'$ and $(\sqrt{J} + 1)(\sqrt{J'} + 1) \neq 1$ (for all choices of cube roots) then $E$ and $E'$ are $(3,1)$-congruent if and only if there exist $\alpha, \beta, \tau \in K$ such that
\[
\alpha^3 - 3JJ'\alpha - JJ'(J + J') = 0,
\]
\[
\beta^4 - 6(\alpha + 1)(J - 1)(J' - 1)^2\beta^2 - 8(\alpha + 1)^2(\alpha - 1)^2(\beta - 1)^2 = 0,
\]
\[
\tau^2 = 3c_6'\delta,
\]
where
\[
d = -6 \left( \frac{2\beta^3 - (5\alpha + 2)^2\beta^2 - 10(\alpha + 1)(\alpha - 1)^5(\beta - 1)^2}{\beta^3 - 3(\alpha - 1)^2(\beta - 1)^2} \right).
\]

(iv) If $J \neq J'$ then $E$ and $E'$ are $(3,2)$-congruent if and only if there exists $\alpha, \beta, \tau \in K$ such that
\[
\alpha^3 - JJ' = 0,
\]
\[
\beta^4 - 6\alpha(J - 1)(J' - 1)^2\beta^2 - 8(\alpha^2 - 1)^2(\beta - 1)^2 = 0,
\]
\[
\tau^2 = \begin{cases} 3c_6'\beta & \text{if } \beta \neq 0, \\ -2c_6' & \text{if } \beta = 0. \end{cases}
\]

**Remark 3.4.** Note that in Theorem 3.3

(i) The conditions on $\alpha$ are convenient ways of writing the conditions that $\Delta\Delta'$ is a square when $N = 2, 4$ and that $\Delta'\Delta$ is a cube when $(N, r) = (3, 2)$. In the case when $(N, r) = (3, 1)$ if we define $\alpha' = \frac{\alpha}{JJ'}$ then $(\alpha')^3 = J/J'$. In particular when $(N, r) = (3, 1)$ the condition on $\alpha$ is equivalent to $\Delta/\Delta'$ being a cube.

When $N = 4$ the period $\delta$ is equal to $\Delta$ (and $\Delta'$) up to a square factor (modulo squares we have $\delta/\Delta \equiv 3\delta(J - 1) \equiv (\alpha - (J - 1)^2)$. The conditions on $\tau$ are therefore equivalent to the fact that $\Delta/\Delta'$ is a fourth power when $(N, r) = (4, 1)$ and $\Delta/\Delta'$ is a fourth power when $(N, r) = (4, 3)$.

(ii) When $K$ contains an $N$th root of unity, it is clear that the polynomials in $\alpha$ in Theorem 3.3 may have more than one root in $K$. Indeed, the theorem would be false if we required the existence of a $\beta$ (and $\gamma, \tau$) for a fixed choice of $\alpha$ (and $\beta$). For example, the curves with LMFDB labels [196.b1] and [196.b2] are 3-isogenous and therefore $(4, 3)$-congruent. In this example the polynomial in $\beta$ has no root when the negative root $\alpha$ is chosen. When $\alpha$ is chosen to be positive the polynomial in $\beta$ splits, but the polynomial in $\gamma$ has a root for only one of the possible choices of $\beta$.

When $(N, r) = (3, 1)$ a similar example is given over $\mathbb{Q}(\zeta_3)$ by the pair [15.a1] and [15.a2] and when $(N, r) = (3, 2)$ by the pair [11.a1] and [11.a2].

(iii) When $(N, r) = (3, 1)$ the condition that $(\sqrt{J} + 1)(\sqrt{J'} + 1) \neq 1$ is necessary. The elliptic curves with LMFDB labels [245.a1] and [1323.a1] are not (quadratic twists of) $(3, 1)$-congruent elliptic curves, however there do exist $\alpha, \beta \in \mathbb{Q}$ satisfying Theorem 3.3 (iii). Moreover when $N = 3, 4$ the theorem is false when $J = J'$. Counterexamples are given by the pairs of elliptic curves [14.a1] and [126.b1] when $(N, r) = (3, 1)$, [245.a1] and [245.b1] when $(N, r) = (3, 2)$, [14.a6] and [112.c6] when $(N, r) = (4, 1)$, and [14.a6] and [784.b6] when $(N, r) = (4, 3)$.

**Proof of Theorem 3.3.** If $j = j'$ then $E$ and $E'$ are 2-congruent (since an elliptic curve is 2-congruent to any quadratic twist and $j, j' \notin \{0, 1728\}$ by assumption). Condition (i) is always satisfied in this case, so we are free to assume that $j \neq j'$ when $(N, r) = (2, 1)$.

For each $(N, r)$ let $\mathcal{P}_\alpha \in K[J, J', \alpha], \mathcal{P}_\beta \in K[J, J', \alpha, \beta]$ (and $\mathcal{P}_\gamma \in K[J, J', \alpha, \beta, \gamma]$ when $N = 4$) be the polynomials from the statement of the theorem.

When $N = 2, 3$ let $\mathcal{Z}(N, r) = \text{Spec } K[J, J', \alpha, \beta]/(\mathcal{P}_\alpha, \mathcal{P}_\beta)$ and $\mathcal{Z}(4, r) = \text{Spec } K[J, J', \alpha, \beta, \gamma]/(\mathcal{P}_\alpha, \mathcal{P}_\beta, \mathcal{P}_\gamma)$. Similarly when $N = 2, 3$ let $\mathcal{W}(N, r) = \text{Spec } K[JJ', (J - 1)(J' - 1), \alpha, \beta]/(\mathcal{P}_\alpha, \mathcal{P}_\beta)$ and let $\mathcal{W}(4, r) = \text{Spec } K[JJ', (J - 1)(J' - 1), \alpha, \beta, \gamma]/(\mathcal{P}_\alpha, \mathcal{P}_\beta, \mathcal{P}_\gamma)$.
Write, in the notation of Section 3.2

\[(N, r) = (2, 1) : \quad \alpha = \frac{4w_0 - \frac{3}{2}w_1 - w_2}{w_2}, \quad \beta = \frac{w_1}{w_2}, \quad \gamma = \frac{J'w_2}{\beta w_3}\]

\[(N, r) = (4, r) : \quad \alpha = \frac{4w_0 - \frac{3}{2}w_1 - (w_2^2/w_2)}{(w_2^2/w_2)}, \quad \beta = \frac{w_1}{w_2^2/w_2}, \quad \gamma = \frac{\left(\frac{3}{2}(3w_1 - w_3)/w_3\right)^2 - 3(\alpha + 1)}{2}\]

\[(N, r) = (3, 1) : \quad \alpha = \frac{\eta}{12w_0w_3}, \quad \beta = \frac{(\frac{3}{2}(3w_1 - w_3)/w_3)^2 - 3(\alpha + 1)}{2}, \quad \gamma = \frac{J'w_2}{\beta w_3}\]

\[(N, r) = (3, 2) : \quad \alpha = w_1/w_2, \quad \beta = (w_0/w_2)^2 - 3(\alpha^2 + \alpha + 1)\]

where \(\eta = (w_0 + 3w_1 - 3w_3)(8w_0w_1 - 3w_2^2 + 6w_1w_3 - 3w_3^2)\). Then these choices induce maps \(S(N, r) \rightarrow W(N, r)\) (where \(S(N, r)\) are the surfaces defined in Sections 3.2.1, 3.2.3) and therefore maps \(W(N, r) \rightarrow W(N, r)\).

In particular we have a commutative diagram

\[
\begin{array}{ccc}
Z(N, r) & \xrightarrow{\pi} & Z(N, r) \\
J_Z & \downarrow & \downarrow J_Z \\
Z(1) & & Z(1)
\end{array}
\]

where \(J_Z\) and \(J_Z\) are morphisms. The degree of the morphism \(J_Z\) is equal to \(|SL_2(\mathbb{Z}/N\mathbb{Z})|/2\) and the degree of \(J_Z\) may be read off from the degrees of the polynomials \(P_\alpha, P_\beta,\) and \(P_\gamma\). Since these degrees are equal for each \((N, r)\) the map \(\pi\) is birational.

Write \(R = K[J, J']\left[\frac{1}{J(J-1)(J-1)(J-J')}\right]\) where

\[\xi = \begin{cases} 
1 & \text{if } N \in \{2, 4\}, \text{ or } (N, r) = (3, 2) \\
(JJ')^3 + 3(JJ')^2(J + J') - 27(JJ')^2 + 3(JJ')(J + J')^2 + (J + J')^3 & \text{if } (N, r) = (3, 1).
\end{cases}\]

Letting \(Z'(1) = \text{Spec } R\) we have a natural open immersion \(Z'(1) \subset Z(1)\). Let \(Z'(N, r)\) and \(Z'(N, r)\) be the preimages of \(Z'(1)\) under the maps \(J_Z\) and \(J_Z\) respectively.

Explicitly \(Z'(N, r)\) and \(Z'(N, r)\) are the surfaces given by deleting the points on \(Z(N, r)\) and \(Z(N, r)\) above the loci:

\[(N, r) = (2, 1) : \quad J = J' \text{ and } J, J' \in \{0, 1\},\]
\[(N, r) = (4, r) : \quad J = J' \text{ and } J, J' \in \{0, 1\},\]
\[(N, r) = (3, 1) : \quad J = J', J, J' \in \{0, 1\}, \text{ and } (\sqrt[3]{J} + 1)(\sqrt[3]{J'}) = 1,\]
\[(N, r) = (3, 2) : \quad J = J' \text{ and } J, J' \in \{0, 1\}.
\]

We next show that \(\pi\) extends to an isomorphism \(\bar{\pi} : Z'(N, r) \rightarrow Z'(N, r)\). Note that the morphism \(Z'(N, r) \rightarrow Z'(1)\) is finite étale since \(X(N) \rightarrow X(1)\) is finite étale away from \(j = 0, 1728, \infty\).

When \(N = 2, 3\) we see that the finite morphism \(Z'(N, r) \rightarrow Z'(1)\) factors via

\[Z'(N, r) = \text{Spec } R[\alpha, \beta]/(P_\alpha, P_\beta) \longrightarrow \text{Spec } R[\alpha]/(P_\alpha) \longrightarrow Z'(1)\]

and similarly when \(N = 4\) with an extra factor accounting for the polynomial in \(\gamma\). In particular when \(N = 2, 3\), to show that \(Z'(N, r) \rightarrow Z'(1)\) is étale it suffices to show that \(\partial P_\alpha/\partial \alpha\) and \(\partial P_\beta/\partial \beta\) are units in \(R[\alpha]/(P_\alpha)\) and \(R[\alpha, \beta]/(P_\alpha, P_\beta)\) respectively. When \(N = 4\) we must also check that \(\partial P_\gamma/\partial \gamma\) is a unit in \(R[\alpha, \beta, \gamma]/(P_\alpha, P_\beta, P_\gamma)\).

Computing successive resultants in \texttt{Magma} and using the fact that \(2, 3, J, J', J-1, J'-1, J-J', \) and \(\xi\) are units in \(R\) shows that the ideals \((P_\alpha, \frac{\partial P_\alpha}{\partial \alpha})\), \((P_\alpha, P_\beta, \frac{\partial P_\beta}{\partial \beta})\), and \((P_\alpha, P_\beta, P_\gamma, \frac{\partial P_\gamma}{\partial \gamma})\) contain 1. In particular, the morphisms \(Z'(N, r) \rightarrow Z'(1)\) are finite étale.
Applying the following lemma with \( X = Z'(N, r), Y = Z'(N, r) \), and \( S = Z'(1) \) shows that \( \pi \) extends to an isomorphism \( \tilde{\pi}: Z'(N, r) \to Z'(N, r) \).

**Lemma 3.5.** Let \( X, Y \), and \( S \) be integral \( K \)-varieties. Suppose that \( S \) is smooth and that there exists a commutative diagram

\[
\begin{array}{ccc}
X & \xrightarrow{\pi} & Y \\
\downarrow^{p_X} & & \downarrow^{p_Y} \\
S & \xrightarrow{\pi} & S
\end{array}
\]

where \( p_X \) and \( p_Y \) are finite étale morphisms and \( \pi \) is birational. Then \( \pi \) extends uniquely to an isomorphism \( \tilde{\pi}: X \to Y \).

**Proof.** Because \( \pi \) is birational there exist dense open subschemes \( U \subset X \) and \( V \subset Y \) such that \( \pi|_U: U \to V \) is an isomorphism. Since \( p_X \) and \( p_Y \) are finite étale we may choose \( U \) and \( V \) such that \( p_X|_U: U \to S \) and \( p_Y|_V: V \to S \) are finite étale.

By assumption \( S \) is integral and nonsingular, so the natural functor from the category of finite étale covers of \( S \) to the category of finite étale covers of \( p_X(U) \) is fully faithful (see \[41, Lemma 0BQG\] noting the proof of \[41, Lemma 0BQI\]). In particular the isomorphism \( \pi|_U: U \to V \) extends uniquely to a morphism \( \tilde{\pi}: X \to Y \). A symmetrical argument shows that the inverse of \( \pi|_U \) extends uniquely to a morphism \( Y \to X \). Therefore by uniqueness \( \tilde{\pi} \) is an isomorphism. \( \square \)

The surface \( Z(N, r)/K \) acts as a fine moduli space for pairs of elliptic curves \( E/K \) and \( E'/K \) with \( j(E), j(E') \notin \{0, 1728\} \) which are \( (N, r) \)-congruent up to a simultaneous quadratic twist (or simply up to quadratic twist if \( N = 2 \)). Therefore we have only shown that elliptic curves \( E/K \) and \( E'/K \) satisfying the conditions on \( \alpha, \beta \) (and \( \gamma \) is \( N = 4 \)) are \( (N, r) \)-congruent up to quadratic twist. When \( N = 3, 4 \) it remains to show that the condition on \( \tau \) is satisfied if and only if \( E \) and \( E' \) are \( (N, r) \)-congruent.

The following lemma will allow us to identify the correct quadratic twist.

**Lemma 3.6** (cf., \[13, Proposition 13(A)]). Let \( N \geq 3 \) be an integer and let \( K \) be the field of fractions of a complete discrete valuation ring with residue field of characteristic coprime to \( N \). Suppose that \( E/K \) has good reduction and \( E'/K \) has potential good reduction. If \( E \) and \( E' \) are \( N \)-congruent over \( K \) then \( E' \) has good reduction over \( K \).

**Proof.** Let \( K^{ur} \) be the maximal unramified extension of \( K \) and let \( L = K^{ur}(E[N]) \) and \( L' = K^{ur}(E'[N]) \). Since \( E \) and \( E' \) are \( N \)-congruent \( L = L' \).

But \( L \) (resp. \( L' \)) is the smallest extension of \( K^{ur} \) over which \( E \) (resp. \( E' \)) obtains good reduction (see \[38, §2 Corollary 3\]). Since \( E \) has good reduction over \( K \) we have \( L' = L = K^{ur} \). Therefore \( E' \) has good reduction over \( K \). \( \square \)

The fibres of the maps \( Z'(N, r) \to X(1) \) have genus 0 and are birational to the curves \( X_E(N) \) where \( E \) is an elliptic curve with \( j \)-invariant \( j \). By parametrising the generic fibre we obtain a birational map \( \lambda: Z'(N, r) \to X(1) \times \mathbb{P}^1 \) which is an isomorphism onto its image since the fibres of \( Z'(N, r) \to X(1) \) are nonsingular.

Let \( \mathcal{E} \to Z'(N, r) \) be given by the Weierstrass equation

\[
y^2 = x^3 - 27\frac{j}{j - 1728}x - 54\frac{j}{j - 1728}
\]

and let \( \mathcal{E}' \to Z'(N, r) \) be given by the Weierstrass equation

\[
y^2 = x^3 - 27d^2\frac{j'}{j' - 1728}x - 54d^3\frac{j'}{j' - 1728}
\]
where

\begin{align*}
(N, r) = (4, 1) : & \quad d = \frac{3\delta_{\alpha}jj'}{(j - 1728)(j' - 1728)}, \\
(N, r) = (4, 3) : & \quad d = \frac{3\alpha jj'}{(j - 1728)(j' - 1728)}, \\
(N, r) = (3, 1) : & \quad d = \frac{3\beta jj'}{(j - 1728)(j' - 1728)}, \\
(N, r) = (3, 2) : & \quad d = \frac{3\beta jj'}{(j - 1728)(j' - 1728)}. 
\end{align*}

By construction the rational functions \( j, j', (j - 1728), \) and \((j' - 1728)\) are units in \( R \). We check in Magma that when \( N = 4 \) the functions \( \delta \) and \( \alpha \) are units in \( R[\alpha, \beta, \gamma]/(P_\alpha, P_\beta, P_\gamma) \). Similarly when \( (N, r) = (3, 1) \) the function \( \delta \) is a unit in \( R[\alpha, \beta, \gamma]/(P_\alpha, P_\beta, P_\gamma) \). Computing the discriminants of the Weierstrass equations in \([1]\) and \([2]\) we see that the fibres of \( \mathcal{E}, \mathcal{E}' \to \mathcal{Z}'(N, r) \) are nonsingular except when \( (N, r) = (3, 2) \) and \( \beta = 0 \).

The generic fibres of \( \mathcal{E}, \mathcal{E}' \to \mathcal{Z}'(N, r) \) are elliptic curves \( \mathcal{E}/\mathbb{Q}(j, t) \) and \( \mathcal{E}'/\mathbb{Q}(j, t) \) and we may choose models such that \( \Delta(\mathcal{E}), \Delta(\mathcal{E}') \in \mathbb{Z}[j, t] \), where \( j \) and \( t \) are coordinates on \( X(1) \times \mathbb{P}^1 \).

Since \( \mathcal{E} \) and \( \mathcal{E}' \) are \((N, r)\)-congruent up to quadratic twist there exists some squarefree \( D \in \mathbb{Z}[j, t] \) such \( \mathcal{E} \) is \((N, r)\)-congruent to \( (\mathcal{E}')^D \). If \( D \) has an irreducible factor \( q \) not dividing \( \Delta(\mathcal{E})\Delta(\mathcal{E}') \) then applying Lemma \([3, 1]\) over the completion of \( \mathbb{Z}[j, t] \) at \( q \) we see that \( \mathcal{E} \) and \( (\mathcal{E}')^D \) are not \( N \)-congruent, hence \( D \) divides \( \Delta(\mathcal{E})\Delta(\mathcal{E}') \). In particular, there are finitely many possibilities for \( D \in \mathbb{Z}[j, t] \).

Explicitly computing the parametrisation \( \lambda \) in Magma, specialising at a small number of \( j, t \in \mathbb{Q} \), and comparing traces of Frobenius is enough to prove that \( D = 1 \) when \( N = 3 \), and \( D = 1 \) or \( \delta \) when \( N = 4 \).

The condition on \( \tau \) follows immediately when \( (N, r) = (3, 1) \) and when \( (N, r) = (3, 2) \) and \( \beta \neq 0 \). Moreover we see that elliptic curves are \( 4 \)-congruent if and only if they satisfy one of the conditions on \( \tau \) in \([ii]\).

Note that \( 3c_0c'_0\alpha \) is not a square for the pair of 5-isogenous (hence \((4, 1)\)-congruent) elliptic curves with LMFDB labels \([38, b1]\) and \([38, b2]\). Therefore \( D = 1 \) when \( (N, r) = (4, 1) \). Similarly \( 3c_0c'_0\delta\alpha \) is not a square for the pair of 3-isogenous elliptic curves \([44, a1]\) and \([44, a2]\) so \( D = 1 \) when \( (N, r) = (4, 3) \).

The curve on \( \mathcal{Z}'(3, 2) \) given by the vanishing of \( \beta \) admits an obvious parametrisation by setting \( J = t \), \( J' = 1/t \), \( \alpha = 1 \), and \( \beta = 0 \). Repeating the above calculation with \( d = \frac{-2jj'}{(j - 1728)(j' - 1728)} \) completes the proof.

\begin{flushright}
\Box
\end{flushright}

Remark 3.7. For \( N \leq 4 \), rather than recovering \( X_0^+(N) \) it is also possible to give a parametrisation \( \mathbb{A}^2 \to Z(N, r) \) so that the involution swapping the roles of \( \mathcal{E} \) and \( \mathcal{E}' \) is given by swapping the coordinates on \( \mathbb{A}^2 \). In the electronic data \([17]\) we record these symmetric families of \((N, r)\)-congruent elliptic curves over \( \mathbb{Q}(a, b) \). These parametrisations were found by first parametrising the surfaces \( S(N, r) \) which are birational to \( W(N, r) \).

4. Constructing \( Z(N, r) \) via fibre products

Let \( N_1, N_2 \geq 2 \) be coprime integers and let \( N = N_1N_2 \). We define \( Z^+(N, r) \) to be the fibre product

\[
\begin{array}{ccc}
Z^+(N, r) & \xleftarrow{\cdot} & Z(N_1, r) \\
\downarrow & & \downarrow \\
Z(N_2, r) & \xrightarrow{\cdot} & Z(1)
\end{array}
\]

and similarly for \( W^+(N, r) \).

Remark 4.1. Note that the surfaces \( Z^+(N, r) \) and \( W^+(N, r) \) may depend implicitly on the factorisation \( N = N_1N_2 \).
The surface $Z^+(N, r)$ has the following moduli interpretation: for each point $P \in Z^+(N, r)(K)$ with $j(P), j'(P) \not\in \{0, 1728\}$ there exist pairs of elliptic curves $(E_1, E'_1)$ and $(E_2, E'_2)$ defined over $K$ such that for $i = 1, 2$ we have

- $j(P) = j(E_i)$ and $j'(P) = j(E'_i)$, and
- $E_i$ and $E'_i$ are $(N, r)$-congruent over $K$.

The surface $W^+(N, r)$ is then obtained from $Z^+(N, r)$ by taking the quotient by the involution swapping the roles of $E_i$ and $E'_i$.

**Remark 5.1.** Suppose that $N_1 = 4$ and that $r_1, r_2 \in (\mathbb{Z}/N\mathbb{Z})^\times$ are equal (up to a square) modulo $N_2$. Then the surfaces $Z^+(N, r_1)$ and $Z^+(N, r_2)$ are isomorphic since $Z(4, 1)$ and $Z(4, 3)$ are isomorphic (see Remark 3.2) and the isomorphism respects the maps $Z(4, r) \to Z(1)$.

By taking simultaneous quadratic twists of $E_2$ and $E'_2$ we may assume that $E_1 = E_2$. If $N_1 = 2$ then we immediately see that $Z^+(N, r)$ is birational to $Z(N, r)$ – every elliptic curve is 2-congruent to any quadratic twist, so we may replace $E'_1$ by its quadratic twist $E'_2$ so that $E_1$ is $(N, r)$-congruent to $E'_1$.

Otherwise, assume that $N_1 \neq 2$ for $i = 1, 2$. By the above discussion if $E/Q(Z^+(N, r))$ is an elliptic curve with $j$-invariant $j$ then there exists a pair of elliptic curves $E_i/Q(Z^+(N, r))$ and $E'_i/Q(Z^+(N, r))$ with $j$-invariant $j'$ such that $E$ and $E'_i$ are $(N, r)$-congruent. Let $d \in \mathbb{Q}(Z(N, r))$ be such that $E'_i$ is isomorphic to the quadratic twist of $E'_2$ by $d$. Then the modular diagonal quotient surface $Z(N, r)$ is birational to the double cover of $Z^+(N, r)$ whose function field is given by adjoining the square root of $d$ to $\mathbb{Q}(Z(N, r))$.

5. Computing $Z(12, r)$

We now prove Theorem 1.1 by applying Theorem 3.3 to compute the fibre products described in Section 3. To compute the surfaces $Z(12, r)$ for $r = 1, 7$ we use Theorem 3.3(i) and (ii) to construct the covers $Z(12, r) \to Z(3, 1)$. In contrast, to compute the surfaces $Z(12, r)$ for $r = 5, 11$ we use Theorem 3.3(iv) to construct the covers $Z(12, r) \to Z(4, r)$.

**Remark 5.1.** It is also possible to compute $Z(12, r)$ for $r = 1, 7$ by using Theorem 3.3(iv) to construct the covers $Z(12, r) \to Z(4, r)$, and similarly when $r = 5, 11$ it is possible to compute $Z(12, r)$ by using Theorem 3.3(ii)(iv) to construct the covers $Z(12, r) \to Z(3, 2)$.

5.1. Choosing parametrisations via Cremona transformations. Since a model for $W(N, r)$ consists of both a birational model for the surface and equations for the forgetful maps we naturally want to simplify both the equations for the surface and the maps. When the surface in question is rational we exploit the birational automorphisms of $\mathbb{P}^2$ to simplify the forgetful maps.

It is well known that $\text{Bir}_0(\mathbb{P}^2)$, the birational automorphism group of $\mathbb{P}^2$ over $\mathbb{Q}$, contains $\text{PGL}_3(\mathbb{Q})$ and the Cremona transformations – that is, birational automorphisms of the form

$$[x_0 : x_1 : x_2] \mapsto [Q_0(x_0, x_1, x_2) : Q_1(x_0, x_1, x_2) : Q_2(x_0, x_1, x_2)]$$

where $Q_0, Q_1, Q_2 \in \mathbb{Q}[x_0, x_1, x_2]$ are homogeneous forms of degree 2 which vanish simultaneously at three $G_0$-conjugate points $q_1, q_2, q_3 \in \mathbb{P}^2(\overline{\mathbb{Q}})$ in general position.

Geometrically this operation blows up $q_1, q_2, q_3$ and blows down the three lines which contain exactly two of $q_1, q_2, q_3$.

This suggests the following approach for simplifying a model for $W(N, r)$. Let $C/\mathbb{Q}$ be a curve in $\mathbb{P}^2$ given by the vanishing of a factor of the numerator of $J J'$, $(J-1)(J'-1)$, or $(J-J')^2$. Applying a generic Cremona transformation to $\mathbb{P}^2$ will double the degree of $J J'$, $(J-J')^2$, and $(J-1)(J'-1)$. If instead we apply a Cremona transformation centred at a $G_0$-stable triple of singular points $q_1, q_2, q_3 \in C(\overline{\mathbb{Q}})$ we may hope to decrease their degrees.

In the discussion that follows we often make choices of parametrisation which give rise to models for $W(N, r)$ with $j$-maps of small degree. In general, the parametrisations we give were not our first choice. Once we have a birational map $\mathbb{A}^2 \dashrightarrow W(N, r)$ (e.g., by spotting a genus 0 fibration over $\mathbb{P}^1$), we apply iterative Cremona transformations as described above to simplify the $j$-maps.
5.2. Models for $Z(12, 1)$ and $Z(12, 7)$. We will use Theorem 3.3 to compute a model for the fibre product $W^+(12, r)$.

As in the proof of Theorem 3.3 let $W(3, 1)$ be the surface in $\mathbb{A}^3$ defined by the polynomials in Theorem 3.3(iii). We check in Magma that the rational map $\mathbb{A}^2 \dashrightarrow W(3, 1)$ given by taking

$$J J' = \frac{-(-2ab + b^2 - 4a - 4b)^3}{(2b + 1)^3(-ab + b^2 - 2a - 2b)^2},$$

$$(J - 1)(J' - 1) = \frac{(b + 2)(a^2 - 2ab^2 + b^3 + 2a^2 + ab - 2b^2 + a + b)^2}{(2b + 1)^3(-ab + b^2 - 2a - 2b)^2},$$

(and solving for $\alpha$ and $\beta$) is birational. In particular $W(3, 1)$ is birational to $\mathbb{A}^2$ with the forgetful map $W(3, 1) \to W(1)$ given by the formulae for $J J'$ and $(J - 1)(J' - 1)$ above.

Let $\Delta = \Delta(\mathcal{E})$ and $\Delta' = \Delta(\mathcal{E}')$ be the discriminants of the elliptic curves $\mathcal{E}/\mathbb{Q}(Z(3, 1))$ and $\mathcal{E}'/\mathbb{Q}(Z(3, 1))$ with $j$-invariants 1728J and 1728J$'$ respectively. We write $W(3, 1)\sqrt{\Delta \Delta'}$ for the double cover of $W(3, 1)$ whose function field is given by adjoining $\sqrt{\Delta \Delta'}$ to $\mathbb{Q}(W(3, 1))$.

Then $W(3, 1)\sqrt{\Delta \Delta'}$ is birational to the surface given by

$$\alpha_4^2 - (J - 1)(J' - 1) = 0$$

in $\mathbb{A}^3$. By setting

$$\alpha_4 = \frac{-(b + 2)(a^2 - 2ab^2 + b^3 + 2a^2 + ab - 2b^2 + a + b)}{(2b + 1)^3(-ab + b^2 - 2a - 2b)} \alpha_4,$$

we see that $W(3, 1)\sqrt{\Delta \Delta'}$ is birational to the surface given by

$$(\alpha_4')^2 - (2b + 1) = 0$$

in $\mathbb{A}^3$. We parametrise this surface by setting $(a, b, \alpha_4') = \left( c, \frac{d^2 + 1}{2}, d \right)$. Therefore $W(3, 1)\sqrt{\Delta \Delta'}$ is birational to $\mathbb{A}^2$ and the forgetful map $W(3, 1)\sqrt{\Delta \Delta'} \to W(3, 1)$ is given by $(c, d) \mapsto \left( c, \frac{d^2 + 1}{2} \right)$.

By Theorem 3.3(i) we may write $W(6, 1)$ as a degree 3 cover of $\mathbb{A}^2$ given by the vanishing of

$$\beta_4^3 - 3J J' \beta_4 - 2J J'(\alpha_4 + 1) = 0$$

in $\mathbb{A}^3$. After making the change of coordinates

$$\beta_4 = \frac{(d^4 - 4cd^2 - 10d^2 - 12c + 9)(d^2 - 2d - 3)\beta_4' - d^4 + 2cd^2 + 2d^3 + 6d^2 + 6c - 6d - 9)}{2d^3(d^4 - 2cd^2 - 6d^2 - 6c + 5)} \cdot \frac{1}{\beta_4'},$$

we find that $W(6, 1)$ is birational to the surface given by

$$(\beta_4')^3 + 6(\beta_4')^2 - 3(d + 1)(d - 3)\beta_4' - (2cd^2 + 6c - d^4 + 2d^3 + 6d^2 - 6d - 9) = 0$$

in $\mathbb{A}^3$. We parametrise the above surface by setting

$$(c, d, \beta_4') = \left( \frac{p^3 q + 6p^2 q^2 + 9pq^3 + 12pq^2 - 12pq + 9q^4 + 12q^3 - 24q^2 - 16q + 16 \cdot \frac{2}{q}}{2q^2(3q^2 + 4)} \right).$$

Hence $W(6, 1)$ is birational to $\mathbb{A}^2$ and the forgetful map $W(6, 1) \to W(3, 1)\sqrt{\Delta \Delta'}$ is given by $(p, q) \mapsto (c, d)$.

By Theorem 3.3(iii) the surface $W^+(12, 1)$ (which by Remark 3.2 is isomorphic to $W^+(12, 7)$) is birational to the surface given by

$$\gamma_4^2 - 6J J' \beta_4 \gamma_2 - 16(J J')^2 \gamma_4 + 3(J J')^2 (4J J' - \beta_4^2) = 0$$

in $\mathbb{A}^3$. After making the birational transformation

$$\gamma_4 = \frac{(2p^3 q + 12p^2 q^2 + 18pq^3 + 9q^4 + 24pq^2 + 24q^3 - 24pq - 8q^2 - 32q + 16)^2}{64(p + 4q - 4)(p + q + 2)^3},$$

$$q = \frac{((\gamma_4')^2 - 3p + 4\gamma_4 - 8)q' - 2p\gamma_4 - 4p + 4\gamma_4'}{6\gamma_4'},$$

we find that $W^+(12, 1)$ is birational to the quadric surface

$$3(q')^2 - 2\gamma_4 q' + 8q' + p + 4 = 0$$
respectively. We parametrise this surface by setting
\[
(p, q', \gamma_4') = \left( \frac{-4(s - 3)(s + 1)(3s - 2t - 1)^2}{3(s - 1)^2(s - 2t - 1)(3s + 2t + 1)}, \frac{8s(t - 1)}{3(s - 1)(s - 2t - 1)(3s + 2t + 1)}, \frac{4s(s - 3)(3s - 2t - 1)}{(s - 1)(s - 2t - 1)(3s + 2t + 1)} \right).
\]
The forgetful map \(W^+(12, 1) \to W(6, 1)\) is given by \((s, t) \mapsto (p, q)\).

5.2.1. The Surface \(Z(12, 1)\). The \(\alpha_4, \beta_4\), and \(\gamma_4\) are elements of \(\mathbb{Q}(W^+(12, 1))\) which satisfy the conditions of Theorem \([3, (ii)]\). Let \(\delta_4 = 3(J' - (\alpha_4 + 1)^2)\) be as in Theorem \([3, (ii)]\). By construction there exist \(\alpha_3, \beta_3, \delta_3 \in \mathbb{Q}(W^+(12, 1))\) which satisfy Theorem \([3, (iii)]\).

As in Section 4 let \(E/\mathbb{Q}(Z^+(12, 1))\) be an elliptic curve with \(j\)-invariant 1728. Let \(E'_1/\mathbb{Q}(Z^+(12, 1))\) and \(E'_2/\mathbb{Q}(Z^+(12, 1))\) be elliptic curves with \(j\)-invariant 1728. It follows from Theorem \([3, (ii)]\) and \([3, (iii)]\) that up to square factors \(c_0(E)\) is equal to both \(3\delta_3 c_6(E'_1)\) and \(3\alpha_4 \delta_4 c_6(E'_2)\). In particular \(E'_1\) is isomorphic to the quadratic twist of \(E'_2\) by \(\alpha_4 \delta_4 \delta_3\).

Therefore by the discussion in Section 4 the surface \(W(12, 1)\) is birational to the double cover of \(\mathbb{A}^2\) given by
\[
w^2 = \alpha_4 \delta_4 \delta_3.
\]
The rational function \(\alpha_4 \delta_4 \delta_3\) is equal to \(3s(t - 1)(-s + 2t + 1)(3s + 2t + 1)(st + 2s - 2t - 1)\) up to a square factor. Therefore the surface \(W(12, 1)\) is birational to the affine surface given by
\[
(w')^2 = 3s(t - 1)(-s + 2t + 1)(3s + 2t + 1)(st + 2s - 2t - 1).
\]
We parametrise this surface by setting
\[
(s, t, w') = \left( \frac{-2u^2 - uv^2 - u + 4v^2}{uv^2 + u + 4v^2}, \frac{2u^2v^2 - 4u^2 + uv^4 - 6uv^2 - 3u - 8v^4}{(2u + v^2 + 3)(uv^2 + u + 4v^2)}, \frac{36uv(u + 2)(u + v^2 + 1)(u + 2v)(2u^2 + uv^2 + u - 4v^2)^2}{(2u + v^2 + 3)^2(uv^2 + u + 4v^2)^3} \right).
\]
Hence \(W(12, 1)\) is birational to \(\mathbb{A}^2\) and the forgetful map \(W(12, 1) \to W^+(12, 1)\) is given by \((u, v) \mapsto (s, t)\).

Let \(F_{12, 1}(u, v)\) be the polynomial from the statement of Theorem \([11]\). It follows immediately that \(Z(12, 1)\) is birational to the affine surface given by the equation
\[
z^2 = F_{12, 1}(u, v)
\]
since \((J - J')^2\) is equal to \(F_{12, 1}(u, v)\) up to a square factor.

5.2.2. The Surface \(Z(12, 7)\). By Theorem \([3, \beta]\) the surface \(W(12, 7)\) is birational to the double cover of \(W^+(12, 1)\) given by
\[
w^2 = \alpha_4 \delta_3.
\]
The rational function \(\alpha_4 \delta_3\) is equal to \(3(t - 1)(-9s^3 + 12s^2t + 4st^2 + 15s^3 + 4st - 12t^2 - s - 12t - 3)\) up to a square factor.

Therefore the surface \(W(12, 7)\) is birational to the affine surface given by \((w')^2 = 3(t - 1)(-9s^3 + 12s^2t + 4st^2 + 15s^3 + 4st - 12t^2 - s - 12t - 3)\). We parametrise this surface by setting
\[
(s, t, w') = \left( \frac{(u - 1)(u^2 - v^2 + 4u + 1)}{u^2 + u^2 - uv^2 - 3u - v^2 + 1}, \frac{u^3 - uv^2 + 7u^2 - v^2 + 9u + 1}{u^3 + u^2 - uv^2 - 3u - v^2 + 1}, \frac{36uv(u + 2)(u^2 + 4u - v^2 + 1)}{(u^3 + u^2 - uv^2 - 3u - v^2 + 1)^2} \right).
\]
Hence \(W(12, 7)\) is birational to \(\mathbb{A}^2\) and the forgetful map \(W(12, 7) \to W^+(12, 1)\) is given by \((u, v) \mapsto (s, t)\).

Let \(F_{12, 7}(u, v)\) be the polynomial from the statement of Theorem \([11]\). It follows immediately that \(Z(12, 7)\) is birational to the affine surface given by the equation
\[
z^2 = F_{12, 7}(u, v)
\]
since \((J - J')^2\) is equal to \(F_{12, 7}(u, v)\) up to a square factor.
5.3. Models for $Z(12, 5)$ and $Z(12, 11)$. For each $r = 1, 3$ let $W(4, r)$ be the surface in $\mathbb{A}^5$ defined by the polynomials in Theorem 3.3 (ii). The rational map $\mathbb{A}^2 \to W(4, r)$ given by taking

$$J, J' = \frac{16(-2ab + b^2 + 2a + 2b)^3}{27(b-1)^2(-a+b+1)^4},$$

$$(J - 1)(J' - 1) = \frac{(a^2b + 2ab^2 + b^3 - a^2 + b^2 - 2a + b + 1)^2}{(b-1)^2(-a+b+1)^4},$$

(and solving for $\alpha$, $\beta$, and $\gamma$) is birational. In particular $W(4, r)$ is birational to $\mathbb{A}^2$ and the forgetful maps $W(4, r) \to W(1)$ are given by the rational functions $J, J'$ and $(J - 1)(J' - 1)$ above.

Let $\Delta = \Delta(\mathcal{E})$ and $\Delta' = \Delta(\mathcal{E}')$ be the discriminants of elliptic curves $\mathcal{E}/\mathbb{Q}(Z(4, 1))$ and $\mathcal{E}'/\mathbb{Q}(Z(4, 1))$ with $j$-invariants $1728J$ and $1728J'$ respectively. We write $W(4, 1)\sqrt[3]{\Delta \Delta'}$ for the triple cover of $W(4, 1)$ whose function field is given by adjoining $\sqrt[3]{\Delta \Delta'}$ to $\mathbb{Q}(W(4, 1))$.

Then $W(4, 1)\sqrt[3]{\Delta \Delta'}$ is birational to the surface given by

$$\alpha^3 - J, J' = 0$$

in $\mathbb{A}^3$. By making a change of coordinates $\alpha_3 = \frac{2(-2ab + b^2 + 2a + 2b)}{3(b-1)(-a+b+1)}\alpha_3'$ we see that $W(4, 1)\sqrt[3]{\Delta \Delta'}$ is birational to the surface

$$(\alpha_3')^3 - 2(b-1)(-a+b+1)^2 = 0$$

in $\mathbb{A}^3$. We parametrise this cubic surface by setting

$$(a, b, \alpha_3') = \left(\frac{-cd^3 + 8d^3 + 4}{2(c+2d^3+1)}, \frac{-c + 2d^3 + 1}{c + 2d^3 + 1}, \frac{-cd^2}{c + 2d^3 + 1}\right).$$

Hence $W(4, 1)\sqrt[3]{\Delta \Delta'}$ is birational to $\mathbb{A}^2$ and the forgetful map $W(4, 1)\sqrt[3]{\Delta \Delta'} \to W(4, 1)$ is given by $(c, d) \to (a, b)$.

By Theorem 3.4 (iv), the surface $W^+(12, 5)$ (which by Remark 4.2 is isomorphic to $W^+(12, 11)$) is birational to the surface given by

$$\beta_3^2 - 6(\alpha_3 + 1)(J - 1)(J' - 1)\beta_3 - 8((J - 1)(J' - 1))^2 \beta_3 - 3((\alpha_3 - 1)(J - 1)(J' - 1))^2 = 0$$

in $\mathbb{A}^3$. This is clearly birational to the surface given by

$$\beta_3^2 - \theta = 0$$

$$\theta^2 - 6(\alpha_3 + 1)(J - 1)(J' - 1)\theta - 8((J - 1)(J' - 1))^2 \beta_3 - 3((\alpha_3 - 1)(J - 1)(J' - 1))^2 = 0$$

in $\mathbb{A}^4$. To simplify the equations for this surface, we view the forms above as defining a quadric intersection in $\mathbb{A}^6_{(c,d)}$. By using ‘minimisation’ techniques similar to those in [7, Section 4.3], but applied over the base ring $\mathbb{Z}[c, d]$, we arrive at the change of coordinates

$$\theta = \frac{g_3(c, d)^2(g_1(c, d)\theta' + g_2(c, d)\beta_3' + 2(2d^3 + 1)g_2(c, d))}{3(\beta_3^2 + 2(2d^3 + 1))},$$

$$\beta_3 = \frac{g_3(c, d) (-3(d^2c + 4(2d^3 + 1)\beta_3' + 2(2d^3 + 1)(2c^2 - 3(d^2 + 4)c + 6(2d^3 + 1)))}{3(\beta_3^2 + 2(2d^3 + 1))}$$

where

$$g_1(c, d) = 8(2d^3 + 1)(c^2 - 6c + 9(2d^3 + 1)),$$

$$g_2(c, d) = (3d^4 - 8d^3 - 4)c^2 + 24(d^2 + 1)(2d^3 + 1)c + 12(2d^3 + 1)^2,$$

$$g_3(c, d) = \frac{d^6c^3 - 8(2d^3 + 1)^2c^2 + 48(2d^3 + 1)^2c - 8(2d^3 + 1)^3}{c^2d^8}.$$

It follows that $W^+(12, 5)$ is birational to the surface given by the pair of equations

$$2(\beta_3')^2 - 2\beta_3'\theta' - (\theta')^2 + (-8d^3 - 4)\beta_3' + (-8d^3 - 4)\theta' + c^2d^4 - 8cd^5 - 4cd^2 = 0,$$

$$-3(\beta_3')^2 + 3(\theta')^2 - 6cd^2\beta_3' - 3c^2d^4 + 8c^2d^3 - 48cd^3 + 4c^2 - 24c = 0$$

16
in $\mathbb{A}^4$. We parametrise this surface by setting
\[ (c, d, \beta_3', \theta') = \left( \frac{6(s + t)h_1(s, t)}{h_3(s, t)} \cdot \frac{t}{s + t + 2} \cdot \frac{2h_1(s, t)h_2(s, t) - 4(s - 1)(s^2 + st + s + 2t + 1)h_1(s, t)}{(s + t + 2)^2h_3(s, t)} \right) \]
where
\begin{align*}
h_1(s, t) &= s^3 + (3t + 6)s^2 + (3t^2 + 12t + 12)s + 3t^3 + 6t^2 + 12t + 8, \\
h_2(s, t) &= 4s^3 + 4s^2t - 3st^2 - 2st - 6s - 3t^3 - 2t + 2, \\
h_3(s, t) &= 2s^4 + (4t + 4)s^3 + (5t^2 + 18t + 12)s^2 + (6t^3 + 20t^2 + 24t + 10)s \\
 &\quad + 3t^4 + 6t^3 + 11t^2 + 8t - 1.
\end{align*}
Therefore $W^+(12, 5)$ is birational to $\mathbb{A}^2$ and the forgetful map $W^+(12, 5) \to W(4, 1)^{3\Delta \Sigma}$ is given by $(s, t) \mapsto (c, d)$.

5.3.1. The Surface $Z(12, 5)$. Note that $\alpha_3, \beta_3 \in \mathbb{Q}(W^+(12, 5))$ satisfy the conditions of Theorem 3.3(iv)
By construction there exist elements $\alpha_4, \beta_4, \gamma_4$ of $\mathbb{Q}(W^+(12, 1))$ which satisfy Theorem 3.3(iv)(ii). Let $\delta_4 = 3(J' - (\alpha_4 + 1)^2)$ be as in Theorem 3.3(ii).

By Theorem 3.3 the surface $W(12, 5)$ is birational to the double cover of $W^+(12, 5)$ given by
\[ w^2 = \alpha_4 \delta_4 \beta_3. \]
The rational function $\alpha_4 \delta_4 \beta_3$ is equal to $-s^2 + t^2 + 1$ up to a square factor.

Therefore the surface $W(12, 5)$ is birational to the affine surface $(w')^2 = -s^2 + t^2 + 1$. We parametrise this surface by setting
\[ (s, t, w') = \left( \frac{-w^2 + v^2 + 2u - 2}{u^2 - 2u - v^2}, \frac{2u - 2}{u^2 - 2u - v^2}, \frac{2v}{u^2 - 2u - v^2} \right). \]
Hence $W(12, 5)$ is birational to $\mathbb{A}^2$ and the forgetful map $W(12, 5) \to W^+(12, 5)$ is given by $(u, v) \mapsto (s, t)$.

Let $F_{12,5}(u, v)$ be the polynomial from the statement of Theorem 1.1. It follows immediately that $Z(12, 5)$ is birational to the affine surface given by the equation
\[ z^2 = F_{12,5}(u, v) \]
since $(J - J')^2$ is equal to $F_{12,5}(u, v)$ up to a square factor.

5.3.2. The Surface $Z(12, 11)$. By Theorem 3.3 the surface $W(12, 11)$ is birational to the double cover of $W^+(12, 5)$ given by
\[ w^2 = \alpha_4 \beta_3. \]
The rational function $\alpha_4 \beta_3$ is equal to $-(s + t)(s + t + 2)$ up to a square factor.

Therefore the surface $W(12, 11)$ is birational to the affine surface $(w')^2 = -(s + t)(s + t + 2)$. We parametrise this surface by
\[ (s, t, w') = \left( \frac{-uv^2 + u - 3v^2 - 1}{uv^2 + u + v^2 + 1}, \frac{-u + 1}{u + 1}, \frac{2v}{v^2 + 1} \right). \]
Hence $W(12, 11)$ is birational to $\mathbb{A}^2$ and the forgetful map $W(12, 11) \to W^+(12, 5)$ is given by $(u, v) \mapsto (s, t)$.

Let $F_{12,11}(u, v)$ be the polynomial from the statement of Theorem 1.1. It follows immediately that $Z(12, 11)$ is birational to the affine surface given by the equation
\[ z^2 = F_{12,11}(u, v) \]
since $(J - J')^2$ is equal to $F_{12,11}(u, v)$ up to a square factor.

6. CURVES ON Z(12, r) AND EXAMPLES OF 12-CONGRUENCES

We now identify some curves of small genus on our models for $Z(12, r)$ and we prove Theorem 1.4.
6.1. The modular curves $X_0(m)$ on $Z(12, r)$. Let $m$ be an integer coprime to $N$, and suppose that $m$ is equal to $r$ modulo $N$ (up to a square factor). The (non-compact) modular curve $Y_0(m)$ may be naturally embedded in $Z(N, r)$. More precisely we may regard a non-cuspidal $K$-point on $Y_0(m)$ as a triple $(E, E', \phi)$ where $E/K$ and $E'/K$ are elliptic curves and $\phi$ is a cyclic $m$-isogeny. In particular we have a natural map

$$Y_0(m) \xrightarrow{\psi} Z(N, m)$$

$$(E, E', \phi) \mapsto (E, E', \phi|_{E[N]})$$

defined over $\mathbb{Q}$. A pair of points $(E_1, E_1', \phi_1)$ and $(E_2, E_2', \phi_2)$ are identified under this morphism if and only if the the pairs $(E_1, E_1')$ and $(E_2, E_2')$ are simultaneous quadratic twists, in which case they define the same point on $Y_0(m)$. In particular $\psi$ is an embedding.

Remark 6.1. In fact, let $P = (E, E', \phi)$ be a $K$-point on $Z(N, r)$. Then for each integer $k$ such that $k^2 \equiv 1 \pmod{N}$ we obtain another $K$-point $P_a = (E, E', \phi \circ [k])$ on $Z(N, r)$ which is equal to $P$ if and only if $k$ is equal to either 1 or $-1$ modulo $N$.

In particular when $N = 12$ points on $Z(N, r)$ come in pairs, namely $P_1$ and $P_5$ in the above notation, which have the same image under $Z(12, r) \to Z^+(12, r)$. Hence each modular curve $Y_0(m)$ as above appears twice on $Z(12, m)$. In the notation of Kani–Schanz [19] these are the “Hecke curves” $T_{m,1}$ and $T_{m,5}$.

The image of $Y_0(m)$ under the quotient $Z(N, r) \to W(N, r)$ is $Y_0^+(m) := Y_0(m)/w_m$, where $w_m$ denotes the Fricke involution on $X_0(m)$.

We identify the curves $X_0(m)$ on our models for $Z(N, r)$ for each $m$ such that $X_0(m)$ appears in Magma’s SmallModularCurve database. The equations for these curves are recorded in Tables 3–6, the two choices of sign give the pair of curves $T_{m,1}$ and $T_{m,5}$.

Note that the modular curves $X_0(5)$ on $Z(12, 5)$ and $X_0(7)$ on $Z(12, 7)$ have been blown down (this is the case since we determined $Z(12, r)$ only up to birational equivalence). Equations for these curves on a blowup of our models are given by

$$z^2 = F_{12,5} \left( \frac{1}{2}(3 - \varepsilon), \frac{1}{2}(\pm 1 \pm \varepsilon + \varepsilon^2 t) \right) = \frac{1}{4} (1 \mp 2 + 44t + 16) \varepsilon^4 + O(\varepsilon^5)$$

and

$$z^2 = F_{12,7} (-\varepsilon, \pm 1 \pm \varepsilon + \varepsilon^2 t) = (4t^2 \mp 52t - 27) \varepsilon^4 + O(\varepsilon^5)$$

respectively.

| $m$    | Equation for $X_0^+(m)$ on $W(12, 1)$ |
|--------|---------------------------------------|
| 13     | $\pm v + 1$                           |
| 25     | $2u + \nu^2 \mp 2v + 1$               |
| 37     | $2u^2 + (\nu^2 \pm 2v + 1)u \pm v^3 - 3\nu^2 \pm 3v - 1$ |
| 49     | $4u^2 + 2(3\nu^2 + 2v + 3)u + \nu^4 \pm 4\nu^3 + 6\nu^2 \pm 4v + 1$ |
| 61     | $4\nu^3 + 2(\nu^2 \pm 2v + 5)u^2 + (-\nu^4 \pm 6\nu^3 \mp 4\nu^2 \pm 10v + 5)u \pm \nu^5 - 5\nu^4 \mp 10\nu^3 \mp 10\nu^2 \pm 5v - 1$ |

| $m$    | Equation for $X_0^+(m)$ on $W(12, 5)$ |
|--------|---------------------------------------|
| 17     | $u \pm v$                            |
| 29     | $u^2 + 2u - \nu^2 \pm 2v - 4$        |
| 41     | $u^3 - (\pm \nu - 2)u^2 + (-\nu^2 - 12)u \pm v^3 - 2\nu^2 \pm 4v + 8$ |
| 53     | $u^4 - (2\nu^2 \pm 4v)u^2 + (\pm 8v - 16)u \pm v^4 \pm 4v^3 + 8\nu^2 + 16$ |

Table 3. Modular curves on $Z(12, 1)$.

Table 4. Modular curves on $Z(12, 5)$. 

18
Equation for $X_0^+(m)$ on $W(12, 7)$

| $m$  | Equation for $X_0^+(m)$ on $W(12, 7)$                               |
|------|---------------------------------------------------------------------|
| 19   | $1 \pm v$                                                          |
| 31   | $u^2 - (\pm v - 1)u \pm 2v - 2$                                     |
| 43   | $-(\pm v - 1)u^2 + (v^2 \pm 2v + 1)u + 2v^2 - 2$                   |
| 55   | $(v^2 \mp 6v + 1)u^2 + (-2v^2 \mp 4v - 2)u - v^4 \mp 2v^3 \pm 2v + 1$ |

Table 5. Modular curves on $Z(12, 7)$.

Equation for $X_0^+(m)$ on $W(12, 11)$

| $m$  | Equation for $X_0^+(m)$ on $W(12, 11)$                               |
|------|---------------------------------------------------------------------|
| 11   | $1 \pm v$                                                          |
| 23   | $\pm vu + v^2 \pm v + 1$                                           |
| 35   | $-(\pm v^3 \pm 3v)u - v^4 \pm 3v^3 \pm v + 1$                      |
| 47   | $(\pm 3v^3 \pm 2v^2 \pm 3v)u + v^4 \pm v^3 + 4v^2 \pm v + 1$       |
| 59   | $(-3v^4 \pm 3v^3 - v^2 \pm v)u \pm v^5 \mp 8v^4 \pm 7v^3 + 11v^2 \pm 4v + 1$ |
| 71   | $(\pm 7v^5 \mp 10v^3 \mp v)u + v^6 \mp v^5 + 15v^3 \mp 15v^2 \mp 7v + 1$ |

Table 6. Modular curves on $Z(12, 11)$.

6.2. **Infinite families of 12-congruent elliptic curves and examples over $\mathbb{Q}(t)$.** We now prove Theorem 1.4. Specifically, we identify curves $C \subset Z(12, r)$ of genus 0 or 1 with infinitely many rational points. We use these to construct pairs of elliptic curves defined over $\mathbb{Q}(C)$ which are $(12, r)$-congruent. Once we have such a pair of elliptic curves the following lemma will allow us to deduce Theorem 1.4.

Recall that if $E/\mathbb{Q}$ is an elliptic curve, then fixing a basis for $\text{End}(E)$ we have that $\rho_{E[N]}: G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which we call the mod $N$ Galois representation attached to $E/\mathbb{Q}$ (for more details see [32, Section 2.2]).

**Lemma 6.2.** Let $C/\mathbb{Q}$ be a smooth projective curve with infinitely many rational points and let $\mathcal{E}/\mathbb{Q}(C)$ and $\mathcal{E}'/\mathbb{Q}(C)$ be elliptic curves which are not both isotrivial. For a point $P \in C(\mathbb{Q})$ let $\mathcal{E}_P/\mathbb{Q}$ be the specialisation of $\mathcal{E}$ at $P$ (and similarly for $\mathcal{E}'$).

(i) Suppose there exists a point $P \in C(\mathbb{Q})$ such that $\mathcal{E}_P$ and $\mathcal{E}'_P$ are nonsingular and do not have CM. Then $j(\mathcal{E}_P)$ and $j(\mathcal{E}'_P)$ are distinct $j$-invariants of $m$-isogenous elliptic curves over $\mathbb{Q}$ for any integer $m$ and for all but finitely many $Q \in C(\mathbb{Q})$ we have that $j(\mathcal{E}_Q)$ and $j(\mathcal{E}'_Q)$ are distinct $j$-invariants of $m$-isogenous elliptic curves for any integer $m$.

(ii) Suppose there exists a point $P \in C(\mathbb{Q})$ such that $\mathcal{E}_P$ is nonsingular and the mod $N$ Galois representation attached to $\mathcal{E}_P/\mathbb{Q}$ is surjective. Then there exist infinitely many $Q \in C(\mathbb{Q})$ such that the mod $N$ Galois representation attached to $\mathcal{E}_Q/\mathbb{Q}$ is surjective.

**Proof.** (i) This follows from a similar argument to [11, Theorem 1.5] which we reproduce here for completeness.

First suppose $E$ and $E'$ are non-CM elliptic curves defined over $\mathbb{Q}$ and $\phi: E \rightarrow E'$ is an isogeny defined over $\overline{\mathbb{Q}}$. Then $\hat{\phi} = [n] \in \text{End}(E)$ for some $n \in \mathbb{Z}$ and by comparing degrees for any $\sigma \in G_{\overline{\mathbb{Q}}}$ we have $(\hat{\phi})^\sigma \phi = \chi(\sigma) [n] \in \text{End}(E)$ for some character $\chi: G_{\overline{\mathbb{Q}}} \rightarrow \{\pm 1\}$. Let $d \in \mathbb{Q}$ be such that $\mathbb{Q}(\sqrt{d})$ is cut out by the kernel of $\chi$. Let $E^d/\mathbb{Q}$ be the quadratic twist of $E$ by $d$ and let $t: E^d \rightarrow E$ be a $\overline{\mathbb{Q}}$-isomorphism. Define $\phi' = \phi \circ t$, then for each $\sigma \in G_{\overline{\mathbb{Q}}}$ we have $(\hat{\phi'})^\sigma \phi' = [n] = \hat{\phi} \phi'$. But $\phi'$ is a surjection on $\overline{\mathbb{Q}}$-points so
Moreover the sections with \( \phi' \) for all \( \sigma \in G_Q \). Therefore \( \phi' : E^d \to E' \) is a \( \mathbb{Q} \)-isogeny. That is, \( j(E) \) and \( j(E') \) are the \( j \)-invariants of \( \mathbb{Q} \)-isogenous elliptic curves.

It therefore suffices to show that there are at most finitely many \( \mathbb{Q} \) \( j \)-invariants of \( \mathbb{Q} \)-isogenous elliptic curves.

Let \( C' \) be the image of the map \( C \to X(1) \times X(1) \) given by extending \( t \mapsto (j(E), j(E')) \). Consider the curves, \( T_m \), on \( X(1) \times X(1) \) which are the image of the modular curves \( X_m \) under the graph of the Hecke correspondence. Since the curves \( T_m \) are geometrically irreducible and \( j(E_P) \) and \( j(E'_P) \) are \( j \)-invariants of \( \mathbb{Q} \)-isogenous elliptic curves, the curve \( C' \) meets each \( T_m \) at finitely many points (over \( \overline{\mathbb{Q}} \)).

Mazur [28] and Kenku [21] showed that if an elliptic curve admits a cyclic \( m \)-isogeny over \( \mathbb{Q} \) then \( m \leq 163 \). In particular there are finitely many rational points on \( C' \) which lie on the union of all \( T_m \). The claim follows since the map \( j : C \to C' \) has finite degree.

(ii) We define a morphism \( j : C \to \mathbb{P}^1 \cong X(1) \) by extending \( j(E) \). Let \( M \) be the set of all maximal subgroups of \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \). For each \( H \in M \) let \( X(H)/\mathbb{Q} \) denote the modular curve whose \( K \)-points parametrise elliptic curves \( E/K \) such that \( \beta_{E,N}(G_Q) \) is contained in a subgroup of \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \) conjugate to \( H \) (see e.g., [32, Section 2]). Let \( C_H \) be the fibre product

\[
\begin{array}{ccc}
C_H & \longrightarrow & X(H) \\
\phi_H \downarrow & & \downarrow \\
C & \underset{j}{\longrightarrow} & X(1)
\end{array}
\]

We claim that the set

\[
C(\mathbb{Q}) \setminus \bigcup_{H \in M} \phi_H(C_H(\mathbb{Q}))
\]

is infinite.

First suppose that \( C \) has genus 0. Note that the morphisms \( \phi_H \) have degree greater than \( > 1 \) because \( E_P/\mathbb{Q} \) has surjective mod \( N \) Galois representation. Therefore since \( M \) is finite \( \bigcup_{H \in M} \phi_H(C_H(\mathbb{Q})) \) is a thin set in the sense of Serre. The claim follows from Hilbert’s Irreducibility Theorem [37, Proposition 3.4.2].

If \( C \) has genus 1 we make \( C \) into an elliptic curve by declaring \( P \) to be the identity. By Faltings’ theorem any of the curves \( C_H \) of genus \( \geq 2 \) have finitely many rational points. Therefore we may assume without loss of generality that for each \( H \) the curve \( C_H \) has genus 1 (and that \( C_H(\mathbb{Q}) \) is non-empty).

Since every morphism between elliptic curves is the composition of a translation and an isogeny [40, Example 4.7] the images \( \phi_H(C_H(\mathbb{Q})) \) are cosets of subgroups \( \Phi_H \subset C_H(\mathbb{Q}) \) which have finite index by the weak Mordell–Weil theorem. Because \( E_P/\mathbb{Q} \) has surjective mod \( N \) Galois representation the point \( P \) is not contained in \( \phi_H(C_H(\mathbb{Q})) \) for any \( H \).

Since we took \( P \) to be the identity, for each \( H \) the image \( \phi_H(C_H(\mathbb{Q})) \) is a non-trivial coset of \( \Phi_H \). In particular the subgroup \( \bigcap_H \Phi_H \subset C(\mathbb{Q}) \) is disjoint from \( \phi_H(C_H(\mathbb{Q})) \) for every \( H \). The claim follows by noting that the intersection \( \bigcap_H \Phi_H \) has finite index in \( C(\mathbb{Q}) \), and is therefore infinite.

\begin{example}[Family of (12, 1)-Congruences] Examples of pairs of \( (12, 1) \)-congruent elliptic curves over \( \mathbb{Q}(t) \) have previously been given by Chen [5, Section 7.3] and Fisher [13]. We include one here for completeness. The model \( z^2 = F_{12,1}(u, v) \) has an obvious elliptic fibration over the \( t \)-line given by \( y^2 = F_{12,1}(x, t) \). This model has a pair of sections with \( x \)-coordinates 0. By putting this fibration in Weierstrass form we see that \( Z(12, 1) \) is birational to the elliptic K3 surface with Weierstrass equation

\[
y^2 = x^3 - 27(t^8 + 46t^6 + 859t^4 - 186t^2 + 9)x - 54(t^{12} + 69t^{10} + 2082t^8 + 24731t^6 - 7848t^4 + 621t^2 + 27).
\]

Moreover the sections with \( x \)-coordinate \( \frac{3(2t^8 + 37t^6 + 4504t^4 - 27t^2 + 54)}{(t^2 - 3)^2} \) have infinite order. Taking multiples of this section gives an infinite family of examples over \( \mathbb{Q}(t) \) (a different family is given by Fisher [13, Corollary 1.3]).

In order to give a family where the 12-congruent elliptic curves have simple Weierstrass equations we instead note that the curve on \( Z(12, 1) \) given by the vanishing of \( 2u + v^2 + 3v \) has genus 0. By parametrising
this curve we obtain a pair of $(12,1)$-congruent elliptic curves $E_{12,1}/\mathbb{Q}(t)$ and $E'_{12,1}/\mathbb{Q}(t)$ where
\[
E_{12,1} : y^2 = x^3 - 3(t^2 + 1)(4t^2 + 2t + 1)p(t)x - 2(t^2 + 1)^2(4t^2 + 2t + 1)q(t)
\]
\[
E'_{12,1} : y^2 = x^3 - 3(t^2 + 1)(4t^2 + 2t + 1)p'(t)x + 2(t^2 + 1)^2(4t^2 + 2t + 1)q'(t)
\]
and
\[
p(t) = 36t^{12} + 234t^{11} + 693t^{10} + 1530t^9 + 2808t^8 + 4128t^7 + 4964t^6 + 4792t^5 + 3652t^4 + 2000t^3 + 736t^2 + 160t + 16,
\]
\[
q(t) = 432t^{18} + 4320t^{17} + 20196t^{16} + 63720t^{15} + 159111t^{14} + 330453t^{13} + 581103t^{12} + 875862t^{11}
\]
\[+ 1137762t^{10} + 1270440t^9 + 1208628t^8 + 960528t^7 + 622592t^6 + 320528t^5 + 127472t^4 + 37728t^3 + 7840t^2 + 1024t + 64,
\]
\[
p'(t) = 55396t^{12} - 97238t^{11} + 230581t^{10} - 206878t^9 + 177280t^8 - 86384t^7 + 2612t^6 - 6600t^5 + 900t^4 - 1008t^3 + 288t^2 + 288t + 144,
\]
\[
q'(t) = 2607612t^{18} - 62137376t^{17} + 165178492t^{16} - 207914808t^{15} + 236336753t^{14} - 163049017t^{13}
\]
\[+ 71325401t^{12} - 36145662t^{11} + 7345854t^{10} - 7544088t^9 + 2972844t^8 + 1350576t^7 + 531072t^6
\]
\[+ 1378085t^5 - 17712t^4 - 4320t^3 + 14688t^2 + 6912t + 1728.
\]

**Example 6.4** (A family of $(12,5)$-Congruences). Our model for the surface $Z(12,5)$ contains the genus 1 curve given by the vanishing of $v^3 + 3u^2 - (v^2 + 10)u - 3u^2 + 6$. This curve is birational over $\mathbb{Q}$ to the elliptic curve $C/\mathbb{Q}$ given by the Weierstrass equation
\[
C : y^2 = \xi^3 - \xi^2 - 16\xi + 16.
\]
The elliptic curve $C$ has LMFDB label $240.a.33$ and rank 1.

Using the moduli interpretation for $Z(12,5)$ it is possible to give an explicit pair of $(12,5)$-congruent elliptic curves over $\mathbb{Q}(C)$ in terms of $\xi$ and $\eta$. The Weierstrass equations are too complicated to reproduce here, but we include them in the electronic data $[17]$.

**Example 6.5** (A family of $(12,7)$-Congruences). Our model for the surface $Z(12,7)$ contains the genus 0 curve given by the vanishing of $u^2 + 3u - 2v^2 + 2$. By parametrising this curve we obtain a pair of $(12,7)$-congruent elliptic curves $E_{12,7}/\mathbb{Q}(t)$ and $E'_{12,7}/\mathbb{Q}(t)$ where
\[
E_{12,7} : y^2 = x^3 - 3(t^2 + 3)(t^4 - 3t^2 + 9)p(t)x - 2(t^2 + 3)(t^4 - 3t^2 + 9)q(t)
\]
\[+ t^2(t^4 + 3)(t^4 + 27)q'(t)x
\]
\[
E'_{12,7} : y^2 = x^3 - 3(t^2 + 3)(t^4 - 3t^2 + 9)(t^4 + 3)(t^4 + 27)p'(t)x
\]
\[+ 2(t^2 + 3)(t^4 - 3t^2 + 9)(t^4 + 3)(t^4 + 27)q'(t)
\]
and
\[
p(t) = t^{18} - 18t^{16} + 135t^{14} - 729t^{12} + 2889t^{10} - 7533t^8 + 15093t^6 - 15795t^4 + 53946t^2 + 2187,
\]
\[
q(t) = t^{26} - 27t^{24} + 309t^{22} - 2133t^{20} + 10341t^{18} - 35559t^{16} + 85158t^{14} - 109350t^{12} - 141345t^{10}
\]
\[+ 1337715t^8 - 3133971t^6 + 4183731t^4 + 3483891t^2 - 59049,
\]
\[
p'(t) = t^{18} + 222t^{16} + 585t^{14} + 5031t^{12} - 22599t^{10} + 78003t^8 - 177147t^6 + 295245t^4 - 354294t^2 + 177147,
\]
\[
q'(t) = t^{26} - 531t^{24} - 5739t^{22} + 38691t^{20} - 148635t^{18} + 141345t^{16} + 984150t^{14} - 6897798t^{12} + 25922511t^{10}
\]
\[+ 67847301t^8 + 129591517t^6 - 164215269t^4 + 129140163t^2 - 43046721.
\]

**Example 6.6** (A family of $(12,11)$-Congruences). Our model for the surface $Z(12,11)$ contains a pair of genus 0 curves given by the vanishing of $(9v^4 + 30v^2 + 5)u - 45v^4 - 6v^2 + 7$. By parametrising one of these
curves we obtain a pair of $(12, 11)$-congruent elliptic curves $E_{12,11}/\mathbb{Q}(t)$ and $E'_{12,11}/\mathbb{Q}(t)$ where

$$E_{12,11} : y^2 = x^3 - 3\left(\frac{25t^6 + 63t^4 + 27t^2 - 27}(t^4 + 18t^2 - 27)(t^4 + 6t^2 - 3)\right)x$$

$$- 2\left(\frac{25t^6 + 63t^4 + 27t^2 - 27}(5t^8 - 24t^6 - 78t^4 + 81)}{(t^4 + 18t^2 - 27)(t^4 + 6t^2 - 3)}\right)$$

and

$$E'_{12,11} : y^2 = x^3 - 3(t^4 - 18t^2 - 27)(t^4 + 6t^2 - 3)p'(t)x - 2\left(\frac{(t^4 - 18t^2 - 27)(t^4 + 6t^2 - 3)^2q'(t)}{(25t^6 + 63t^4 + 27t^2 - 27)}\right)$$

and

$$p'(t) = 25t^{20} + 18t^{18} - 1971t^{16} - 16200t^{10} - 500526t^8 - 332424t^6 - 13851t^4$$

$$+ 1458t^2 + 6561,$$

$$q'(t) = 3125t^{32} + 30000t^{30} + 94800t^{28} + 878688t^{26} + 25070580t^{24} + 173317968t^{22} + 693690912t^{20}$$

$$+ 1821351744t^{18} + 3069524646t^{16} + 3140007120t^{14} + 1733188752t^{12} + 288404064t^{10} - 233440380t^8$$

$$- 163447632t^6 + 7558272t^4 - 1594323.$$

We now complete the proof of Theorem 1.4.

Proof of Theorem 1.4 Consider the pairs of elliptic curves, $E_{12,r}/\mathbb{Q}$ and $E'_{12,r}/\mathbb{Q}$ given by specialising the pairs in Examples 6.3, 6.5 and 6.6 at $t = 2$ and the pair in Example 6.4 at the point $(\xi, \eta) = (0, 4)$. The hypotheses of condition (i) in Lemma 6.2 are satisfied since for each $r$ the curve $E_{12,r}$ is alone in its $\mathbb{Q}$-isogeny class. The first claim then follows from Lemma 6.2(i).

Note that if the mod $N$ Galois representation attached to an elliptic curve $E/\mathbb{Q}$ is not surjective then there exists a maximal subgroup $H \subset GL_2(\mathbb{Z}/N\mathbb{Z})$ such that $\rho_{E,N}(G_\mathbb{Q})$ is contained in a subgroup conjugate to $H$. In particular if $p$ is a prime number not dividing $N$ or the denominator of $j(E)$ then the reduction of $j(E)$ modulo $p$ is the $j$-invariant of an $F_p'$-rational point on $X(H)$.

Consider using code of Rouse, Sutherland, and Zureick-Brown [32] that for each $r$ and each maximal subgroup $H \subset GL_2(\mathbb{Z}/12\mathbb{Z})$ there exists a prime $p$ as above such that $j(E_{12,r})$ is not the $j$-invariant of an $F_p'$-rational point on $X(H)$ (specifically we use the intrinsic $GL_2$InvTest in [33] g12groups.m]). The claim follows from Lemma 6.2(ii). \qed

6.3. Further points and curves on $Z(12, r)$. Since the surfaces $Z(12, r)$ are of general type for $r \neq 1$ we would expect by the Bombieri–Lang conjecture that they contain at most finitely many curves of genus 0 or 1. In Tables 1–4 we record examples of curves of genus 0 or 1 on $Z(12, r)$ where $r \neq 1$ which do not map to a Hecke correspondence on $Z(1)$ and do not lie above the loci where $j = 0, 1728, \infty$ or $j' = 0, 1728, \infty$.

In Tables 1–4 an irreducible curve $C \subset Z(12, r)$ is recorded by its image $C^+$ under the map $Z(12, r) \to W(12, r)$. The column “genus” records the genus of $C$. If $C$ is not geometrically irreducible we write $g^*$ where $g$ is the genus of a geometrically irreducible component. The column “has $\mathbb{Q}$-point” records whether a smooth projective curve birational over $\mathbb{Q}$ to $C$ has a rational point.

Remark 6.7. It is natural to ask for which pairs $(N, r)$ there exist pairs of non-isogenous $(N, r)$-congruent elliptic curves $E/\mathbb{Q}(t)$ and $E'/\mathbb{Q}(t)$?

In view of this question it would be interesting to determine whether or not there exists an example of a genus 0 curve (which is birational over $\mathbb{Q}$ to $\mathbb{P}^1$) on $Z(12, 5)$ which does not lie above $j = \infty, j' = \infty$, or a Hecke correspondence on $Z(1)$.

Remark 6.8. It is possible to find examples of curves of genus 0 and 1 on $Z(12, r)$ which do not arise as the image of a map $Y_0(m) \to Z(12, r)$ as described in Section 6.1 but which nevertheless map to the graph of a Hecke correspondence on $Z(1)$.

Examples are furnished by the genus 0 curve $u^2 + 2 = 0$ on $Z(12, 1)$ and the genus 1 curve $uv^2 - v^2 - 2 = 0$ on $Z(12, 11)$. Points on these curves give rise to pairs of 12-congruent elliptic curves which are 7 and 5-isogenous respectively.

We do not attempt to classify all such examples.
When $r \neq 1$ the surfaces $Z(12, r)$ are of general type [19] so we expect by the Bombieri–Lang conjecture that there are at most finitely many rational points on $Z(12, r)$ which do not lie on a known curve of genus 0 or 1. In total we were able to find

- 248 points on $Z(12, 5)$ which correspond to 61 pairs of $(12, 5)$-congruent elliptic curves,
- 232 points on $Z(12, 7)$ which correspond to 58 pairs of $(12, 7)$-congruent elliptic curves, and
• 8 points on \( Z(12, 11) \) which correspond to 2 pairs of \((12, 11)\)-congruent elliptic curves. These points are recorded (together with the corresponding congruent elliptic curves) in the electronic data attached to this paper \[17\].

6.4. Examples of 12-congruent elliptic curves with small conductor. In Table \[10\] we give examples of non-isogenous \((12, r)\)-congruent elliptic curves which have small conductor. For each \( r \neq 1 \) we list all examples which we found (up to simultaneous quadratic twist) with conductor \( \leq 10^{10} \). These examples were constructed by searching for rational points on \( Z(12, r) \). When \( r = 1 \) we were able to find too many examples to record here, the 18 examples we found where both \( E \) and \( E' \) are contained in the LMFDB are recorded in the electronic data \[17\].

We do not include examples where \( E \) and \( E' \) are quadratic twists since many such examples may be constructed for \( r = 7, 11 \) by searching for points on the modular curves in \[16, \text{Lemmas 6.2 and 6.3}\].

The pair of \((12, 5)\)-congruent elliptic curves \[60450.cx2\] and \[60450.cw2\] appearing in Table \[10\] are notable since they give rise to 8 points on \( Z(12, 5) \). This corresponds to the fact that \[60450.cx2\] admits a non-trivial \( G_{\mathbb{Q}} \)-equivariant automorphism of its 12-torsion subgroup with power 1.

\[
\begin{array}{cccccc}
 r & E & E' & r & E & E' \\
 7 & 735.d2 & 24255.bh1 & 5 & 16039350* & 176432850* \\
 7 & 11830.x2 & 11830.ml1 & 7 & 25860114* & 336181482* \\
 5 & 60450.cx2 & 60450.cw2 & 7 & 28594930* & 2030240030* \\
 5 & 76614.ol1 & 76614.q1 & 7 & 29894410* & 29894410* \\
 5 & 92510.w1 & 92510.h1 & 5 & 39160576* & 39160576* \\
 5 & 769515* & 45401385* & 7 & 123160716* & 578853652* \\
 7 & 838240* & 838240* & 7 & 124010865* & 124010865* \\
 5 & 1991985* & 1991985* & 7 & 159365310* & 159365310* \\
 5 & 4353790* & 4353790* & 11 & 388152270* & 388152270* \\
 11 & 4976690* & 4976690* & 5 & 1885556560* & 1885556560* \\
 5 & 5144914* & 5144914* & 5 & 2016538368* & 2016538368* \\
 5 & 5355525* & 91043925* & 5 & 2992233426* & 2992233426* \\
 7 & 10691890* & 10691890* & 7 & 8900609640* & 8900609640* \\
 5 & 13286570* & 13286570* & \\
\end{array}
\]

Table 10. Known examples of pairs of geometrically non-isogenous \((12, r)\)-congruent elliptic curves \( E/\mathbb{Q} \) and \( E'/\mathbb{Q} \) (up to simultaneous quadratic twist) of conductors \( \leq 10^{10} \) where \( r \neq 1 \). We write \( N^* \) for an elliptic curve of conductor \( N \) which does not appear in the LMFDB \[27\] (i.e., of conductor \( N \geq 500000 \)).

References

[1] Ane S. I. Anema, Jaap Top, and Anne Tuijp, Hesse pencils and 3-torsion structures, SIGMA Symmetry Integrability Geom. Methods Appl. 14 (2018), Paper No. 102, 13. MR 3856778
[2] Nicolas Billerey, On some remarkable congruences between two elliptic curves, arXiv e-prints (2016), arXiv:1605.09205.
[3] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen, Genus-2 curves and Jacobians with a given number of points, LMS J. Comput. Math. 18 (2015), no. 1, 170–197. MR 3349314
[4] Nils Bruin and Kevin Doerksen, The arithmetic of genus two curves with \((4, 4)\)-split Jacobians, Canad. J. Math. 63 (2011), no. 5, 992–1024. MR 2866066
[5] Zexiang Chen, Congruences of elliptic curves, Ph.D. thesis, University of Cambridge, 1 2016, http://zc231.user.srcf.net/Maths/PhDThesis.pdf
[6] Zexiang Chen, Families of elliptic curves with the same mod 8 representations, Math. Proc. Cambridge Philos. Soc. 165 (2018), no. 1, 137–162. MR 3811549
[40] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[41] The Stacks project authors, *The stacks project*, https://stacks.math.columbia.edu, 2022.

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

Email address: sam.frengley@gmail.com