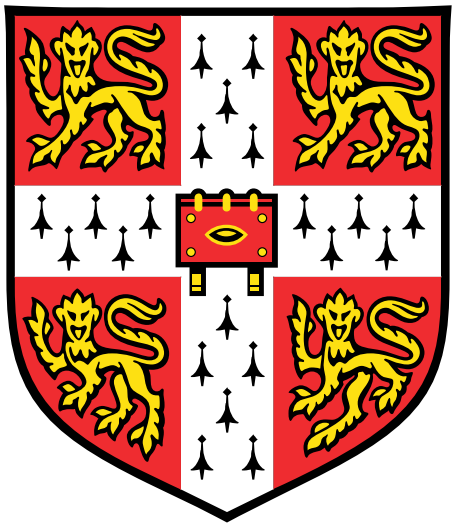
Explicit moduli spaces for curves of genus 1 and 2



Samuel Todd Frengley

Department of Pure Mathematics and Mathematical Statistics
University of Cambridge

This thesis is submitted for the degree of
Doctor of Philosophy

Fitzwilliam College

December 2023

Declaration

This thesis is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the preface and specified in the text. It is not substantially the same as any work that has already been submitted, or, is being concurrently submitted, for any degree, diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the preface and specified in the text. It does not exceed the prescribed word limit for the relevant Degree Committee.

The exposition in Section 2.5.1 (in particular Example 2.5.2) is based on joint work with Alex Cowan and Kimball Martin, and the example in Section 6.5.2 was provided to me by Timo Keller.

Samuel Todd Frengley
December 2023

Abstract

In this thesis we study pairs of N-congruent elliptic curves. That is, we study pairs of elliptic curves whose N-torsion subgroups are isomorphic as Galois modules. In particular, we study the moduli surfaces $Z_{N,r}$ which parametrise N-congruences of elliptic curves which raise the Weil pairing to a power of r.

We first study the birational geometry of the surfaces $Z_{N,r}^{\mathrm{sym}}$ which arise as quotients of the surfaces $Z_{N,r}$ by the involution swapping the roles of the N-congruent elliptic curves. Building on previous work of Kani–Schanz and Hermann we compute the geometric genus of $Z_{N,r}^{\mathrm{sym}}$ and place them within the Enriques–Kodaira classification in many cases. As a corollary we deduce that the Humbert surface of discriminant N^2 is rational if and only if $N \leq 16$, or if $N = 18$, 20, or 24.

We then study N-congruences between quadratic twists of elliptic curves. If N has exactly two distinct prime factors we show that these are parametrised by double covers of certain modular curves. In many, but not all, cases the modular curves in question correspond to the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. By computing explicit models for these double covers we find all pairs, (N, r), such that there exist infinitely many j-invariants of elliptic curves $E/\mathbb{Q}$ which are N-congruent with power r to a quadratic twist of E. We also find an example of a 48-congruence over $\mathbb{Q}$. We make a conjecture classifying nontrivial (N, r)-congruences between quadratic twists of elliptic curves over $\mathbb{Q}$. We give a more detailed analysis of the level 15 case and use elliptic Chabauty to determine the rational points on a modular curve of genus 2 and Jacobian of rank 2 which arises as a double cover of the modular curve $X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+)$. As a consequence we obtain a new proof of the class number 1 problem.

We construct infinite families of pairs of (geometrically non-isogenous) 12 and 14-congruent elliptic curves defined over $\mathbb{Q}$. We also find two pairs of 15-congruent elliptic curves over $\mathbb{Q}$. Our approach is to compute explicit birational models for the moduli surfaces $Z_{N,r}$ for each $N = 12$, 14 and 15. 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.

Finally, we study an application of congruences to visualising elements of the Tate–Shafarevich group of an abelian variety. In particular, we construct a number of genus 2 Jacobians $J/\mathbb{Q}$ with real multiplication by $\mathbb{Z}[\sqrt{2}]$ and whose Tate–Shafarevich groups contain an element of order 7. Our approach is to find elliptic curves whose 7-torsion subgroups are isomorphic as Galois modules to the $(3 \pm \sqrt{2})$-torsion subgroups of $J/\mathbb{Q}$.

Acknowledgements

This thesis would not have been completed, or even started, without the help of many people. Firstly, it is my great pleasure to thank my supervisor Tom Fisher for all the suggestions, comments, and ideas which he has contributed to this work. Thank you, Tom, for being so generous with your time, and for tolerating our many over-run meetings (especially those conducted during lock-downs when I had no one else to pester).

I am thankful to Ernst Kani for pointing out to me the work of Hermann which directly led to Chapter 3, and to Timo Keller for allowing me to use the example in Section 6.5.2. I am also very grateful to Jef Laga for comments, discussions, and feedback which greatly improved this thesis. I also thank Sven Cats, Craig Costello, Alex Cowan, Patrick Kennedy-Hunt, Kimball Martin, Oana Padurariu, Noah Porcelli, Dhruv Ranganathan, Tony Scholl, Alice Silverberg, Jack Thorne, Dmitri Whitmore, Hanneke Wiersema, and Rong Zhou for helpful conversations.

My PhD was been funded by the Woolf Fisher and Cambridge trusts. It has been a quite extraordinary privilege to be Woolf Fisher scholar, and it is an experience I will cherish forever. This thesis would not exist without their support.

On a more personal note I'd like to thank everyone in Cambridge who has made my time here so memorable. In particular I thank my friends in pav E for the many laughs, coffee breaks, and pub evenings which we shared.

I am extremely grateful for the people I have around me, especially my parents, my family, and my friends (those in New Zealand, the UK, and my amazing homies spread around the world). Thank you all for your love and support.

Finally, I owe a world of thanks to Maria Corte-Real Santos, for sharify and so much more.

Table of contents

1 Introduction **1**

1.1 Open questions and future work . . . 9

1.2 Outline . . . 10

2 Background **13**

2.1 Congruences of elliptic curves . . . 13

2.2 Modular curves . . . 14

2.2.1 Invariant theory for $X(N)$ . . . 15

2.2.2 The modular curve $X(H)$ with H-level structure . . . 16

2.2.3 The modular curves $X_0(N)$ and $X_0^+(N)$ . . . 17

2.2.4 The modular curves $X_1(N)$ and $X_\mu(N)$ . . . 18

2.2.5 The modular curves attached to Cartan subgroups . . . 18

2.2.6 Fibre products of modular curves . . . 19

2.2.7 The modular curves X_g and X_g^+ . . . 19

2.2.8 Generalised elliptic curves . . . 22

2.2.9 The yoga of twisting and $X_M(N)$ . . . 24

2.3 Hilbert modular surfaces . . . 24

2.3.1 Quadratic orders . . . 25

2.3.2 The Hilbert modular group for quadratic orders . . . 26

2.3.3 Compactifications . . . 27

2.3.4 Models over $\mathbb{Q}$ and moduli interpretations . . . 29

2.3.5 Hecke correspondences . . . 31

2.3.6 Symmetric Hilbert modular surfaces . . . 32

2.4 On algebraic surfaces . . . 34

2.4.1 On the Enriques–Kodaira classification . . . 35

2.4.2 Resolution of cyclic quotient singularities . . . 36

2.5 Minimisation over polynomial rings . . . 37

2.5.1 Arithmetic blowups . . . 37

2.5.2 "Birational minimisation" and Cremona transformations . . . 40

3 On the geometry of the symmetric Hilbert modular surface $Z_{N,r}^{\mathrm{sym}}$ **43**

3.1 An outline of the proof of Theorems 1.0.4 and 1.0.6 . . . 43

3.1.1 A simple example . . . 43

3.1.2 An outline in the general case . . . 44

3.2 The surface $Z_{N,r}$ . . . 44

3.2.1 The minimal resolution of singularities . . . 45

3.2.2 Intersections of the modular curves $\widetilde{F}_{m,\lambda}$ on $\widetilde{Z}_{N,r}$ . . . 46

3.3 The fixed points of τ . . . 49

3.3.1 Modular curves and the one dimensional fixed locus . . . 50

3.3.2 The fixed points above 0 and 1728 . . . 55

3.3.3 The action of τ on the cusps . . . 61

3.4 The genera of the modular curves X_g^+ . . . 67
3.5 Intersection numbers on the surface $\widetilde{Z}_{N,r}$ . . . 69
3.6 A non-singular model for $Z_{N,r}^{\mathrm{sym}}$ . . . 71
3.6.1 The numerical invariants . . . 72
3.6.2 Bounds on $p_g(W_{N,r})$ and K_W^2 and the proof of Theorem 1.0.4 . . . 75
3.7 Modular curves on $W_{N,r}$ . . . 76
3.7.1 Rational modular curves on $W_{N,r}$ . . . 77
3.7.2 The lifted $X_0(2)$ when $N \equiv 2 \pmod 4$ . . . 77
3.7.3 The exceptional $(F_g^+)^*$ when $N \equiv 3 \pmod 9$ . . . 78
3.8 The Kodaira dimension and Theorem 1.0.6 . . . 79
3.8.1 The rational cases . . . 79
3.8.2 The cases of general type . . . 82

4 Congruences between quadratic twists of elliptic curves 85
4.1 Quadratic twist-type p^l-congruences of elliptic curves . . . 86
4.1.1 Quadratic twist-type p^l-congruences . . . 86
4.1.2 Quadratic twist-type 2^k-congruences . . . 87
4.2 Trivial quadratic twist-type congruences and CM . . . 89
4.3 Double covers of modular curves and composite level quadratic twist-type congruences 94
4.4 Computing modular curves of genus 0 or 1 . . . 96
4.5 Evidence for Conjecture 1.0.17 . . . 102
4.5.1 Computing modular curves of genus ≤ 4 . . . 104
4.5.2 A review of the Mordell-Weil sieve . . . 109
4.6 2-cover descent on genus 2 curves admitting a Richelot isogeny . . . 110
4.6.1 The rational points on $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ . . . 111

5 Families of (N, r)-congruent elliptic curves 115
5.1 Symmetric equations for families of N-congruent elliptic curves . . . 115
5.1.1 Computing quotients of $X(N) \times X(N)$ . . . 116
5.1.2 Symmetric bi-invariants . . . 117
5.1.3 Symmetric conditions for 2, 3, and 4-congruences . . . 121
5.1.4 Parametrisations of $W_{N,r}$ for $N \leq 5$ and $N = 7$ . . . 126
5.2 Constructing $Z_{N,r}$ via fibre products . . . 128
5.3 Computing the surfaces $Z_{N,r}$ . . . 129
5.3.1 Computing models for $Z_{12,1}$ and $Z_{12,7}$ . . . 129
5.3.2 Computing models for $Z_{12,5}$ and $Z_{12,11}$ . . . 132
5.3.3 Computing models for $Z_{14,1}$ and $Z_{14,3}$ . . . 134
5.3.4 Computing models for $Z_{15,2}$ and $Z_{15,11}$ . . . 136
5.4 Modular curves on $W_{N,r}$ . . . 140
5.4.1 The Hecke correspondences $F_{m,\lambda}$ . . . 140
5.4.2 The modular curves F_g^+ . . . 143
5.5 Families of congruences and Theorem 1.0.10 . . . 143
5.5.1 Families of 12-congruences . . . 143
5.5.2 Families of 14-congruences . . . 145
5.5.3 Proof of Theorem 1.0.10 . . . 145
5.6 The proof of Theorem 1.0.12 . . . 147
5.7 Further examples of N-congruences . . . 147

5.7.1 Examples of N-congruent elliptic curves with small conductor 149

6 Elements in the Tate–Shafarevich group of genus 2 Jacobians **153**
6.1 Visibility 155
6.2 The twisting principle for $X(7)$ 155
6.3 An algorithm to compute an approximation to $X^r_{J[3\pm\sqrt{2}]}(7)$ 156
6.3.1 Hilbert's Theorem 90 is effective 157
6.3.2 The main algorithm 157
6.4 Proving $([3 \pm \sqrt{2}], [7])$-congruences 159
6.5 Examples 160
6.5.1 The proof of Theorem 1.0.18 160
6.5.2 A (non)-example worthy of further study 160

Appendices **163**

A Models for $Z_{N,r}$ **163**
A.1 Equations defining $Z_{N,r}$ 163
A.2 j-invariant maps for $W_{N,r}$ 165

B Tables **167**

Bibliography **175**

Chapter 1

Introduction

Let K be a field of characteristic zero and let N be a positive integer. We write $G_K := \mathrm{Gal}(\overline{K}/K)$ for the absolute Galois group of K. Let $E[N]$ denote the N-torsion subgroup of $E(\overline{K})$. We say that a pair of elliptic curves E/K and E'/K are *N-congruent* if there exists an isomorphism $\phi\colon E[N] \to E'[N]$ of G_K-modules. In this case the isomorphism ϕ is said to be an *N-congruence*.

If $\phi\colon E[N] \to E'[N]$ 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

$$e_{E,N}(P,Q)^r = e_{E',N}(\phi(P), \phi(Q))$$

where $e_{E,N}$ and $e_{E',N}$ denote the Weil pairings on E and E' respectively. The congruence ϕ is then said to be an *(N,r)-congruence* or an *N-congruence with power r*. For each integer m coprime to N, composing ϕ with multiplication by m changes the power of ϕ by a factor of m^2, so we consider the power of ϕ only up to multiplication by a square in $(\mathbb{Z}/N\mathbb{Z})^\times$.

A simple example of N-congruent elliptic curves is provided by isogenies. If $\psi\colon E \to E'$ is an m-isogeny and $(N,m) = 1$, then the restriction of ψ to $E[N]$ is an (N,m)-congruence. Indeed, it is a conjecture of Frey and Mazur that for sufficiently large integers N, all N-congruent elliptic curves are in fact isogenous.

Conjecture 1.0.1 (Frey–Mazur)**.** *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 $\mathbb{Q}$.*

The study of congruences has a long history, which can be traced back to Legendre, Jacobi, and Abel [Leg28, Jac29, Abe29] in the guise of reducing hyperelliptic integrals to elliptic integrals (see [Kra03, Chapter XI] for an overview of the classical literature). This connection was revisited by Kuhn, Frey, and Kani [Kuh88, FK91, Fre95]. Let E/K be an elliptic curve and C/K be a genus 2 curve admitting an *optimal* morphism $\psi\colon C \to E$ of degree N (i.e., a morphism which does not factor through an isogeny), then there exists an elliptic curve E'/K and an $(N,-1)$-congruence $\phi\colon E[N] \to E'[N]$. Conversely, if $\phi\colon E[N] \to E'[N]$ is an $(N,-1)$-congruence, then (if E and E' are not isogenous) there exists a genus 2 curve C/K and an optimal morphism $\psi\colon C \to E$. In particular, Conjecture 1.0.1 predicts that for sufficiently large integers N, there exist no genus 2 curves over $\mathbb{Q}$ admitting an optimal morphism of degree N to an elliptic curve.

Congruences also appear naturally in the study of Diophantine problems. Frey [Fre97] proved that the *asymptotic Fermat conjecture* follows from Conjecture 1.0.1. Poonen, Schaefer, and Stoll [PSS07] resolved the integer solutions to the generalised Fermat equation $x^2 + y^3 = z^7$ by determining every elliptic curve 7-congruent to one of a finite number of given elliptic curves.

In order to refine Conjecture 1.0.1 we consider the following questions.

Question 1.0.2. *For which pairs (N,r) do there exist examples of pairs of non-isogenous (N,r)-congruent elliptic curves over $\mathbb{Q}$? For which (N,r) do there exist infinitely many pairs of (j-invariants of) non-isogenous (N,r)-congruent elliptic curves over $\mathbb{Q}$?*

To study Question 1.0.2 we consider the (compactified) coarse moduli space $Z_{N,r}$ whose points parametrise triples (E, E', ϕ) where $\phi\colon E[N] \to E'[N]$ is an (N, r)-congruence (see Section 2.3.4 for a precise definition). We call $Z_{N,r}$ a *Hilbert modular surface of discriminant* N^2. The surface $Z_{N,r}$ admits a natural involution swapping the roles of the elliptic curves. More precisely, we define $\tau\colon Z_{N,r} \to Z_{N,r}$ to be given by $(E, E', \phi) \mapsto (E, E', r\phi^{-1})$ and we write $Z_{N,r}^{\mathrm{sym}}$ for the quotient of $Z_{N,r}$ by τ.

The birational geometry of Hilbert modular surfaces (which may be defined more generally for any positive discriminant $D \equiv 0, 1 \pmod 4$, see Section 2.3) has been well studied. In the case of fundamental discriminants, work of Hirzebruch, Van den Ven, Van der Geer, and Zagier [Hir71, HVdV74, HZ77, vdG88] places each surface within the Enriques–Kodaira classification, see [vdG88, Theorem VII.3.3]. It is an active area of research to address these questions when level structure is also imposed (see e.g., [ABB$^+$23]).

In our case, the Hilbert modular surfaces $Z_{N,r}$ were placed in the Enriques–Kodaira classification by Kani–Schanz [KS98, Theorem 4] and Hermann[1] [Her91, Satz 2]. If $S/\mathbb{C}$ is a smooth algebraic surface, we write $p_g(S)$ and $\kappa(S)$ for the geometric genus and Kodaira dimension of S respectively. In what follows, we adopt the convention that the Kodaira dimension of a rational surface is equal to -1.

Theorem 1.0.3 ([KS98, Theorem 4])**.** *The minimal desingularisation $\widetilde{Z}_{N,r}$ of the surface $Z_{N,r}$ is:*

(i) *rational if $N \leq 5$, or $(N, r) = (6, 1)$, $(7, 1)$, or $(8, 1)$,*

(ii) *a (blown up) elliptic K3 surface if $(N, r) = (6, 5)$, $(7, 3)$, $(8, 3)$, $(8, 5)$, $(9, 1)$, or $(12, 1)$,*

(iii) *a (blown up) elliptic surface of Kodaira dimension 1 if $(N, r) = (8, 7)$, $(9, 2)$, $(10, 1)$, $(10, 3)$, or $(11, 1)$, and*

(iv) *a surface of general type otherwise, i.e., if $N \geq 13$ or $(N, r) = (11, 2)$, $(12, 5)$, $(12, 7)$, or $(12, 11)$.*

Moreover, for every pair (N, r), we have $\kappa(\widetilde{Z}_{N,r}) = \min(p_g(Z_{N,r}) - 1, 2)$. That is, the Kodaira dimension of $\widetilde{Z}_{N,r}$ is entirely determined by its geometric genus.

For (fundamental) discriminants, the study of symmetric Hilbert modular surfaces (which we describe in Section 2.3.6 for any positive discriminant $D \equiv 0, 1 \pmod 4$) was initiated by Hirzebruch [Hir73b, Section 5.8]. This work was continued by Hirzebruch, Zagier, Hausmann, and Bassendowski [HZ76, Hir78, Hau79, Hau82, Bas85] culminating in a classification theorem for fundamental discriminants congruent to 1 modulo 4, which may be found in [Bas85, Satz 4.1]. Bassendowski observed that the Kodaira dimensions of these symmetric Hilbert modular surfaces are entirely determined by their geometric genera.

When p is an odd prime, Hermann [Her92] placed the surfaces $Z_{p,r}^{\mathrm{sym}}$ in the Enriques–Kodaira classification. It follows from Hermann's result that the Kodaira dimension of the surface $Z_{p,r}^{\mathrm{sym}}$ is again determined entirely by its geometric genus. In Chapter 3 we extend Hermann's results to the case when N is composite. More precisely in Section 3.6 we construct a smooth projective algebraic surface $W_{N,r}$ which is birational over $\mathbb{C}$ to $Z_{N,r}^{\mathrm{sym}}$, and we prove the following theorem classifying their geometric genera.

[1] As pointed out in [KS98] Hermann's list of elliptic surfaces is incomplete, missing the case when $(N, r) = (10, 3)$. This is remedied in [KS98].

Theorem 1.0.4. *We have:*

(i) $p_g(W_{N,r}) = 0$ *when* $N \leq 14$ *and when* $(N,r) = (15,1)$, $(15,2)$, $(15,11)$, $(16,1)$, $(16,3)$, $(16,7)$, $(18,5)$, $(20,11)$, *and* $(24,23)$,

(ii) $p_g(W_{N,r}) = 1$ *when* $N = 17$, *and when* $(N,r) = (16,5)$, $(18,1)$, $(20,1)$, $(20,3)$, *and* $(21,2)$,

(iii) $p_g(W_{N,r}) = 2$ *when* $N = 19$ *and when* $(N,r) = (15,7)$, $(21,5)$, $(22,1)$, *and* $(24,11)$, *and*

(iv) $p_g(W_{N,r}) \geq 3$ *otherwise, i.e., if* $N = 23$, $N \geq 25$, *or* $(N,r) = (20,13)$, $(21,1)$, $(21,10)$, $(22,3)$, $(24,1)$, $(24,5)$, $(24,7)$, $(24,13)$, $(24,17)$, *or* $(24,19)$.

We have the following natural conjecture, mimicking the known results for fundamental discriminants and the surfaces $Z_{N,r}$.

Conjecture 1.0.5. *For every pair* (N,r) *we have* $\kappa(W_{N,r}) = \min(p_g(W_{N,r}) - 1, 2)$. *Moreover,* $W_{N,r}$ *is rational whenever* $p_g(W_{N,r}) = 0$, *a (blown-up) elliptic K3 surface whenever* $p_g(W_{N,r}) = 1$, *a (blown-up) properly elliptic surface whenever* $p_g(W_{N,r}) = 2$, *and of general type otherwise.*

Conjecture 1.0.5 was proved by Hermann [Her92] when $N = p$ is a prime number. In this work we prove the following result towards Conjecture 1.0.5. A full proof of Conjecture 1.0.5 is the subject of ongoing work, however the cases when $N = 24$ and when $W_{N,r}$ is an elliptic fibration require careful analysis, which has yet to be completed.

Theorem 1.0.6. *The surface* $W_{N,r}$ *is:*

(i) *rational if and only if* $N \leq 14$ *or* $(N,r) = (15,1)$, $(15,2)$, $(15,11)$, $(16,1)$, $(16,3)$, $(16,7)$, $(18,5)$, $(20,11)$, *or* $(24,23)$,

(ii) *a (blown up) elliptic K3 surface if* $N = 17$,

(iii) *a (blown up) elliptic surface of Kodaira dimension* 1 *if* $N = 19$, *and*

(iv) *of general type if* $N = 23$, $N \geq 25$, *or* $(N,r) = (21,1)$, $(21,10)$, $(24,13)$, *or* $(24,19)$.

Remark 1.0.7. Several cases of Theorem 1.0.6 have previously been proved by explicitly computing the surfaces $Z_{N,r}$ for small integers N. In particular, Kumar [Kum15] showed that $Z^{\mathrm{sym}}_{N,-1}$ is a rational surface for each $N \leq 11$, calculations of Fisher [Fis19, Fis21] verify Hermann's theorem for each r when $p = 13, 17$. Remarkably Fisher showed that the elliptic K3 surfaces $Z^{\mathrm{sym}}_{17,1}$ and $Z^{\mathrm{sym}}_{17,3}$ are in fact birational over $\mathbb{Q}$ [Fis21, Theorem 1.2].

In Theorem 1.0.9 we compute $Z^{\mathrm{sym}}_{N,r}$ where $N = 12, 14$ and when $(N,r) = (15,2)$ and $(15,11)$. In the file `N-congruences/ZNr-equations.m` in [Fre23b] we also give equations for $Z^{\mathrm{sym}}_{N,r}$ when $N = 18$, 20, and 24 for several r, though we do not prove them here (as we discuss in Section 1.1).

Let $\mathcal{M}_2$ denote the (coarse) moduli space of genus 2 curves. By [Kan94, Corollary 1.8] (see [Kan23, Theorem 8.3]) the symmetric Hilbert modular surface $Z^{\mathrm{sym}}_{N,-1}$ is birational to the *Humbert surface of discriminant* N^2, the surface $\mathcal{H}_{N^2} \subset \mathcal{M}_2$ parametrising genus 2 curves admitting an optimal morphism of degree N to an elliptic curve. As an immediate corollary of Theorem 1.0.6 we have the following result, which addresses a recent question of Kani [Kan21, Remark 3.5] (note that the missing case $N = 21$ in the corollary is predicted to be an elliptic surface of Kodaira dimension 1 by Conjecture 1.0.5).

Corollary 1.0.8. *The Humbert surface* $\mathcal{H}_{N^2} \subset \mathcal{M}_2$ *of discriminant* N^2 *is birational over* $\mathbb{C}$ *to a smooth projective surface which is:*

(i) *rational if* $N \leq 16$ *and if* $N = 18, 20, 24$,

(ii) *an elliptic K3 surface if* $N = 17$,

(iii) *an elliptic surface of Kodaira dimension* 1 *if* $N = 19$, *and*

(iv) *of general type if* $N \geq 22$ *and* $N \neq 24$.

By the classification of Kani–Schanz [KS98], the surface $Z_{N,r}$ is a surface of general type whenever $N \geq 11$ and $(N, r) \neq (11, 1), (12, 1)$ (the full classification is stated in Theorem 1.0.3). In this case (by the Bombieri–Lang conjecture) we expect that there are at most finitely many curves of geometric genus 0 or 1 on $Z_{N,r}$.

When $N = p$ is prime, Bakker and Tsimerman [BT16] prove the function field analogue of Conjecture 1.0.1. They prove that for any $g \geq 0$, there exists a constant $C_{0,g} > 0$ such that if $X \subset Z_{p,r}$ is a curve of genus g, then either X is a modular curve (i.e., points on X correspond to pairs of isogenous elliptic curves) or $p \leq C_{0,g}$. In particular, infinite families of (p, r)-congruences arising from specialisations of examples over a function field do not exist for sufficiently large p. Note that the Bombieri–Lang conjecture predicts that all but finitely many rational points on $Z_{p,r}$ should lie on curves of genus 0 or 1.

Conversely, 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 1.1). A pair of non-isogenous $(17, 3)$-congruent elliptic curves appearing in the LMFDB [LMFDB] has been found by Cremona (see [Fis14, Bil16, CF22]). Fisher [Fis21] also found a pair of non-isogenous $(17, 1)$-congruent elliptic curves over $\mathbb{Q}$, and has conjectured that these are the only such 17-congruences over $\mathbb{Q}$. Moreover, Fisher gave a refined form of Conjecture 1.0.1, conjecturing that there exist no pairs of non-isogenous, p-congruent, elliptic curves over $\mathbb{Q}$ for $p \geq 19$ (see [Fis21, Conjecture 1.1]). Cremona and Freitas [CF22, Theorem 1.3] have determined all pairs of non-trivially p-congruent elliptic curves with conductor less than 500 000. Specifically they showed that when $p > 17$ there exist no pairs of non-isogenous, p-congruent elliptic curves with conductor $< 500\,000$.

When N is composite, 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 1.1). In every case, we give an example of an (N, r)-congruence in Table B.4 (in fact, we give an example where the mod N Galois representation is surjective).

Following the approach of Cremona–Freitas [CF22, Section 3] it is not difficult to find examples of 12 and 14-congruent elliptic curves in the LMFDB [LMFDB]. The power of these congruences may be determined using the equations of Rubin, Silverberg, and Fisher [Fis12, RS95, RS01, Sil97, Fis14]. For example, the pairs of elliptic curves with LMFDB labels (`55.a1`, `1045.b1`), (`60450.cx2`, `60450.cw2`), and (`735.d2`, `24255.bh1`) are not geometrically isogenous and are $(12, 1)$, $(12, 5)$, and $(12, 7)$-congruent respectively. Similarly, the pairs of elliptic curves with LMFDB labels (`632.a1`, `36757.a1`) and (`40362.n1`, `40362.o2`) are not geometrically isogenous and are $(14, 1)$ and $(14, 3)$-congruent. Conversely, we were not able to find any such pairs of $(12, 11)$ or $(15, r)$-congruent elliptic curves with conductor less than 500 000.

The objective of Chapter 5 is to prove Theorem 1.0.10 which shows that there exist infinitely many pairs of geometrically non-isogenous (N, r)-congruent elliptic curves over $\mathbb{Q}$ for each $(N, r) = (12, 1)$, $(12, 5)$, $(12, 7)$, $(12, 11)$, and $(14, 1)$. We also give examples of $(14, 3)$, $(15, 2)$, and $(15, 11)$-congruent elliptic curves over $\mathbb{Q}$ (see Theorems 1.0.11 and 1.0.12).

Our approach to proving Theorems 1.0.10, 1.0.11, and 1.0.12 is to compute explicit models for the surfaces $Z_{N,r}$. We give explicit birational models (over $\mathbb{Q}$) for the moduli surfaces $Z_{N,r}$ for

(N,r)	References	(N,r)	References
$(2,1)$	[Fis12, Kum15, RS01]	$(8,7)$	[Che16, Che18, Fis20, Kum15]
$(3,1)$	[ATT18, Fis12, Kuw12, RS95]	$(9,1)$	[Fis15, Fis20]
$(3,2)$	[Fis12, BHLS15, Kum15, Kuw12]	$(9,2)$	[Fis15, Fis20, Kum15]
$(4,1)$	[Fis12, Sil97]	$(10,1)$	[Fis20, Kum15]
$(4,3)$	[BD11, Fis12, Kum15]	$(10,3)$	[Fis20]
$(5,1)$	[Fis12, Kum15, RS95]	$(11,1)$	[Fis14, Fis20, KR00]
$(5,2)$	[Fis12]	$(11,2)$	[Fis14, Kum15]
$(6,1)$	[Che16, Pap99, Rob99, RS99]	$(12,1)$	[Che16, Fis20, Fre22], Thm. 1.0.10
$(6,5)$	[Che16, Kum15]	$(12,5)$	[Fre22], Thm. 1.0.10
$(7,1)$	[Che16, Fis14, HK03]	$(12,7)$	[Che16, Fre22], Thm. 1.0.10
$(7,3)$	[Che16, Fis14, Fis20, PSS07, Kum15]	$(12,11)$	[Fre22], Thm. 1.0.10
$(8,1)$	[Che16, Che18]	$(13,1)$	[Fis19]
$(8,3)$	[Che16, Che18, Fis20]	$(13,2)$	[Fis19]
$(8,5)$	[Che16, Che18, Fis20]	$(14,1)$	Thm. 1.0.10

Table 1.1: Pairs (N,r) for which it is known that there are infinite families of geometrically non-isogenous (N,r)-congruent elliptic curves over $\mathbb{Q}$, together with authors who have computed a model for either of the moduli spaces $X_E^r(N)$ or $Z_{N,r}$ defined in Sections 2.2.9 and 2.3.4 respectively.

each r when $N = 12, 14$ and for $(N,r) = (15,2), (15,11)$. A key observation which makes these calculations practical and which follows the approach of Kumar [Kum15] and Fisher [Fis19, Fis21] (and Elkies–Kumar [EK14] in the case of Hilbert modular surfaces of fundamental discriminant), is to write $Z_{N,r}$ as a double cover of $Z_{N,r}^{\mathrm{sym}}$. The symmetric Hilbert modular surface $Z_{N,r}^{\mathrm{sym}}$ is less geometrically complicated than $Z_{N,r}$ (and, by Theorem 1.0.4, can be rational even when $Z_{N,r}$ is of general type).

Theorem 1.0.9. *For each $(N,r) = (12,1)$, $(12,5)$, $(12,7)$, $(12,11)$, $(14,1)$, $(14,3)$, $(15,2)$, and $(15,11)$ the surface $Z_{N,r}^{\mathrm{sym}}$ is birational over $\mathbb{Q}$ to $\mathbb{A}^2$. In each case, the surface $Z_{N,r}$ is birational over $\mathbb{Q}$ to the affine surface in $\mathbb{A}^3$ given by*

$$z^2 = P_{N,r}(u,v)$$

where the polynomials $P_{N,r}(u,v) \in \mathbb{Z}[u,v]$ are recorded in Appendix A. The involution τ is given on these models for $Z_{N,r}$ by $z \mapsto -z$.

The maps $Z_{N,r} \to Z_1 = X(1) \times X(1)$ which give the moduli interpretations for the surfaces $Z_{N,r}$ in Theorem 1.0.9 are too complicated to reproduce here but may be recovered from the computations in Section 5.3. We record them in the electronic data accompanying this thesis [Fre23b].

The surface $Z_{12,1}$ is an elliptic K3 surface and models were computed by Chen and Fisher (see [Che16, Chapter 7] and [Fis20]) using equations for the twist $X_E^1(12)$ of $X(12)$ which parametrises elliptic curves which are $(12,1)$-congruent to E (see Section 2.2.9). They, however, did not give equations for $Z_{12,1}^{\mathrm{sym}}$. Chen [Che16, Chapter 7.4] also computed equations for the twist $X_E^7(12)$.

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 $\mathbb{Q}$ [Che16, 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 $\mathbb{Q}(t)$ [Fis20, Corollary 1.3].

By finding points and curves on our models for the surfaces $Z_{N,r}$ we prove the following theorems in Sections 5.5 and 5.6.

Theorem 1.0.10. *For each $(N,r) \in \{(12,1),(12,5),(12,7),(12,11),(14,1)\}$ there are infinitely many pairs of j-invariants of (N,r)-congruent elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ which are not geo-*

metrically isogenous. Moreover, in each case there are infinite sub-families such that the mod N Galois representation attached to $E/\mathbb{Q}$ (and $E'/\mathbb{Q}$) is surjective.

Theorem 1.0.11. *There exist at least* 21 *pairs of (j-invariants of) geometrically non-isogenous $(14,3)$-congruent elliptic curves over $\mathbb{Q}$.*

Theorem 1.0.12. *Consider the pairs of elliptic curves $E_{(15,2)}$, $E'_{(15,2)}$ and $E_{(15,11)}$, $E'_{(15,11)}$ given by the Weierstrass equations*

$$\begin{aligned}
E_{(15,2)} &: y^2 = x^3 - 108244904599x - 13707533205528591,\\
E'_{(15,2)} &: y^2 = x^3 - 1993453644299x - 1083321408492185434,
\end{aligned}$$

$$\begin{aligned}
E_{(15,11)} &: y^2 + xy + y = x^3 - x^2 - 5978298027424617040871x\\
&\qquad - 17791581668504438650617886792043 8,\\
E'_{(15,11)} &: y^2 = x^3 - 213560743733198984194354071078281 1x\\
&\qquad + 37915783123298007085317147066745283477127543370806.
\end{aligned}$$

Then for each $r = 2, 11$ the elliptic curves $E_{(15,r)}$ and $E'_{(15,r)}$ are not geometrically isogenous and are $(15,r)$-congruent over $\mathbb{Q}$.

Both $E_{(15,2)}$ and $E'_{(15,2)}$ have conductor $2^3 \cdot 7 \cdot 13^2 \cdot 17 \cdot 41 \cdot 61$ and $E_{(15,11)}$ and $E'_{(15,11)}$ have conductor $3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 61 \cdot 199^2 \cdot 2341^2$.

Remark 1.0.13. If E/K and E'/K are (N,r)-congruent elliptic curves, then their simultaneous quadratic twists, E^d and E'^d, by an element $d \in K^\times$ are also (N,r)-congruent (see e.g., [FK22, Lemma 4.15]). The conditions on j-invariants in Theorems 1.0.10 and 1.0.11 are in order to exclude such "infinite families" of examples.

Relaxing the condition that E and E' are not geometrically isogenous (e.g., allowing E and E' to be non-trivial quadratic twists) yields many more examples of congruences. It was observed by Halberstadt [Hal98, Section 2] (cf. [CF22, Theorem 2.4]) that an elliptic curve such that the image of the associated mod p Galois representation is contained in the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, but not the Cartan subgroup itself, admits a p-congruence with a non-trivial quadratic twist. An elliptic curve is 2-congruent to every quadratic twist, hence such a congruence is automatically a $2p$-congruence. Based upon this observation Halberstadt [Hal98] found examples of non-trivial $10, 14$, and 22-congruences of elliptic curves over $\mathbb{Q}$ by using explicit models for the modular curves $X(\mathrm{ns}\, p^+)$ for $p = 5, 7, 11$.

Definition 1.0.14. We say that an (N,r)-congruence between elliptic curves E/K and E'/K is of *quadratic twist-type* if E is a non-trivial quadratic twist of E'. In this case we say that E (and E') *admits a quadratic twist-type (N,r)-congruence*. We say that a quadratic twist-type congruence is *non-trivial* if E and E' are not isogenous over K.

A trivial quadratic twist-type congruence may only occur when E has complex multiplication (CM) (see Lemma 4.2.1). Halberstadt's examples of $2p$-congruences can therefore be extended to infinite families since the modular curves $X(\mathrm{ns}\, p^+)$ for $p = 5, 7, 11$ have infinitely many non-exceptional points (a non-cuspidal point is said to be *exceptional* if it corresponds to an elliptic curve which does not have CM).

Cremona–Freitas [CF22, Theorem 2.4] proved that (under their condition "**(S)**", which is satisfied when $K = \mathbb{Q}$ and $p \geq 7$) quadratic twist-type p-congruences occur *if and only if* the image of

the corresponding mod p Galois representation is contained in the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, but not the Cartan subgroup itself.

By a different proof we extend this result to odd prime powers (see Proposition 4.1.4). Our result is that if p is an odd prime and $l \geq 1$ is an integer, then an elliptic curve E/K admits a quadratic twist-type p^l-congruence if and only if the image of the corresponding mod p^l Galois representation is contained in the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$, but not the Cartan subgroup itself. Note that we avoid condition "**(S)**".

Therefore, classifying quadratic twist-type p^l-congruences (hence $2p^l$-congruences) is equivalent to finding all (non-cuspidal) rational points on the modular curves $X(\mathrm{s}\,p^{l^+})$ and $X(\mathrm{ns}\,p^{l^+})$ which do not lift to points on $X(\mathrm{s}\,p^l)$ respectively $X(\mathrm{ns}\,p^l)$. The curves $X(\mathrm{s}\,p^{l^+})$ have no exceptional points for $p^l > 7$ (see [BPR13, Theorem 1.1] for $p > 7$ except $p = 13$, [BDM$^+$19] in the level 13 case, and [RSZ22] when $p^l = 9, 25, 49$). It is a well known open problem to determine the rational points on $X(\mathrm{ns}\,p^{l^+})$ when $p^l \geq 19$ (when $p^l = 13$ and 17 this has been resolved in [BDM$^+$19] and [BDM$^+$23] respectively).

We extend the results of Halberstadt and Cremona–Freitas to composite N, and in particular we prove:

Theorem 1.0.15. *There are infinitely many j-invariants of elliptic curves $E/\mathbb{Q}$ admitting non-trivial quadratic twist-type (N, r)-congruences if and only if $(N, r) \in \mathcal{S}$ where*

$$\mathcal{S} = \left\{ \begin{array}{l} (2,1),(3,1),(3,2),(4,1),(4,3),(5,1),(5,2),(6,1),(6,5),(7,1),(7,3), \\ (8,1),(8,3),(8,5),(8,7),(9,1),(10,1),(10,3),(11,1),(12,7),(12,11), \\ (14,1),(14,3),(16,3),(18,1),(20,3),(22,1),(24,19),(28,3),(28,11),(36,19) \end{array} \right\}$$

and the second entry is viewed as an element of $(\mathbb{Z}/N\mathbb{Z})^\times$ modulo squares.

In the spirit of Mazur's "Program B" (and other work on modular curves - see e.g., [RZ15a, SZ17, RSZ22]) it would be interesting to extend Theorem 1.0.15 to classify *all* non-trivial quadratic twist-type (N, r)-congruences (assuming the conjecture that the modular curves $X(\mathrm{ns}\,p^{l^+})$ have no exceptional points for $p^l \geq 19$, see e.g., [RSZ22, Conjecture 1.5]).

Towards this goal we exhibit the following examples of non-trivial quadratic twist-type congruences not arising from the families in Theorem 1.0.15.

Theorem 1.0.16. *Let $E_{(30,7)}$, $E_{(32,3)a}$, $E_{(32,3)b}$, and $E_{(48,19)}$ be the elliptic curves defined over $\mathbb{Q}$ by the Weierstrass equations*

$$\begin{aligned} E_{(30,7)} &: y^2 + xy = x^3 - x^2 - 273176601587417x - 1741818799948905109620, \\ E_{(32,3)a} &: y^2 + y = x^3 - 3014658660x + 150916472601529, \\ E_{(32,3)b} &: y^2 + y = x^3 - 26668521183591560x - 16763728762567544566631251, \\ E_{(48,19)} &: y^2 + y = x^3 + 468240736152891010x - 14837458662446487624731695 7. \end{aligned}$$

Then $E_{(30,7)}$ is $(30, 7)$-congruent (over $\mathbb{Q}$) to its quadratic twist by -214663, and $E_{(32,3)a}$, $E_{(32,3)b}$, and $E_{(48,19)}$ are $(32, 3)$, $(32, 3)$, and $(48, 19)$-congruent respectively to their quadratic twists by their discriminants.

By searching for points on the relevant modular curves of small genus we give evidence for the following conjecture:

Conjecture 1.0.17. *If $E/\mathbb{Q}$ is an elliptic curve admitting a non-trivial quadratic twist-type (N, r)-congruence then either $(N, r) \in \mathcal{S}$ or E is a quadratic twist of either $E_{(30,7)}$, $E_{(32,3)a}$, $E_{(32,3)b}$, or $E_{(48,19)}$.*

We prove in Theorem 4.5.1 that Conjecture 1.0.17 is true after assuming a mild hypothesis about rational points on a finite number of modular curves together with [RSZ22, Conjecture 1.5].

The final contribution of this thesis is to study the application of congruences to *visibility* of elements of the Tate–Shafarevich group of an abelian variety (see e.g., [CM00, AS02, AS05]). Recall that if $\psi\colon A \to B$ is an isogeny of abelian varieties $A/\mathbb{Q}$ and $B/\mathbb{Q}$, then we have the descent short exact sequence

$$0 \to B(\mathbb{Q})/\psi(A(\mathbb{Q})) \to S^{(\psi)}(A/\mathbb{Q}) \to Ш(A/\mathbb{Q})[\psi] \to 0$$

where $S^{(\psi)}(A/\mathbb{Q})$ denotes the ψ-Selmer group of A, and $Ш(A/\mathbb{Q})$ is the Tate–Shafarevich group of A (see [Sil09, X] for the definitions of these groups).

The group $Ш(A/\mathbb{Q})$ is a torsion group and is conjectured to be finite. It is conjectured that for every prime number $p > 0$ and each integer $g > 0$ there exists an absolutely simple abelian variety (i.e., one which is not isogenous over $\overline{\mathbb{Q}}$ to a product) of dimension g for which $Ш(A/\mathbb{Q})[p] \neq 0$. Indeed, it is even conjectured that $Ш(A^d/\mathbb{Q})[p] \neq 0$ for a positive proportion of quadratic twists of a *fixed* abelian variety $A/\mathbb{Q}$ (see e.g., [BKLS21, Conjecture 1.1]).

In spite of this, for general values of g and p, constructing an example of an absolutely simple g-dimensional abelian variety $A/\mathbb{Q}$ with an p-torsion element contained in $Ш(A/\mathbb{Q})$ is an open problem. By allowing the dimension of A to increase with p, Shnidman and Weiss [SW22] construct examples of absolutely simple abelian varieties with $Ш(A/\mathbb{Q})[p] \neq 0$. Flynn and Shnidman [FS22] extended this result to show $Ш(A/\mathbb{Q})[p]$ can be arbitrarily large.

When A has dimension 2 Bruin, Flynn, and Testa [BFT14, Fly15] found examples of absolutely simple genus 2 Jacobians with 3 and 5-torsion in their Tate–Shafarevich groups. Their approach relies on (p, p)-*descent*. That is, for several explicit examples of genus 2 curves $C/\mathbb{Q}$ they determined the ψ-Selmer groups of their Jacobians $J/\mathbb{Q}$ where ψ is an (p, p)-isogeny (i.e., a polarised isogeny with kernel isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$) for each $p = 3, 5$.

However, performing a (p, p)-descent becomes computationally costly as p increases, due to the need to perform class and unit group calculations in (a subfield of) the field $\mathbb{Q}(J[\psi])$. Our approach is to instead leverage visibility to construct absolutely simple genus 2 Jacobians such that $Ш(J/\mathbb{Q})[7] \neq 0$. To the best of our knowledge these are the first such examples.

Theorem 1.0.18. *Let $J/\mathbb{Q}$ be the Jacobian of the genus 2 curve $C/\mathbb{Q}$ given by the Weierstrass equation*

$$C : y^2 = 165(x^6 + 6x^5 + 27x^4 - 2x^3 + 45x^2 + 20)$$

Then J has conductor 39325^2, is absolutely simple, and its Tate–Shafarevich group contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$.

The Jacobian in Theorem 1.0.18 has real multiplication (RM) by the order $\mathbb{Z}[\sqrt{2}]$. In Theorem 6.0.1 we prove the analogue of Theorem 1.0.18 for 18 other genus 2 curves $C/\mathbb{Q}$ whose Jacobians have RM by $\mathbb{Z}[\sqrt{2}]$ and whose conductors are at most $(500\,000)^2$ (in each case $\sqrt{N_J}$ is the level of the corresponding weight 2 newform with coefficients in $\mathbb{Q}(\sqrt{2})$).

Our approach to proving Theorem 1.0.18 is essentially the mirror image of Fisher's approach for visualising elements of $Ш(E/\mathbb{Q})[7]$ in [Fis16]. In both cases, the Jacobian $J/\mathbb{Q}$ has real multiplication by $\mathbb{Z}[\sqrt{2}]$. We construct elliptic curves $E/\mathbb{Q}$ which are $([3 \pm \sqrt{2}], [7])$-*congruent* to

J (for some choice of sign). That is, for which there exists a Galois equivariant isomorphism $\phi\colon J[3\pm\sqrt{2}] \to E[7]$.

The observation of visibility in [CM00] is that the isomorphism ϕ allows one to transport information about the Selmer group of one abelian variety to another, under mild local hypotheses at their bad primes. Because of this, the proof of Theorem 1.0.18 may be reduced to simply computing the rank of an elliptic curve. Indeed, in both these cases the elliptic curves may already be found in the LMFDB [LMFDB].

The key technical input in Chapter 6 is an algorithm which, on input a genus 2 curve $C/\mathbb{Q}$ (whose Jacobian has real multiplication by $\mathbb{Z}[\sqrt{2}]$) outputs twists of the Klein quartic curve $X(7)$ which parametrise elliptic curves $([3\pm\sqrt{2}],[7])$-congruent to J.

1.1 Open questions and future work

The following two questions concern the existence of further curves on the surfaces $Z_{12,5}$ and $Z_{14,3}$. In order to prove Theorem 1.0.10 we find examples of (geometrically non-isogenous) $(12,1)$, $(12,7)$, $(12,11)$, and $(14,1)$-congruent elliptic curves over $\mathbb{Q}(t)$ (see Section 5.5.1). Conversely, the infinite family of $(12,5)$-congruent elliptic curves in Theorem 1.0.10 arises from specialising a pair defined over the function field of a rank 1 elliptic curve (see Example 5.5.2). It is then natural to ask whether a pair of $(12,5)$-congruent elliptic curves over $\mathbb{Q}(t)$ exists.

Question 1.1.1. *Does there exist a pair of non-isotrivial geometrically non-isogenous* $(12,5)$*-congruent elliptic curves over* $\mathbb{Q}(t)$*?*

As described in Theorem 1.0.11 we were able to find many examples of $(14,3)$-congruences over $\mathbb{Q}$, but we were unable to find an infinite family. It is not clear to us whether such a family exists.

Question 1.1.2. *Do there exist infinitely many* j*-invariants of geometrically non-isogenous* $(14,3)$*-congruent elliptic curves over* $\mathbb{Q}$*?*

After searching for rational points on our models for the surfaces $Z_{15,2}$ and $Z_{15,11}$ we have significant evidence for the following conjecture.

Conjecture 1.1.3. *For each* $r=2,11$*, the elliptic curves* $E_{(15,r)}$ *and* $E'_{(15,r)}$ *in Theorem 1.0.12 are the only pair of non-isogenous* $(15,r)$*-congruent elliptic curves over* $\mathbb{Q}$ *(up to simultaneous quadratic twists).*

The approach we use for computing the surfaces $Z_{N,r}$ when $N=12,14,15$ can be extended to compute further examples. In the file `N-congruences/ZNr-equations.m` at [Fre23b] we give equations for the surfaces $Z^{\mathrm{sym}}_{N,r}$ and $Z_{N,r}$ for each $(N,r)=(18,1)$, $(18,5)$, $(20,1)$, $(20,11)$, $(22,1)$, $(24,11)$, and $(24,23)$. It is simple to verify the correctness of these equations using formulae of Fisher [Fis12, Fis14, Fis15], Kumar [Kum15], and Chen [Che16, Che18], but we leave an exposition of their construction to future work. In each case we were unable to find any examples of geometrically non-isogenous (N,r)-congruent elliptic curves over $\mathbb{Q}$.

We hope to extend these calculations to give models for the surfaces $Z_{N,r}$ for all (N,r) such that $Z^{\mathrm{sym}}_{N,r}$ is not of general type. Unfortunately, our approach is not applicable in the case when $N=16$ and further input is likely required. For example, it may be possible to extend the approach of Fisher [Fis19, Fis21] if one can give a model for $X(16)\subset\mathbb{P}^n$ with a linear action of $\mathrm{SL}_2(\mathbb{Z}/16\mathbb{Z})$.

In Theorem 1.0.9 we saw that the surface $Z^{\mathrm{sym}}_{N,r}$ was birational over $\mathbb{Q}$ to $\mathbb{A}^2$ for each $(N,r)=(12,1)$, $(12,5)$, $(12,7)$, $(12,11)$, $(14,1)$, $(14,3)$, $(15,2)$, and $(15,11)$. Indeed, in each case where we

have computed $Z^{\mathrm{sym}}_{N,r}$ if it is geometrically rational (by Theorem 1.0.4) then it is in fact rational over $\mathbb{Q}$. This leads to a natural conjecture.

Conjecture 1.1.4. *Each of the surfaces $Z^{\mathrm{sym}}_{N,r}$ appearing in Theorem 1.0.4*(i) *are in fact rational over $\mathbb{Q}$ (i.e., birational over $\mathbb{Q}$ to $\mathbb{A}^2$). In particular, for each such pair (N,r), there exist infinitely many quadratic points on $Z_{N,r}$ and hence infinitely many pairs of j-invariants of non-isogenous (N,r)-congruent elliptic curves defined over a quadratic extension of $\mathbb{Q}$.*

Finally we mention a natural extension of Chapter 6 and Theorem 1.0.18. Since 11 splits in both $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{3})$ the same approach that we take in Chapter 6 should naturally extend to twisting the modular curve $X(11)$ (as in [Fis14, Section 3.3]). It would be interesting to compute these twists systematically and exhibit examples of genus 2 curves (with RM) whose Tate–Shafarevich groups contain an element of order 11.

1.2 Outline

We begin with the background for this thesis in Chapter 2. First we give a brief recap of results on symplectic abelian groups and congruences, followed by giving the necessary background on modular curves. The construction of the modular curves X_g and X_g^+ in Section 2.2.7 is the key novel construction allowing us to classify quadratic twist-type congruences in Chapter 4. This construction gives a pleasing moduli interpretation for the modular curves associated to an *extended Cartan subgroup* (see Lemma 2.2.13). This construction also provides the central tool for determining the Kodaira dimension of $Z^{\mathrm{sym}}_{N,r}$ in Chapter 3 and is the key technical improvement on our previous work [Fre23a] which forms the basis of Chapter 4.

In Section 2.3 we unify the description of Hilbert modular surfaces of discriminant N^2 (in the case when $r=-1$) given by McMullen [McM07] and Kumar [Kum15] with the classical definition of Hilbert modular surfaces (given in e.g., [vdG88]). This is (to the best of our knowledge) original, but it is likely known to experts. In particular, we give a construction for the surfaces $Z_{N,r}$ by taking (compactifications of) quotients of $\mathbb{H}^2$ by a subgroup defined analagously to the Hilbert modular group, but for a more general quadratic étale algebra.

In Section 2.5 we discuss minimisation of étale cubic and quartic algebras over a multivariate polynomial ring $\mathbb{Z}[t_1,...,t_n]$. The approach described in this section allows us to compute simplifying changes of coordinates in Section 5.3, and can therefore be safely ignored until the reader wishes to understand how the calculations of the fibre products in Section 5.3 were performed.

The goal of Chapter 3 is to prove Theorems 1.0.4 and 1.0.6. We begin by recalling a number of facts about the Hilbert modular surfaces $Z_{N,r}$ in Section 3.2, after which we study the fixed points of the involution on $Z_{N,r}$ which swaps the roles of the pair of (N,r)-congruent elliptic curves. Following an approach of Hirzebruch [Hir73b, §5] we compute the geometric genus of (a smooth projective surface birational to) $Z^{\mathrm{sym}}_{N,r}$ and prove Theorem 1.0.4 in Section 3.6. By studying the intersections of certain curves on $Z^{\mathrm{sym}}_{N,r}$, we prove Theorem 1.0.6 in Section 3.8.

In Chapter 4 we study quadratic twist-type congruences of elliptic curves over $\mathbb{Q}$. We begin by proving Lemma 4.1.1 which places a group theoretic restriction on the image of the mod N Galois representation of an elliptic curve which admits a quadratic twist-type N-congruence. We use this condition to prove Proposition 4.2.4 which proves Theorem 1.0.15 in the case when $N=p^l$ is a prime power (and Conjecture 1.0.17 under the assumption of [RSZ22, Conjecture 1.5]). When $N=p^lq^k$ is a product of prime powers, we relate quadratic twist-type N-congruences to rational points on certain (double covers of) fibre products of modular curves in Section 4.3. By explicitly

computing all such curves of genus 0 or 1, we prove Theorem 1.0.15 in Section 4.4. In the remainder of Chapter 4, we prove Theorem 4.5.1 and Proposition 4.6.2 which give partial results towards Conjecture 1.0.17.

Chapter 5 contains our computations of the surfaces $Z_{N,r}$, and in particular we prove Theorems 1.0.9–1.0.12. Key to our approach is to first use the invariant theoretic description of $Z_{N,r}$ given in Section 2.3.4 to find simple conditions for a pair of elliptic curves to be 2, 3, or 4-congruent (see Theorem 5.1.4). We then apply these conditions to compute the fibre products $Z_{N_1,r} \times_{Z_1} Z_{N_2,r}$ where N_1 and N_2 are coprime integers such that $N = N_1N_2 = 12$, 14, or 15. By computing certain double covers of these fibre products we compute models for $Z_{N,r}$ in Section 5.3. In Sections 5.5 and 5.6 we prove Theorems 1.0.10–1.0.12 by finding rational points and curves of genus 0 or 1 on $Z_{N,r}$.

Finally in Chapter 6 we prove Theorem 1.0.18. In fact, we prove Theorem 6.0.1 which gives additional examples of genus 2 curves $C/\mathbb{Q}$ with Jacobians whose Tate–Shafarevich groups contain an element of order 7. We briefly recall some facts about visibility of Tate–Shafarevich groups in Section 6.1 before outlining our algorithm for twisting $X(7)$ in Sections 6.2 and 6.3. We prove Theorems 1.0.18 and 6.0.1 in Section 6.4 and conclude by studying examples in Section 6.5.

Code accompanying this thesis

The code accompanying this thesis is written primarily in `Magma` [BCP97] with small sections in `SageMath` [Sage]. It has been made publicly available on GitHub in the repository [Fre23b] which may be accessed at

`https://github.com/SamFrengley/thesis.git`

To increase the chance that it is available so long as this thesis is, the code has also been uploaded to the University of Cambridge "Apollo" research data repository

`https://www.repository.cam.ac.uk/`

though it will not be updated there. Throughout this work we will reference the relevant GitHub repositories, though the code may be found in similarly named directories on Apollo.

Chapter 2

Background

In this chapter we give background on the moduli spaces which appear in this thesis. Let $\mathbb{H}$ denote the complex upper half plane and let $\mathrm{GL}_2(\mathbb{R})^+$ denote the subgroup of $\mathrm{GL}_2(\mathbb{R})$ consisting of matrices with positive determinant. Then $\mathrm{GL}_2(\mathbb{R})^+$ acts on $\mathbb{H}$ via Möbius transformations.

2.1 Congruences of elliptic curves

Let N be a positive integer and let K be a field of characteristic coprime to N. Let G_K denote the absolute Galois group of K. We first recall several definitions and standard facts about congruences of elliptic curves.

Definition 2.1.1. We say that a pair of elliptic curves E/K and E'/K are *N-congruent over K*, or simply *N-congruent*, if there exists a G_K-equivariant group isomorphism $\phi\colon E[N] \to E'[N]$.

Definition 2.1.2. A *symplectic abelian group (scheme)* is a pair $(M, \langle\cdot,\cdot\rangle)$ where M is a finite abelian group (scheme) and $\langle\cdot,\cdot\rangle : M \times M \to \mu_N$ is bi-linear, alternating, and non-degenerate morphism of group (schemes).

Example 2.1.3. In this work we will consider the following symplectic abelian groups often.

(i) Over a field of characteristic coprime to N, the group scheme $\mu_N \times \mathbb{Z}/N\mathbb{Z}$ may be equipped with the structure of a symplectic abelian group scheme with the pairing $\langle(\zeta, a), (\xi, b)\rangle = \zeta^b\xi^{-a}$.

(ii) If E/K is an elliptic curve then by [Sil09, Proposition III.8.1] the N-torsion subgroup $E[N]$ is a symplectic abelian group when equipped with the Weil pairing $e_{E,N}\colon E[N] \times E[N] \to \mu_N$.

Lemma 2.1.4. *Let M and M' be symplectic abelian groups which are isomorphic as abstract groups to $(\mathbb{Z}/N\mathbb{Z})^2$. If $\phi\colon M \to M'$ is an isomorphism of abstract groups then there exists an element $r \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $\langle x, y\rangle^r = \langle\phi(x), \phi(y)\rangle$ for each $x, y \in M$.*

In this case we say that the isomorphism ϕ has power r. *Moreover, if $r = 1$ (respectively $r = -1$ the isomorphism ϕ is said to be* symplectic *(respectively* anti-symplectic*).*

Proof. Let $\{m, n\}$ be a $\mathbb{Z}/N\mathbb{Z}$-basis for M. It follows that $\langle m, n\rangle$ is a primitive N^{th}-root of unity, and so we may choose a $\mathbb{Z}/N\mathbb{Z}$-basis $\{m', n'\}$ for M' such that $\langle m, n\rangle = \langle m', n'\rangle$. There exists a matrix $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $\left(\begin{smallmatrix}\phi(m)\\ \phi(n)\end{smallmatrix}\right) = g\left(\begin{smallmatrix}m'\\ n'\end{smallmatrix}\right)$, so in particular $\langle\phi(m), \phi(n)\rangle = \langle m', n'\rangle^{\det(g)} = \langle m, n\rangle^{\det(g)}$. □

Definition 2.1.5. We say that elliptic curves E/K and E'/K are *N-congruent with power r* or *(N, r)-congruent* if there exists an N-congruence $\phi\colon E[N] \to E'[N]$ with power r (where $E[N]$ and $E'[N]$ are equipped with the Weil pairing).

The following well known lemma justifies the name "congruence".

Lemma 2.1.6. *Let K be a number field and E/K and E'/K be N-congruent elliptic curves and suppose that $\mathfrak{p}$ is a prime of K not dividing N at which both E and E' have good reduction. Then we have $a_\mathfrak{p}(E) \equiv a_\mathfrak{p}(E') \pmod N$, where $a_\mathfrak{p}$ denotes the trace of Frobenius at $\mathfrak{p}$.*

Proof. Since E and E' are N-congruent over K the mod N Galois representations $\bar\rho_{E,N}$ and $\bar\rho_{E',N}$ are isomorphic. Since E and E' have good reduction at $\mathfrak{p}$ the extension $K(E[N])/K$ is unramified at $\mathfrak{p}$ (note that $K(E[N]) = K(E'[N])$). In particular modulo N we have

$$a_\mathfrak{p}(E) \equiv \operatorname{tr} \bar\rho_{E,N}(\mathrm{Frob}_\mathfrak{p}) \equiv \operatorname{tr} \bar\rho_{E',N}(\mathrm{Frob}_\mathfrak{p}) \equiv a_\mathfrak{p}(E')$$

as required. □

2.2 Modular curves

We recall a number of generalities about modular curves. The reader seeking more details is encouraged to consult e.g., [Bar10, Section 3], [DR73, Section IV-3], [RSZ22, Section 2.3], [RZ15a, Section 2], [Ser08, A.5], or [SZ17, Section 2].

Fix a positive integer N. Let I denote the identity matrix, and let

$$\Gamma(N) = \{A \in \mathrm{SL}_2(\mathbb{Z}) : A \equiv I \pmod N\}$$

be the congruence subgroup of full level N. The group $\Gamma(N) \subset \mathrm{GL}_2(\mathbb{R})^+$ acts on the complex upper half plane $\mathbb{H}$ on the left by Möbius transformations, explicitly $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z = \frac{az+b}{cz+d}$. It can be shown that there exists an algebraic curve $Y/\mathbb{C}$ such that $Y(\mathbb{C}) \cong \Gamma(N)\backslash\mathbb{H}$ as Riemann surfaces.

In fact the curve Y admits a model defined over $\mathbb{Z}[1/N]$, that is, there exists a (smooth, affine, algebraic) curve $Y(N)$ over $\operatorname{Spec}\mathbb{Z}[1/N]$ such that $Y \cong Y(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{C}$. We define $X(N)$ to be the smooth compactification of $Y(N)$, i.e., the smooth projective curve defined over $\mathbb{Z}[1/N]$ which is birational to $Y(N)$. We call the curve $X(N)$ the *modular curve of full level N*.

We say that a pair (E, ι) is an *elliptic curve with full (symplectic) level N structure* if E/K is an elliptic curve and $\iota\colon E[N] \to \mu_N \times \mathbb{Z}/N\mathbb{Z}$ is an isomorphism of symplectic K-group schemes. A morphism of elliptic curves with full level N structure (E, ι) and (E', ι') is a morphism $\phi\colon E \to E'$ such that $\iota'\phi = \iota$.

The curve $Y(N)$ is the coarse moduli space of the stack whose K-rational points parametrise isomorphism classes of elliptic curves with full level N structure. More concretely, the K-rational points on $Y(N)$ are in bijective correspondence with isomorphism classes of pairs (E, ι) (modulo taking quadratic twists of E when $N = 1, 2$).

The action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ induces an action of $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on the $\mathbb{C}$-points of $Y(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{C}$. Since $-I$ acts trivially on $Y(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{C}$ this action in turn induces an action of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. In fact, this action descends to an action defined over any field K of characteristic coprime to N in the following way.

Let Υ_N denote the K-group scheme of symplectic K-group automorphisms of $\mu_N \times \mathbb{Z}/N\mathbb{Z}$. We understand Υ_N to act on $\mu_N \times \mathbb{Z}/N\mathbb{Z}$ from the left. On $\overline{K}$-points we have an isomorphism of groups $\Upsilon_N \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, however Υ_N comes equipped with a G_K-action. In this case Υ_N acts on $Y(N)$ by $(E, \iota) \mapsto (E, \gamma\iota)$. By the definition of Υ_N this action is G_K-equivariant.

The action of Υ_N extends to an action on $X(N)$. By forgetting the level structure on $Y(N)$ we have a natural forgetful map $Y(N) \to Y(1)$, where the latter we identify with $\mathbb{A}^1$ by taking j-invariants. This extends to a morphism $X(N) \to X(1)$ which quotients by the action of $\Upsilon_N/\{\pm 1\}$.

Remark 2.2.1. As stated above, with our conventions the modular curve $X(N)$ is a smooth, projective, reduced, geometrically connected algebraic curve defined over $\operatorname{Spec}\mathbb{Z}[1/N]$. This construction will be sufficient for the majority of this work, however in Section 2.2.7 we will define modular curves which will necessarily be geometrically reducible.

For this reason, following [DR73, IV-3] we define $\mathbb{Y}(N)/\mathbb{Z}[1/N]$ to be the coarse moduli space such that, for each field K of characteristic coprime to N, the K-points on $\mathbb{Y}(N)$ parametrise isomorphisms $\iota\colon E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ of (abstract) K-group schemes. Define $\mathbb{X}(N)/\mathbb{Z}[1/N]$ to be the smooth compactification of $\mathbb{Y}(N)$. The modular curve $X(N)$ is isomorphic (over $\mathbb{Q}(\zeta_N)$) to one (any) of the $\varphi(N)$ components of the modular curve $\mathbb{X}(N)$.

The curve $\mathbb{X}(N)$ comes equipped with a forgetful morphism $\mathbb{X}(N) \to X(1)$ which quotients by the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ where the action is given by extending the action on $\mathbb{Y}(N)$ given by $(E, \iota) \mapsto (E, \gamma\iota)$.

2.2.1 Invariant theory for $X(N)$

We briefly recall the classical invariant theory of the modular curve $X(N)$ in the cases when $N = 2$, 3, 4, 5, and 7. Let K be a field of characteristic coprime to N. For each $N \leq 5$ we have a K-isomorphism $X(N) \cong \mathbb{P}^1$, and when $N = 7$ the modular curve $X(7)$ is K-isomorphic to the Klein quartic $\{x_0^3x_1 + x_1^3x_2 + x_0x_2^3 = 0\} \subset \mathbb{P}^2$ (see e.g., [Elk99, Section 4.1]).

The invariant theory of these curves (when acted on by $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$) was studied by Klein [Kle78, Kle56]. Our description follows Fisher [Fis12] and [Fis14]. Consider the generators $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ of $\mathrm{SL}_2(\mathbb{Z})$.

For convenience we define the group $\mathrm{SL}_2'(\mathbb{Z}/2\mathbb{Z})$ to be the unique non-split extension of the group $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$ by C_2. We write $\mathrm{SL}_2'(\mathbb{Z}/N\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ when $N \neq 2$. We write $S', T' \in \mathrm{SL}_2'(\mathbb{Z}/N\mathbb{Z})$ for the pre-images of S and T of order 4 and N respectively (these are simply S and T when $N \neq 2$).

For each $k > 0$, let $\zeta_k \in \overline{K}$ be a primitive k^{th}-root of unity. For each $2 \leq N \leq 5$ we define a representation $\mathrm{SL}_2'(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\overline{K})$ by defining the images of the generators S' and T' to be

$$
\begin{aligned}
N = 2: &\quad \begin{pmatrix} 1/2 & 1/16 \\ -12 & 1/2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
N = 3: &\quad \frac{1}{\sqrt{-3}} \begin{pmatrix} 1 & 1/3 \\ 6 & -1 \end{pmatrix} \quad \text{and} \quad \zeta_3 \begin{pmatrix} 1 & 0 \\ 0 & \zeta_3 \end{pmatrix} \\
N = 4: &\quad \frac{1}{\sqrt{-2}} \begin{pmatrix} 1 & 1/2 \\ 2 & -1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & \zeta_4 \end{pmatrix} \\
N = 5: &\quad \frac{1}{g_5} \begin{pmatrix} \varphi & 1 \\ 1 & \varphi \end{pmatrix} \quad \text{and} \quad \zeta_5^2 \begin{pmatrix} 1 & 0 \\ 0 & \zeta_5 \end{pmatrix}
\end{aligned}
$$

where $g_5 = \zeta_5^3 + \zeta_5^2 + 2\zeta_5 + 1$.

When $N = 7$ we consider the representation $\mathrm{SL}_2'(\mathbb{Z}/7\mathbb{Z}) \to \mathrm{GL}_3(\overline{K})$ defined on the generators S and T by

$$
\frac{1}{\sqrt{-7}} \begin{pmatrix} \zeta_7 - \zeta_7^6 & \zeta_7^2 - \zeta_7^5 & \zeta_7^4 - \zeta_7^3 \\ \zeta_7^2 - \zeta_7^5 & \zeta_7^4 - \zeta_7^3 & \zeta_7 - \zeta_7^6 \\ \zeta_7^4 - \zeta_7^3 & \zeta_7 - \zeta_7^6 & \zeta_7^2 - \zeta_7^5 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \zeta_7 & 0 & 0 \\ 0 & \zeta_7^4 & 0 \\ 0 & 0 & \zeta_7^2 \end{pmatrix}.
$$

Recall that we have an isomorphism $\Upsilon_N \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ defined over $\overline{K}$. We define Υ_N' by analogy to Υ_N. Composing this isomorphism with the above representations of $\mathrm{SL}_2'(\mathbb{Z}/N\mathbb{Z})$ we

obtain a representation $\rho\colon \Upsilon'_N \to \mathrm{GL}_n(\overline{K})$ where $n = 2$ for each $N \leq 5$ and $n = 3$ when $N = 7$. Moreover, the induced projective representations $\bar{\rho}\colon \Upsilon_N \to \mathrm{PGL}_n(\overline{K})$ are G_K-equivariant.

Denote by $G_N \subset \mathrm{GL}_n(\overline{K})$ the image of the representation ρ. Let $\widetilde{G}_N$ be the commutator subgroup of G_N (in particular, when $N = 5, 7$ we have $G_N = \widetilde{G}_N$). It is a classical theorem of Klein that for each $N \leq 5$ the invariant ring $K[x_0, x_1]^{\widetilde{G}_N}$ is generated by invariants c_4, c_6, and D of weights $4N$, $6N$, and 12 subject only to the relation $c_4^3 - c_6^2 = 1728D^N$ (see [Fis12, Theorem 3.3]). Klein showed similarly that the invariant ring $K[x_0, x_1, x_2]^{G_7}$ is generated by invariants[1] c_4, c_6, D, and F where $F = x_0^3x_1 + x_1^3x_2 + x_0x_2^3$ is the defining equation of the Klein quartic and c_4, c_6, and D have weights $4N$, $6N$, and 12. Moreover we similarly have $c_4^3 - c_6^2 \equiv 1728D^7 \pmod{F}$. More explicitly, we may take

$$\begin{aligned}
N = 2&: \quad D = x_0(64x_0^2 - x_1^2),\\
N = 3&: \quad D = -x_0(27x_0^3 + x_1^3),\\
N = 4&: \quad D = x_0x_1(16x_0^4 - x_1^4),\\
N = 5&: \quad D = x_0x_1(x_0^{10} - 11x_0^5x_1^5 - x_1^{10}),\\
N = 7&: \quad D = x_0^5x_2 - 5x_0^2x_1^2x_2^2 + x_0x_1^5 + x_1x_2^5.
\end{aligned}$$

When $N \leq 5$ further define

$$c_4 = \tfrac{-1}{((\deg D)-1)^2} \times \begin{vmatrix} \frac{\partial^2 D}{\partial x_0^2} & \frac{\partial^2 D}{\partial x_0 \partial x_1} \\ \frac{\partial^2 D}{\partial x_0 \partial x_1} & \frac{\partial^2 D}{\partial x_1^2} \end{vmatrix} \qquad \text{and} \qquad c_6 = \tfrac{1}{\deg c_4} \times \begin{vmatrix} \frac{\partial D}{\partial x_0} & \frac{\partial D}{\partial x_1} \\ \frac{\partial c_4}{\partial x_0} & \frac{\partial c_4}{\partial x_1} \end{vmatrix}.$$

Recalling that when $N = 7$ we write $F = x_0^3x_1 + x_1^3x_2 + x_0x_2^3$ we define

$$c_4 = \frac{1}{9} \times \begin{vmatrix} \frac{\partial^2 F}{\partial x_0^2} & \frac{\partial^2 F}{\partial x_0 \partial x_1} & \frac{\partial^2 F}{\partial x_0 \partial x_2} & \frac{\partial D}{\partial x_0} \\ \frac{\partial^2 F}{\partial x_0 \partial x_1} & \frac{\partial^2 F}{\partial x_1^2} & \frac{\partial^2 F}{\partial x_1 \partial x_2} & \frac{\partial D}{\partial x_1} \\ \frac{\partial^2 F}{\partial a \partial x_2} & \frac{\partial^2 F}{\partial x_1 \partial x_2} & \frac{\partial^2 F}{\partial x_2^2} & \frac{\partial D}{\partial x_2} \\ \frac{\partial D}{\partial x_0} & \frac{\partial D}{\partial x_1} & \frac{\partial D}{\partial x_2} & 0 \end{vmatrix} \qquad \text{and} \qquad c_6 = \frac{1}{14} \times \begin{vmatrix} \frac{\partial F}{\partial x_0} & \frac{\partial F}{\partial x_1} & \frac{\partial F}{\partial x_2} \\ \frac{\partial D}{\partial x_0} & \frac{\partial D}{\partial x_1} & \frac{\partial D}{\partial x_2} \\ \frac{\partial c_4}{\partial x_0} & \frac{\partial c_4}{\partial x_1} & \frac{\partial c_4}{\partial x_2} \end{vmatrix}.$$

The following lemma follows by noting that the only points at which the map $X(N) \to X(1)$ ramifies are those above 0, 1728, and ∞ with ramification index 2, 3, and 7 respectively (see [Fis12, Lemma 4.4] and [Fis14, Lemma 3.5] for proofs in the cases $N \leq 5$ and $N = 7$ respectively).

Lemma 2.2.2. *For each $N = 2$, 3, 4, 5, or 7 the forgetful map $X(N) \to X(1)$ is given by c_4^3/D^N.*

It will be useful for us to note that with these models for $X(4)$ and $X(2)$ the forgetful map $X(4) \to X(2)$ is given by $[x_0 : x_1] \mapsto [-x_0^2x_1^2 : 16x_0^4 + x_1^4]$.

2.2.2 The modular curve $X(H)$ with H-level structure

We define the *modular curve, $X(H)$, with level H-structure* for each subgroup $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. In most cases in this work (except for some examples of the modular curves X_g^+ in Section 2.2.7) the modular curves $Y(H)$ may be constructed from quotients of the upper half plane (see Lemma 2.2.5).

[1] In this case, when $N = 7$, the form which we here denote D is often called H in the literature.

Definition 2.2.3. Let $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a subgroup. We define $Y(H)$, respectively $X(H)$, to be the (scheme) quotient of $\mathbb{Y}(N)$, respectively $\mathbb{X}(N)$, by the action of H. We say that a point $x \in X(H)$ is a *cusp* if $x \in X(H) \setminus Y(H)$.

Remark 2.2.4. If the determinant character is surjective on the subgroup $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (i.e., if $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$) then $X(H)$ is a geometrically irreducible curve. In this case $Y(H)$, respectively $X(H)$, is isomorphic (over $\mathbb{Q}(\zeta_N)$) to the (scheme) quotient of $Y(N)$, respectively $X(N)$, by the action of $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

We have a natural forgetful morphism $j\colon X(H) \to X(1)$ defined over K. The following well known result is immediate from the construction, together with Remark 2.2.4.

Lemma 2.2.5. *Suppose that $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ has $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$. Let $\Gamma(H) \subset \mathrm{SL}_2(\mathbb{Z})$ be the pre-image of $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ under the reduction-modulo-N map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Then $Y(H)(\mathbb{C})$ and $\Gamma(H)\backslash\mathbb{H}$ are isomorphic as Riemann surfaces.*

We now recall the following result, which gives a moduli interpretation for the modular curve $X(H)$ outside those points with j-invariant 0, 1728, or ∞.

Definition 2.2.6. Let K be a field of characteristic coprime to N and let E/K be an elliptic curve. Viewing $E[N]$ as a $\mathbb{Z}/N\mathbb{Z}$-module without symplectic structure and fixing a $\mathbb{Z}/N\mathbb{Z}$ basis for $E[N]$ we obtain an isomorphism $\mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. In this way we obtain a representation

$$\bar{\rho}_{E,N}\colon G_K \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

which we call the *mod N Galois representation attached to E/K*.

Lemma 2.2.7. *Let K be a field of characteristic 0. If $-I \notin H$ then the K-rational points on $Y(H)\setminus j^{-1}\{0, 1728\}$ parametrise elliptic curves E/K such that the image, $\bar{\rho}_{E,N}(G_K)$, of the corresponding mod N Galois representation is contained in a subgroup conjugate to H.*

Similarly if $-I \in H$ then the K-rational points on $Y(H) \setminus j^{-1}\{0, 1728\}$ parametrise $\overline{K}$-isomorphism classes of elliptic curves E/K such that the image, $\bar{\rho}_{E,N}(G_K)$, of the corresponding mod N Galois representation is contained in a subgroup conjugate to H.

Proof. This is e.g., [RZ15a, Lemma 2.1] and [Zyw15b, Proposition 3.2]. □

We now give examples of the modular curves which will appear in this work.

2.2.3 The modular curves $X_0(N)$ and $X_0^+(N)$

The Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is the subgroup

$$G(\mathrm{b}\, N) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in (\mathbb{Z}/N\mathbb{Z})^\times, b \in \mathbb{Z}/N\mathbb{Z} \right\} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

consisting of upper triangular matrices. We define the modular curve $X_0(N)$ to be the modular curve $X(G(\mathrm{b}\, N))$. It follows immediately from Lemma 2.2.7 that if K is a field of characteristic coprime to N then the non-cuspidal K-rational points on $X_0(N)$ parametrise $\overline{K}$-isomorphism classes of pairs (E, ϕ) where E/K is an elliptic curve (defined up to a twist) and $\phi\colon E \to E'$ is a cyclic N-isogeny defined over K.

The existence of the dual isogeny gives rise to the *Fricke involution* on $X_0(N)$. More precisely there is an involution $w_N\colon X_0(N) \to X_0(N)$ extending the morphism $Y_0(N) \to Y_0(N)$ given by

$(E,\phi) \mapsto (E', \hat{\phi})$, where $\hat{\phi}$ is the dual of ϕ. We write $X_0^+(N)$ for the quotient of $X_0(N)$ by the involution w_N.

2.2.4 The modular curves $X_1(N)$ and $X_\mu(N)$

Consider the subgroup

$$G(\mathrm{b}_1\, N) = \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} : a \in \mathbb{Z}/N\mathbb{Z}, b \in (\mathbb{Z}/N\mathbb{Z})^\times \right\} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

and define the modular curve $X_1(N) = X(G(\mathrm{b}_1\, N))$.

Again by Lemma 2.2.7 if K is a field of characteristic coprime to N the non-cuspidal K-rational points on $X_1(N)$ parametrise K-isomorphism classes of pairs (E,P) where E/K is an elliptic curve and $P \in E(K)$ is a point of exact order N.

We define $X_\mu(N)$ to be the moduli space whose non-cuspidal K-points parametrise isomorphism classes of pairs (E,ι) where E/K is an elliptic curve and $\iota\colon \mu_N \hookrightarrow E[N]$ is G_K-equivariant. Note that if $P \in E(K)$ is a point of exact order N then there exists a unique cyclic N-isogeny $\phi\colon E \to E'$ with kernel containing P. The kernel of $\hat{\phi}$ is K-isomorphic to μ_N (the Cartier dual of the constant group scheme $\mathbb{Z}/N\mathbb{Z}$). Fix a primitive N^{th} root of unity $\zeta \in \mu_N$. This gives rise to an isomorphism $X_1(N) \to X_\mu(N)$ which is given on non-cuspidal points by $(E,P) \mapsto (E', \iota_P)$ where $\iota_P\colon \mu_N \hookrightarrow E'[N]$ is the inclusion given by $\zeta \mapsto \phi(Q)$ and $Q \in E[N]$ is chosen so that $e_N(P,Q) = \zeta$.

2.2.5 The modular curves attached to Cartan subgroups

Let p be a prime number, and let $l \geq 1$ be an integer. We briefly summarise some facts about Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$. Our exposition closely follows that of Baran [Bar10].

Let $\mathcal{O}$ be an order in a quadratic number field such that p is unramified in $\mathcal{O}$. Consider the free, rank 2, $\mathbb{Z}/p^l\mathbb{Z}$-algebra $A = \mathcal{O}/p^l\mathcal{O}$. Now A/pA is either isomorphic to $\mathbb{F}_p \times \mathbb{F}_p$ or $\mathbb{F}_{p^2}$, in the first case we say that A is *split*, and in the second case we say A is *non-split*. Up to isomorphism there is a unique split (respectively non-split) $\mathbb{Z}/p^l\mathbb{Z}$-algebra A.

Let $A^\times$ act on A by multiplication. By choosing a $\mathbb{Z}/p^l\mathbb{Z}$-basis for A we obtain an embedding $A^\times \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$.

Definition 2.2.8. A *Cartan subgroup* of $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ is any subgroup occurring as the image of such an embedding $A^\times \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$. We say that a Cartan subgroup is *split* (respectively *non-split*) if A is split (respectively non-split).

The image of the representation $A^\times \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ depends only on the basis we choose for A. In particular all split (respectively non-split) Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ are conjugate in $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$.

We now describe how to explicitly construct Cartan subgroups. Explicit descriptions of these (and other) subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ may also be found in e.g., [DLM22, Section 3].

A split Cartan subgroup. Let p be a prime number and let $G(\mathrm{s}\, p^l) \subset \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ denote the subgroup of diagonal matrices. Then $G(\mathrm{s}\, p^l)$ is a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ since it is the regular representation of $A = (\mathbb{Z}/p^l\mathbb{Z})^2$ with respect to the standard basis. For each $l \geq 1$ we write $G(\mathrm{s}\, p^{l^+})$ for the subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ generated by $G(\mathrm{s}\, p^l)$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

If p^l is a prime power we define the modular curves $X(\mathrm{s}\, p^l) = X(G(\mathrm{s}\, p^l))$ and $X(\mathrm{s}\, p^{l^+}) = X(G(\mathrm{s}\, p^{l^+}))$.

Remark 2.2.9. The (conjugacy class of the) subgroup $G(\mathrm{s}\,p^{l^+})$ is often referred to as the *normaliser of a split Cartan subgroup*. However it is only true that $G(\mathrm{s}\,p^{l^+})$ is equal to the normaliser of $G(\mathrm{s}\,p^l)$ in $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ when p is odd. The subgroup $G(\mathrm{s}\,2^{k^+})$ is *strictly* contained in the normaliser of $G(\mathrm{s}\,2^k)$ in $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ since, for example, $\left(\begin{smallmatrix}1 & 2^{k-1}\\ 0 & 1\end{smallmatrix}\right)$ normalises $G(\mathrm{s}\,2^k)$[2].

A non-split Cartan subgroup. Let p be prime and let $\mathcal{O} = \mathbb{Z}[\alpha]$ be a quadratic order such that p is inert in $\mathcal{O}$. Let $f(x) = x^2 - ux + v \in \mathbb{Z}[x]$ be the minimal polynomial of α. For the purposes of this work we take $f(x) = x^2 + x + 1$ when $p = 2$, and when p is odd, we take $f(x) = x^2 - \xi$ where $\xi \in \mathbb{Z}$ is a quadratic non-residue modulo p.

The $\mathbb{Z}/p^l\mathbb{Z}$-algebra $A = \mathcal{O}/p^l\mathcal{O}$ is non-split. Fix the $\mathbb{Z}/p^l\mathbb{Z}$-basis $\{1, \alpha\}$ for A, then $A^\times$ embeds in $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ by its regular action on this basis. By construction the image is a non-split Cartan subgroup, which we denote $G(\mathrm{ns}\,p^l)$. Explicitly for each integer $k \geq 1$ we take

$$G(\mathrm{ns}\,2^k) = \left\{ \begin{pmatrix} a & -b \\ b & a-b \end{pmatrix} : a, b \in \mathbb{Z}/2^k\mathbb{Z} \text{ such that } (a,b) \not\equiv (0,0) \pmod 2 \right\}$$

and when p is odd we take

$$G(\mathrm{ns}\,p^l) = \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}/p^l\mathbb{Z} \text{ such that } (a,b) \not\equiv (0,0) \pmod p \right\}.$$

For any prime number p, the normaliser $G(\mathrm{ns}\,p^{l^+})$ of $G(\mathrm{ns}\,p^l)$ in $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ is generated by $G(\mathrm{ns}\,p^l)$ and the matrix $\left(\begin{smallmatrix}1 & u\\ 0 & -1\end{smallmatrix}\right)$ (i.e., $\left(\begin{smallmatrix}1 & -1\\ 0 & -1\end{smallmatrix}\right)$ when $p = 2$ and $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ when p is odd).

For any prime power p^l we define the modular curves $X(\mathrm{ns}\,p^l) = X(G(\mathrm{ns}\,p^l))$ and $X(\mathrm{ns}\,p^{l^+}) = X(G(\mathrm{ns}\,p^{l^+}))$.

2.2.6 Fibre products of modular curves

Suppose that N factors as a product $p_1^{l_1}...p_r^{l_r}$, where $p_1, ..., p_r$ are distinct primes. Let

$$H = H_1 \times ... \times H_r \subset \mathrm{GL}_2(\mathbb{Z}/p_1^{l_1}\mathbb{Z}) \times ... \times \mathrm{GL}_2(\mathbb{Z}/p_r^{l_r}\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

be a subgroup. In this case we denote the curve $X(H)$ by $X(H_1, ..., H_r)$. It is clear that $X(H)$ is birational to the fibre product $X(H_1) \times_{X(1)} ... \times_{X(1)} X(H_n)$.

When the groups H_i are equal to (a conjugate of) $G(\mathrm{s}\,p^l)$, $G(\mathrm{s}\,p^{l^+})$, $G(\mathrm{ns}\,p^l)$, or $G(\mathrm{ns}\,p^{l^+})$ we will replace H_i with the label $\mathrm{s}\,p^l$, $\mathrm{s}\,p^{l^+}$, $\mathrm{ns}\,p^l$, and $\mathrm{ns}\,p^{l^+}$ respectively.

2.2.7 The modular curves X_g and X_g^+

Many of the ideas which appear in this section are generalisations of those previously presented in [Fre23a]. Let N be a positive integer and let g be an element in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We define the subgroup

$$H_g = \{h \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : ghg^{-1} = h\}$$

to be the centraliser of g in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, and define

$$H_g^+ = \{h \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : ghg^{-1} = \pm h\}.$$

[2]This observation means that it is often convenient to define the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ to be a subgroup which contains a Cartan subgroup with index 2 (see e.g., [LMFDB, Normalizer of a Cartan subgroup]).

For brevity we write X_g and X_g^+ for the modular curves $X(H_g)$ and $X(H_g^+)$ respectively.

Remark 2.2.10. Note that it is not necessarily true that the determinant character is surjective on H_g and H_g^+. For example, consider the matrix $g = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. In this case $X_g \cong X_g^+$ is a geometrically reducible modular curve whose two geometrically irreducible components are isomorphic, over $\mathbb{Q}(\sqrt{p^*})$, to $X_1(p)$, where $p^* = (-1)^{(p-1)/2}p$.

The modular curves X_g and X_g^+ will play an important role in this work, which is best illustrated by the following proposition.

Proposition 2.2.11. *Let K be a field of characteristic zero. The non-cuspidal K-rational points on $X_g^+ \setminus j^{-1}\{0, 1728, \infty\}$ parametrise triples (E, E^d, ϕ), defined up to quadratic twist. Here E/K is an elliptic curve, E^d/K is a quadratic twist of E, and $\phi\colon E[N] \to E^d[N]$ is an N-congruence such that, after choosing a basis for $E[N]$, the congruence ϕ is given by $t \circ g'$ where $g' \in \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is conjugate to g and $t\colon E \to E^d$ is an isomorphism defined over $K(\sqrt{d})$.*

Moreover, in this case $d \in K^\times$ is such that $\bar{\rho}_{E,N}^{-1}(H) = G_{K(\sqrt{d})}$ and the power of the congruence ϕ is $\det(g)$.

Proof. By Lemma 2.2.7 it suffices to show that such a congruence exists if and only if the image of the mod N Galois representation $\bar{\rho}_{E,N}$ is contained in a subgroup conjugate to H_g^+. The subgroups conjugate to H_g^+ are precisely the subgroups $H_{g'}^+$ where g' is conjugate to g.

For any $d \in K^\times$ let $t\colon E \to E^d$ be an isomorphism defined over $K(\sqrt{d})$. Then for any $P \in E$ and any $\sigma \in G_K$ we have

$$\sigma(t(P)) = \chi_d(\sigma)t(\sigma(P))$$

where $\chi_d\colon G_K \to \{\pm 1\}$ is the quadratic character attached to $K(\sqrt{d})/K$. Fix a basis for $E[N]$ and use t to choose a compatible basis for $E^d[N]$. Then for any $\sigma \in G_K$ we have that

$$\bar{\rho}_{E^d,N}(\sigma) = \chi_d(\sigma)\bar{\rho}_{E,N}(\sigma). \tag{2.1}$$

Suppose that $\phi = t \circ g'\colon E[N] \to E^d[N]$ is an N-congruence between E and its quadratic twist E^d, where $g' \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is conjugate to g. Note that $g'\,\bar{\rho}_{E,N}(\sigma)\,(g')^{-1} = \bar{\rho}_{E^d,N}(\sigma) = \pm\bar{\rho}_{E,N}(\sigma)$ for all $\sigma \in G_K$. Thus the image of $\bar{\rho}_{E,N}$ is contained in a subgroup conjugate to H_g^+.

Conversely, suppose that the image of $\bar{\rho}_{E,N}$ is contained in $H_{g'}^+$ where g' is conjugate to g. Take $d \in K^\times$ so that $G_{K(\sqrt{d})} = \bar{\rho}_{E,N}^{-1}(H_{g'})$. Then by (2.1) we have

$$g'\,\bar{\rho}_{E,N}(\sigma)\,(g')^{-1} = \chi_d(\sigma)\bar{\rho}_{E,N}(\sigma) = \bar{\rho}_{E^d,N}(\sigma) \quad \text{for all } \sigma \in G_K.$$

Thus $t \circ g'$ gives an N-congruence between E and E^d.

Finally note that $t|_{E[N]}$ preserves the Weil pairing. Therefore

$$e_{E^d,N}(\phi^{-1}(P), \phi^{-1}(Q)) = e_{E^d,N}(t(P), t(Q))^{\det(g)} = e_{E,N}(P, Q)^{\det(g)}.$$

Hence ϕ has power $\det(g)$, as required. □

Let p be a prime number and $l \geq 1$ be an integer. If p is odd let $\xi \in \mathbb{Z}$ be a quadratic non-residue

modulo p. Define $g_{\mathrm{s}}, g_{\mathrm{ns}} \in \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ to be the matrices

$$g_{\mathrm{s}} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$$
$$g_{\mathrm{ns}} = \begin{cases} \left(\begin{smallmatrix} 1 & -2 \\ 2 & -1 \end{smallmatrix}\right) & \text{if } p = 2, \text{ and} \\ \left(\begin{smallmatrix} 0 & \xi \\ 1 & 0 \end{smallmatrix}\right) & \text{if } p \text{ is odd.} \end{cases}$$

The following lemmas give a precise relationship between X_g and X_g^+ and the modular curves $X(\mathrm{ns}\, p^l)$ and $X(\mathrm{ns}\, p^{l^+})$.

Lemma 2.2.12. *Let p be a prime number and $l \geq 1$ be an integer. Let $\pi\colon \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p^{l-1}\mathbb{Z})$ denote the natural reduction map. Then*

$$H_{g_{\mathrm{s}}} = \begin{cases} \pi^{-1}G(\mathrm{s}\, 2^{l-1}) & \text{if } p = 2, \text{ and} \\ G(\mathrm{s}\, p^l) & \text{otherwise,} \end{cases} \qquad H^+_{g_{\mathrm{s}}} = \begin{cases} \pi^{-1}G(\mathrm{s}\, 2^{l-1^+}) & \text{if } p = 2, \text{ and} \\ G(\mathrm{s}\, p^{l^+}) & \text{otherwise,} \end{cases}$$

and

$$H_{g_{\mathrm{ns}}} = \begin{cases} \pi^{-1}G(\mathrm{ns}\, 2^{l-1}) & \text{if } p = 2, \text{ and} \\ G(\mathrm{ns}\, p^l) & \text{otherwise,} \end{cases} \qquad H^+_{g_{\mathrm{ns}}} = \begin{cases} \pi^{-1}G(\mathrm{ns}\, 2^{l-1^+}) & \text{if } p = 2, \text{ and} \\ G(\mathrm{ns}\, p^{l^+}) & \text{otherwise.} \end{cases}$$

Proof. First suppose that p is odd. Note that g_{s} commutes with the elements of $G(\mathrm{s}\, p^l)$ since $G(\mathrm{s}\, p^l)$ is abelian and $g_{\mathrm{s}} \in G(\mathrm{s}\, p^l)$. Similarly g_{ns} commutes with the elements of $G(\mathrm{ns}\, p^l)$ since $g_{\mathrm{ns}} \in G(\mathrm{ns}\, p^l)$. Conversely, if $g_{\mathrm{s}}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) g_{\mathrm{s}}$ then $b = -b$ and $c = -c$. Since p is odd $b = c = 0$, hence $H_{g_{\mathrm{s}}} = G(\mathrm{s}\, p^l)$. A similar calculation shows that $H_{g_{\mathrm{ns}}} = G(\mathrm{ns}\, p^l)$.

Now $\pi^{-1}G(\mathrm{s}\, 2^{l-1})$ contains $G(\mathrm{s}\, 2^l)$ as an abelian subgroup of index 4. Moreover, $\pi^{-1}G(\mathrm{s}\, 2^{l-1})$ is generated by $G(\mathrm{s}\, 2^l)$ and the matrices of the form $I + 2^{l-1}M$. But since g_{s} is contained in $G(\mathrm{s}\, 2^l)$ it commutes with the elements of $G(\mathrm{s}\, 2^l)$. Note that $g_{\mathrm{s}}^{-1}(I + 2^{l-1}M)g_{\mathrm{s}} = I + 2^{l-1}g_{\mathrm{s}}^{-1}Mg_{\mathrm{s}}$ depends only on $g_{\mathrm{s}} \equiv I$ modulo 2. Thus g_{s} commutes with the elements of $\pi^{-1}G(\mathrm{s}\, 2^{l-1})$.

Similarly g_{ns} is contained in $G(\mathrm{ns}\, 2^l)$ and $g_{\mathrm{ns}} \equiv I \pmod 2$, hence g_{ns} commutes with elements of $\pi^{-1}G(\mathrm{ns}\, 2^{l-1})$. As in the odd prime case, a direct calculation shows that $H_{g_{\mathrm{s}}} = \pi^{-1}G(\mathrm{s}\, 2^{l-1})$ and $H_{g_{\mathrm{ns}}} = \pi^{-1}G(\mathrm{ns}\, 2^{l-1})$.

To see the analogous result for H_g^+, note that the index of H_g in H_g^+ is at most 2. It therefore suffices to show that there exists an element $h \in G(\mathrm{s}\, p^{l^+}) \backslash G(\mathrm{s}\, p^l)$ (respectively $G(\mathrm{ns}\, p^{l^+}) \backslash G(\mathrm{ns}\, p^l)$) such that $g_{\mathrm{s}}^{-1}hg_{\mathrm{s}} = -h$ (respectively $g_{\mathrm{ns}}^{-1}hg_{\mathrm{ns}} = -h$).

For all p we have $g_{\mathrm{s}}^{-1}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)g_{\mathrm{s}} = -\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Similarly when p is odd $g_{\mathrm{ns}}^{-1}\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)g_{\mathrm{ns}} = -\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and when $p = 2$ we have $g_{\mathrm{ns}}^{-1}\left(\begin{smallmatrix} 1 & -1 \\ 0 & -1 \end{smallmatrix}\right)g_{\mathrm{ns}} = -\left(\begin{smallmatrix} 1 & -1 \\ 0 & -1 \end{smallmatrix}\right)$. □

Lemma 2.2.13. *Let N be an integer. Let $\tilde{N} = N/2$ if N is even and $\tilde{N} = N$ if N is odd. If N is a prime power then the modular curves X_g and X_g^+ are respectively isomorphic to*

(i) *$X(\mathrm{s}\, \tilde{N})$ and $X(\mathrm{s}\, \tilde{N}^+)$ if $g = g_{\mathrm{s}}$, and*

(ii) *$X(\mathrm{ns}\, \tilde{N})$ and $X(\mathrm{ns}\, \tilde{N}^+)$ if $g = g_{\mathrm{ns}}$.*

More generally let $N = p_1^{l_1} \cdots p_n^{l_n}$ and $\tilde{N} = p_1^{\tilde{l}_1} \cdots p_n^{\tilde{l}_n}$ be the factorisations of N and $\tilde{N}$ into distinct prime powers. Fix compatible isomorphisms $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{i=1}^n \mathrm{GL}_2(\mathbb{Z}/p_i^{l_i}\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/\tilde{N}\mathbb{Z}) \cong \prod_{i=1}^n \mathrm{GL}_2(\mathbb{Z}/p_i^{\tilde{l}_i}\mathbb{Z})$.

Let $H = \prod_{i=1}^n H_i \subset \mathrm{GL}_2(\mathbb{Z}/\tilde{N}\mathbb{Z})$ be a subgroup and $g = (g_1, ..., g_n) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be an element such that for each i either $g_i = g_{\mathrm{s}}$ and $H_i = G(\mathrm{s}\, p_i^{\tilde{l}_i})$ or $g_i = g_{\mathrm{ns}}$ and $H_i = G(\mathrm{ns}\, p_i^{\tilde{l}_i})$. Then X_g

is isomorphic to the modular curve $X(H) = X(H_1, ..., H_n)$. In this case the modular curve X_g^+ is isomorphic to the quotient of $X_g \cong X(H_1, ..., H_n)$ by the involution which acts diagonally on the fibre product.

Proof. The prime power case follows immediately from Lemma 2.2.12. For the second claim, note first that by Lemma 2.2.12 we have $H_g = H$, so $X_g \cong X(H)$. Moreover, for each i, the image of H_g^+ under the reduction modulo $p_i^{\tilde{l}_i}$ map $\mathrm{GL}_2(\mathbb{Z}/p_i^{l_i}\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p_i^{\tilde{l}_i}\mathbb{Z})$ is equal to H_i^+ (in obvious notation). We have strict containments $H_i \subset H_i^+$ for every i, so the involution on X_g induced by the containment $H_g \subset H_g^+$ acts non-trivially on each component of the fibre product $X_g \cong X(H_1) \times_{X(1)} \cdots \times_{X(1)} X(H_n)$. □

Remark 2.2.14. We make a few brief comments on Lemma 2.2.13:

(i) If E/K is an elliptic curve then $\bar{\rho}_{E,\tilde{N}}(G_K) \subset G(\mathrm{s}\,\tilde{N})$ if and only if E admits two cyclic $\tilde{N}$-isogenies over K. Consider a cyclic $\tilde{N}^2$ isogeny $\phi\colon E \to E'$ and decompose ϕ as a composition of cyclic $\tilde{N}$-isogenies $\phi = \psi_1\psi_2$. Letting F denote the image of ψ_1, we obtain the well known isomorphism

$$\begin{aligned} X_0(\tilde{N}^2) &\to X(\mathrm{s}\,\tilde{N}) \\ (E, \phi) &\mapsto (F, \hat{\psi_1}, \psi_2) \end{aligned}$$

for each $\tilde{N}$ (cf. [BPR13, Section 2.4] or [Hal21, Théorème II.4.3]). Lemma 2.2.13 therefore implies that if $g \equiv g_{\mathrm{s}} \pmod{p^l}$ for each prime power $p^l | N$, then $X_g \cong X_0(\tilde{N}^2)$. In this case it is easy to verify that the diagonal involution on the fibre product agrees with the Fricke involution on $X_0(\tilde{N}^2)$, and therefore $X_g^+ \cong X_0^+(\tilde{N}^2)$.

(ii) As in Lemma 2.2.13 let $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be so that for each prime power $p^k | N$ either $g \equiv g_{\mathrm{s}}$ or $g_{\mathrm{ns}} \pmod{p^k}$. In this case the (reduction modulo $\tilde{N}$ of the) subgroup H_g^+ is known by some authors (e.g., the LMFDB's modular curves database [LMFDB], see `https://www.lmfdb.org/knowledge/show/gl2.cartan`) as an *extended Cartan subgroup of* $\mathrm{GL}_2(\mathbb{Z}/\tilde{N}\mathbb{Z})$.

2.2.8 Generalised elliptic curves

Let N be a positive integer and let K be a field of characteristic coprime to N. For a (possibly not irreducible) curve C/K we write $C^{\mathrm{sm}} \subset C$ for the subvariety whose $\overline{K}$-points are the smooth points of C.

Definition 2.2.15. For each integer $N \geq 2$, we define the *standard N-gon* $\mathcal{E}_N$ (over K) by gluing the points (∞, i) and $(0, i+1)$ on $\mathbb{P}^1_K \times \mathbb{Z}/N\mathbb{Z}$ for each $i \in \mathbb{Z}/N\mathbb{Z}$. When $N = 1$, we define $\mathcal{E}_1$ to be the nodal cubic curve over K.

Informally, for $N \geq 2$, the variety $\mathcal{E}_N$ consists of N copies of $\mathbb{P}^1_K$, indexed by elements $i \in \mathbb{Z}/N\mathbb{Z}$, and such that the i^{th}-component intersects only the $(i \pm 1)^{\mathrm{th}}$-components and meets them with multiplicity 1. That is, when $N \geq 2$, the variety $\mathcal{E}_N$ resembles an N-gon.

We denote the smooth subscheme of $\mathcal{E}_N$ by $\mathcal{E}_N^{\mathrm{sm}}$. The variety $\mathcal{E}_N^{\mathrm{sm}}$ is obtained from $\mathcal{E}_N$ by deleting the points of intersection between the copies of $\mathbb{P}^1_K$ in $\mathcal{E}_N$ (see Figure 2.1). Indeed, we have a K-isomorphism $\mathcal{E}_N^{\mathrm{sm}} \cong \mathbb{G}_m \times \mathbb{Z}/N\mathbb{Z}$ and therefore $\mathcal{E}_N^{\mathrm{sm}}$ inherits the structure of a group variety (and this extends to an action of $\mathcal{E}_N^{\mathrm{sm}}$ on $\mathcal{E}_N$).

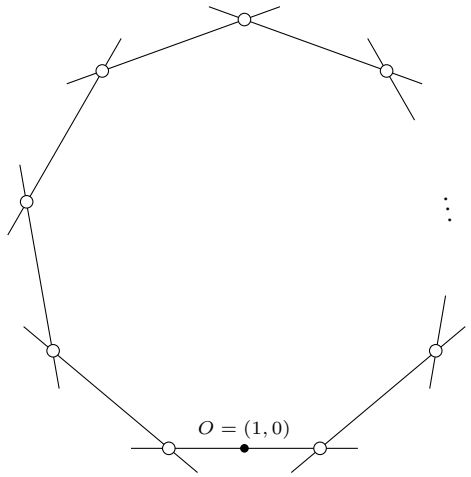


FIGURE 2.1: The smooth locus, $\mathcal{E}_N^{\mathrm{sm}}$, of the standard N-gon.

Definition 2.2.16. A *generalised elliptic curve* over a field K is a triple $(E, O, +)$, where E/K is either isomorphic to a smooth projective irreducible curve of genus 1 or an N-gon for some integer $N \geq 1$, $O \in E^{\mathrm{sm}}(K)$ is a smooth K-rational point, and $+\colon E^{\mathrm{sm}} \times E \to E$ is a morphism which equips E^{sm} with the structure of a group variety with identity O.

As with elliptic curves, we will write E/K for a generalised elliptic curve over K with the identity and group law suppressed. If $\mathcal{E}_N/K$ is the standard N-gon we write $\mathcal{E}_N[N] = \mathcal{E}_N^{\mathrm{sm}}[N]$, and equip $\mathcal{E}_N[N] \cong \mu_N \times \mathbb{Z}/N\mathbb{Z}$ with the structure of a symplectic abelian group as in Example 2.1.3.

The following lemma is simple to prove.

Lemma 2.2.17. *The automorphism group of the generalised elliptic curve $\mathcal{E}_N$ is isomorphic to D_N, the dihedral group with $2N$ elements. More precisely choosing an isomorphism of group varieties $\mathcal{E}_N^{\mathrm{sm}} \cong \mathbb{G}_m \times \mathbb{Z}/N\mathbb{Z}$ induces an isomorphism*

$$\mathrm{Aut}(\mathcal{E}_N) \cong G_\infty = \left\{ \begin{pmatrix} \pm 1 & \alpha \\ 0 & \pm 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : \alpha \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

Here, the action of $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right) \in G_\infty$ on $\mathcal{E}_N^{\mathrm{sm}}$ is given by $(x, i) \mapsto (\zeta^{i\alpha} x, i)$ for some fixed primitive N^{th}-root of unity ζ.

Definition 2.2.18. Let $N \geq 1$ be an integer. An *N-congruence of generalised elliptic curves* is an isomorphism $\phi\colon E[N] \to E'[N]$ where E/K and E'/K are generalised elliptic curves which are either smooth or N-gons.

In this work, we will need moduli interpretations for the cusps on the modular curves $X(N)$ and $X_\mu(N)$.

Proposition 2.2.19. *The K-rational points on the modular curve $X(N)$ are in bijective correspondence with isomorphism classes of pairs (E, ι) where E/K is a generalised elliptic curve and $\iota\colon E[N] \to \mu_N \times \mathbb{Z}/N\mathbb{Z}$ is an isomorphism of symplectic abelian group varieties, such that the image of ι^{-1} meets every irreducible component of E.*

In particular the cusps on $X(N)$ are in bijective correspondence with isomorphism classes of symplectic isomorphisms $\iota\colon \mathcal{E}_N[N] \to \mu_N \times \mathbb{Z}/N\mathbb{Z}$. That is, symplectic isomorphisms, ι, defined up to pre-composition with an element of $\mathrm{Aut}(\mathcal{E}_N)$.

Proof. This is [DR73, V.4.4]. □

Proposition 2.2.20. *The K-rational points on the modular curve $X_\mu(N)$ are in bijective correspondence with isomorphism classes of pairs (E, ι) where E/K is a generalised elliptic curve which is isomorphic to either an elliptic curve or an N-gon, together with an embedding $\iota\colon \mu_N \hookrightarrow E[N]$.*

In particular the cusps on $X_\mu(N)$ are in bijective correspondence with isomorphism classes of embedding $\iota\colon \mu_N \hookrightarrow \mathcal{E}_N[N]$. That is, embeddings ι, defined up to pre-composition with an element of $\mathrm{Aut}(\mathcal{E}_N)$.

Proof. This follows immediately by taking the Cartier dual of the moduli interpretation for $X_1(N)$ in [DR73, Construction 4.14]. □

2.2.9 The yoga of twisting and $X_M(N)$

We follow [PSS07, Section 4.4]. Consider a symplectic abelian group M/K together with a fixed $\overline{K}$-isomorphism of symplectic abelian groups $\iota\colon M \cong \mu_N \times \mathbb{Z}/N\mathbb{Z}$. Recall that we write Υ_N for the group of symplectic automorphisms of $\mu_N \times \mathbb{Z}/N\mathbb{Z}$. By the twisting principle ι gives rise to a Galois cohomology class $[\iota] \in H^1(K, \Upsilon_N)$.

The G_K-equivariant homomorphism $\Upsilon_N \to \mathrm{Aut}(X(N)_{\overline{K}})$ induces a map on Galois cohomology $H^1(K, \Upsilon_N) \to H^1(K, \mathrm{Aut}(X(N)_{\overline{K}}))$. Once again by the twisting principle we may associate to the image of $[\iota]$ a twist $X_M(N)/K$ of $X(N)$. We have:

Lemma 2.2.21. *For each field L/K the non-cuspidal L-rational points on the twist $X_M(N)$ parametrise pairs (E, ϕ) where E/L is an elliptic curve and $\phi\colon E[N] \to M$ is an L-isomorphism of symplectic groups with power 1, up to pre-composition with an automorphism of E (and up to quadratic twist if $N = 1, 2$).*

Let M_r denote the symplectic abelian group $(M, \langle\cdot,\cdot\rangle^r)$ obtained by equipping M with the r^{th}-power of its pairing. We write $X_M^r(N)$ for the twist $X_{M_r}(N)$.

A specific case which we will be particularly interested in is when E/K is an elliptic curve and $(M, \langle\cdot,\cdot\rangle)$ is the symplectic abelian group $(E[N], e_{E,N})$. In this case we write $X_E^r(N)$ for the twisted modular curve $X_M^r(N)$. By Lemma 2.2.21, if $N \geq 3$ then for each field L/K the non-cuspidal L-rational points on $X_E^r(N)$ parametrise pairs (E', ϕ) where $\phi\colon E[N] \to E'[N]$ is an (N, r)-congruence of elliptic curves.

2.3 Hilbert modular surfaces

We give a uniform treatment of Hilbert modular surfaces attached to quadratic orders of positive discriminant $D \equiv 0, 1 \pmod 4$. In particular we unify the "modular diagonal quotient surfaces" of Hermann [Her91] and Kani–Schanz [KS98] and (a generalisation of) Kumar's [Kum15] "Hilbert modular surfaces of square discriminant". It seems likely to us that the results in this section are known to experts. For example, Hermann refers to their surfaces as "Hilbertsche Modulflächen quadratischer Diskriminante" (Hilbert modular surfaces of square discriminant), but does not give precise reasoning for this. Carlton [Car01, Sections 2 and 7] gives a more in-depth discussion of this phenomenon (relating the constructions in [Her91] and [KS98] to quotients of the upper half plane), and also gives a nice description of the adelic viewpoint which we will not discuss here. We have not been able to find a complete treatment in the literature, and hope this exposition will prove valuable.

Much of our treatment follows closely that of van der Geer's book on Hilbert modular surfaces [vdG88] (see also [EK14]). The construction of Hilbert modular surfaces attached to quadratic

orders of square discriminant generalises and closely follows [McM07] and [Kum15]. The case when the congruences parametrised are anti-symplectic with respect to the Weil pairing (the surfaces $Y_-(N^2)$ and $Z_{N,-1}$) may be found in both [McM07] and [Kum15, Section 2.2].

2.3.1 Quadratic orders

Let $\mathcal{O}_D$ be the quadratic order of discriminant $D > 0$. More explicitly, either

(A) the discriminant $D \equiv 0, 1 \pmod 4$ is not a square and $\mathcal{O}_D$ is an order in a real quadratic field, or

(B) the discriminant $D = N^2$ is a square and we fix an isomorphism

$$\mathcal{O}_D \cong \{(a_1, a_2) \subset \mathbb{Z}^2 : a_1 \equiv a_2 \mod N\}.$$

In both cases we write $F_D = \mathcal{O}_D \otimes \mathbb{Q}$. There are two obvious ring homomorphisms $\sigma\colon F_D \to \mathbb{R}$ and $\sigma'\colon F_D \to \mathbb{R}$ (when D is not a square these are the real embeddings of F_D and when $D = N^2$ these are the projections onto the factors of $F_D \cong \mathbb{Q} \times \mathbb{Q}$). We say that an element $\lambda \in F_D$ is *totally positive* if $\sigma(\lambda) > 0$ and $\sigma'(\lambda) > 0$.

Denote by $\mathrm{I}(\mathcal{O}_D)$ the set of invertible (i.e., finitely generated, projective, rank 1) $\mathcal{O}_D$-modules $\mathfrak{a} \subset F_D$. Equip $\mathrm{I}(\mathcal{O}_D)$ with the structure of an abelian group by declaring $\mathfrak{a} \cdot \mathfrak{b}$ to be the product of $\mathfrak{a}$ and $\mathfrak{b}$ as submodules of F_D. Write $\mathrm{P}^+(\mathcal{O}_D)$ for the subgroup of $\mathrm{I}(\mathcal{O}_D)$ consisting of invertible $\mathcal{O}_D$-modules of the form $\lambda\mathcal{O}_D$ for some totally positive $\lambda \in F_D$.

Definition 2.3.1. The *narrow class group* $\mathrm{Cl}^+(\mathcal{O}_D)$ of $\mathcal{O}_D$ is the group $\mathrm{I}(\mathcal{O}_D)/\mathrm{P}^+(\mathcal{O}_D)$. We say that two $\mathcal{O}_D$-modules $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}(\mathcal{O}_D)$ are in the same *genus* if they have the same image $\mathfrak{A} \in \mathrm{Cl}^+(\mathcal{O}_D)/(\mathrm{Cl}^+(\mathcal{O}_D))^2$. In this case $\mathfrak{A}$ is said to be the *genus* of $\mathfrak{a}$ (and $\mathfrak{b}$).

The following lemma gives a complete and explicit characterisation of the narrow class group of the quadratic order $\mathcal{O}_{N^2}$.

Lemma 2.3.2. *When $D = N^2$ is a square there exists a group isomorphism $(\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Cl}^+(\mathcal{O}_D)$ given by $r \mapsto [\mathfrak{a}_{\tilde{r}}]$ where $\tilde{r} \in \mathbb{Z}_{>0}$ is a positive integer chosen such that $\tilde{r} \equiv r \pmod N$ and $\mathfrak{a}_{\tilde{r}}$ is the invertible $\mathcal{O}_D$-module $\tilde{r}\mathbb{Z} + (N, 0)\mathbb{Z} \subset \mathcal{O}_D$.*

Proof. Suppose that n, m are positive integers coprime to N, such that $n \equiv m \pmod N$. Note that

$$\begin{aligned}\frac{(m,n)}{m}\mathfrak{a}_m &= (m,n)\mathbb{Z} + (N,0)\mathbb{Z} \\ &= n\mathbb{Z} + (N,0)\mathbb{Z} = \mathfrak{a}_n.\end{aligned}$$

Note that here (m, n) is an element of $\mathcal{O}_D$, not a greatest common divisor. In particular the map $\mathbb{Z}_{>0} \to \mathrm{I}(\mathcal{O}_D)$ given by $n \mapsto \mathfrak{a}_n$ descends to a well defined map $\varphi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathrm{Cl}^+(\mathcal{O}_D)$. For any $n, m \in \mathbb{Z}_{>0}$ coprime to N we have $\mathfrak{a}_n\mathfrak{a}_m = \mathfrak{a}_{nm}$, so φ is a group homomorphism.

To see that φ is an isomorphism we construct an explicit inverse following the standard approach for binary quadratic forms (see e.g., [Coh93, Section 5.2]). Let $\mathfrak{a} \in \mathrm{I}(\mathcal{O}_D)$ be an invertible $\mathcal{O}_D$-module and let ω_1, ω_2 be a $\mathbb{Z}$-basis for $\mathfrak{a}$. Since $\mathfrak{a}$ is invertible, the binary quadratic form $f(x, y) = \mathrm{Nm}_{F_D/\mathbb{Q}}(\omega_1 x + \omega_2 y)/\mathrm{Nm}(\mathfrak{a})$ is a primitive form of discriminant N^2. In particular $f(x, y)$ is $\{\pm 1\} \times \mathrm{SL}_2(\mathbb{Z})$-equivalent to a form $nx^2 + Nxy$ for some $n \geq 1$ coprime to N. Moreover the $\{\pm 1\} \times \mathrm{SL}_2(\mathbb{Z})$-orbit of $f(x, y)$ is independent of both the choice of basis for $\mathfrak{a}$ and the choice of representative for

the class $[\mathfrak{a}] \in \mathrm{Cl}^+(\mathcal{O}_D)$. It is then easy to check that the map $\mathrm{Cl}^+(\mathcal{O}_D) \to (\mathbb{Z}/N\mathbb{Z})^\times$ given by $[\mathfrak{a}] \mapsto n \pmod N$ is an inverse to φ. □

Remark 2.3.3. As indicated by the proof, Lemma 2.3.2 has an interpretation in terms of primitive binary quadratic forms of discriminant N^2. If $f(x,y)$ is a primitive binary quadratic form of discriminant $D = N^2$ then $f(x,y)$ is $\{\pm 1\} \times \mathrm{SL}_2(\mathbb{Z})$-equivalent to a form $nx^2 + Nxy$ where $n \in \mathbb{Z}_{>0}$ is coprime to N. If we define $\sqrt{D} \in \mathcal{O}_D$ to be the element $(N, -N)$ then the usual association between binary quadratic forms and ideal classes reduces to $f(x,y) \mapsto n\mathbb{Z} + \frac{N+\sqrt{D}}{2}\mathbb{Z} = \mathfrak{a}_n$.

Remark 2.3.4. When $D = N^2$ is a perfect square Kumar [Kum15] defines an invertible $\mathcal{O}_D$-module $\mathcal{O}_D^* = \frac{1}{N}(1,-1)\mathcal{O}_D$. Note that

$$(N, N(N-1))\mathcal{O}_D^* = (-1, N-1)\mathbb{Z} + (N,0)\mathbb{Z} = \mathfrak{a}_{N-1}$$

hence $\mathcal{O}_D^*$ and $\mathfrak{a}_{N-1}$ define the same narrow class in $\mathrm{Cl}^+(\mathcal{O}_D)$.

Given an invertible $\mathcal{O}_{N^2}$-module $\mathfrak{a}_n \subset F_{N^2}$ it is simple to check that in $\mathrm{I}(\mathcal{O}_{N^2})$ we have

$$\mathfrak{a}_n^{-1} = \left\{ \frac{1}{n}(na, a') : (na, a') \in \mathcal{O}_{N^2} \right\} \subset F_{N^2}. \tag{2.2}$$

2.3.2 The Hilbert modular group for quadratic orders

Let $\mathfrak{a}$ be an invertible $\mathcal{O}_D$-module. We define the group

$$\mathrm{SL}_2(\mathcal{O}_D, \mathfrak{a}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(F_D) : a, d \in \mathcal{O}_D, b \in \mathfrak{a}^{-1}, c \in \mathfrak{a} \right\},$$

and similarly $\mathrm{PSL}_2(\mathcal{O}_D, \mathfrak{a}) = \mathrm{SL}_2(\mathcal{O}_D, \mathfrak{a})/\{\pm 1\}$. The homomorphisms σ and σ' allow us to define an injective homomorphism

$$\mathrm{SL}_2(\mathcal{O}_D, \mathfrak{a}) \hookrightarrow \mathrm{GL}_2^+(\mathbb{R}) \times \mathrm{GL}_2^+(\mathbb{R})$$

given by $A \mapsto (\sigma(A), \sigma'(A))$. The image of this homomorphism, which we denote by $\Gamma(\mathcal{O}_D, \mathfrak{a})$ is called the *generalised Hilbert modular group*, or simply the *Hilbert modular group* in the case when $\mathfrak{a} = \mathcal{O}_D$. Write $\mathbb{H}^2 = \mathbb{H} \times \mathbb{H}$.

Proposition 2.3.5. *The isomorphism class of the quotient $\Gamma(\mathcal{O}_D, \mathfrak{a})\backslash\mathbb{H}^2$ depends only on the genus, $\mathfrak{A}$, of $\mathfrak{a}$. In particular, when $D = N^2$ is a square the isomorphism class of the surface $\Gamma(\mathcal{O}_{N^2}, \mathfrak{a}_{\tilde{r}})\backslash\mathbb{H}^2$ depends only on $r \in (\mathbb{Z}/N\mathbb{Z})^\times$ modulo squares.*

We call the complex manifold $\Gamma(\mathcal{O}_D, \mathfrak{a})\backslash\mathbb{H}^2$ a Hilbert modular surface[3] *of discriminant D and genus $\mathfrak{A}$. By abuse of notation we often replace the genus $\mathfrak{A}$ by the invertible $\mathcal{O}_D$-module $\mathfrak{a}$.*

Proof. Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are invertible $\mathcal{O}_D$-modules of the same genus. Write $\mathfrak{a} = \lambda\mathfrak{c}^2\mathfrak{b}$ where $\mathfrak{c}$ is an invertible $\mathcal{O}_D$-module and $\lambda \in F_D$ is a totally positive element. Following [vdG88, p.12] let g be any element of

$$\begin{pmatrix} \mathfrak{c} & \mathfrak{a}^{-1}\mathfrak{c}^{-1} \\ \mathfrak{a}\mathfrak{c} & \mathfrak{c} \end{pmatrix}$$

[3] As is standard in the literature (cf. [vdG88, p. 44]) we will remain ambiguous about whether a Hilbert modular surface refers directly to the quotient of $\mathbb{H}^2$, or another (possibly non-compact) birationally equivalent algebraic surface (for example its compactification(s) and desingularisation(s)). Indeed, we will refer to any complex algebraic surface in the birational equivalence class of $\Gamma(\mathcal{O}_D, \mathfrak{a})\backslash\mathbb{H}^2$ as a Hilbert modular surface of discriminant D and genus $\mathfrak{A}$.

with determinant 1. Conjugating by $h = \left(\begin{smallmatrix}\lambda & 0\\ 0 & 1\end{smallmatrix}\right)g$ gives an isomorphism $\mathrm{SL}_2(\mathcal{O}_D, \mathfrak{b}) \to \mathrm{SL}_2(\mathcal{O}_D, \mathfrak{a})$ which induces an isomorphism $\phi\colon \Gamma(\mathcal{O}_D, \mathfrak{b}) \to \Gamma(\mathcal{O}_D, \mathfrak{a})$. Let ψ be the automorphism of $\mathbb{H}^2$ given by $(z, z') \mapsto (\sigma(h)z, \sigma'(h)z')$, then we have a commutative diagram

$$\begin{array}{ccc} \Gamma(\mathcal{O}_D, \mathfrak{b}) \times \mathbb{H}^2 & \longrightarrow & \mathbb{H}^2 \\ \downarrow{\scriptstyle \phi\times\psi} & & \downarrow{\scriptstyle \psi} \\ \Gamma(\mathcal{O}_{N^2}, \mathfrak{a}) \times \mathbb{H}^2 & \longrightarrow & \mathbb{H}^2 \end{array}$$

which induces an isomorphism between the quotients. The second claim follows from the isomorphism

$$\mathrm{Cl}^+(\mathcal{O}_{N^2})/(\mathrm{Cl}^+(\mathcal{O}_{N^2}))^2 \cong (\mathbb{Z}/N\mathbb{Z})^\times/((\mathbb{Z}/N\mathbb{Z})^\times)^2$$

given by Lemma 2.3.2. □

It can be shown (see [vdG88, I.5] and [KS97, Section 2.1]) that the (non-compact) complex manifold $\Gamma(\mathcal{O}_D, \mathfrak{a})\backslash\mathbb{H}^2$ is non-singular outside a finite number of *elliptic fixed points* which are cyclic quotient singularities (see Section 2.4.2) of order at most 6.

2.3.3 Compactifications

Since the complex manifold $\Gamma(\mathcal{O}_D, \mathfrak{a})\backslash\mathbb{H}^2$ is the quotient of a Hermitian locally symmetric space by a semi-simple linear algebraic group it admits a *Bailey–Borel compactification* (see e.g., [AMRT10, Section 6.1]).

It will be necessary for us to distinguish between the cases when D is and is not a perfect square. The Bailey–Borel compactification in the case of fundamental discriminants is given by adding finitely many points of $\Gamma(\mathcal{O}_D, \mathfrak{a})\backslash\mathbb{H}^2$. Conversely it is clear when $D = 1$ that $\Gamma(\mathcal{O}_1, \mathfrak{a}) \cong \mathrm{SL}_2(\mathbb{Z})^2$, hence $\Gamma(\mathcal{O}_1, \mathfrak{a})\backslash\mathbb{H}^2 \cong \mathbb{A}^2(\mathbb{C})$ does not admit a compactification by finitely many points. We will see that this persists whenever $D = N^2$ is a perfect square.

In the remainder of this section we give explicit descriptions of compactifications of Hilbert modular surfaces (focusing mainly on the case when $D = N^2$).

A compactification when D is not a perfect square

Suppose that F_D is a real quadratic field and let $\Gamma = \Gamma(\mathcal{O}_D, \mathfrak{a})$. The non-compact complex surface $\Gamma\backslash\mathbb{H}^2$ admits a compactification (in the category of complex manifolds) whose $\mathbb{C}$-points are given by $\Gamma\backslash\mathbb{H}^2 \cup \Gamma\backslash\mathbb{P}^1(F_D)$ (see [vdG88, Section II.7]). This projective surface (which is often given as the simplest non-curve-example of the Bailey–Borel compactification) is singular at the elliptic points and the cusps. We denote its minimal desingularisation by $Y_{\mathfrak{a}}(D)$ (an explicit description of the resolution cycles at the cusps was given by Hirzebruch [Hir53, Hir71] see [vdG88, Section II.6]).

A compactification when D is a perfect square

Now suppose that $D = N^2$ is a square. In Lemma 2.3.2 we associated to each $r \in (\mathbb{Z}/N\mathbb{Z})^\times$ a well defined narrow class $[\mathfrak{a}_{\tilde{r}}]$. We will show that for each integer $r \in (\mathbb{Z}/N\mathbb{Z})^\times$ the surface $\Gamma(\mathcal{O}_{N^2}, \mathfrak{a}_{\tilde{r}})\backslash\mathbb{H}^2$ is isomorphic to an open subvariety of a compact "modular diagonal quotient surface" considered by Kani–Schanz [KS98] (the same surfaces are considered by Hermann [Her91], though in their terminology these *are* "Hilbertsche Modulflächen quadratischer Diskriminante").

Recall that we denote[4] by $Y(N)$ the non-compact modular curve of full level N and $X(N)$ its smooth compactification. Recall that the $\mathbb{C}$-points of $Y(N)$ are given by $\Gamma(N)\backslash\mathbb{H}$.

Let $\varepsilon \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a matrix of determinant $r \in (\mathbb{Z}/N\mathbb{Z})^\times$. We consider the subgroup $\Delta_\varepsilon \subset \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ given by

$$\Delta_\varepsilon = \{(g, \varepsilon g \varepsilon^{-1}) : g \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\}.$$

Definition 2.3.6. For each positive integer N and integer $r \in (\mathbb{Z}/N\mathbb{Z})^\times$ we define the *modular diagonal quotient surface* $Z_{N,r}$ to be the quotient $\Delta_\varepsilon\backslash(X(N) \times X(N))$.

Note that if $\varepsilon' \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ also has determinant r then the quotient surfaces $\Delta_\varepsilon\backslash(X(N) \times X(N))$ and $\Delta_{\varepsilon'}\backslash(X(N)\times X(N))$ are isomorphic, hence the isomorphism class of $Z_{N,r}$ is independent of the choice of matrix ε. We therefore fix the matrix $\varepsilon_r = \left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and define $\Delta_r := \Delta_{\varepsilon_r}$.

The following proposition shows that modular diagonal quotient surfaces are (compactifications of) Hilbert modular surfaces of discriminant N^2. The proof is closely related to [Car01, Section 2].

Proposition 2.3.7. *For each $r \in (\mathbb{Z}/N\mathbb{Z})^\times$ and each positive $\tilde{r} \in \mathbb{Z}_{>0}$ such that $\tilde{r} \equiv r \pmod N$ the surfaces $\Delta_r\backslash(Y(N) \times Y(N))(\mathbb{C})$ and $\Gamma(\mathcal{O}_{N^2}, \mathfrak{a}_{\tilde{r}})\backslash\mathbb{H}^2$ are isomorphic as complex manifolds, where $\mathfrak{a}_{\tilde{r}}$ is the invertible $\mathcal{O}_{N^2}$-module defined in Lemma 2.3.2.*

Proof. Consider the group

$$\Gamma_r := \left\{(A, A') \in \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) : A' \equiv \varepsilon_r A \varepsilon_r^{-1} \mod N\right\}.$$

Note that we have an exact sequence of groups

$$1 \longrightarrow \Gamma(N) \times \Gamma(N) \longrightarrow \Gamma_r \longrightarrow \Delta_r \longrightarrow 1$$

where the homomorphism $\Gamma_r \to \Delta_r$ is given by reduction modulo N. We then obtain an isomorphism of quotients $\Delta_r\backslash(Y(N) \times Y(N)) \cong \Gamma_r\backslash\mathbb{H}^2$. Let $e = \left(\begin{smallmatrix} \tilde{r} & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})$. Applying (2.2) we see that

$$\Gamma(\mathcal{O}_{N^2}, \mathfrak{a}_{\tilde{r}}) = \left\{(A, A') \in \mathrm{SL}_2(\mathbb{Q}) \times \mathrm{SL}_2(\mathbb{Q}) : A \in \begin{pmatrix} \mathbb{Z} & \mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} \end{pmatrix} \text{ and } A' \in \begin{pmatrix} \mathbb{Z} & \frac{1}{r}\mathbb{Z} \\ r\mathbb{Z} & \mathbb{Z} \end{pmatrix}\right\}$$

and there is therefore a group isomorphism

$$\begin{aligned} \phi\colon \Gamma_r &\to \Gamma(\mathcal{O}_{N^2}, \mathfrak{a}_{\tilde{r}}) \\ (A, A') &\mapsto (A, eA'e^{-1}) \end{aligned}$$

with the conjugation occurring in $\mathrm{GL}_2(\mathbb{Q})$. Moreover, we have a commutative diagram

$$\begin{array}{ccc} \Gamma_r \times \mathbb{H}^2 & \longrightarrow & \mathbb{H}^2 \\ \downarrow{\scriptstyle \phi\times\psi} & & \downarrow{\scriptstyle \psi} \\ \Gamma(\mathcal{O}_{N^2}, \mathfrak{a}_{\tilde{r}}) \times \mathbb{H}^2 & \longrightarrow & \mathbb{H}^2 \end{array}$$

where ψ is given by $(z, z') \mapsto (z, ez')$. Hence $\Gamma(\mathcal{O}_{N^2}, \mathfrak{a}_{\tilde{r}})\backslash\mathbb{H}^2 \cong \Gamma_r\backslash\mathbb{H}^2$ and the claim follows. □

[4]With apologies for the notational clash: $Y(N)$ denotes the non-compact modular curve of full level N, and $Y_{\mathfrak{a}}(D)$ denotes the Hilbert modular surface of discriminant D and genus $\mathfrak{a}$.

From Propositions 2.3.5 and 2.3.7 we immediately deduce the following corollary.

Corollary 2.3.8. *Let N be a positive integer and let $r_1, r_2 \in (\mathbb{Z}/N\mathbb{Z})^\times$. If r_1 and r_2 are equal modulo squares then Z_{N,r_1} and Z_{N,r_2} are isomorphic.*

We will see in Section 2.3.4 that points on $Z_{N,r}$ parametrise (N,r)-congruences. The isomorphism in Corollary 2.3.8 has the moduli interpretation of post-composing an (N,r_1)-congruence with the multiplication-by-k isogeny where $k^2 \equiv r_1/r_2 \pmod N$.

2.3.4 Models over $\mathbb{Q}$ and moduli interpretations

We write $Y_-(D) := Y_{\mathcal{O}_D^*}(D)$ when $\mathfrak{a} = \mathcal{O}_D^*$ is the *dual lattice* of $\mathcal{O}_D$ with respect to the trace form, i.e., $\mathcal{O}_D^* = \frac{1}{\sqrt{D}}\mathcal{O}_D$ (see e.g., [EK14, Section 3]).

When D is not a perfect square, it is well known that $Y_{\mathfrak{a}}(D)$ admits a model defined over $\mathbb{Q}$. Moreover, (a Zariski open subset of) the surface $Y_-(D)$ parametrises principally polarised abelian surfaces (A,λ) with an embedding $\mathcal{O}_D \subset \mathrm{End}(A)$ whose image is invariant under the *Rosati involution*. That is, for every $\psi \in \mathcal{O}_D$ we have $\psi = \lambda^{-1}\hat{\psi}\lambda$, where $\hat{\psi}$ denotes the dual of ψ. In fact, the same is true when D is a perfect square [Kum15], and similar moduli interpretations may be given (with more complicated data coming from the polarisation) for the surfaces $Y_{\mathfrak{a}}(D)$ [vdG88, IX].

In what follows, we describe an alternative moduli interpretation in the case when $D = N^2$ is a perfect square, following Kani–Schanz [KS98].

Definition 2.3.9. Let $\phi\colon E[N] \to E'[N]$ and $\phi'\colon F[N] \to F'[N]$ be N-congruences of generalised elliptic curves over K (see Definition 2.2.18). We say that ϕ and ϕ' are isomorphic if there exist $\overline{K}$-isomorphisms $\psi\colon E \to F$ and $\psi'\colon E' \to F'$ such that $\psi'\phi = \phi'\psi$.

The following result is due to Kani–Schanz [KS98], see also [Fis19, Lemma 3.2]. Note that the adjective "coarse" in [KS98, p. 339] accounts for the "up to quadratic twists" in [Fis19, Lemma 3.2] and also allows the authors to avoid carefully defining an isomorphism of (N,r)-congruences.

Proposition 2.3.10. *The surface $Z_{N,r}$ admits a model defined over $\mathbb{Q}$. For each field K of characteristic 0 the K-rational points of $Z_{N,r}$ parametrise isomorphisms classes of (N,r)-congruences $\phi\colon E[N] \to E'[N]$, where E/K and E'/K are generalised elliptic curves. For brevity we will write (E,E',ϕ) for an isomorphism class of congruences with a representative $\phi\colon E[N] \to E'[N]$.*

Proof. The group Υ_N acts on $X(N)$ and the action is defined over $\mathbb{Q}$. Recall that we define $\varepsilon_r = \left(\begin{smallmatrix} r & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Fixing an isomorphism $\Upsilon_N \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ we define

$$\mathbf{\Delta}_r = \{(g, \varepsilon_r g \varepsilon_r^{-1}) : g \in \Upsilon_N\}.$$

As abstract groups $\mathbf{\Delta}_r$ and Δ_r are isomorphic, however $\mathbf{\Delta}_r$ inherits a non-trivial action of $G_\mathbb{Q}$ from Υ_N. In particular, the diagonal action of $\mathbf{\Delta}_r$ on $X(N) \times X(N)$ is $G_\mathbb{Q}$-equivariant, and therefore the (scheme) quotient $\mathbf{\Delta}_r\backslash(X(N) \times X(N))$ is defined over $\mathbb{Q}$.

Let $\mathfrak{z} \in Z_{N,r}(K)$ be a K-rational point. Let $E/\overline{K}$ and $E'/\overline{K}$ be generalised elliptic curves such that $\mathfrak{Z} = ((E,\iota),(E',\iota')) \in X(N)\times X(N)$ is a pre-image of $\mathfrak{z}$. Since the morphism $X(N)\times X(N) \to X(1)\times X(1)$ factors through $Z_{N,r}$ the elliptic curves E and E' which *a priori* are defined only over a finite extension of K may be assumed to be defined over K.

Consider the isomorphism $\phi\colon E[N] \to E'[N]$ given by $\phi = (\iota')^{-1}\varepsilon_r\iota$. Clearly ϕ has power r. To show that ϕ is an (N,r)-congruence defined over K it remains to show that $\sigma^{-1}\phi\sigma = \phi$

for any $\sigma \in G_K$. Note that the action of $\sigma \in G_K$ on the point $(E, \iota) \in X(N)$ is given by $\sigma(E, \iota) = (E, \sigma\iota\sigma^{-1})$, and similarly for (E', ι').

Since the orbit of $\mathfrak{Z}$ is G_K-stable, for any $\sigma \in G_K$ there exists an element $g \in \Upsilon_N$ such that $g\iota = \sigma\iota\sigma^{-1}$ and $(\varepsilon_r g \varepsilon_r^{-1})\iota' = \sigma\iota'\sigma^{-1}$. Therefore

$$\begin{aligned}\sigma^{-1}\phi\sigma &= \sigma^{-1}(\iota')^{-1}\varepsilon_r\iota\sigma \\ &= (\varepsilon_r^{-1}\iota'\sigma)^{-1}\iota\sigma \\ &= (g^{-1}\varepsilon_r^{-1}\sigma\iota')^{-1}g^{-1}\sigma\iota \\ &= (\iota')^{-1}(\sigma^{-1}\varepsilon_r\sigma)\iota.\end{aligned}$$

But σ acts on $\mu_N \times \mathbb{Z}/N\mathbb{Z}$ through the diagonal matrix $\left(\begin{smallmatrix}\chi(\sigma) & 0 \\ 0 & 1\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, where χ denotes the mod N cyclotomic character. Therefore, since ε_r is diagonal, we have $\sigma^{-1}\varepsilon_r\sigma = \varepsilon_r$. In particular $\sigma^{-1}\phi\sigma = \phi$ and therefore ϕ is G_K-equivariant.

It remains to show that the isomorphism class of ϕ does not depend on the choice of lift $\mathfrak{Z} \in X(N) \times X(N)$. Suppose that $((F, \kappa), (F', \kappa')) \in X(N) \times X(N)$ is another choice of pre-image for $\mathfrak{z} \in Z_{N,r}(K)$, where F and F' are elliptic curves defined over K. Let $\phi' = (\kappa')^{-1}\varepsilon_r\kappa$. By assumption, there exist isomorphisms $\psi\colon E \to F$ and $\psi'\colon E' \to F'$ such that $((E, \kappa\psi), (E', \kappa'\psi'))$ is contained in the same $\mathbf{\Delta}_r$-orbit as $\mathfrak{Z}$. In particular, there exists $g \in \Upsilon_N$ such that $\iota = g\kappa\psi$ and $\iota' = \varepsilon_r g \varepsilon_r^{-1}\kappa'\psi'$. But then

$$\begin{aligned}\phi &= (\iota')^{-1}\varepsilon_r\iota \\ &= (\varepsilon_r g\varepsilon_r^{-1}\kappa'\psi')^{-1}\varepsilon_r g\kappa\psi \\ &= (\psi')^{-1}(\kappa')^{-1}\varepsilon_r\kappa\psi \\ &= (\psi')^{-1}\phi'\psi\end{aligned}$$

and therefore ϕ and ϕ' are isomorphic (N, r)-congruences, as required.

Conversely let E/K and E'/K be generalised elliptic curves and let $\phi\colon E[N] \to E'[N]$ be an (N, r)-congruence. Choose a point $(E', \iota') \in X(N)(L)$ in the fibre of $X(N) \to X(1)$ above $j(E')$, where L/K is a finite extension. Consider the point $(E, \iota) \in X(N)$ in the fibre of $X(N) \to X(1)$ above $j(E)$ where $\iota = \varepsilon_r^{-1}\iota'\phi$. Since ϕ is G_K-equivariant (hence G_L-equivariant) the point (E, ι) is also L-rational. A symmetric argument to the above shows that the orbit of $((E, \iota), (E', \iota'))$ is G_K-stable and independent of the choice of pre-image (E', ι'). □

Remark 2.3.11. Note that the proof of Proposition 2.3.10 holds with $\mathbb{Q}$ replaced by $\mathbb{Z}[1/N]$ and with K restricted only to being a field of characteristic coprime to N (in fact with appropriate definitions this could be replaced with an arbitrary $\mathbb{Z}[1/N]$-scheme).

Remark 2.3.12. By Proposition 2.3.10 the points of $Z_{N,r}$ parametrise isomorphism classes of (N, r)-congruences. In particular for an elliptic curve E/K with $j(E) \notin \{0, 1728, \infty\}$ the fibres $\mathfrak{j}^{-1}(j(E))$ of the first projection map $\mathfrak{j}\colon Z_{N,r} \to X(1) \times X(1) \to X(1)$ are isomorphic to the twist $X_E^r(N)$. This fails to be true when $j(E) \in \{0, 1728, \infty\}$. To see this, recall that points on $X_E^r(N)$ parametrise isomorphism classes of symplectic isomorphisms $E'[N] \to E[N]$, in particular we are allowed to pre-compose with an automorphism of E', but *cannot* post-compose with an automorphism of $E[N]$, except for ± 1. In particular the fibres $\mathfrak{j}^{-1}(0)$, $\mathfrak{j}^{-1}(1728)$, and $\mathfrak{j}^{-1}(\infty)$ are isomorphic, at least over $\mathbb{C}$, to quotients of $X(N)$ by the subgroups G_0, G_{1728}, and G_∞ of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ generated by $\left(\begin{smallmatrix}0 & -1 \\ 1 & 1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0 & 1 \\ -1 & 0\end{smallmatrix}\right)$, and $\left(\begin{smallmatrix}1 & 1 \\ 0 & 1\end{smallmatrix}\right)$ respectively.

Bearing in mind Remark 2.3.12 we give a precise formulation of the moduli interpretation of the cuspidal locus on $Z_{N,r}$ which will be useful later. Over $\mathbb{C}$ this result is given in [KS98, Section 1.1], however Proposition 2.3.13 is more precise in that we describe the Galois action.

Proposition 2.3.13. *Let* $\mathfrak{j}\colon Z_{N,r} \to X(1) \times X(1) \to X(1)$ *be the first projection. Consider the curve* $C_{\infty,1} = \mathfrak{j}^{-1}(\{\infty\} \times X(1))$ *on the surface* $Z_{N,r}$*. The map*

$$\begin{aligned} C_{\infty,1} &\to X_\mu(N) \\ (\mathcal{E}_N^{\mathrm{sm}}, E, \phi) &\mapsto (E, \phi|_{\mu_N \times \{0\}}) \end{aligned}$$

is an isomorphism of curves defined over $\mathbb{Q}$*.*

Proof. We construct an explicit inverse. Fix a primitive N^{th}-root of unity $\zeta \in \mu_N$. For each non-cuspidal point (E, ι) on $X_\mu(N)$ let $Q \in E[N]$ be a point such that $e_N(\iota(\zeta), Q) = \zeta^r$. Consider the isomorphism

$$\phi\colon \mathcal{E}_N^{\mathrm{sm}}[N] \to E[N]$$

given by $(\zeta, 0) \mapsto \iota(\zeta)$ and $(1, 1) \mapsto Q$. Clearly ϕ has power r, so it suffices to show that ϕ is well defined up to composing with automorphisms of $\mathcal{E}_N^{\mathrm{sm}}$ and E. Suppose that $Q' \in E[N]$ is another point such that $e_N(\iota(\zeta), Q') = \zeta^r$. From the properties of the Weil pairing $Q' = a\iota(\zeta) + Q$ for some $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. By Lemma 2.2.17 the isomorphism class of the congruence ϕ is well defined, since $\phi' = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\phi$.

Now consider a cusp $(\mathcal{E}_N^{\mathrm{sm}}, \iota) \in X_\mu(N)$ as in Proposition 2.2.20. We partition the cusps into two subsets:

(A) for each $d|N$ with $d \neq 1$ we have $\iota(\zeta) = (\zeta^a, bd)$ for some $0 < a < d$ and $b \in (\mathbb{Z}/(N/d)\mathbb{Z})^\times$,

(B) the cusps where $d = 1$ and $\iota(\zeta) = (1, a)$ for some $a \in (\mathbb{Z}/N\mathbb{Z})^\times$.

In case (A) we associate the (N, r)-congruence

$$\begin{aligned} \phi\colon \mathcal{E}_N^{\mathrm{sm}}[N] &\to \mathcal{E}_N^{\mathrm{sm}}[N] \\ \left(\begin{smallmatrix} \omega \\ n \end{smallmatrix}\right) &\mapsto \left(\begin{smallmatrix} a & 0 \\ bd & a^{-1}r \end{smallmatrix}\right)\left(\begin{smallmatrix} \omega \\ n \end{smallmatrix}\right). \end{aligned} \tag{2.3}$$

In case (B) we associate the (N, r)-congruence

$$\begin{aligned} \phi\colon \mathcal{E}_N^{\mathrm{sm}}[N] &\to \mathcal{E}_N^{\mathrm{sm}}[N] \\ \left(\begin{smallmatrix} \omega \\ n \end{smallmatrix}\right) &\mapsto \left(\begin{smallmatrix} 0 & -a^{-1}r \\ a & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} \omega \\ n \end{smallmatrix}\right). \end{aligned} \tag{2.4}$$

In each case, a simple calculation shows that ϕ has power r. In particular, the birational morphism $C_{\infty,1} \to X_\mu(N)$ is a set theoretic bijection on $\mathbb{C}$-points, hence an isomorphism. Finally, by Galois descent the morphism $C_{\infty,1} \to X_\mu(N)$, and its inverse, are defined over $\mathbb{Q}$. □

2.3.5 Hecke correspondences

We now introduce a number of interesting "modular curves" on the surface $Z_{N,r}$. The constructions in this section exist for Hilbert modular surfaces, even if we do not restrict to the case when D is a perfect square, and are often known as *Hirzebruch–Zagier divisors* or *modular curves*. However, the construction is more involved when starting from the quotient $\Gamma(\mathcal{O}_D, \mathfrak{a})\backslash\mathbb{H}^2$ (it is the direct analogy of [McM07, Section 3] and [vdG88, Definition V.1.3], cf. [Her91, Section 5]). In the case when D is a fundamental discriminant van der Geer [vdG88, p. 86] describes that "if one considers

the surface $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}^2$ as a degenerate Hilbert modular surface, then... the modular curves are just the Hecke correspondences". Indeed we will see that in our setting when $D = N^2$ is a square, this description can be generalised directly.

Let N be an integer and let r and m be integers coprime to N. Suppose that there exists an integer $a \in \mathbb{Z}$ such that $r = a^2 m \pmod N$. Let $\mathcal{E}/\mathbb{Q}(X_0(m))$ be a generic curve equipped with a cyclic m-isogeny $\Phi\colon \mathcal{E} \to \mathcal{E}'$ for some elliptic curve $\mathcal{E}'/\mathbb{Q}(X_0(m))$. Restricting Φ to $\mathcal{E}[N]$ gives an (N, m)-congruence between $\mathcal{E}$ and $\mathcal{E}'$, so $a\Phi|_{\mathcal{E}[N]}$ is an (N, r)-congruence. That is, we have a map $(\mathcal{E}, \Phi) \mapsto (\mathcal{E}, \mathcal{E}', a\Phi|_{\mathcal{E}[N]})$, which, after taking Zariski closures, induces a morphism

$$\psi_{m,a}\colon X_0(m) \to Z_{N,r}.$$

Indeed, for each choice of $\lambda \in \{x \in \mathbb{Z}/N\mathbb{Z} : x^2 = 1\}$ we obtain such a morphism $\psi_{m,\lambda a}$ whose image is equal to that of $\psi_{m,a}$ if and only if $\lambda = \pm 1$.

Definition 2.3.14. For each $\lambda \in \{x \in \mathbb{Z}/N\mathbb{Z} : x^2 = 1\}/\{\pm 1\}$ we define the *Hirzebruch–Zagier divisor*, $F_{m,\lambda}$, to be the image of $\psi_{m,\lambda a}$. We further define

$$F_m = \sum_{\lambda} F_{m,\lambda}.$$

Making a different choice of $a \in \mathbb{Z}$ will possibly permute the terms in the above sum, however throughout this thesis we only deal collectively with the irreducible components of F_m and therefore this distinction will play no role.

The K-rational points on F_m correspond to N-congruences $\phi\colon E[N] \to E'[N]$ such that ϕ arises by composing the restriction of an N-isogeny to $E[N]$ with the multiplication-by-a-map, for some $a \in \mathbb{Z}$.

2.3.6 Symmetric Hilbert modular surfaces

The following surfaces have previously been studied by the Hirzebruch school [Hir73b, HZ76, Hir78, Hau79, Hau82, Bas85] when D is a fundamental discriminant. When $D = p^2$ their geometry is studied by Hermann [Her92]. Studying the geometry of these quotients when $D = N^2$, extending the work of Hermann, will be the main concern of Chapter 3.

Every Hilbert modular surface comes equipped with a natural involution which descends the involution which swaps the copies of the upper half plane. More precisely consider the involution $\mathbb{H}^2 \to \mathbb{H}^2$ given by

$$(z_1, z_2) \mapsto \left(\frac{-1}{\mathrm{Nm}(\mathfrak{a})z_2}, \frac{-1}{\mathrm{Nm}(\mathfrak{a})z_1}\right).$$

This induces an involution τ of the Hilbert modular surface $\Gamma(\mathcal{O}_D, \mathfrak{a})\backslash\mathbb{H}^2$. Note that τ extends to an involution $\tilde{\tau}$ of $Y_{\mathfrak{a}}(D)$. The morphism $\tilde{\tau}$ is often referred to as the *Galois involution*, owing to the fact that in the moduli interpretation of $Y_{-}(D)$ (as described in Section 2.3.4) the involution $\tilde{\tau}$ acts as pre-composing the embedding $\mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ with the action of the non-trivial element of $\mathrm{Aut}(F_D/\mathbb{Q})$ on $\mathcal{O}_D$.

Definition 2.3.15. We define the *symmetric Hilbert modular surface* $Y_{\mathfrak{a}}^{\mathrm{sym}}(D)$ to be the quotient variety $Y_{\mathfrak{a}}(D)/\tilde{\tau}$. We write $Y_{-}^{\mathrm{sym}}(D) = Y_{-}(D)/\tilde{\tau}$.

When $D = N^2$ is a perfect square, the involution $\tilde{\tau}$ also has a natural interpretation in terms of the surface $Z_{N,r}$. To see this, let $\varepsilon \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ have determinant r, and let $\bar{\tau}$ be the morphism

$X(N) \times X(N) \to X(N) \times X(N)$ given by

$$(x, x') \mapsto (x', (r^{-1}\varepsilon^2)x).$$

It is clear that $\bar{\tau}^2 \in \Delta_\varepsilon$ and $\bar{\tau}\Delta_\varepsilon\bar{\tau}^{-1} = \Delta_\varepsilon$, so $\bar{\tau}$ descends to an involution τ acting on $Z_{N,r}$. It is simple to check using the isomorphism in Proposition 2.3.7 that τ restricts to the involution on $\Gamma(\mathcal{O}_{N^2}, \mathfrak{a}_r)\backslash\mathbb{H}$ defined above. We define the *symmetric Hilbert modular surface* $Z^{\mathrm{sym}}_{N,r}$ to be the quotient of $Z_{N,r}$ by the involution τ. An advantage of this description is that it is simple to see that the action of τ is defined over $\mathbb{Q}$.

2.3.6.1 Humbert surfaces

In the following we treat the relationship between symmetric Hilbert modular surfaces and Humbert surfaces in the case when the abelian varieties parametrised are principally polarised. Similar results for other genera of Hilbert modular surfaces may be obtained by relaxing the requirement for the polarisation to be principal (cf. [vdG88, IX.1–2]). A nice exposition is also given in [HvdG81, Chapter 8].

Let $\mathfrak{H}_2$ denote the Siegel upper half space of degree 2, that is, the set of matrices $M \in \mathrm{M}_2(\mathbb{C})$ such that $M^{\mathrm{T}} = M$ and $\mathrm{Im}(M)$ is positive definite.

The symplectic group $\mathrm{Sp}_4(\mathbb{R})$ acts naturally on $\mathfrak{H}_2$ by "Möbius transformations", that is, a block matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_4(\mathbb{R})$ acts on $M \in \mathfrak{H}_2$ by $M \mapsto (AM+B)(CM+D)^{-1}$. The quotient $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$ is isomorphic to $\mathcal{A}_2(\mathbb{C})$, where $\mathcal{A}_2$ denotes the (coarse) moduli space of principally polarised abelian surfaces.

For each discriminant D we define the *Humbert surface* of discriminant D to be the surface $\mathcal{H}_D \subset \mathcal{A}_2$ whose $\mathbb{C}$-points parametrise principally polarised abelian surfaces with an endomorphism of discriminant D fixed by the Rosati involution.

The complex manifold $\mathcal{H}_D(\mathbb{C})$ admits a very explicit description as a subspace of $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$, which follows by combining Proposition 2.3 and Theorem 2.4 of [vdG88]:

- If $D \equiv 0 \pmod 4$ then $\mathcal{H}_D(\mathbb{C})$ is equal to the image of

$$\left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \mathfrak{H}_2 : a - \frac{Dc}{4} = 0 \right\}$$

  in $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$.

- If $D \equiv 1 \pmod 4$ then $\mathcal{H}_D(\mathbb{C})$ is equal to the image of

$$\left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \mathfrak{H}_2 : a + b - \frac{(D-1)c}{4} = 0 \right\}$$

  in $\mathrm{Sp}_4(\mathbb{Z})\backslash\mathfrak{H}_2$.

The following proposition is well known, even when D is a perfect square, and the proof is the direct analogue of [vdG88, IX, Proposition 2.5] (see also [Kan23, Theorem 8.3]).

Proposition 2.3.16. *The Humbert surface $\mathcal{H}_D$ of discriminant D is $\mathbb{Q}$-birational to the symmetric Hilbert modular surface $Y^{\mathrm{sym}}_-(D)$.*

2.4 On algebraic surfaces

In this section, all surfaces are assumed to be reduced, irreducible, algebraic surfaces defined over the complex numbers.

For an irreducible projective variety $X/\mathbb{C}$ let Ω_X^d denote the sheaf of holomorphic d-forms on X. If X has dimension n we write $p_g(X) = h^0(X, \Omega_X^n)$ for the *geometric genus* of X and $p_a(X) = (-1)^n(\chi(\mathcal{O}_X) - 1)$ for the *arithmetic genus* of X.

Let K_X be a canonical divisor for X. For each positive integer m, consider the rational map

$$\Psi_m \colon X \dashrightarrow \mathbb{P}H^0(X, mK_X)$$

given by the linear system $|mK_X|$. We define the *Kodaira dimension of* X to be the integer $\kappa(X) = \max_{m\geq 1}\{\dim(\operatorname{im}\Psi_m)\}$. By convention we define $\kappa(X) = -1$ if $|mK_X| = \emptyset$ for all $m \geq 1$.

If $S/\mathbb{C}$ is a non-singular, projective algebraic surface, we write $q(S) = p_g(S) - p_a(S) = h^0(S, \Omega_S^1)$ for the *irregularity* of S. When $q(S) = 0$ we will say that S is a *regular* surface[5].

Following e.g., [Bea96, I], we recall that there exists a symmetric bilinear *intersection pairing* $\operatorname{Pic}(S) \times \operatorname{Pic}(S) \to \mathbb{Z}$. If D_1 and D_2 are divisors on S we denote their intersection by $D_1 \cdot D_2 \in \mathbb{Z}$. Moreover, if D_1 and D_2 are distinct irreducible curves which intersect transversally on S then $D_1 \cdot D_2 = \#(D_1 \cap D_2)$. If D is a divisor on S we write $D^2 = D \cdot D$ for the *self-intersection* of D. A pair divisor classes $D_1, D_2 \in \operatorname{Pic}(S)$ are said to be *numerically equivalent* if $D_1 \cdot E = D_2 \cdot E$ for all classes $E \in \operatorname{Pic}(S)$.

Taking cohomology in the exponential exact sequence yields a homomorphism

$$\operatorname{Pic}(S) \to H^2(S, \mathbb{Z}) \cong H_2(S, \mathbb{Z})$$

whose kernel is $\operatorname{Pic}^0(S)$, and the intersection pairing on $\operatorname{Pic}(S)$ agrees with the intersection pairing on $H_2(S, \mathbb{Z})$. The intersection of divisors D_1 and D_2 therefore only depends on the *algebraic equivalence class* of D_1 and D_2, that is, their images in the *Néron-Severi group* $\operatorname{NS}(S) = \operatorname{Pic}(S)/\operatorname{Pic}^0(S)$.

If $C \subset S$ is a smooth, (reduced, irreducible) rational curve of self-intersection $C^2 = -d$, where $d > 0$ is a positive integer, then we say that C is a $(-d)$*-curve*.

We will often use the following two facts without reference. The first of these is the adjunction formula, which may be viewed as a generalisation of the genus-degree formula for plane curves. The latter is known as the projection formula.

Proposition 2.4.1 (Adjunction formula)**.** *Let $S/\mathbb{C}$ we a smooth, projective, algebraic surface and let $C \subset S$ be an irreducible curve. Then*

$$p_a(C) = 1 + \frac{1}{2}C \cdot (K_S + C)$$

where K_S is a canonical divisor on S.

Proof. See [Bea96, I.15] or Proposition V.1.5 and Exercise V.1.3(a) of [Har77]. □

Proposition 2.4.2 (Projection formula)**.** *Let $S/\mathbb{C}$ be a projective algebraic surface and let D_1, D_2 be divisors on S. If $S'/\mathbb{C}$ is a projective algebraic surface and $f \colon S' \to S$ is a generically finite morphism of degree d, then*

$$f^*D_1 \cdot f^*D_2 = d(D_1 \cdot D_2).$$

[5] With all the necessary apologies for this mildly annoying clash of terminology. For this reason we will always avoid using the adjective regular to describe any smoothness criteria.

Proof. This is [Bea96, Proposition I.8], see also [Har77, Exercise II.5.1(d)]. □

The following is a useful application of the projection formula, which we will use often.

Lemma 2.4.3. *Let $S/\mathbb{C}$ and $S'/\mathbb{C}$ be smooth, projective, algebraic surfaces and let $f\colon S' \to S$ be the blowup of S at a point. Let K_S and $K_{S'}$ be canonical divisors for S and S' respectively, then*

$$K_{S'}^2 = K_S^2 - 1.$$

Proof. Let E be the exceptional divisor of f and note that $K_{S'} = f^*K_S + E$. Since both S and S' are smooth, $E^2 = -1$. By the projection formula we therefore have

$$\begin{aligned} K_S^2 &= (K_{S'} - E)^2 \\ &= K_{S'}^2 - 2K_{S'} \cdot E + E^2 \\ &= K_{S'}^2 - 1 \end{aligned}$$

as required. □

2.4.1 On the Enriques–Kodaira classification

We give a brief overview of the Enriques–Kodaira classification, or (more precisely) the part of the Enriques–Kodaira classification which deals with surfaces $S/\mathbb{C}$ with $q(S) = 0$. In addition we state several results which will be useful for classifying the birational geometry of the symmetric Hilbert modular surfaces $Z_{N,r}^{\mathrm{sym}}$ defined in Section 2.3.6. The reader seeking a more thorough exposition is encouraged to consult [Bea96] or [BHPV04, Chapter VI].

Rational surfaces: $\kappa(S) = -1$

A regular surface $S/\mathbb{C}$ with Kodaira dimension -1 is *rational*, i.e., birational to $\mathbb{P}^2$. We recall the following lemma, which follows from Castelnuovo's rationality criterion, and which places strong restrictions on rational curves on regular, non-rational, complex algebraic surfaces.

Lemma 2.4.4 ([Hir73b, 4.4 I–III])**.** *Let $S/\mathbb{C}$ be a smooth, regular, projective algebraic surface. Let K_S be a canonical divisor of S. If $C \subset S$ is an irreducible curves such that either:*

(i) $K_S \cdot C \leq -2$,

(ii) $K_S \cdot C \leq -1$ *and C is either singular, or is not rational*

then S is a rational surface. Furthermore, if $C, D \subset S$ are distinct smooth, irreducible, rational (-1)-curves which meet, then S is a rational surface.

In particular, if S is not rational and $K_S \cdot C \leq -1$, then C is a non-singular rational curve, $K_S \cdot C = C^2 = -1$, and C does not meet another (-1)-curve on S.

Enriques and K3 surfaces: $\kappa(S) = 0$

Let $S/\mathbb{C}$ be a regular algebraic surface and let K_S be a canonical divisor for S. We say that S is an *Enriques surface* if $2K_S = 0$, but $K_S \neq 0$ (as elements of $\mathrm{Pic}(S)$). We say that S is a *K3 surface* if $K_S = 0$. We say that a K3 surface S is an *elliptic K3 surface* if there exists a dominant morphism $S \to \mathbb{P}^1$ whose generic fibre is a smooth curve of genus 1 (note that we *do not* require the fibration to have a section). Indeed, it will turn out that in this work all surfaces of Kodaira dimension 0 will be elliptic K3 surfaces.

Proposition 2.4.5. *A regular algebraic surface $S/\mathbb{C}$ of Kodaira dimension 0 is either an Enriques surface or a K3 surface. Moreover, if S is an Enriques surface then $p_g(S) = 0$ and if S is a K3 surface then $p_g(S) = 1$.*

Proof. This follows from [Bea96, Theorem VIII.2]. □

Properly elliptic surfaces: $\kappa(S) = 1$

A smooth projective surface $S/\mathbb{C}$ is said to be *properly elliptic* if S has Kodaira dimension 1. As we would hope, properly elliptic surfaces are in fact elliptic fibrations.

Lemma 2.4.6. *Let $S/\mathbb{C}$ be a minimal properly elliptic surface and let K_S be a canonical divisor for S. Then $K_S^2 = 0$ and there exists a smooth curve $C/\mathbb{C}$ together with a surjective morphism $S \to C$ whose generic fibre is an elliptic curve.*

Proof. See e.g., [Bea96, Proposition IX.2]. □

Surfaces of general type: $\kappa(S) = 2$

A smooth projective surface $S/\mathbb{C}$ is said to be of *general type* if S has Kodaira dimension 2. The following lemma will provide us with our main criteria for proving that a regular surface is of general type.

Lemma 2.4.7. *Let $S/\mathbb{C}$ be a smooth, regular surface and let K be a canonical divisor on S. If $K_S^2 > 0$, then S is either rational or of general type.*

Proof. If S is not rational, let S' be a minimal model for S. If $K_{S'}$ is a canonical divisor on S', then since S' is obtained from S by repeatedly blowing down (-1)-curves, we have $(K_{S'})^2 > K_S^2 > 0$. By [Bea96, Proposition X.1] the surface S' (and therefore S) is of general type. □

2.4.2 Resolution of cyclic quotient singularities

In order to construct smooth models for the surfaces $Z_{N,r}$ we briefly recall some general facts about cyclic quotient singularities. Let $d \geq 1$ be an integer and let $\mu_d \subset \mathbb{C}^\times$ denote the subgroup of d^{th}-roots of unity. Let $\zeta \in \mu_d$ be a primitive d^{th}-root of unity and let $0 < q < d$ be an integer coprime to d.

Definition 2.4.8. Consider the action of μ_d on $\mathbb{C}^2$ given by $(z_1, z_2) \mapsto (\zeta z_1, \zeta^q z_2)$. If $S/\mathbb{C}$ is an algebraic surface we say that a point $\mathfrak{z} \in S(\mathbb{C})$ is a *cyclic quotient singularity of type* (d, q) if locally analytically in a neighbourhood of $\mathfrak{z}$ the surface S is isomorphic to $\mathbb{C}^2/\mu_d$.

Definition 2.4.9. Let d and q be positive, coprime integers and suppose that $q < d$. We define the *Hirzebruch–Jung continued fraction of d/q* to be the (unique) expression

$$\frac{d}{q} = a_1 - \frac{1}{a_2 - \frac{1}{\cdots - \frac{1}{a_k}}}.$$

where $a_1, ..., a_k > 2$ are integers. We often write $[[a_1, ..., a_k]]$ for the Hirzebruch–Jung continued fraction of d/q, and we say that the integer $k \geq 1$ is the *length* of $[[a_1, ..., a_k]]$.

The following proposition shows us how to resolve cyclic quotient singularities. Its proof is a lovely application of the toric dictionary.

Proposition 2.4.10. *Let $d \geq 1$ be an integer, and let $0 < q < d$ be an integer coprime to d. Let $S/\mathbb{C}$ be a projective algebraic surface and suppose that $\mathfrak{z} \in S(\mathbb{C})$ is a cyclic quotient singularity of type (d, q). Let $[[a_1, ..., a_k]]$ denote the Hirzebruch–Jung continued fraction of d/q.*

There exists a unique projective surface $\widetilde{S}/\mathbb{C}$, which is known as the minimal resolution of the singularity $\mathfrak{z}$, together with a birational morphism $\pi\colon \widetilde{S} \to S$ such that:

(i) *$\widetilde{S}$ is non-singular in a neighbourhood of $\pi^{-1}(\mathfrak{z})$, and*

(ii) *the exceptional divisor of π does not contain a (-1)-curve.*

Moreover, the exceptional divisor of the morphism π (equivalently, the fibre $\pi^{-1}(\mathfrak{z})$) consists of a chain of k smooth, rational curves where the i^{th} curve has self-intersection $-a_i$.

Proof. See e.g., [vdG88, II.6] or [BHPV04, III.5]. □

2.5 Minimisation over polynomial rings

The following section may comfortably be skipped until such a time that the reader wishes to understand how the calculations in Sections 4.4, 4.5.1, and 5.3 were performed. We outline a method for making "simplifying transformations" to the defining equations of a variety[6]. Our setting will often be that of degree 2, 3, or 4 covers of curves or surfaces defined over $\mathbb{Q}$. This naturally leads us to consider schemes of dimension zero defined over function fields of transcendence degree 1 or 2 over $\mathbb{Q}$.

For example, consider a double cover $S \to \mathbb{A}^2$. By considering the corresponding extension of function fields it follows that there exists a polynomial $f \in \mathbb{Z}[t_0, t_1]$ such that S is birational to the surface $S' = \{X_0^2 - fX_1^2 = 0\} \subset \mathbb{P}^1 \times \mathbb{A}^2$. A natural step for simplifying the equations for S' within its birational equivalence class is to remove square factors from f, i.e., "minimising" the discriminant of the binary quadratic form $T_0^2 - fT_1^2 \in \mathbb{Z}[t_0, t_1][X_0, X_1]$. What follows can be interpreted as a generalisation of this procedure of "minimising the discriminant", which we dub *minimisation*.

Much of this section is motivated by Tate's algorithm for computing the reduction type of an elliptic curve over a local field (see [Sil94, IV.9]). Our treatment is motivated by Cremona–Fisher–Stoll's algorithms for minimising 2, 3, and 4-coverings of elliptic curves [CFS10].

2.5.1 Arithmetic blowups

Let R be a discrete valuation ring with maximal ideal $\mathfrak{p} = (\pi)$. Let S/R be an affine scheme $S = \operatorname{Spec} A$ flat of relative dimension 0 or 1 over $\operatorname{Spec} R$ and suppose that S has smooth generic fibre. Explicitly we may take S to be given by the vanishing of polynomials $f_1, ..., f_m \in R[x_1, ..., x_n]$ in $\mathbb{A}^n_R$ such that $f_i \notin \pi R[x_1, ..., x_n]$ for all $i = 1, ..., m$. After applying a linear change of coordinates (i.e., given by an element of $\mathrm{GL}_n(R)$) we may assume that the point $\mathfrak{m} = (\pi, x_1, ..., x_n)$ lies on S (this is the origin on the special fibre of S). Following [Sil94, IV.7] we describe the *blowup* of S at $\mathfrak{m}$ to be the subscheme of $S \times \mathbb{P}^n_{\mathbb{Z}}$ given by the equations

$$x_i y_0 - \pi y_i \quad \text{and} \quad x_i y_j - x_j y_i$$

[6] The concept of "nicer equations" will remain un-defined throughout this work, though in general the best measure is probably the degree of the polynomials which define the variety. In any case, many of the equations which appear in this thesis start out in the category of "it takes a non-trivial amount of time for the computer to print this out" or, as Noah Porcelli once put it, "do your eyes not hurt?". "Does it fit on a page of A4?" is therefore probably also a useful metric.

where $1 \leq i, j \leq n$.

Just as curve and surface singularities (over $\mathbb{C}$) may be resolved by iterated blowups and normalisations, we may hope that in our setting arithmetic blowups will (at least partially) resolve the singular points on the special fibre of S. Indeed, this approach is utilised in Tate's algorithm for finding the minimal regular model of an elliptic curve over a DVR [Sil94, IV.7]. We will refer to this process as *minimisation* in reference to the fact that when $E/\mathbb{Z}_{(p)}$ is an elliptic curve repeatedly applying the above algorithm "minimises the exponent of p in the discriminant of E".

If B is a unique factorisation domain and $\pi \in B$ is an irreducible element, we write $v_\pi(x)$ for the π-adic valuation of an element $x \in \operatorname{Frac} B \setminus \{0\}$. In the following examples we avoid characteristics 2 and 3 for simplicity.

Example 2.5.1 (An algorithm for minimising an étale cubic algebra over $\mathbb{Q}$)**.** Let $K/\mathbb{Q}$ be an étale cubic algebra and let $f(X_0, X_1) \in \mathbb{Z}[X_0, X_1]$ be a homogeneous cubic form such that $K \cong \mathbb{Q}[x]/(f(x, 1))$. Since K is étale, the binary form $f(X_0, X_1)$ has no repeated factors. Let $\Delta(f)$ and $m(f)$ be the discriminant and content (i.e., the gcd of the coefficients) of $f(x, 1)$ respectively. Let $\mathcal{C} \subset \mathbb{P}^1_{\mathbb{Z}[1/6]}$ be the subscheme given by the vanishing of $f(X_0, X_1)$.

If $p^3 | \Delta(f)$ consider the scheme $\mathcal{C}_p = \mathcal{C} \times_{\mathbb{Z}[1/6]} \mathbb{Z}_{(p)}$. Since $p | \Delta(f)$ the singular subscheme of the special fibre of $\mathcal{C}_p$ consists of either a double or triple point. Let $\overline{U} \in \mathrm{SL}_2(\mathbb{F}_p)$ be a matrix which moves the singular point to $(0 : 1)$. By the existence of Smith normal form the matrix $\overline{U}$ lifts to a matrix $U \in \mathrm{SL}_2(\mathbb{Z})$ which may be applied to $\mathcal{C}$, leaving $\Delta(f)$ unchanged.

Choosing the affine patch where $X_1 = 1$, and setting $x = X_0/X_1$, we blow up the singular point $\mathfrak{m} = (p, x)$ on $\mathcal{C}_p$. This blowup is given by the vanishing of the binary cubic form $f'(X_0, X_1) = f(pX_0, X_1)/p^k$ in $\mathbb{P}^1_{\mathbb{Z}[1/6]}$, where $k \in \{2, 3\}$ is chosen so that $m(f') \not\equiv 0 \pmod{p}$. Note that $v_p(\Delta(f')) = v_p(\Delta(f)) - k(k-1)$, and therefore after finitely many iterations $v_p(\Delta(f)) \leq 2$.

Example 2.5.2 (An algorithm for minimising a conic in $\mathbb{P}^2_{\mathbb{Q}}$)**.** In the following example we illustrate how arithmetic blowups allow us to reproduce the classical reduction algorithm for ternary quadratic forms over $\mathbb{Q}$. The approach we present here is a closely related to [CR03, Algorithm I].

Let $Q(X_0, X_1, X_2) \in \mathbb{Z}[X_0, X_1, X_2]$ be a (homogeneous) degree 2 polynomial which defines a non-singular curve $C \subset \mathbb{P}^2_{\mathbb{Q}}$. After possibly rescaling Q there exists a symmetric matrix $M \in \mathrm{M}_3(\mathbb{Z})$ of non-zero determinant such that if $\mathbf{x} = (X_0, X_1, X_2)$ then

$$Q(X_0, X_1, X_2) = \mathbf{x}^{\mathrm{T}} M \mathbf{x}$$

Define the *discriminant of* Q to be $\Delta(Q) = \det(M)$.

For simplicity we avoid characteristic 2 and consider Q as defining a scheme $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{Z}[1/2]}$. For each prime number $p \neq 2$ the fibre of $\mathcal{C}$ at p is singular if and only if $\Delta(Q) \equiv 0 \pmod{p}$. This suggests the following minimisation algorithm:

If $p^2 | \Delta(Q)$ we consider the arithmetic surface $\mathcal{C}_p = \mathcal{C} \times_{\mathbb{Z}[1/2]} \operatorname{Spec} \mathbb{Z}_{(p)}$. The singular subscheme of the special fibre at p consists of either a point, or a double line. Let $\overline{U} \in \mathrm{SL}_3(\mathbb{F}_p)$ be a matrix which transforms the singular locus to $(0 : 0 : 1) \in \mathbb{P}^2_{\mathbb{F}_p}$, respectively the line $\{X_2 = 0\} \subset \mathbb{P}^2_{\mathbb{F}_p}$. By the existence of Smith normal form the matrix $\overline{U}$ lifts to a matrix $U \in \mathrm{SL}_3(\mathbb{Z})$, which we then apply to $\mathcal{C}$ by setting $M' = U^{\mathrm{T}} M U$. Since $\det(U) = 1$ this leaves $\Delta(Q)$ unchanged.

In the former case, choosing the affine patch where $X_2 = 1$, and setting $x_0 = X_0/X_2$ and $x_1 = X_1/X_2$ we blowup the singular point $\mathfrak{m} = (p, x_0, x_1)$ on $\mathcal{C}_p$. Since $p^2 | \Delta(Q)$ this is given (on an open subscheme of the blowup) by the vanishing of the integral non-homogeneous quadratic form $Q(px_0, px_1, 1)/p^2$. After homogenising we obtain the ternary quadratic form $Q'(X_0, X_1, X_2) =$

$Q(X_0, X_1, p^{-1}X_2)$. Similarly, in the case of the double line at $X_2 = 0$, we set $Q'(X_0, X_1, X_2) = Q(X_0, X_1, pX_2)/p$.

Both operations decrease the p-adic valuation of $\Delta(Q)$, therefore after finitely many iterations we have $v_p(\Delta(Q)) \leq 1$.

Example 2.5.3 (An approach for minimising a quadric intersection in $\mathbb{P}^2_{\mathbb{Q}}$)**.** We describe two operations which are helpful for minimising a quadric intersection in $\mathbb{P}^2_{\mathbb{Q}}$. The approach we describe here is similar to the algorithm given by Cremona–Fisher–Stoll [CFS10] for minimising a 4-covering of an elliptic curve (i.e., a quadric intersection in $\mathbb{P}^3_{\mathbb{Q}}$) and it may be possible give a rigorous algorithm by adapting their proof.

Consider a pair of (homogeneous) degree 2 polynomials $Q_1(X_0, X_1, X_2)$ and $Q_2(X_0, X_1, X_2) \in \mathbb{Z}[X_0, X_1, X_2]$ and let $M_1, M_2 \in \mathrm{M}_3(\mathbb{Z})$ be their matrices of second partial derivatives. Define the homogeneous quartic form $f(x, z) = \det(M_1 x + M_2 z) \in \mathbb{Z}[x, z]$ and define the discriminant of the pair of quadrics (Q_1, Q_2) to be $\Delta = \Delta(Q_1, Q_2) = \mathrm{disc}(f(x, 1))$.

Let $G = \mathrm{GL}_2 \times \mathrm{GL}_3$ act naturally on the space of pairs of ternary quadratic forms (the first factor acts by adding linear combinations of Q_1 and Q_2 and the second factor acts by automorphisms of $\mathbb{P}^2$).

Let $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{Z}[1/2]}$ be the subscheme cut out by the pair (Q_1, Q_2). In particular, if $\Delta \neq 0$ then the generic fibre of $\mathcal{C}$ is an étale quartic algebra over $\mathbb{Q}$. Let p be a prime number such that $v_p(\Delta) \geq 1$. Write $\overline{Q}_1$ and $\overline{Q}_2$ for the reductions of Q_1 and Q_2 modulo p respectively. Suppose that either:

(i) $\overline{Q}_1$ is equal to $\lambda \overline{Q}_2$ for some $\lambda \in \mathbb{F}_p$, or

(ii) the reduction of $\mathcal{C}$ modulo p has a multiple point.

In case (i) there exists $\overline{U} \in \mathrm{SL}_2(\mathbb{F}_p)$ so that if $\bar{g} = (\overline{U}, I) \in G(\mathbb{F}_p)$ then $\bar{g} \cdot (\overline{Q}_1, \overline{Q}_2) = (0, \mu \overline{Q}_2)$ for some $\mu \in \mathbb{F}_p$. In case (ii) choose $\overline{V} \in \mathrm{SL}_3(\mathbb{F}_p)$ which moves the singular point to $(0 : 0 : 1) \in \mathbb{P}^2_{\mathbb{F}_p}$. Let V be a lift of $\overline{V}$ to $\mathrm{SL}_3(\mathbb{Z})$ and choose a matrix $U \in \mathrm{SL}_2(\mathbb{Z})$ such that the coefficient of X_2^2 in Q_2' is divisible by the maximal power of p among elements of $(Q_1', Q_2') = g \cdot (Q_1, Q_2)$ where $g = (U, V)$ (i.e., where Q_2' is chosen in the $\mathbb{Z}$-span of $V \cdot Q_1$ and $V \cdot Q_2$).

In case (i) we may choose a lift $g \in \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ of $\bar{g}$. Let $(Q_1', Q_2') = g \cdot (Q_1, Q_2)$, let k be the p-adic valuation of the content of Q_1' and set $(Q_1'', Q_2'') = (Q_1'/p^k, Q_2')$. In case (ii) let $(Q_1', Q_2') = g \cdot (Q_1, Q_2)$. For each $i = 1, 2$ let k_i be the p-adic valuation of the content of $V' \cdot Q_i'$ where V' is the diagonal matrix with diagonal entries $(p, p, 1)$. Now set $(Q_1'', Q_2'') = g' \cdot (Q_1', Q_2')$ where $g' = (U', V')$ and U' is diagonal with diagonal entries (p^{-k_1}, p^{-k_2}).

It is important to note that the "global" approach in Examples 2.5.1–2.5.3 may fail when the base ring (in that case $\mathbb{Z}$) fails to be a principal ideal domain. More specifically, if R is an integral domain and (π) is a prime ideal of R it is not necessarily true (unless R is a PID) that we may lift a matrix $\overline{U} \in \mathrm{SL}_n(R/(\pi))$ to a matrix $U \in \mathrm{SL}_n(R)$.

Nevertheless, we will see that applying these approaches in the case when $R = \mathbb{Z}[t_1, ..., t_n]$ provides a useful "algorithm" for minimising forms with coefficients in $\mathbb{Z}[t_1, ..., t_2]$. Let $\pi \in \mathbb{Z}[t_1, ..., t_2]$ be a factor of Δ. While we cannot, in general, hope for a lift of our matrix $\overline{U} \in \mathrm{SL}_n(R/(\pi))$ we can always choose a lift $U \in \mathrm{M}_n(R) \cap \mathrm{GL}_n(R_{(\pi)})$. In this case we introduce a factor of $\det(U)^k$ into Δ, for some $k > 0$.

Example 2.5.4 (An approach for minimising an étale cubic algebra over $\mathbb{P}^1_{\mathbb{Q}(t_1,...,t_n)}$)**.** Let $K/\mathbb{Q}$ be an étale cubic algebra, and let $f(X, Y) \in \mathbb{Z}[t_1, ..., t_n][X_0, X_1]$ be a homogeneous degree 3 polynomial such that K is isomorphic to $\mathbb{Q}(t_1, ..., t_n)[x]/(f(x, 1))$. Let $R = \mathbb{Z}[1/6][t_1, ..., t_n]$, and let $\mathcal{C} \subset \mathbb{P}^1_R$ be the subscheme given by the vanishing of $f(X_0, X_1)$.

Let $\Delta = \mathrm{disc}(f(x,1))$ be the discriminant of $f(x,1)$. For each irreducible divisor $\pi|\Delta$ such that $v_\pi(\Delta) \geq 2$ let $\overline{U} \in \mathrm{SL}_2(R/(\pi))$ be a matrix which transforms the singular locus of the special fibre of $\mathcal{C}$ at (π) to the point $(0:1)$. Let $U \in \mathrm{GL}_2(R_{(\pi)}) \cap \mathrm{M}_2(R)$ be an element which reduces to $\overline{U}$ modulo (π).

Applying U to $\mathcal{C}$ changes the discriminant to $\det(U)^6\Delta$. As in Example 2.5.1, replace $f(X_0, X_1)$ with $f(\pi X_0, X_1)/\pi^k$ for some appropriate $k \in \{2,3\}$.

By analogy between Example 2.5.2 and Example 2.5.4 we therefore have a minimisation construction for conic bundles fibred over $\mathbb{P}^n$. Or, equivalently, a theory of minimisation for conics with coefficients in $\mathbb{Q}(t_1,..,t_n)$. Similarly, the analogue between Example 2.5.3 and Example 2.5.4 provides a theory of minimisation for clusters of 4 points in $\mathbb{P}^2$ over $\mathbb{Q}(t_1,...,t_n)$.

Remark 2.5.5. Unfortunately, since $\mathbb{Z}[t_1,...,t_n]$ is far from being a principal ideal domain it seems too much to hope for that we could obtain any sort of "minimisation theorem" for the approach in Example 2.5.4. Indeed, there is no reason to believe that we may "simultaneously minimise" at different factors of the discriminant (for example, we may not be able to remove a factor introduced from $\det(U)$).

However, in many practical cases (e.g., Section 5.3) applying Example 2.5.4 (and its quartic analogue from Example 2.5.3) allowed us to minimise at most discriminant factors. It should be noted that the order in which these minimisation steps are carried out seemingly has a large impact on whether latter steps could be performed (without introducing large, spurious, factors into the discriminant).

In Section 4.4 we use this approach to compute a number of modular curves of composite level via fibre products, and similarly in Section 5.3 we compute fibre products of the surfaces $Z_{N,r}$. Throughout we suppress the details of these minimisation steps.

2.5.2 "Birational minimisation" and Cremona transformations

In the computations in this thesis we often want to compute birational models for moduli surfaces (e.g., the surfaces $Z^{\mathrm{sym}}_{N,r}$). Such models consist of the data for the surface *and* equations for the forgetful maps. Therefore we naturally want to simplify (i.e., reduce the degree of) 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 $\mathrm{Bir}_{\mathbb{Q}}(\mathbb{P}^2)$, the birational automorphism group of $\mathbb{P}^2$ over $\mathbb{Q}$, contains $\mathrm{PGL}_3(\mathbb{Q})$ 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 $G_{\mathbb{Q}}$-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 $Z^{\mathrm{sym}}_{N,r}$. Suppose that $Z^{\mathrm{sym}}_{N,r}$ is birational to $\mathbb{P}^2$. Let $j, j' \in \mathbb{Q}(Z_{N,r})$ be rational functions giving the moduli interpretation of $Z_{N,r}$ (i.e., such that the forgetful map $Z_{N,r} \to Z_1 = X(1) \times X(1)$ is given by (j,j')). For notational simplicity we define $J = j/1728$ and $J' = j'/1728$. It is clear that the rational functions JJ', $(J-1)(J'-1)$, and $(J-J')^2$ are rational functions on $Z^{\mathrm{sym}}_{N,r}$.

Let $C/\mathbb{Q}$ be a curve in $\mathbb{P}^2$ given by the vanishing of a factor of the numerator of JJ', $(J-1)(J'-1)$, or $(J-J')^2$. Applying a generic Cremona transformation to $\mathbb{P}^2$ will double the degree

of JJ', $(J-J')^2$, and $(J-1)(J'-1)$. If instead we apply a Cremona transformation centred at a $G_{\mathbb{Q}}$-stable triple of singular points $q_1, q_2, q_3 \in C(\overline{\mathbb{Q}})$ we may hope to decrease their degrees.

In Section 5.3 we often make choices of parametrisation which give rise to models for $Z^{\mathrm{sym}}_{N,r}$ with j-maps of small degree. In nearly every case the parametrisations we give were not our first choice. Once we have a birational map $\mathbb{A}^2 \dashrightarrow Z^{\mathrm{sym}}_{N,r}$ (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.

Chapter 3

On the geometry of the symmetric Hilbert modular surface $Z^{\mathrm{sym}}_{N,r}$

3.1 An outline of the proof of Theorems 1.0.4 and 1.0.6

In this chapter we prove Theorems 1.0.4 and 1.0.6. Our approach roughly follows the approach first applied by Hirzebruch [Hir73b] who studied the geometry of the symmetric Hilbert modular surfaces $Y^{\mathrm{sym}}_{\mathfrak{a}}(p)$, when p is a prime number. Our results extend work of Hermann [Her92] who studied the surfaces $Z^{\mathrm{sym}}_{p,r}$.

3.1.1 A simple example

In order to illustrate our approach to proving Theorems 1.0.4 and 1.0.6, we sketch the proof that the surface $Z^{\mathrm{sym}}_{33,5}$ is of general type.

First consider minimal desingularisation $\widetilde{Z}_{33,5}$ of $Z_{33,5}$. This is a smooth, projective surface of general type and it follows from [KS97, Theorem 2] that the geometric genus of $\widetilde{Z}_{33,5}$ is equal to 84. We wish to study the quotient $\widetilde{Z}_{33,5}$ by the involution $\tilde{\tau}$ induced by τ.

We will see in Proposition 3.3.17 that $\tilde{\tau}$ acts without isolated fixed points on $\widetilde{Z}_{33,5}$. It follows that the quotient $W_{33,5} = \widetilde{Z}_{33,5}/\tilde{\tau}$ is a smooth, projective surface.

When $(N, r) = (33, 5)$, the locus, $\boldsymbol{F}_{\tilde{Z}}$, of fixed points of $\tilde{\tau}$ consists of exactly one geometrically irreducible component. In fact, $\boldsymbol{F}_{\tilde{Z}}$ is isomorphic to the modular curve X_g^+ which arises as the quotient of $X(\mathrm{s}\,3, \mathrm{ns}\,11)$ by the diagonal involution (as described in Lemma 2.2.13). This modular curve has LMFDB label `33.660.40.b.1`.

A result of Hermann [Her91] gives a convenient description of the (numerical equivalence class of a) canonical divisor $K_{\tilde{Z}}$ on $\widetilde{Z}_{N,r}$ (see (3.2)). The quotient $W_{33,5}$ is a regular surface (see Theorem 3.6.1) and an observation of Hirzebruch [Hir73b, 5.1(1)] implies that the geometric genus of $W_{33,5}$ is given by

$$p_g(W_{33,5}) = \frac{1}{2}\left(p_g(\widetilde{Z}_{33,5}) - \frac{1}{4}K_{\tilde{Z}} \cdot \boldsymbol{F}_{\tilde{Z}} - 1\right).$$

From (3.2) we may compute $K_{\tilde{Z}} \cdot \boldsymbol{F}_{\tilde{Z}} = \frac{1}{3}\cdot 660 - 2\cdot 20 - \frac{1}{3}\cdot 0 = 180$ using only the index and number of cusps and elliptic points of order 3 on X_g^+ (see Lemma 3.5.2). Therefore $p_g(W_{33,5}) = 19$.

To determine the Kodaira dimension of $W_{33,5}$ we use Lemma 2.4.7, noting that since $p_g(W_{33,5}) \neq 0$ the surface $W_{33,5}$ cannot be rational. Let $\pi\colon \widetilde{Z}_{33,5} \to W_{33,5}$ denote the quotient morphism. If K_W is a canonical divisor on $W_{33,5}$, then $\pi^* K_W = K_{\tilde{Z}} - \boldsymbol{F}_{\tilde{Z}}$. In particular by the projection formula (Proposition 2.4.2) we have $2K_W^2 = K_{\tilde{Z}}^2 - 2K_{\tilde{Z}} \cdot \boldsymbol{F}_{\tilde{Z}} + \boldsymbol{F}_{\tilde{Z}}^2$. By [KS98, Theorem 2] we have $K_{\tilde{Z}}^2 = 536$, and by the adjunction formula (Proposition 2.4.1)

$$\begin{aligned}\boldsymbol{F}_{\tilde{Z}}^2 &= 2p_g(X_g^+) - K_{\tilde{Z}} \cdot \boldsymbol{F}_{\tilde{Z}} - 2\\ &= 2\cdot 40 - 180 - 2 = -102.\end{aligned}$$

Therefore $K_W^2 = 37 > 0$, and it follows from Lemma 2.4.7 that $Z_{33,5}^{\mathrm{sym}}$ is of general type.

3.1.2 An outline in the general case

The analysis for general pairs (N, r) follows the same rough structure, but is necessarily more complicated. Firstly, it is not always the case that $\tilde{\tau}$ acts without isolated fixed points on $\widetilde{Z}_{N,r}$. To remedy this, in Section 3.6 we construct a smooth birational model $Z_{N,r}^{\circ}$ for $\widetilde{Z}_{N,r}$ on which involution τ° induced by $\tilde{\tau}$ has no isolated fixed points.

The one dimensional component of the fixed point locus of $\tilde{\tau}$ is also more complicated for general N, and may consist of more than one irreducible component. Fortunately, these may be described explicitly in terms of the modular curves X_g^+ defined in Section 2.2.7 (see Corollary 3.3.11).

A final complication is that the criteria in Section 2.4.1 for classifying algebraic surfaces may not immediately be applicable to the quotients $W_{N,r} = Z_{N,r}^{\circ}/\tau^{\circ}$. To apply these results when N is small it is necessary to identify and contract (-1)-curves on $W_{N,r}$, and this is the subject of Sections 3.7 and 3.8.

At a first reading, the reader is encouraged to specialise first to the case when N is an odd prime power, and then to the case when N is odd and composite.

In Section 3.2 we restate several results from previous work of Hermann [Her91] and Kani–Schanz [KS98] who studied the geometry of the surfaces $Z_{N,r}$. They in particular give explicit formulae for geometric invariants of (certain models for) the surface $Z_{N,r}$.

Recall that $Z_{N,r}^{\mathrm{sym}}$ is defined to be the quotient of $Z_{N,r}$ by the involution τ constructed in Section 2.3.6. Following Hirzebruch's approach we determine the fixed points of the action of τ on $Z_{N,r}$ and its minimal desingularisation $\widetilde{Z}_{N,r}$ in Section 3.3. In particular, we show that the one dimensional component of the locus of fixed points is given by a union of curves which we call *diagonal Hirzebruch–Zagier divisors*, and for each pair (N, r) we determine these components explicitly in Corollary 3.3.11. This result is reminiscent of a result of Hausmann [Hau82, §2.2 Proposition] for the surface $Y_{\mathfrak{a}}(D)$ when D is fundamental (see also [vdG88, Proposition V.9.1]).

In Section 3.4 we determine the genera of the curves which appear in this way (which includes giving a genus formula for the modular curve associated to the *extended Cartan subgroups* of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$). We study the intersection theory of these and other curves on $\widetilde{Z}_{N,r}$ in Section 3.5.

By combining these contributions, in Section 3.6 we give an explicit construction for a non-singular projective surface $W_{N,r}$ which is birational to $Z_{N,r}^{\mathrm{sym}}$, and show that it is regular (i.e., $q(W_{N,r}) = 0$). We proceed to calculate its geometric genus and Chern number $c_1^2(W_{N,r})$ (the self-intersection of a canonical divisor), see Theorem 3.6.3 and Lemma 3.6.4. At this point Theorem 1.0.4 follows by bounding $p_g(W_{N,r})$ from below for large N.

To place these surfaces within the Enriques–Kodaira classification we make a brief detour in Section 3.7 to construct several additional modular curves on $W_{N,r}$ and we compute their self-intersections. Finally, equipped with bounds on the geometric genus and Chern numbers of $W_{N,r}$ obtained in Section 3.6.2, we prove Theorem 1.0.6 in Section 3.8. A key step in this proof is to use our construction of modular curves on $W_{N,r}$ to identify a number of contractible curves which we blow-down in order to arrive at a "close-to-minimal model" for the surface $W_{N,r}$.

3.2 The surface $Z_{N,r}$

We recall several facts about the surfaces $Z_{N,r}$ which we will use repeatedly in this work and fix notation for a number of interesting curves on $Z_{N,r}$. The results stated here can be found in greater detail in [KS98] and [Her91]. We summarise the notation from this section in Table 3.1.

Fix a matrix $\varepsilon \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of determinant r. Recall that by construction (see Definition 2.3.6) we have morphisms

$$X(N) \times X(N) \to \Delta_\varepsilon \backslash (X(N) \times X(N)) = Z_{N,r} \to Z_1 = X(1) \times X(1).$$

We write $\mathfrak{j}\colon Z_{N,r} \to X(1)$ and $\mathfrak{j}'\colon Z_{N,r} \to X(1)$ for the morphisms given by composing the forgetful map $Z_{N,r} \to X(1) \times X(1)$ with the projection maps onto the first and second factors respectively. We write $\mathfrak{D}$ for the diagonal in $X(1) \times X(1)$.

If $j \in X(1)$ is a general point (i.e., $j \notin \{0, 1728, \infty\}$) then, following Hermann [Her91, Her92] we define $C_{\star,1} = \mathfrak{j}^{-1}(j)$ and $C_{\star,2} = (\mathfrak{j}')^{-1}(j)$. Each fibre $C_{\star,i}$ is isomorphic to $X(N)$ over $\mathbb{C}$. In fact if K is a field of characteristic zero and $j \in K$ then each is K-isomorphic to the twist $X_E^r(N)$ where E/K is an elliptic curve with j-invariant j.

We recall that the support of the fibres $\mathfrak{j}^{-1}(\infty)$ and $(\mathfrak{j}')^{-1}(\infty)$ are irreducible curves which we denote by $C_{\infty,1}$ and $C_{\infty,2}$ respectively. Over $\mathbb{C}$ these are isomorphic (as covers of $X(1)$ given by $\mathfrak{j}'$, respectively $\mathfrak{j}$) to $X_1(N)$. In fact, as we saw in Proposition 2.3.13, the curves $C_{\infty,i}$ are naturally $\mathbb{Q}$-isomorphic to $X_\mu(N)$ as coverings of $X(1)$. Write $C_\infty = C_{\infty,1} + C_{\infty,2}$.

3.2.1 The minimal resolution of singularities

Points on $X(N)$ have stabilisers in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ whose image in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ are cyclic of order 1, 2, 3, or N. It follows that all singularities on $Z_{N,r}$ are cyclic quotient singularities (of order 2, 3, or d where $d|N$) and map to one of $(0,0)$, $(1728, 1728)$, or (∞, ∞) under the forgetful map $Z_{N,r} \to Z_1$. Moreover one can show that the only singularities are of type $(2,1)$, $(3,1)$, $(3,2)$, and (d,q) (see Definition 2.4.8) for some $q \in (\mathbb{Z}/d\mathbb{Z})^\times$ such that qr is a square mod d.

More precisely we have the following theorem of Hermann [Her91, Hilfssatz 1] and Kani–Schanz [KS98, Theorem 2.1]. For each integer m we define

$$\rho(d,m) = \begin{cases} \#\{x \in \mathbb{Z}/d\mathbb{Z} : x^2 = m\} & \text{if } (d,m) = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

For brevity we also define $\rho(d) := \rho(d,1)$, note that by definition $\rho(1,m) = \rho(1) = 1$.

Theorem 3.2.1 ([Her91, Hilfssatz 1], [KS98, Theorem 2.1])**.** *Let $h(-n)$ denote the class number of the imaginary quadratic order of discriminant $-n$.*

(i) *There are exactly $h(-4N^2)$ singular points on $Z_{N,r}$ above $(1728, 1728) \in Z_1$ all of which have type $(2,1)$.*

(ii) *There are exactly $h(-3N^2)$ singular points on $Z_{N,r}$ above $(0,0) \in Z_1$. If $3 \nmid N$ then $\frac{1}{2}h(-3N^2)$ are of type $(3,1)$ and $\frac{1}{2}h(-3N^2)$ are of type $(3,2)$, whereas if $3|N$ then all $h(-3N^2)$ are of type $(3,q)$ where $q \equiv r \pmod 3$.*

(iii) *For each $d|N$ such that $d \neq 1$, the surface $Z_{N,r}$ has exactly $\frac{1}{2}\rho(d, qr)\varphi(N/d)$ singular points of type (d,q) above $(\infty, \infty) \in Z_1$.*

The minimal resolution of singularities $\widetilde{Z}_{N,r} \to Z_{N,r}$ is therefore given by resolving these singularities as described in Proposition 2.4.10. In particular, the exceptional divisors of the resolution above each singular point of type (n,q) (with $n, q \in \mathbb{Z}$ chosen so that $q \in \{1, ..., n-1\}$) consists of chains of rational curves with self-intersection determined by the Hirzebruch–Jung continued fraction of the rational number n/q (see Proposition 2.4.10). The surface $\widetilde{Z}_{N,r}$ is regular

(see [Her91, Satz 1] and [KS98, Theorem 1]) and its geometric genus, Chern numbers, and Kodaira dimension are given by [KS98, Theorems 2 and 3].

We write $E_{2,1}$ for the divisor consisting of curves in the resolution of the singularities of type $(2,1)$ above $(1728, 1728) \in Z_1$. Similarly for each $q = 1, 2$ we define $E_{3,q}$ to be the divisor consisting of curves in the resolution of the singularities of type $(3,q)$ above $(0,0) \in Z_1$. Finally for each $d|N$ we define $E_{\infty,d,q}$ to be the divisor consisting of the curves in the resolution of the singularities of type (d,q) above $(\infty,\infty) \in Z_1$.

Define $\tilde{\mathfrak{j}}$ (resp. $\tilde{\mathfrak{j}}'$) to be the morphisms given by composing the resolution of singularities $\widetilde{Z}_{N,r} \to Z_{N,r}$ with $\mathfrak{j}$ (resp. $\mathfrak{j}'$). Hermann [Her91, p. 98] and Kani–Schanz [KS98, Proposition 2.5] give the following description of the multiplicities of the components of $\tilde{\mathfrak{j}}^*(\infty)$.

Lemma 3.2.2 ([Her91, p. 98], [KS98, Proposition 2.5])**.** *Let $\mathfrak{z}$ be a singular point of $Z_{N,r}$ of type (d,q) contained in $\mathfrak{j}^*(\infty)$, let $\sum_{i=1}^{\ell} E_{\mathfrak{z},i}$ be the component of $E_{\infty,d,q}$ in the resolution of $\mathfrak{z}$, and let $[[c_1, ..., c_\ell]]$ be the Hirzebruch–Jung continued fraction expansion of d/q.*

Consider the integers $a_i := a_i(d,q)$ and $a'_i := a'_i(d,q)$ defined by the recurrence relations

$$a_{i+1} = c_i a_i - a_{i-1} \qquad \text{and} \qquad a'_{i+1} = c_i a'_i - a'_{i-1}$$

and the boundary conditions $a_0 = a'_{\ell+1} = N$ and $a_{\ell+1} = a'_0 = 0$. Let $E_{\mathfrak{z},0} = \widetilde{C}_{\infty,1}$ and $E_{\mathfrak{z},\ell+1} = \widetilde{C}_{\infty,2}$, then for each $i = 0, ..., \ell+1$ the multiplicity of the component of $E_{\mathfrak{z},i}$ in $\tilde{\mathfrak{j}}^*(\infty)$ (respectively $(\tilde{\mathfrak{j}}')^*(\infty)$) is equal to a_i (respectively a'_i).

If D is a divisor on $Z_{N,r}$ we write $\widetilde{D}$ for the strict transform of D under the morphism $\widetilde{Z}_{N,r} \to Z_{N,r}$. The class of $\widetilde{C}_{\star,i}$ in the Néron–Severi group of $\widetilde{Z}_{N,r}$ is unchanged by the choice of $j \in X(1) \setminus \{0, 1728, \infty\}$, and we therefore obtain a well defined class $\widetilde{C}_\star = \widetilde{C}_{\star,1} + \widetilde{C}_{\star,2} \in \mathrm{NS}(\widetilde{Z}_{N,r})$.

Let $K_{\tilde{Z}}$ be a canonical divisor on $\widetilde{Z}_{N,r}$ and let $D_\infty = \widetilde{C}_\infty + \sum E_{\infty,d,q}$ where the sum is taken over all pairs (d,q) with $d|N$ and $q \in r((\mathbb{Z}/d\mathbb{Z})^\times)^2$. By [Her91, (4) p. 102] we have an algebraic equivalence

$$6K_{\tilde{Z}} \sim \widetilde{C}_\star - 6D_\infty - 2E_{3,1}$$

and therefore an equivalence of rational homology classes (i.e., elements of $H_2(\widetilde{Z}_{N,r}, \mathbb{Q})$)

$$K_{\tilde{Z}} \sim \frac{1}{6}\widetilde{C}_\star - D_\infty - \frac{1}{3}E_{3,1}. \tag{3.2}$$

Remark 3.2.3. The relation in (3.2) is the analogue of [Hir73b, 4.3 (19)] and [vdG88, VI. Proposition 2.8] for the surfaces $Y_{\mathfrak{a}}(D)$ when D is a fundamental discriminant. It is possible that this result can be generalised directly from their proof with the viewpoint in Section 2.3.

3.2.2 Intersections of the modular curves $\widetilde{F}_{m,\lambda}$ on $\widetilde{Z}_{N,r}$

Finally, we recall the following result of Hermann [Her91] which describes the components of D_∞ which meet the modular curves $\widetilde{F}_{m,\lambda}$ (see Definition 2.3.14), and the self-intersections of the modular curves $\widetilde{F}_{m,\lambda}$ (cf. the proof of [KS98, Proposition 2.14]).

One would expect from the relation in (3.2) that the intersection number $\widetilde{F}_{m,\lambda} \cdot K_{\tilde{Z}}$ should be predicted by the index of the Borel subgroup $\psi(m) = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G(\mathrm{b}\, m)]$ together with the number $\nu_\infty(m)$ of cusps on $X_0(m)$, and the number $\nu_3(m)$ of elliptic points of order 3 on $X_0(m)$. Indeed, the following result (which is due to Hermann [Her91, Hilfssätze 12–16]) shows that if $\widetilde{F}_{m,\lambda}$ is non-singular and if its intersections with the divisors $\widetilde{C}_\star$, D_∞, and $E_{3,1}$ occur with multiplicity one, then $\widetilde{F}_{m,\lambda} \cdot K_{\tilde{Z}} = \frac{1}{3}\psi(m) - \nu_\infty(m) - \frac{1}{3}\nu_3(m)$ as expected. However, if $m > N$ it can be the case

Surface	Divisor	Description	Image on Z_1
Z_1	$\mathfrak{D}$	$\{(x,x) : x \in X(1)\}$	
$Z_{N,r}$	$C_{\infty,1}$, $C_{\infty,2}$	The image of $\{\infty\} \times X(N)$ (resp. $X(N) \times \{\infty\}$) on $Z_{N,r}$	$\{\infty\} \times X(1)$, $X(1) \times \{\infty\}$
	C_∞	$C_{\infty,1} + C_{\infty,2}$	$(\{\infty\} \times X(1)) \cup (X(1) \times \{\infty\})$
	$C_{\star,1}$, $C_{\star,2}$	The image of $\{j\} \times X(N)$ (resp. $X(N) \times \{j\}$) on $Z_{N,r}$	$\{j\} \times X(1)$, $X(1) \times \{j\}$
$\widetilde{Z}_{N,r}$	$\widetilde{D}$	Strict transform of a divisor D on $Z_{N,r}$	$(\mathfrak{j} \times \mathfrak{j}')(D)$
	$E_{2,1}$	Total transform of singularities of type $(2,1)$ on $Z_{N,r}$ above $(1728, 1728)$	$(1728, 1728)$
	$E_{3,q}$	Total transform of singularities of type $(3,q)$ on $Z_{N,r}$ above $(0,0)$	$(0,0)$
	$E_{\infty,d,q}$	Total transform of singularities of type (d,q) on $Z_{N,r}$ above (∞,∞)	(∞,∞)
	D_∞	Total transform of C_∞ equivalently $\widetilde{C}_\infty + \sum E_{\infty,d,q}$	$(\{\infty\} \times X(1)) \cup (X(1) \times \{\infty\})$
	$\widetilde{C}_\star$	$\widetilde{C}_{\star,1} + \widetilde{C}_{\star,2}$	$(\{j\} \times X(1)) \cup (X(1) \times \{j\})$

Table 3.1: Our notation for certain divisors on the surfaces Z_1, $Z_{N,r}$ and $\widetilde{Z}_{N,r}$.

(even when $\widetilde{F}_{m,\lambda}$ is smooth) that the curve $\widetilde{F}_{m,\lambda}$ meets D_∞ at two components simultaneously. The function $\mathfrak{e}(N,m)$ in the lemma counts the contribution of these additional intersections to $\widetilde{F}_{m,\lambda} \cdot K_{\widetilde{Z}}$.

Lemma 3.2.4. *Let $m > 0$ be an integer such that mr is a square modulo N. For each divisor n of m let $q \in \{1, ..., N\}$ be chosen such that $m = n^2 q \pmod N$. Denote by $k := k(n)$ the unique index such that*

$$\frac{a_{k-1}(N,q)}{a'_{k-1}(N,q)} > \frac{m}{n^2} \geq \frac{a_k(N,q)}{a'_k(N,q)},$$

where $a_i(N,q)$ are the integers defined in Lemma 3.2.2. Let $s(n) > 0$, $t(n) \geq 0$ be the unique integers such that $m/n = s(n)a_k(N,q) + t(n)a_{k-1}(N,q)$ and $n = s(n)a'_k(N,q) + t(n)a'_{k-1}(N,q)$. Define the function[1]

$$\mathfrak{e}(N,m) = \sum_{n|m} \varphi\big(\gcd(s(n), t(n))\big) \left(\frac{s(n)+t(n)}{\gcd(s(n),t(n))} - 1\right).$$

Finally, let $\psi(m) = [\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : G(\mathfrak{b}\, m)]$ be the index of the Borel subgroup, $\nu_\infty(m)$ be the number of cusps on $X_0(m)$, and $\nu_3(m)$ be the number of elliptic points of order 3 on $X_0(m)$. Then we have:

(i) *The modular curve $\widetilde{F}_m$ meets the divisor D_∞ only at points in the pre-image of a singular point $\mathfrak{z} \in Z_{N,r}$ of type (N,q) where $m \equiv n^2 q \pmod N$ for some divisor n of m.*

[1] This is the function called $\rho(N,m)$ by Hermann [Her91].

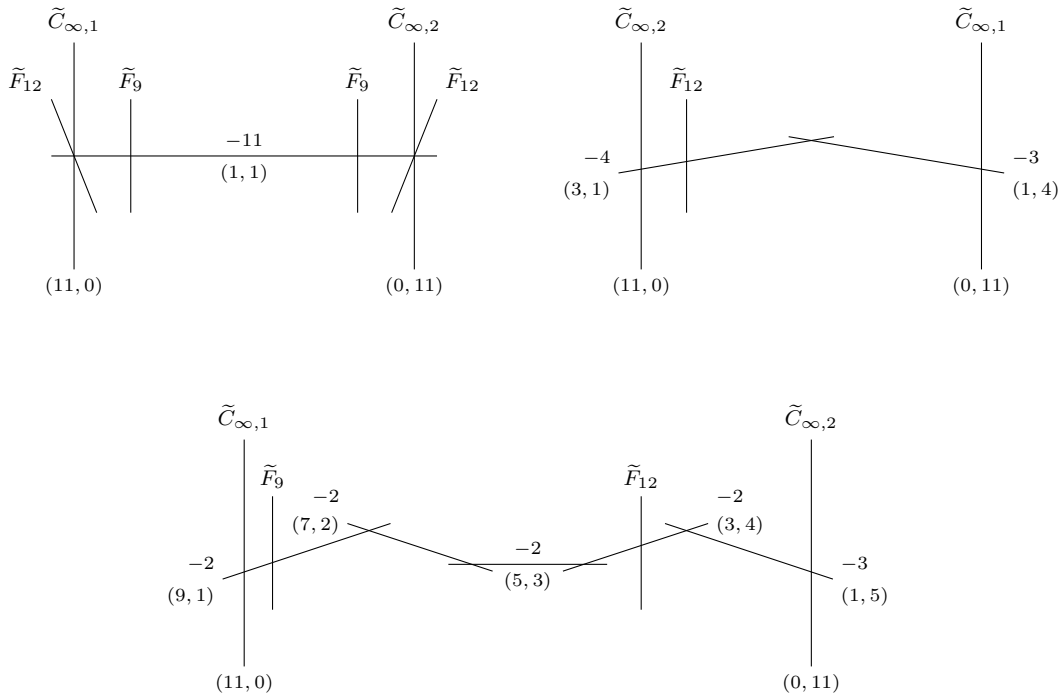


FIGURE 3.1: Intersections between the modular curves $\widetilde{F}_9$ and $\widetilde{F}_{12}$ and the divisor D_∞ on the surface $\widetilde{Z}_{11,1}$ as described in Example 3.2.6. The top left is a depiction in a neighbourhood of $E_{\infty,11,1}$, the top right is in a neighbourhood of $E_{\infty,11,3}$, and the bottom is in a neighbourhood of $E_{\infty,11,9}$. Self intersections of the components of $E_{\infty,11,q}$ and their muliplicities $(a_i(11,q), a_i'(11,q))$ in $\mathrm{j}^*(\infty)$ and $(\mathrm{j}')^*(\infty)$ are recorded. The intersections near $E_{\infty,11,4}$ and $E_{\infty,11,5}$ are respectively given by reflecting the divisors $E_{\infty,11,3}$ and $E_{\infty,11,9}$ across the vertical axis.

(ii) *If $\widetilde{F}_{m,\lambda}$ is an irreducible component of $\widetilde{F}_m$, then*

$$K_{\tilde{Z}} \cdot \widetilde{F}_{m,\lambda} = \frac{1}{3}\psi(m) - \nu_\infty(m) - \frac{1}{3}\nu_3(m) - \mathfrak{e}(N,m).$$

(iii) *For each $m < N$ each of the components $\widetilde{F}_{m,\lambda}$ of the curves $\widetilde{F}_m$ are non-singular, and in this case $\mathfrak{e}(N,m) = 0$.*

(iv) *If m and m' are integers such that $\widetilde{F}_{m,\lambda}$ and $\widetilde{F}_{m',\lambda'}$ are non-singular curves on $Z_{N,r}$ then if $m \neq m'$ or $\lambda \neq \lambda'$ we have $\widetilde{F}_{m,\lambda} \cdot \widetilde{F}_{m',\lambda'} = 0$.*

In particular if $N \geq 5$, $m \in \{1,2,3,4\}$ is coprime to N, and mr is a square modulo N, then all the irreducible components of $\widetilde{F}_{m,\lambda}$ are (-1)-curves.

Proof. The result is an abbreviation of Hilfssätze 12–16 of [Her91]. □

Remark 3.2.5. In the code attached to this work [Fre23b] we give functions which compute the data in Lemma 3.2.4 for any pair of coprime integers N and m.

We conclude this background section with an example illustrating the intersections of the modular curves $\widetilde{F}_9$ and $\widetilde{F}_{12}$ with the divisor D_∞ on the surface $\widetilde{Z}_{11,1}$.

Example 3.2.6 (Modular curves on $\widetilde{Z}_{11,1}$)**.** By Theorem 3.2.1 the surface $Z_{11,1}$ has exactly 5 singular points above (∞,∞) on Z_1. Indeed, these points are cyclic quotient singularities of type $(11,1)$, $(11,3)$, $(11,4)$, $(11,5)$, and $(11,9)$.

The resolutions of these singularities consist of chains of smooth rational curves whose number and self-intersections are determined by Hirzebruch–Jung continued fractions per Proposition 2.4.10. Indeed, the multiplicities $a_i(11,q)$ and $a'_i(11,q)$ of the components of D_∞ in $\tilde{\mathfrak{j}}^*(\infty)$ and $(\tilde{\mathfrak{j}'})^*(\infty)$ are then determined by the recurrence relations in Lemma 3.2.2. This is recorded in Figure 3.1.

Consider the modular curve $\widetilde{F}_9 \subset \widetilde{Z}_{11,1}$. By Lemma 3.2.4(i) the curve $\widetilde{F}_9$ meets D_∞ only in the resolutions of singularities of type $(11,1)$, $(11,5)$, and $(11,9)$. But the index of $G(\mathfrak{b}\,9)$ in $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ is equal to 12, so by the projection formula $\tilde{\mathfrak{j}}^*(\infty)\cdot\widetilde{F}_9 = 12$ (and similarly $(\tilde{\mathfrak{j}'})^*(\infty)\cdot\widetilde{F}_9 = 12$). This uniquely determines the components of $E_{\infty,11,1}$, $E_{\infty,11,5}$, and $E_{\infty,11,9}$ which $\widetilde{F}_9$ meets (as illustrated in Figure 3.1). Note that, in the notation of Lemma 3.2.4, these are the $k(n)^{\text{th}}$ components of $E_{\infty,11,9/n^2}$ for each $n|9$, and $t(n)=0$ in each case.

Contrast this with the curve $\widetilde{F}_{12} \subset \widetilde{Z}_{11,1}$. Again the components of $E_{\infty,11,1}$, $E_{\infty,11,3}$, $E_{\infty,11,4}$, $E_{\infty,11,5}$, and $E_{\infty,11,9}$ which are met by $\widetilde{F}_{12}$ are determined by the projection formula (see Figure 3.1). Note that $t(1)=t(12)=1$ which reflects the fact that the curve $\widetilde{F}_{12}$ meets (-11)-curve $E_{\infty,11,1}$ transversally at its "0^{th}" and "2^{nd}"-components ($\widetilde{C}_{\infty,1}$ and $\widetilde{C}_{\infty,2}$). This phenomenon is reflected in the fact that $\mathfrak{e}(11,12)=2\neq 0$.

Remark 3.2.7. By the projection formula one expects that (counting multiplicity) the intersection numbers of $\widetilde{F}_m$ with $\tilde{\mathfrak{j}}^*(\infty)$ in an (analytic) neighbourhood of $E_{\infty,N,m/n^2}$ is exactly equal to the set of *cusp width* (see e.g., [LMFDB, `https://www.lmfdb.org/knowledge/show/modcurve.cusp_widths`]) of the cusp(s) of $X_0(m)$ corresponding to the divisor $n|m$. That is, the ramification indices of the morphism $X_0(m)\to X(1)$ at these cusps.

In the code attached to this thesis [Fre23b] we provide `python`/`SageMath` [Sage] functionality (utilising `matplotlib`) to produce figures similar to Figure 3.1 for triples (N,d,q) by applying Remark 3.2.7.

3.3 The fixed points of τ

Let $\tau\colon Z_{N,r}\to Z_{N,r}$ be the involution defined in Section 2.3.6. By definition for a point $\mathfrak{z}=(E,E',\phi)\in Z_{N,r}$ we have $\tau(\mathfrak{z})=(E',E,r\phi^{-1})$. Let $\tilde{\tau}$ be the involution of $\widetilde{Z}_{N,r}$ induced by the action of τ on $Z_{N,r}$.

As in the case of Hilbert modular surfaces (see e.g., [Hir73b, Chapter 5], [HZ77], [Hau79], [Hau82], [Bas85], [vdG88, V.7]) our first task is to understand the locus of fixed points of the action of $\tilde{\tau}$ on the resolution of singularities $\widetilde{Z}_{N,r}$. We begin with a lemma which restricts the points on $Z_{N,r}$ whose total transforms we need to consider.

Lemma 3.3.1. *Suppose that a point $\mathfrak{z}=(E,E',\phi)\in Z_{N,r}$ is fixed by τ then $j(E)=j(E')$ and either*

(i) *the point $\mathfrak{z}$ is singular (hence $j(E)=j(E')\in\{0,1728,\infty\}$), or*

(ii) *the congruence ϕ satisfies $\phi^2=\pm r$ as an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Proof. Let $\varepsilon\in\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a matrix of determinant r. Since $\mathfrak{z}$ is fixed by τ it is immediate that $j(E)=j(E')$. If $\mathfrak{z}$ is non-singular, choose a preimage $\mathfrak{Z}=((E,\iota),(E',\iota'))\in X(N)\times X(N)$, that is, so that $\phi=(\iota')^{-1}\varepsilon\iota$. Since $\mathfrak{z}$ is non-singular the point $\mathfrak{Z}$ is stabilised only by $\pm 1\in\Delta_\varepsilon$. In particular, the assumption that $\mathfrak{z}=\tau(\mathfrak{z})$ implies that $\phi=\pm r\phi^{-1}$ as elements of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. □

We will see that in case (ii) of Lemma 3.3.1 the point $\mathfrak{z}$ is part of the one dimensional fixed locus of τ. We will classify both this fixed locus and the fixed points $\mathfrak{z} \in Z_{N,r}$ above $(0,0)$, $(1728, 1728)$, and (∞, ∞) (which will give rise to the isolated fixed points of the action of τ on $\widetilde{Z}_{N,r}$).

3.3.1 Modular curves and the one dimensional fixed locus

The points in Lemma 3.3.1(ii) appear to, in some sense, be continuously varying and parametrised by a finite number of elements of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. In fact, it is the case that all of these points lie on a finite union of irreducible curves fixed by the action of τ. To see this we make the following definition:

Definition 3.3.2. Let $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be an element of determinant r. We define the *diagonal Hirzebruch–Zagier divisor* $F_g^+ \subset Z_{N,r}$ to be the Zariski closure of the subset of $Z_{N,r}(\mathbb{C})$ consisting of the points $(E, E, \phi) \in Z_{N,r}$ where ϕ ranges over the $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$-conjugacy class of g.

We first show that for each F_g^+ is in fact an irreducible curve. In fact we show that the curves F_g^+ are birational to the modular curves X_g^+ defined in Section 2.2.7.

Lemma 3.3.3. *The curve F_g^+ is $\mathbb{Q}$-birational to the modular curve X_g^+.*

Proof. Let $K \subset \mathbb{Q}(\zeta_N)$ be a subfield over which X_g^+ decomposes into irreducible components and let X/K be such an irreducible component. Consider a generic elliptic curve $\mathcal{E}/K(X)$, and fix a basis for $\mathcal{E}[N]$ such that on this basis $\Phi = t \circ g \colon \mathcal{E}[N] \to \mathcal{E}^d[N]$ is an N-congruence for some choice of quadratic twist $t \colon \mathcal{E} \to \mathcal{E}^d$ of $\mathcal{E}$. Such a basis exists by Proposition 2.2.11. Consider the point $(\mathcal{E}, \mathcal{E}^d, \Phi) \in X_g^+$. By Proposition 2.3.10 it is clear that $(\mathcal{E}, \mathcal{E}^d, \Phi)$ is a point on F_g^+, thus by taking its Zariski closure we obtain a rational map $X \dashrightarrow F_g^+$ defined over K.

The irreducible components of X_g^+ are permuted by $\mathrm{Gal}(K/\mathbb{Q})$ and therefore repeating the above for each irreducible component, we obtain a dominant rational map $X_g^+ \dashrightarrow F_g^+$ defined over $\mathbb{Q}$. We therefore have a commutative diagram

$$\begin{array}{ccc} X_g^+ & \dashrightarrow & F_g^+ \\ & \searrow \quad \swarrow & \\ & X(1) & \end{array}$$

where the map on the right factors through the morphism $F_g^+ \to \mathfrak{D}$, where $\mathfrak{D}$ is the diagonal in $Z_1 = X(1) \times X(1)$. It therefore suffices to show that the morphism $F_g^+ \to \mathfrak{D}$ has degree $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : H_g^+]$. But this is clear since H_g^+ is by definition the preimage in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of the stabiliser of g when $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ acts on itself by conjugation. □

Theorem 3.3.4. *Let $\boldsymbol{F}_Z \subset Z_{N,r}$ be union of the one dimensional irreducible components of the fixed point locus of τ. Then $\boldsymbol{F}_Z = \sum_g F_g^+$ where g ranges over representatives for the conjugacy classes of $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ such that $\det(g) = r$ and $g^2 = \pm \det(g)$ for some choice of sign.*

Proof. The claim follows immediately from Lemmas 3.3.1 and 3.3.3. □

Corollary 3.3.5. *Let $g, h \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be elements such that $g^2 = \pm \det(g)$, $h^2 = \pm \det(g)$ and $\det(g) = \det(h) = r$. The curves $\widetilde{F}_g^+ \subset \widetilde{Z}_{N,r}$ are non-singular and therefore isomorphic to the modular curve X_g^+. Moreover, if $\widetilde{F}_g^+ \neq \widetilde{F}_h^+$ then $\widetilde{F}_g^+ \cdot \widetilde{F}_h^+ = 0$.*

Proof. Both claims follow by combining Theorem 3.3.4 with the fact that the one dimensional fixed component of a holomorphic involution acting on a smooth, projective, algebraic surface is a (possibly reducible) smooth curve. □

3.3.1.1 The components of $\boldsymbol{F}_Z$

By Theorem 3.3.4, in order to explicitly determine all the irreducible components of $\boldsymbol{F}_Z$ we must determine all the matrices $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $g^2 = \pm\det(g)$. We argue using the Chinese remainder theorem, first determining the relevant elements of $\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ in Lemma 3.3.7, and then patching them together in Lemma 3.3.8. This section concludes with Corollary 3.3.11, which describes the irreducible components of $\boldsymbol{F}_Z$. In particular, when N is an odd integer we show that (except for the Hirzebruch–Zagier divisor F_1) the only component of $\boldsymbol{F}_Z$ is an irreducible diagonal Hirzebruch–Zagier divisor "F_{w}^+". When $N = p^k$ is an odd prime power the curve F_{w}^+ is birational to the modular curve attached to the normaliser of a (split or non-split) Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ (when $k = 1$ this is [Her92, Hilfssatz 1]).

We first define a number of elements of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. In Lemmas 3.3.7 and 3.3.8 we will see that, together with the identity, these elements determine all the conjugacy classes of elements $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $g^2 = \pm\det(g)$. If $N = p^k$ is an odd prime power there are only two such elements, corresponding to a non-trivial element normalising the image of the split and non-split Cartan subgroups in $\mathrm{PGL}_2(\mathbb{Z}/p^k\mathbb{Z})$. As one might expect, the analysis is more complicated when $N = 2^k$, which yields additional cases in the following definition.

Definition 3.3.6. Let p be a prime number and $k \geq 1$ be an integer. Let r be an integer coprime to p and if p is odd fix an integer $\xi \in \mathbb{Z}$ which is a quadratic non-residue modulo p. Then:

(i) If $-r$ is a quadratic residue modulo p^k we define the element $g_{\mathrm{s}}(p^k, r) \in \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ to be

$$g_{\mathrm{s}}(p^k, r) = \alpha\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right).$$

Here $\alpha \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ is chosen such that $\alpha^2 \equiv -r \pmod{p^k}$.

(ii) If p is odd and $-r$ is a quadratic non-residue, or if $p = 2$ and $3r$ is a square modulo 2^k we define the element $g_{\mathrm{ns}}(p^k, r) \in \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ to be

$$g_{\mathrm{ns}}(p^k, r) = \begin{cases} \alpha\left(\begin{smallmatrix} 1 & -2 \\ 2 & -1 \end{smallmatrix}\right) & \text{if } p = 2, \text{ and} \\ \alpha\left(\begin{smallmatrix} 0 & \xi \\ 1 & 0 \end{smallmatrix}\right) & \text{if } p \text{ is odd.} \end{cases}$$

Here $\alpha \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ is chosen such that $\alpha^2 \equiv -r/\xi \pmod{p^k}$ if p is odd, and $\alpha^2 \equiv r/3 \pmod{2^k}$ if $p = 2$.

(iii) We define the element $g_{\mathrm{b}}(p^k) \in \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ to be

$$g_{\mathrm{b}}(p^k) = \left(\begin{smallmatrix} 1 & p^{k-1} \\ 0 & 1 \end{smallmatrix}\right).$$

(iv) If $p = 2$ we define the element $g_{\mathrm{c}}(2^k, r) \in \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ to be

$$g_{\mathrm{c}}(2^k, r) = \left(\begin{smallmatrix} 0 & -r \\ 1 & 0 \end{smallmatrix}\right).$$

(v) If p is an odd prime we define[2] $g_{\mathrm{w}}(p^k, r) \in \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ by

$$g_{\mathrm{w}}(p^k, r) = \begin{cases} g_{\mathrm{s}}(p^k, r) & \text{if } -r \text{ is a quadratic residue modulo } p, \text{ and} \\ g_{\mathrm{ns}}(p^k, r) & \text{if } -r \text{ is a quadratic non-residue modulo } p. \end{cases}$$

[2]The symbol "w" is chosen since $g_{\mathrm{w}}(p^k, r)$ is a matrix whose image is the non-trivial element of the Weyl group of an appropriately chosen (split or non-split) torus in $\mathrm{GL}_2/\mathbb{F}_p$.

If M is an odd integer we define $g_{\mathrm{w}}(M,r) \in \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ to be the unique element such that $g_{\mathrm{w}}(M,r) \equiv g_{\mathrm{w}}(p^k,r) \pmod{p^k}$ for each prime power $p^k|M$.

When the integers p^k and r are implicit, we will write $g_{\mathrm{s}} = g_{\mathrm{s}}(p^k,r)$, $g_{\mathrm{ns}} = g_{\mathrm{ns}}(p^k,r)$, $g_{\mathrm{b}} = g_{\mathrm{b}}(p^k)$, $g_{\mathrm{c}} = g_{\mathrm{c}}(2^k,r)$, and $g_{\mathrm{w}} = g_{\mathrm{w}}(p^k,r)$ for brevity.

To classify the irreducible components of $\boldsymbol{F}_Z$ we will need the following lemmas. We write $I \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for the identity matrix. Note that Lemma 3.3.7(i) appears in [Fre23a, Lemma 3.5][3].

Lemma 3.3.7. *Let p be a prime number, $k \geq 1$ be an integer, and let r be coprime to p.*

(i) *If p is odd the conjugacy classes of elements $g \in \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})/\{\pm 1\}$ of determinant r such that $g^2 = \pm\det(g)$ are represented by:*

- *λI and g_{w} if r is a quadratic residue modulo p, and*
- *g_{w} otherwise.*

Here λ ranges over elements of the set $\{x \in (\mathbb{Z}/p^k\mathbb{Z})^\times : x^2 = r\}/\{\pm 1\}$.

(ii) *If $p = 2$ the conjugacy classes of elements $g \in \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})/\{\pm 1\}$ of determinant r such that $g^2 = \pm\det(g)$ are represented by*

- *I and g_{c} if $k = 1$,*
- *I, g_{b}, and g_{c} if $k = 2$ and $r \equiv 1 \pmod 4$,*
- *g_{s}, g_{ns}, and g_{c} if $k = 2$ and $r \equiv 3 \pmod 4$,*
- *λI, λg_{b}, and g_{c} if $k \geq 3$ and $r \equiv 1 \pmod 8$,*
- *ωg_{ns} and g_{c} if $k \geq 3$ and $r \equiv 3 \pmod 8$,*
- *g_{c} if $k \geq 3$ and $r \equiv 5 \pmod 8$, and*
- *ωg_{s} and g_{c} if $k \geq 3$ and $r \equiv 7 \pmod 8$.*

Here λ ranges over elements of the set $\{x \in (\mathbb{Z}/2^k\mathbb{Z})^\times : x^2 = r\}/\{\pm 1\}$ and ω ranges over elements of the set $\{x \in (\mathbb{Z}/2^k\mathbb{Z})^\times : x^2 = 1\}/\{\pm 1\}$.

Proof. Let $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ have determinant r. Note that $g^2 = \pm\det(g)$ if and only if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \pm\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. In particular either $a = -d$, or $a = d$ and $2b = 2c = 0$.

We first prove (i). Suppose that p is odd and $g \neq \lambda I$ for any $\lambda \in (\mathbb{Z}/p^k\mathbb{Z})^\times$. Since p is odd if $\alpha^2 = -\det(g)$ we may choose $u, v \in \mathbb{Z}/p^l\mathbb{Z}$ such that the matrix

$$\gamma = \begin{pmatrix} (a+\alpha)u - bv & -(a-\alpha)u - bv \\ cu + (a-\alpha)v & -cu + (a+\alpha)v \end{pmatrix}$$

is invertible. Note that $\gamma^{-1}g\gamma = g_{\mathrm{s}}$ as required. Similarly if $\beta^2 = -\det(g)/\xi$ we may choose $u, v \in \mathbb{Z}/p^l\mathbb{Z}$ such that

$$\gamma = \begin{pmatrix} \beta u - bv & au \\ av & cu - \beta\xi v \end{pmatrix}$$

is invertible. Moreover $\gamma^{-1}g\gamma = g_{\mathrm{ns}}$.

To prove (ii), suppose that $p = 2$. It is simple to check using computer algebra (for example in `Magma`, see [Fre23b, `geometry/verify`]) that the claim holds for $k = 1$ and 2. We therefore assume

[3] There is a small error in the proof of [Fre23a, Lemma 3.5] since if $c = 0$ the matrix γ given there is not invertible. We provide a corrected proof here.

that $k \geq 3$. If $a = d$ and $2b = 2c = 0$, then g is conjugate to either λI or λg_{b} for some choice of $\lambda \in \{x \in (\mathbb{Z}/2^k\mathbb{Z})^\times : x^2 = r\}$. Suppose, therefore, that $a = -d$.

If either b or c is invertible we may choose $u, v \in \mathbb{Z}/2^k\mathbb{Z}$ such that

$$\gamma = \begin{pmatrix} u - bv & au \\ av & cu + rv \end{pmatrix}$$

is invertible and note that $\gamma^{-1} g \gamma = g_{\mathrm{c}}$. Otherwise we write $b = 2b'$ and $c = 2c'$, and note that $r = -a^2 - 4b'c' \equiv -1 \pmod 4$.

If $\det(g) \equiv -1 \pmod 8$ then for each choice of sign choose $s, t \in \mathbb{Z}/2^k\mathbb{Z}$ so that $2s = a + \alpha$ and $2t = a - \alpha$. Since either $b' \equiv 0 \pmod 2$ or $c' \equiv 0 \pmod 2$ we may choose $u, v \in \mathbb{Z}/2^k\mathbb{Z}$ such that

$$\gamma = \begin{pmatrix} su - b'v & -tu - b'v \\ c'u + tv & -c'u + sv \end{pmatrix}$$

is invertible and in this case $\gamma^{-1} g \gamma = g_{\mathrm{s}} \pmod{2^{k-1}}$. Therefore

$$\gamma^{-1} g \gamma = \begin{pmatrix} x & 2^{k-1}y \\ 2^{k-1}z & -x \end{pmatrix}$$

for some $x \in (\mathbb{Z}/2^k\mathbb{Z})^\times$ and $y, z \in \{0, 1\}$. But conjugating this matrix by $\left(\begin{smallmatrix} 1 & 2^{k-y-1} \\ 2^{k-z-1} & 1 \end{smallmatrix}\right)$ gives $\omega g_{\mathrm{s}}(2^k, r)$ for some choice of $\omega \in \{x \in (\mathbb{Z}/2^k\mathbb{Z})^\times : x^2 = 1\}$, as required.

Finally, suppose that $\det(g) \equiv 3 \pmod 8$, so both b' and c' are invertible. Choose $t \in (\mathbb{Z}/2^k\mathbb{Z})$ such that $2t = a - \beta$. Then $\gamma = \left(\begin{smallmatrix} -b' & 0 \\ t & \beta \end{smallmatrix}\right)$ is invertible and $\gamma^{-1} g \gamma \equiv g_{\mathrm{ns}} \pmod{2^{k-1}}$. Similarly to the previous case we may write

$$\gamma^{-1} g \gamma = \begin{pmatrix} x & 2^{k-1}y - 2 \\ 2^{k-1}z + 2 & -x \end{pmatrix}$$

for some $x \in (\mathbb{Z}/2^k\mathbb{Z})^\times$ and $y, z \in \{0, 1\}$. Conjugating this matrix by $\left(\begin{smallmatrix} 1 & 2^{k-y-1} \\ 2^{k-z-1} & 1 \end{smallmatrix}\right)$ gives $\omega g_{\mathrm{ns}}(2^k, r)$ for some $\omega \in \{x \in (\mathbb{Z}/2^k\mathbb{Z})^\times : x^2 = 1\}$, as required. □

The following lemma now generalises Lemma 3.3.7 to the case when N has two or more distinct prime factors.

Lemma 3.3.8. *Let $N = 2^k M$ where $k \geq 0$ and $M \neq 1$ is an odd integer. Let r be coprime to N and if $k \geq 1$, fix an isomorphism $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$.*

We have the following:

(i) *The element $g_{\mathrm{w}} \in \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})/\{\pm 1\}$ is (up to conjugation) the unique element such that $g_{\mathrm{w}}^2 = \pm\det(g_{\mathrm{w}})$ and such that $g_{\mathrm{w}} \neq \lambda I$ for any $\lambda \in (\mathbb{Z}/M\mathbb{Z})^\times$.*

(ii) *If $k = 0$, the conjugacy classes of elements $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ of determinant r, such that $g^2 = \pm\det(g)$, are represented by λI and g_{w} where λ ranges over elements of the set $\{x \in (\mathbb{Z}/N\mathbb{Z})^\times : x^2 = r\}/\{\pm 1\}$.*

(iii) *If $k \geq 1$, the conjugacy classes of elements $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ of determinant r, such that $g^2 = \pm\det(g)$, are represented by λI, $\lambda(g_{\mathrm{b}}, I)$, $(\omega g_{\mathrm{s}}, g_{\mathrm{w}})$, $(\omega g_{\mathrm{ns}}, g_{\mathrm{w}})$, and $(g_{\mathrm{c}}, g_{\mathrm{w}})$ where λ and ω range over elements of $\{x \in (\mathbb{Z}/N\mathbb{Z})^\times : x^2 = r\}/\{\pm 1\}$ and $\{x \in (\mathbb{Z}/2^k\mathbb{Z})^\times : x^2 = 1\}/\{\pm 1\}$ respectively.*

Proof. For (i), note that by Lemma 3.3.7(i) after conjugating by an element of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ we are free to assume that if $g^2 = \pm\det(g)$, then $g \equiv \lambda I$ or $\pm g_{\mathrm{w}} \pmod{p^k}$ for each prime power p^k dividing M. Note that $(\lambda I)^2 = \det(\lambda I)$ and $g_{\mathrm{w}}^2 = -\det(g_{\mathrm{w}})$. Also note that g_{w} is conjugate to $-g_{\mathrm{w}}$. In particular, we may assume that either $g = \lambda I$ for some $\lambda \in (\mathbb{Z}/M\mathbb{Z})^\times$, or $g \equiv g_{\mathrm{w}} \pmod{p^k}$ for each prime power p^k dividing M. But the latter condition uniquely determines an element of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. The claim in (ii) follows immediately from (i) noting that if $\det(\lambda I) = r$ then $\lambda^2 = r$.

To prove (iii) note that by (ii) and Lemma 3.3.7(ii) after conjugating by $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we may assume that $g \equiv \lambda I$ or $g_{\mathrm{w}} \pmod{M}$ and that $g \equiv \lambda I$, λg_{b}, $\pm\omega g_{\mathrm{s}}$, $\pm\omega g_{\mathrm{ns}}$, or $\pm g_{\mathrm{c}} \pmod{2^k}$ where $\lambda \in (\mathbb{Z}/N\mathbb{Z})^\times$. In $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ we have $(\lambda' I)^2 = \det(\lambda' I)$, $(\lambda' g_{\mathrm{b}})^2 = \det(\lambda' g_{\mathrm{b}})$, $(\omega g_{\mathrm{s}})^2 = -\det(\omega g_{\mathrm{s}})$, $(\omega g_{\mathrm{ns}})^2 = -\det(\omega g_{\mathrm{ns}})$, and $g_{\mathrm{c}}^2 = -\det(g_{\mathrm{c}})$ for each $\lambda' \in (\mathbb{Z}/2^k\mathbb{Z})^\times$. Hence if $g \equiv \lambda I \pmod{M}$ then either $g \equiv \lambda' I$ or $\lambda' g_{\mathrm{b}} \pmod{2^k}$ for some $\lambda' \in (\mathbb{Z}/2^k\mathbb{Z})^\times$. As above note that if $h \in \{\omega g_{\mathrm{ns}}, \omega g_{\mathrm{s}}, g_{\mathrm{c}}\}$ then h is conjugate to $-h$, so if $g \equiv g_{\mathrm{w}} \pmod{M}$ then we may take $g \equiv \omega g_{\mathrm{s}}$, ωg_{ns}, or $g_{\mathrm{c}} \pmod{2^k}$. □

For convenience we introduce the following notation:

Notation 3.3.9. Write $N = 2^k M$ be an integer, where $k \geq 0$ and M is an odd integer. Fix an isomorphism $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$.

(i) If $g_\bullet \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is an element with label "$\bullet$" we abbreviate the notation for the curves $X_\bullet^+ := X_{g_\bullet}^+$ and $F_\bullet^+ := F_{g_\bullet}^+$.

(ii) If $k \neq 0$ if $g_\bullet \in \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ and $g_\blacksquare \in \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ are elements with labels "$\bullet$" and "$\blacksquare$" we write $X_{(\bullet,\blacksquare)}^+ := X_{(g_\bullet, g_\blacksquare)}^+$ and $F_{(\bullet,\blacksquare)}^+ := F_{(g_\bullet, g_\blacksquare)}^+$.

(iii) If $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$ we write $X_{\alpha\bullet}^+ := X_{\alpha g_\bullet}^+$ and $F_{\alpha\bullet}^+ := F_{\alpha g_\bullet}^+$. Similarly if $k \neq 0$ we write $X_{\alpha(\bullet,\blacksquare)}^+ := X_{(\alpha g_\bullet, \alpha g_\blacksquare)}^+$ and $F_{\alpha(\bullet,\blacksquare)}^+ := F_{(\alpha g_\bullet, \alpha g_\blacksquare)}^+$.

(iv) If $k \neq 0$, $\alpha \in (\mathbb{Z}/2^k\mathbb{Z})^\times$, and $\beta \in (\mathbb{Z}/M\mathbb{Z})^\times$ we write $X_{(\alpha\bullet,\beta\blacksquare)}^+ := X_{(\alpha g_\bullet, \beta g_\blacksquare)}^+$ and $F_{(\alpha\bullet,\beta\blacksquare)}^+ := F_{(\alpha g_\bullet, \beta g_\blacksquare)}^+$.

With the convention that $g_I = I$, we will often take "$\bullet$" and "$\blacksquare$" to be "I", "s", "ns", "b", "c", or "w" from Definition 3.3.6 (later we will also take "$I^\sharp$" and "$\mathrm{b}^\sharp$", see Proposition 3.3.20).

Remark 3.3.10. It is simple to check that the diagonal Hirzebruch–Zagier divisor $\sum_\lambda F_{\lambda I}^+$ is exactly the "usual" Hirzebruch–Zagier divisor $F_1 = \sum_\lambda F_{1,\lambda}$.

The following corollary can be seen as a generalisation of an observation of Hermann [Her92, Hilfssatz 1] who notes that when $N = p$ is a prime number the one dimensional fixed locus of τ consists of either one or two irreducible components, one of which is birational to the modular curve associated to the normaliser of a Cartan subgroup[4]. The latter observation is also made by Fisher [Fis19, Sections 2.3 and 7] in the case when $p = 13$, though their argument applies more generally to all odd prime numbers.

[4] As defined therein [Her92, Hilfssatz 1] is false when -1 is a square modulo p. The subgroup $O_\epsilon(p)$ on p. 171 of *loc. cit.* should vary across $\epsilon \in \{1, \xi\}$ where $\xi \in \mathbb{F}_p^\times \setminus \left(\mathbb{F}_p^\times\right)^2$ and $\left(\frac{\epsilon}{p}\right) = \left(\frac{N}{p}\right)\left(\frac{\gamma_\nu}{p}\right)$. This ensures that $O_\epsilon(p)\backslash\mathbb{H}$ is the modular curve associated to the normaliser of the correct Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. This is presumably a typographical error since the genera in [Her92, (7)] agree with those of the *correct* modular curves.

Corollary 3.3.11. *Let $N = 2^k M$ where M is an odd integer and $k \geq 0$. Then $\boldsymbol{F}_Z$ decomposes into irreducible components as:*

$$\boldsymbol{F}_Z = \begin{cases} F^+_{\mathrm{w}} + \sum_\lambda F^+_{\lambda I} & \text{if } k = 0, \\ F^+_{(\mathrm{c,w})} + F^+_{(I,\mathrm{w})} + \sum_\lambda \left(F^+_{\lambda(\mathrm{b},I)} + F^+_{\lambda(I,I)} \right) & \text{if } k = 1, \\ F^+_{(\mathrm{c,w})} + \sum_\lambda \left(F^+_{\lambda(\mathrm{b},I)} + F^+_{\lambda(I,I)} \right) & \text{if } k = 2 \text{ and } r \equiv 1 \pmod 4, \\ F^+_{(\mathrm{c,w})} + F^+_{(\mathrm{s,w})} + F^+_{(\mathrm{ns,w})} & \text{if } k = 2 \text{ and } r \equiv 3 \pmod 4, \\ F^+_{(\mathrm{c,w})} + \sum_\lambda \left(F^+_{\lambda(\mathrm{b},I)} + F^+_{\lambda(I,I)} \right) & \text{if } k \geq 3 \text{ and } r \equiv 1 \pmod 8, \\ F^+_{(\mathrm{c,w})} + F^+_{(\mathrm{ns,w})} + F^+_{(\omega\mathrm{ns,w})} & \text{if } k \geq 3 \text{ and } r \equiv 3 \pmod 8, \\ F^+_{(\mathrm{c,w})} & \text{if } k \geq 3 \text{ and } r \equiv 5 \pmod 8, \\ F^+_{(\mathrm{c,w})} + F^+_{(\mathrm{s,w})} + F^+_{(\omega\mathrm{s,w})} & \text{if } k \geq 3 \text{ and } r \equiv 7 \pmod 8, \end{cases}$$

where $\omega = 2^{k-1} + 1$ and in the sums λ ranges over elements of $\{x \in (\mathbb{Z}/N\mathbb{Z})^\times : x^2 = r\}/\{\pm 1\}$.

Proof. By Theorem 3.3.4 it suffices to classify those $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ such that $g^2 = \pm \det(g)$. The claim then follows from parts (ii) and (iii) of Lemma 3.3.8, noting that in each case $\det(H_g^+) = (\mathbb{Z}/N\mathbb{Z})^\times$. □

Remark 3.3.12. When p is an odd prime number the curve F^+_{w} is equal to the curve which is denoted by Hermann as F_{p^2} [Her92]. The irreducible components of our curve $\boldsymbol{F}_Z$ are closely related to the curves $F_d \subset Y_{\mathfrak{a}}(D)$ for each $d|D$. These curves are closely studied by Hausmann [Hau79, Hau82] (see also [vdG88, Section V.9]) when D is a fundamental discriminant. Indeed, the reader should compare Corollary 3.3.11 and [Hau82, §2.2 Proposition] (see also [vdG88, Proposition V.9.1] and, when D is prime, [Pre73]).

3.3.2 The fixed points above 0 and 1728

We now determine the singular points of $Z_{N,r}$ fixed by the involution τ. We first give a description of the singular points of $Z_{N,r}$ which lends itself to direct calculations with matrices (cf. [KS98, Corollary 2.4]).

Lemma 3.3.13. *Let $E/\mathbb{C}$ be a (generalised) elliptic curve and let $\phi\colon E[N] \to E[N]$ be an (N,r)-congruence. Let G be the image of the homomorphism $\mathrm{Aut}(E) \to \mathrm{Aut}(E[N])$ and let*

$$G_{\mathfrak{z}} = \{g \in G : g\phi = \phi g' \text{ for some } g' \in G\} \subset G.$$

Then the group $\mathrm{PG}_{\mathfrak{z}} := G_{\mathfrak{z}}/\{\pm 1\}$ is cyclic.

The point $\mathfrak{z} = (E, E, \phi) \in Z_{N,r}$ is singular if and only if $\mathrm{PG}_{\mathfrak{z}} \neq 1$. In this case, if $g \in G_{\mathfrak{z}}$ is a generator for $\mathrm{PG}_{\mathfrak{z}}$ then $\mathfrak{z}$ is a cyclic quotient singularity of type (d, ℓ) where $d = |\mathrm{PG}_{\mathfrak{z}}|$ and $\ell \in \mathbb{Z}$ is such that $g\phi = \pm\phi g^\ell$.

Proof. First note that for every (generalised) elliptic curve $E/\mathbb{C}$ the group $G/\{\pm 1\}$ is cyclic (of order 1, 2, 3, or N), hence $\mathrm{PG}_{\mathfrak{z}}$ is cyclic.

Let $\mathfrak{Z} = ((E,\iota),(E,\iota')) \in X(N) \times X(N)$ be a preimage of $\mathfrak{z}$, that is $\phi = (\iota')^{-1}\varepsilon\iota$. The point $\mathfrak{z}$ is singular if and only if there exists $h \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \setminus \{\pm 1\}$ acting trivially on $\mathfrak{Z}$. Equivalently $h \in G$ and both $h\iota = \iota g$ and $\varepsilon h \varepsilon^{-1}\iota' = \iota' g'$ for some $g, g' \in G$. Thus if $\mathfrak{z}$ is singular we have $\phi = (\iota')^{-1}\varepsilon\iota = (\varepsilon h \varepsilon^{-1}\iota')^{-1}\varepsilon(h\iota) = (\iota' g')^{-1}\varepsilon(\iota g) = (g')^{-1}\phi g$.

Conversely assume there exist $g, g' \in G \setminus \{\pm 1\}$ such that $g'\phi = \phi g$. By choosing a basis for $E[N]$ (equivalently, a preimage $\mathfrak{Z}$ of $\mathfrak{z}$) we identify $\mathrm{Aut}(E[N]) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and are free to assume that ι is given on this basis by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. In particular we have $g\iota = \iota g$ and $\varepsilon g \varepsilon^{-1} \iota' = \iota' g'$. Hence $\mathfrak{z}$ is singular.

Let $T_{(E,\iota)}(X(N))$ be the tangent space to $X(N)$ at the point (E, ι). Note that (again choosing a basis for $E[N]$) the element g acts on the tangent space $T_{(E,\iota)}(X(N)) \cong \mathbb{C}$ by $z \mapsto \zeta z$ where $\zeta \in \mu_d$ is a primitive N^{th}-root of unity. Thus fixing an isomorphism $\mathrm{PG}_{\mathfrak{z}} \cong \mu_d$ given by $g \mapsto \zeta$ we see that $\mathrm{PG}_{\mathfrak{z}}$ acts on $T_{\mathfrak{Z}}(X(N) \times X(N)) \cong \mathbb{C}^2$ by $(z_1, z_2) \mapsto (\zeta z_1, \zeta^\ell z_2)$ after choosing ℓ such that $g' = \pm g^\ell$. In particular $\mathfrak{z}$ is a cyclic quotient singularity of type (d, ℓ). □

With the help of Lemma 3.3.13 we are now able to classify all the fixed points of the action of τ on $Z_{N,r}$ away from the cusps. In the case when $N = p$ is an odd prime this is proved in [Her92, Section 4]. Define the subgroups $G_0 = \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $G_{1728} = \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Lemma 3.3.14. *Let $E/\mathbb{C}$ be an elliptic curve of j-invariant 1728. Fix a basis for $E[N]$ so that the image of $\mathrm{Aut}(E) \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is equal to G_{1728}. A singular point $\mathfrak{z} = (E, E, \phi) \in Z_{N,r}$ is fixed by τ if and only if either*

(i) *the isomorphism class of the congruence ϕ contains either $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} a & N/2 \\ N/2 & a \end{smallmatrix}\right)$, or $\left(\begin{smallmatrix} a & -a \\ a & a \end{smallmatrix}\right)$ for some $a \in \mathbb{Z}/N\mathbb{Z}$, or*

(ii) *the isomorphism class of the congruence ϕ contains $\left(\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right)$.*

Proof. Let $\phi = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. By Lemma 3.3.13 the point $\mathfrak{z}$ is singular if and only if there exist $g, g' \in G_{1728} \setminus \{\pm 1\}$ such that $g\phi = \phi g'$. It follows from a direct calculation that either $\phi = \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right)$ (cf. [Her92, p.173]).

Similarly note that $\mathfrak{z}$ is fixed by τ if and only if there exists $g, g' \in G_{1728}$ such that $g\phi = \det(\phi)\phi^{-1} g'$ and it is simple to check that this occurs if and only if the isomorphism class of ϕ (i.e., the double coset $G_{1728}\phi G_{1728}$) contains an element of the form (i) or (ii). □

Lemma 3.3.15. *Let $E/\mathbb{C}$ be an elliptic curve of j-invariant 0. Fix a basis for $E[N]$ so that the image of $\mathrm{Aut}(E) \to \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is equal to G_0. A singular point $(E, E, \phi) \in Z_{N,r}$ is fixed by τ if and only if either*

(i) *the isomorphism class of the congruence ϕ contains either $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} a & 2a \\ -2a & -a \end{smallmatrix}\right)$ for some $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, or*

(ii) *the isomorphism class of the congruence ϕ contains $\left(\begin{smallmatrix} -a & b \\ a+b & a \end{smallmatrix}\right)$ for some $a, b \in \mathbb{Z}/N\mathbb{Z}$.*

Moreover, the singularities in (i) *are of type* $(3, 1)$ *and those in* (ii) *are of type* $(3, 2)$.

Proof. Let $\phi = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. As above by Lemma 3.3.13 the point $\mathfrak{z}$ is singular if and only if there exist $g, g' \in G_{1728} \setminus \{\pm 1\}$ such that $g\phi = \phi g'$. A calculation shows that either $\phi = \left(\begin{smallmatrix} a & b \\ -b & -b+a \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} -a & b \\ a+b & a \end{smallmatrix}\right)$. Similarly to Lemma 3.3.14 we see that $\mathfrak{z}$ is fixed by τ if and only if the isomorphism class of ϕ contains a congruence of the form (i) or (ii).

The second claim follows immediately from Lemma 3.3.13 by noting that in case (i) we have $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)\phi = \phi\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ and in case (ii) we have $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)\phi = \phi\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)^2$. □

It remains to translate the above description of the fixed *singular points* on $Z_{N,r}$ to a classification of fixed points on the resolution of singularities $\widetilde{Z}_{N,r}$. The following lemma allows us to pass easily between both descriptions. Historically it has proved very useful for computing the action

of involutions on Hilbert modular surfaces and this remains true for us (a proof of this lemma may be found in [vdG88, Lemma 7.8]).

Lemma 3.3.16 ([Hir73b, Section 5.3])**.** *Let S be a compact complex manifold, C be a non-singular rational curve on S, let τ be an involution of S such that $\tau(C) = C$. Then either τ acts as the identity on C or τ fixes exactly two points on C. In the latter case either*

(i) *$C \cdot C$ is odd, one of the fixed points of τ on C is an isolated fixed point of τ, and the other is a transversal intersection of C with a curve fixed pointwise by τ, or*

(ii) *$C \cdot C$ is even and either both of the fixed points of τ on C are isolated fixed points of τ, or both are transversal intersection points of C with a curve fixed pointwise by τ.*

Combining the descriptions in Lemmas 3.3.14 and 3.3.15 with Lemma 3.3.16, the following proposition gives a complete description of the fixed point set of the action of τ on $\widetilde{Z}_{N,r}$ away from the cusps. We write $h(-n)$ for the class number of the imaginary quadratic order of discriminant $-n$.

Proposition 3.3.17. *The action of $\tilde{\tau}$ on the open subvariety of $\widetilde{Z}_{N,r}$ outside a neighbourhood of $\tilde{\mathrm{j}}^{-1}(\infty) \cup (\tilde{\mathrm{j}}')^{-1}(\infty)$ is given by Figures 3.2–3.4 in a neighbourhood of the intersections depicted.*

Proof. First let $E/\mathbb{C}$ have $j(E) = 1728$ and fix a basis for $E[N]$ so that the automorphism i acts through $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. The 2-isogeny $(1+i)\colon E \to E$ induces the congruence $\phi = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 1 \end{smallmatrix}\right)$. Hence for each $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ where $2a^2 = r$ the point $(E, E, a\phi)$ from Lemma 3.3.14(i) lies on the divisor F_2.

Similarly let $E/\mathbb{C}$ have $j(E) = 0$ and fix a basis for $E[N]$ so that the automorphism ζ_3 acts through $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$. The 3-isogeny $(1 - 2\zeta_3)\colon E \to E$ induces the congruence $\phi = \left(\begin{smallmatrix} 1 & 2 \\ -2 & -1 \end{smallmatrix}\right)$. For each $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ where $3a^2 = r$ the point $(E, E, a\phi)$ from Lemma 3.3.15(ii) lies on the divisor F_3.

Points on F_g^+ above $j = 0, 1728$ are in bijective correspondence with double cosets $G_0\,\phi\,G_0$ (respectively $G_{1728}\,\phi\,G_{1728}$) where ϕ ranges over $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$-conjugates of g. When $j = 1728$ the congruences $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a & N/2 \\ N/2 & a \end{smallmatrix}\right)$ in Lemma 3.3.14(i) therefore correspond to points on $\sum_\lambda F^+_{\lambda I}$ and $\sum_\lambda F^+_{\lambda(\mathrm{b},I)}$ respectively (the latter occurring only when $2|N$). When $N \equiv 1 \pmod 2$ the former lie on F^+_{w}, when $N \equiv 2 \pmod 4$ the former lie on $F^+_{(I,\mathrm{w})}$ and the latter lie on $F^+_{(\mathrm{c},\mathrm{w})}$, and when $N \geq 4$ both lie on $F^+_{(\mathrm{c},\mathrm{w})}$. Similarly, when $j = 0$ the congruences $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ lie on $\sum_\lambda F^+_{\lambda I}$.

For fixed r there are $\#\{a^2 + b^2 = -r : a, b \in \mathbb{Z}/N\mathbb{Z}\}$ matrices of the form in Lemma 3.3.14(ii). Let $N = 2^k M$ where M is odd. Such matrices then give rise to

$$s_{2,1}(N,r) := \begin{cases} \dfrac{1}{4} \cdot 2^k \cdot M \displaystyle\prod_{p|M} \left(1 - \frac{1}{p}\left(\frac{-1}{p}\right)\right) = \frac{1}{2}h(-4N^2) & \text{if } k \leq 1, \\[2ex] \dfrac{1}{4} \cdot 2^{k+1} \cdot M \displaystyle\prod_{p|M} \left(1 - \frac{1}{p}\left(\frac{-1}{p}\right)\right) = h(-4N^2) & \text{if } k \geq 2 \text{ and } r \equiv 3 \pmod 4, \text{ and} \\[2ex] 0 & \text{if } k \geq 2 \text{ and } r \equiv 1 \pmod 4 \end{cases}$$

points on $Z_{N,r}$ of the type in Lemma 3.3.14(ii). When $k = 0$ all such points lie on F^+_{w} and when $k = 1$ half lie on $F^+_{(I,\mathrm{w})}$ and half lie on $F^+_{(\mathrm{c},\mathrm{w})}$. In the case where $k \geq 2$ exactly $\frac{1}{2}h(-4(N/2)^2)$ lie on $F^+_{\lambda(\mathrm{ns},\mathrm{w})}$, similarly $\frac{1}{2}h(-4(N/2)^2)$ lie on $F^+_{\lambda(\mathrm{s},\mathrm{w})}$, and the remaining 0 or $\frac{1}{2}h(-4N^2)$ (depending on the residue class of r modulo 4) lie on $F^+_{(\mathrm{c},\mathrm{w})}$.

There are $\#\{a^2 + ab + b^2 = -r : a, b \in \mathbb{Z}/N\mathbb{Z}\}$ matrices of the form in Lemma 3.3.15(ii).

Therefore there are

$$s_{3,2}(N,r) := \begin{cases} \frac{1}{6}\cdot N\prod_{p\mid N}\left(1-\frac{1}{p}\left(\frac{-3}{p}\right)\right) = \frac{1}{2}h(-3N^2) & \text{if } 3\nmid N \\ 2\cdot\frac{1}{6}\cdot N\prod_{p\mid N}\left(1-\frac{1}{p}\left(\frac{-3}{p}\right)\right) = h(-3N^2) & \text{if } 3\mid N \text{ and } r\equiv 2 \pmod 3, \text{ and} \\ 0 & \text{if } 3\mid N \text{ and } r\equiv 1 \pmod 3 \end{cases}$$

points on $Z_{N,r}$ of the type in Lemma 3.3.15(ii). When N is odd, respectively even, all of these points lie on F^+_{w}, respectively $F^+_{(\mathrm{c,w})}$.

Finally, to determine the isolated fixed points of $\tilde{\tau}$, we argue as follows. Recall from Lemma 3.2.4 that for $N \geq 5$ the modular curves $\widetilde{F}_{m,\lambda}$ are smooth rational (-1)-curves.

Any irreducible curve C on $\widetilde{Z}_{N,r}$ which intersects $\boldsymbol{F}_{\tilde{Z}}$ cannot be pointwise fixed by $\tilde{\tau}$ (since the one dimensional component of an involution acting on a smooth projective surface is itself smooth). It follows that, away from the cusps, none of the components of the exceptional divisor of the resolution of singularities $\widetilde{Z}_{N,r} \to Z_{N,r}$ are pointwise fixed by $\tilde{\tau}$, except possibly for those in the resolution of the singularities of type $(2,1)$ given by the matrices $\left(\begin{smallmatrix} a & -a \\ a & a \end{smallmatrix}\right)$ (i.e., the only non-cuspidal fixed points of $Z_{N,r}$ which do not lie on $\boldsymbol{F}_Z$). But if a component of the resolution were pointwise fixed by $\tilde{\tau}$, then after blowing down the (-1)-curve $\widetilde{F}_{2,\lambda}$ the one dimensional fixed point locus on the resulting surface would not be smooth.

The claim follows through repeated applications of Lemma 3.3.16. □

Remark 3.3.18. It is no coincidence that the number of fixed points occurring in Proposition 3.3.17 are given by class numbers of imaginary quadratic orders. Indeed, the isolated fixed points lying on a modular curve $F_{m,\lambda}$ may be described in terms of equivalence classes of binary quadratic forms. In the case of fundamental discriminants Hirzebruch–Zagier [HZ76, 1.1] (cf. [vdG88, V.6]) showed how one may attach a positive definite binary quadratic form of discriminant divisible by D to each "special" elliptic point of $\Gamma(\mathcal{O}_D,\mathfrak{a})\backslash\mathbb{H}^2$. It can furthermore be shown that an isolated elliptic point, fixed by $\tilde{\tau}$, must correspond to an *ambiguous* binary quadratic form. This approach is utilised by Hausmann [Hau79, Hau82] to classify the fixed points of the action of $\tilde{\tau}$ on the Hilbert modular surface $Y_{\mathfrak{a}}(D)$ for every fundamental discriminant D.

Hermann [Her92, Section 4] describes how this generalises to the surfaces $Z_{p,r}$ when p is an odd prime number. In their setting all the fixed points of the type in Lemma 3.3.14(i) and Lemma 3.3.15(i) correspond to ambiguous, primitive, binary quadratic forms with content coprime to p and discriminant $-4p^2$ and $-3p^2$ respectively. These $\frac{1}{2}(2\rho(p,r)+\rho(p,2r)+\rho(p,3r))$ fixed points correspond to the forms $[1,0,p^2], [1,1,\frac{3p^2+1}{4}], [2,2,\frac{p^2+1}{2}], [3,3,\frac{p^2+3}{4}]$ given in [Her92, p. 173].

Ernst Kani has shared with us his preprint [Kan23] where he attaches to a modular curve $F_{m,\lambda} \subset Z_{N,-1}$ a binary quadratic form. It may be possible to prove Proposition 3.3.17 using this, together with the analogue of Hausmann and Hermann's approach.

The reader is encouraged to compare the following figures with those of Hirzebruch [Hir73b, 5.4 (8)] for Hilbert modular surfaces for fundamental discriminants.

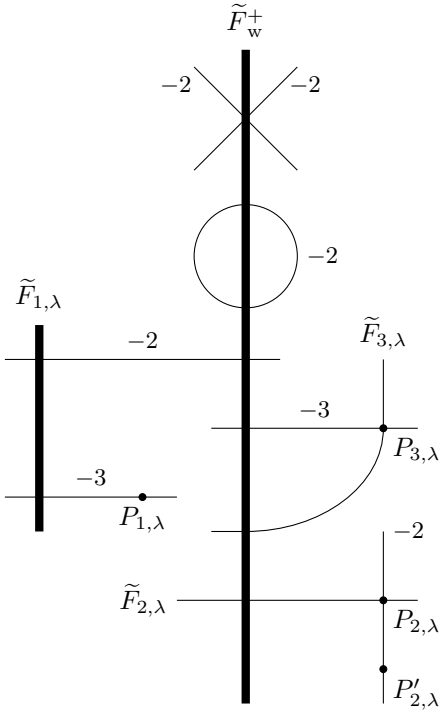


Figure 3.2: The action of the involution $\tilde{\tau}$ on the non-cuspidal locus when N is odd. Curves and points in bold are fixed by $\tilde{\tau}$ and numbers indicate self-intersections of resolution curves. Here

- λ ranges over the $\frac{1}{2}\rho(N,r)$ elements of the group $\{x \in \mathbb{Z}/N\mathbb{Z} : x^2 = r\}/\{\pm 1\}$,
- the circles occur $s_{2,1}(N,r) = \frac{1}{2}h(-4N^2)$ times, and
- the crosses occur $s_{3,2}(N,r)$ times.

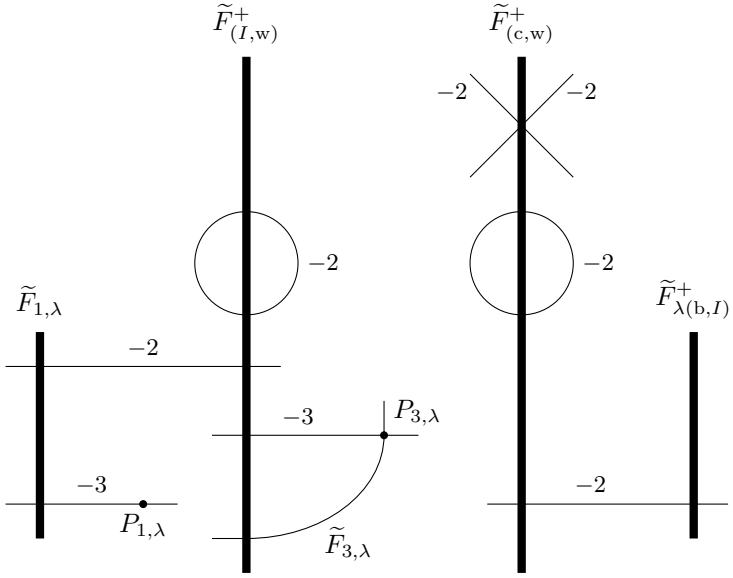


Figure 3.3: The action of the involution $\tilde{\tau}$ on the non-cuspidal locus when $N \equiv 2 \pmod 4$. Curves and points in bold are fixed by $\tilde{\tau}$ and numbers indicate self-intersections of resolution curves. Here

- λ ranges over the $\frac{1}{2}\rho(N,r)$ elements of the group $\{x \in \mathbb{Z}/N\mathbb{Z} : x^2 = r\}/\{\pm 1\}$,
- the circle on $\widetilde{F}^+_{(I,\mathrm{w})}$ occurs $\frac{1}{2}h(-4(N/2)^2)$ times, the circle on $\widetilde{F}^+_{(\mathrm{c},\mathrm{w})}$ occurs $\frac{1}{2}h(-4(N/2)^2)$ times, and
- the cross occurs $s_{3,2}(N,r)$ times.

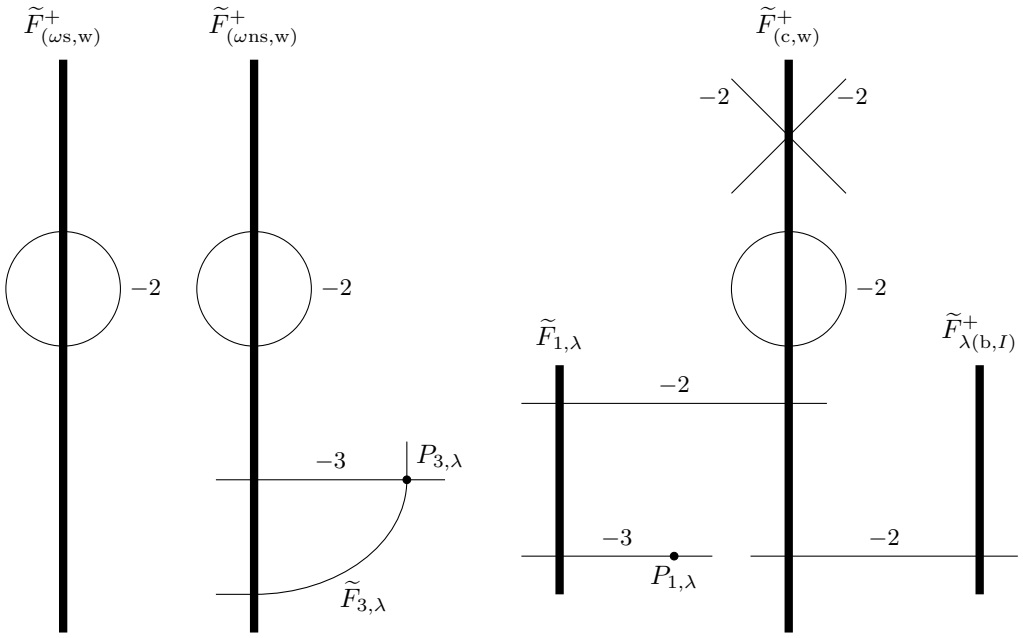


FIGURE 3.4: The action of the involution $\tilde{\tau}$ on the non-cuspidal locus when $N \equiv 0 \pmod 4$. Curves and points in bold are fixed by $\tilde{\tau}$ and numbers indicate self-intersections of resolution curves. Here

- λ ranges over the $\frac{1}{2}\rho(N,r)$ elements of the group $\{x \in \mathbb{Z}/N\mathbb{Z} : x^2 = r\}/\{\pm 1\}$,
- ω ranges over elements of the group $\{x \in \mathbb{Z}/2^k\mathbb{Z} : x^2 = 1\}/\{\pm 1\}$,
- the curves $\widetilde{F}^+_{(\omega\mathrm{s,w})}$ occur only when $7r$ is a square modulo 2^k,
- the curves $\widetilde{F}^+_{(\omega\mathrm{ns,w})}$ occur only when $3r$ is a square modulo 2^k,
- the circles on $\widetilde{F}^+_{(\omega\mathrm{s,w})}$ and $\widetilde{F}^+_{(\omega\mathrm{ns,w})}$ occur $\frac{1}{2}h(-4(N/2)^2)$ times on each irreducible component,
- the circle on $\widetilde{F}^+_{(\mathrm{c,w})}$ occurs $\frac{1}{2}h(-4N^2)$ times if $r \equiv 3 \pmod 4$ and does not occur otherwise,
- the cross occurs $s_{3,2}(N,r)$ times.

3.3.3 The action of τ on the cusps

We now classify the fixed cusps of $Z_{N,r}$ under the action of τ. Let G_∞ denote the subgroup $\left\{\left(\begin{smallmatrix}\pm 1 & \alpha \\ 0 & \pm 1\end{smallmatrix}\right) : \alpha \in \mathbb{Z}/N\mathbb{Z}\right\} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Recall that we write $\mathcal{E}_N$ for the standard N-gon (see Section 2.2.8).

Lemma 3.3.19. *Fix a basis for $\mathcal{E}_N$ such that the image of $\mathrm{Aut}(\mathcal{E}_N) \to \mathrm{Aut}(\mathcal{E}_N[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is equal to G_∞. A cusp $\mathfrak{z} = (\mathcal{E}_N, \mathcal{E}_N, \phi)$ of $C_{\infty,1}$ (and $C_{\infty,2}$) is fixed if and only if either:*

(i) *the congruence ϕ is contained in the isomorphism class of the congruence $\left(\begin{smallmatrix} a & 0 \\ bd & a^{-1}r\end{smallmatrix}\right)$ of type* (2.3) *in Proposition 2.3.13 and one of the following conditions holds:*

  (a) *$d = N$ and $a^2 \equiv r \pmod d$, or*

  (b) *$N \neq 2$ is divisible by 2, $d = N/2$, and $a^2 \equiv r \pmod d$, or*

  (c) *$a^2 \equiv -r \pmod d$.*

(ii) *the congruence ϕ is contained in the isomorphism class of the congruence $\left(\begin{smallmatrix} 0 & -a^{-1}r \\ a & 0\end{smallmatrix}\right)$ of type* (2.4) *in Proposition 2.3.13.*

Moreover in case (i) *the point $\mathfrak{z}$ is a cyclic quotient singularity of type $(d, a^{-2}r)$ and in case* (ii) *the point $\mathfrak{z}$ is a non-singular point of $Z_{N,r}$ at which $C_{\infty,1}$ and $C_{\infty,2}$ intersect transversally.*

Proof. The point $\mathfrak{z}$ is fixed by τ if and only if there exist $g, g' \in G_\infty$ such that $g\phi = r\phi^{-1}g'$.

In case (i) let ϕ be given by $\left(\begin{smallmatrix} a & 0 \\ bd & a^{-1}r\end{smallmatrix}\right)$ where $d|N$, $d \neq 1$, $1 \leq a \leq d$, and $b \in (\mathbb{Z}/(N/d)\mathbb{Z})^\times$, as in Proposition 2.3.13. If (a) or (b) holds then taking $g = g' = I$ we see that $g\phi = r\phi^{-1}g'$ as required. In case (c) we may take $g = \left(\begin{smallmatrix} -1 & \alpha \\ 0 & -1\end{smallmatrix}\right)$ and $g' = \left(\begin{smallmatrix} 1 & \beta \\ 0 & 1\end{smallmatrix}\right)$ where $\alpha = \beta = b^{-1}(a^{-1}r + a)/d$.

Conversely let $\phi = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$. If $\mathfrak{z}$ is fixed by τ then there are $g, g' \in G_\infty$ such that $g\phi = r\phi^{-1}g'$. Letting $g = \left(\begin{smallmatrix} u & \alpha \\ 0 & u\end{smallmatrix}\right)$ and $g' = \left(\begin{smallmatrix} v & \beta \\ 0 & v\end{smallmatrix}\right)$ we have

$$\begin{pmatrix} au + \alpha bd & \alpha a^{-1}r \\ bdu & a^{-1}ru \end{pmatrix} = \begin{pmatrix} a^{-1}rv & \beta a^{-1}r \\ -bdv & av - \beta bd \end{pmatrix} \tag{3.3}$$

and therefore $a^2u \equiv rv \pmod d$ and $bd(u+v) \equiv 0 \pmod N$. Since $u + v \in \{0, \pm 2\}$ and b is invertible modulo N it follows that (a), (b), or (c) respectively hold in the cases where (a) $d = N$, (b) 2 divides N and $d = N/2$, and (c) $u = -v$.

Let $g = \left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1\end{smallmatrix}\right)$. If $\ell \in \mathbb{Z}$ is such that $g\phi = \phi g^\ell$ then a direct calculation shows that $\alpha d = 0$ and $\ell = a^{-2}r$. By Lemma 3.3.13 it follows that $\mathfrak{z}$ is a singular point of type $(d, a^{-2}r)$.

In case (ii) we may take $\phi = \left(\begin{smallmatrix} 0 & -a^{-1}r \\ a & 0\end{smallmatrix}\right)$ and therefore the cusp $\mathfrak{z}$ is fixed since we may take $g = I$ and $g' = -I$. Moreover in this case if $g, g' \in G_\infty$ satisfy $g\phi = \phi g'$ then $g = g' \in \{\pm I\}$, i.e., $\mathfrak{z}$ is non-singular. □

With the aid of Lemma 3.3.16 we now classify the cusps fixed by $\tilde{\tau}$.

Proposition 3.3.20. *The fixed divisor $\boldsymbol{F}_{\widetilde{Z}}$ meets the curves $\widetilde{C}_{\infty,i}$ only at the $\frac{1}{2}\varphi(N)$ intersection points of $\widetilde{C}_{\infty,1}$ and $\widetilde{C}_{\infty,2}$. The intersections of $\boldsymbol{F}_{\widetilde{Z}}$ and $\widetilde{C}_{\infty,i}$ are transversal, when N is odd these occur on the component $\widetilde{F}^+_{\mathrm{w}}$ and when N is even these occur on the component $\widetilde{F}^+_{(\mathrm{c,w})}$.*

The involution $\tilde{\tau}$ acts on the surface $\widetilde{Z}_{N,r}$ in a neighbourhood of the resolution divisors as described in Tables 3.2–3.5.

Proof. The involution $\tilde{\tau}$ takes $\widetilde{C}_{\infty,1}$ to $\widetilde{C}_{\infty,2}$. In particular if a point on $\widetilde{C}_{\infty,i}$ is fixed by $\tilde{\tau}$ then it is contained in their intersection. Such intersection points are precisely the cusps of type (ii) in

Lemma 3.3.19 and meet the divisor $\boldsymbol{F}_{\tilde{Z}}$ at the components indicated. Since the intersections of $\widetilde{C}_{\infty,1}$ and $\widetilde{C}_{\infty,2}$ occur with multiplicity one [KS98, Proposition 2.5(d)] so do the intersections of $\boldsymbol{F}_{\tilde{Z}}$ and $\widetilde{C}_{\infty,1}$ (respectively $\widetilde{C}_{\infty,2}$).

The intersections of the curves F_g^+ with the points on $Z_{N,r}$ above the cusps on the diagonal in $X(1) \times X(1)$ follows from the construction of F_g^+ together with the explicit description of the fixed cusps in Lemma 3.3.19. That is, a point $(\mathcal{E}_N^{\mathrm{sm}}, \mathcal{E}_N^{\mathrm{sm}}, \phi)$ lies on F_g^+ if and only if ϕ is conjugate to an element of the double coset $G_\infty g G_\infty$.

The remaining fixed points of τ acting on C_∞ are those singular points of the type $(d, \pm 1)$ with the case $(d, 1)$ occurring if and only if $d = N, N/2$. The number of such singularities is given in [KS98, Theorem 2.1]. Precisely, on the surface $Z_{N,r}$ there are exactly $\frac{1}{2}\rho(d, qr)\phi(N/d)$ singularities of type (d, q) at the cusp for each $q \in (\mathbb{Z}/d\mathbb{Z})^\times$.

Note that the Hirzebruch–Jung continued fraction of $\frac{d}{1}$ is equal to $[[d]]$, and the continued fraction of $\frac{d}{d-1}$ is $[[2, 2, ..., 2, 2]]$ where the length of this sequence is $d - 1$. In particular the resolution of a singularity of type $(d, 1)$ consists of a single rational curve of self-intersection $-d$, and the resolution of a singularity of type $(d, -1)$ consists of a chain of $d - 1$ rational curves of self-intersection -2. The number and configuration of fixed points on these resolutions follows from Lemmas 3.3.16 and 3.3.19.

It remains to describe the curves which pass through the isolated fixed points. We first recall from [Her91, Hilfssatz 16] that when N is odd the modular curves $\widetilde{F}_{4,\lambda}$ are (-1)-curves on $\widetilde{Z}_{N,r}$. Moreover, the involution $\tilde{\tau}$ acts as the Fricke involution on $\widetilde{F}_{4,\lambda} \cong X_0(4)$, which has a unique fixed cusp. The curve $\widetilde{F}_{4,\lambda}$ meets the 1-dimensional fixed locus $\boldsymbol{F}_Z \subset Z_{N,r}$ at the image of the CM point of $X_0(4)$ corresponding to the order of discriminant -16. By Lemma 3.3.16 the curve $\widetilde{F}_{4,\lambda}$ therefore meets the cusp resolution at an isolated fixed point, which must be $P_{\infty,\lambda}$.

We now turn to the case when $N = 2^k M$ is even. For each $k \geq 1$ define the matrix $g_{I^\sharp}(2^k) \in \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ by

$$g_{I^\sharp}(2^k) = \begin{pmatrix} 1 & 2^{k-1} \\ 2^{k-1} & 2^{k-1}+1 \end{pmatrix},$$

and if $k \geq 2$ define $g_{\mathrm{b}^\sharp}(2^k) \in \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ by

$$g_{\mathrm{b}^\sharp}(2^k) = \begin{pmatrix} 1 & 0 \\ 0 & 2^{k-1}+1 \end{pmatrix}.$$

If $r = \det(g_{I^\sharp}(2^k))$ then $g_{I^\sharp}(2^k)$ is conjugate to $r g_{I^\sharp}(2^k)^{-1}$ and if $r = \det(g_{\mathrm{b}^\sharp}(2^k))$ then $g_{\mathrm{b}^\sharp}(2^k)$ is conjugate to $r g_{\mathrm{b}^\sharp}(2^k)^{-1}$. In particular, the involution $\tilde{\tau}$ takes the curves $\widetilde{F}^+_{\lambda(I^\sharp,I)}$ and $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$ to themselves.

Lemma 3.3.21. *Suppose that $\widetilde{Z}_{N,r}$ is not a rational surface. Then the following hold:*

(i) *If $k \geq 1$ then the modular curves $\widetilde{F}^+_{\lambda(I^\sharp,I)} \subset \widetilde{Z}_{N,r}$ are (-1)-curves and $\widetilde{F}^+_{\lambda(I^\sharp,I)} \cdot \boldsymbol{F}_{\tilde{Z}} = 1$.*

(ii) *If $k \geq 2$ then the modular curves $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)} \subset \widetilde{Z}_{N,r}$ are (-1)-curves and $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)} \cdot \boldsymbol{F}_{\tilde{Z}} = 1$.*

Proof. It is simple to check that $H^+_{(I^\sharp,I)}$ and $H^+_{(\mathrm{b}^\sharp,I)} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ are respectively the full pre-images of the non-split Cartan and trivial subgroups of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ under the reduction mod 2 map. This identification induces isomorphisms of modular curves $X^+_{\lambda(I^\sharp,I)} \cong X(\mathrm{ns}\,2)$ and $X^+_{\lambda(\mathrm{b}^\sharp,I)} \cong X(2)$, so in particular both have genus 0.

Recall from (3.2) that we have a numerical equivalence

$$K_{\tilde{Z}} \sim \frac{1}{6}\widetilde{C}_\star - D_\infty - \frac{1}{3}E_{3,1}.$$

The curve $\widetilde{F}^+_{\lambda(I^\sharp,I)}$ has exactly one cusp and since $\widetilde{C}_\star \cdot \widetilde{F}^+_{\lambda(I^\sharp,I)} = 2[\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : G(\mathrm{ns}\,2)] = 4$ it follows that $\widetilde{F}^+_{\lambda(I^\sharp,I)} \cdot K_{\tilde{Z}} \leq -1$. Similarly the curve $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$ has three cusps, and $\widetilde{C}_\star \cdot \widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)} = 2|\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})| = 12$, hence $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)} \cdot K_{\tilde{Z}} \leq -1$.

Since $\widetilde{Z}_{N,r}$ is regular (see [Her91, Satz 1] and [KS97, Theorem 1]) and is not rational by assumption, by Lemma 2.4.4 the curves $\widetilde{F}^+_{\lambda(I^\sharp,I)}$ and $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$ are non-singular, and $\widetilde{F}^+_{\lambda(I^\sharp,I)} \cdot K_{\tilde{Z}} = \widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)} \cdot K_{\tilde{Z}} = -1$. Since neither $\widetilde{F}^+_{\lambda(I^\sharp,I)}$ nor $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$ is fixed pointwise by $\tilde{\tau}$, by Lemma 3.3.16 we have $\widetilde{F}^+_{\lambda(I^\sharp,I)} \cdot \boldsymbol{F}_{\tilde{Z}} = 1$ and $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)} \cdot \boldsymbol{F}_{\tilde{Z}} = 1$. □

By Lemma 3.3.21 the curves $\widetilde{F}^+_{\lambda(I^\sharp,I)}$ and $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$ are smooth and have self-intersection -1. Since, by assumption, $\widetilde{Z}_{N,r}$ is not rational by Lemma 2.4.4 the curves $\widetilde{F}^+_{\lambda(I^\sharp,I)}$ and $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$ do not intersect each other or $\widetilde{F}^+_{\lambda(\mathrm{b},I)}$. Applying Lemma 3.3.16 it follows that $\widetilde{F}^+_{\lambda(I^\sharp,I)}$ (when $k \geq 1$) and $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$ (when $k \geq 2$) meet the isolated fixed points contained in the resolutions of the cusps of type $(N/2, 1)$ (as indicated in Tables 3.3–3.5). □

Remark 3.3.22. The curves $F^+_{\lambda(I^\sharp,I)}$ and $F^+_{\lambda(\mathrm{b}^\sharp,I)}$ arise naturally in the context of more general "Atkin–Lehner" involutions on $Z_{N,r}$. Let $\omega \in (\mathbb{Z}/N\mathbb{Z})^\times$ be such that $\omega \equiv 2^{k-1}+1 \pmod{2^k}$ and $\omega \equiv 1 \pmod{M}$. Consider the involution $\omega\colon Z_{N,r} \to Z_{N,r}$ given by $(E, E', \phi) \mapsto (E, E', \omega\phi)$, then $\omega\tau$ fixes every point on $F^+_{\lambda(I^\sharp,I)}$ and $F^+_{\lambda(\mathrm{b}^\sharp,I)}$ (indeed, this can be used to show that $\widetilde{F}^+_{\lambda(I^\sharp,I)}$ and $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$ are smooth).

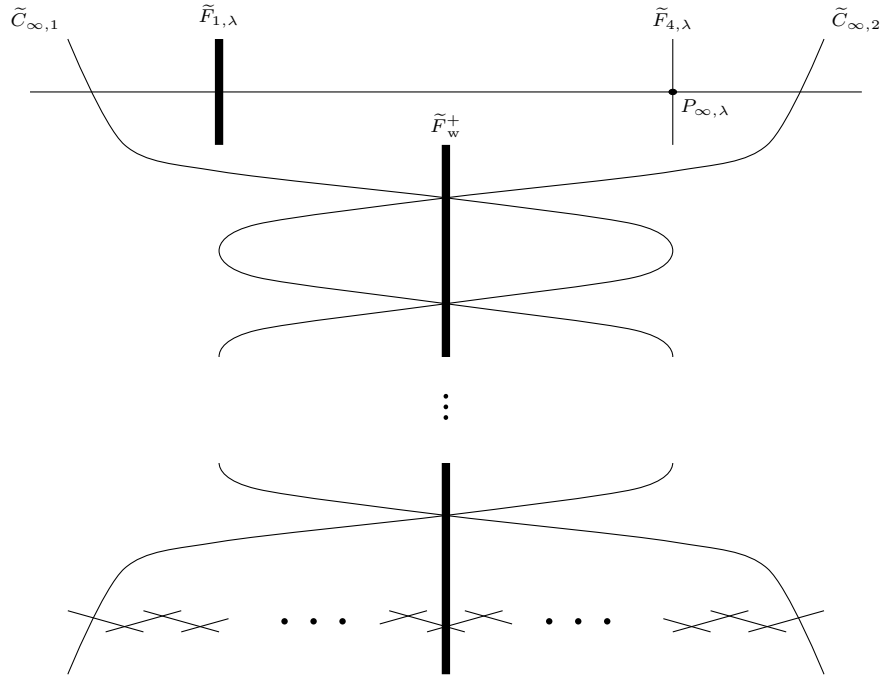


Figure 3.5: The action of the involution $\tilde{\tau}$ in a neighbourhood of the cusps when N is odd. Lines and points in bold are fixed by $\tilde{\tau}$. The curves $\widetilde{C}_{\infty,1}$ and $\widetilde{C}_{\infty,2}$ intersect transversally at $\frac{1}{2}\phi(N)$ points. All horozontal curves are resolution divisors occuring with multiplicity recorded in Table 3.2.

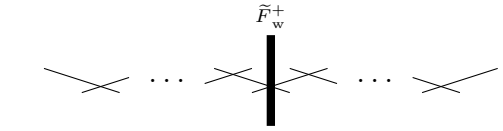
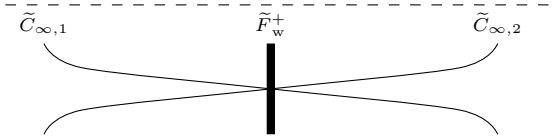
Type	Number of occurrences	Diagram
$(N,1)$	$\frac{1}{2}\rho(N,r)$	
$(d,-1)$	$\frac{1}{2}\rho(d,-r)\varphi(N/d)$	
	$\frac{1}{2}\varphi(N)$	

TABLE 3.2: The action of $\tilde{\tau}$ in a neighbourhood of the resolutions of the fixed cusps when $N \equiv 1 \pmod 2$. Here $d \neq 1$ ranges over divisors of N. Horizontal curves are exceptional divisors of the resolution of singularities $\widetilde{Z}_{N,r} \to Z_{N,r}$ and their self-intersections are determined by Hirzebruch–Jung continued fractions.

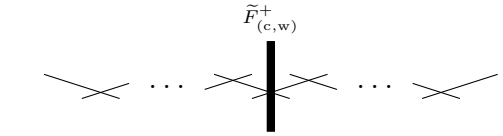
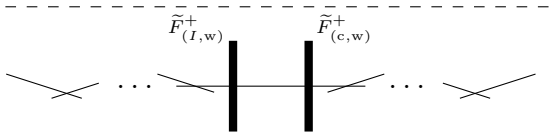
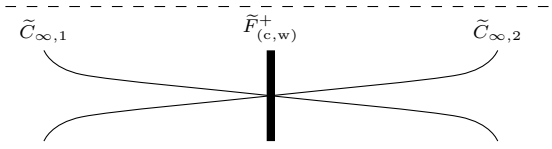
Type	Number of occurrences	Diagram
$(N,1)$	$\frac{1}{2}\rho(M,r)$	
$(M,1)$	$\frac{1}{2}\rho(M,r)$	
$(d,-1)$	$\frac{1}{2}\rho(d,-r)\varphi(M/d)$	
$(2d,-1)$	$\frac{1}{2}\rho(d,-r)\varphi(M/d)$	
	$\frac{1}{2}\varphi(N)$	

TABLE 3.3: The action of $\tilde{\tau}$ in a neighbourhood of the resolutions of the fixed cusps when $N = 2M \equiv 2 \pmod 4$. The integer d ranges over divisors of M such that $d \neq 1$ if the singularity is of type $(d,-1)$.

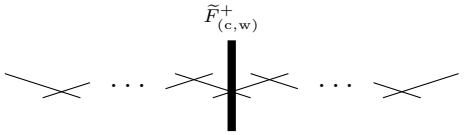
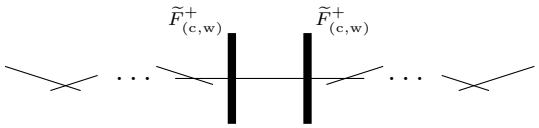
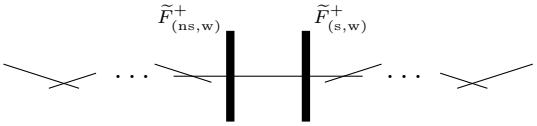
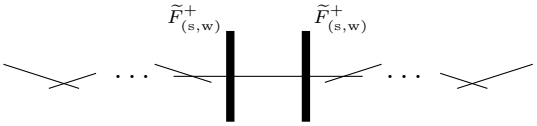
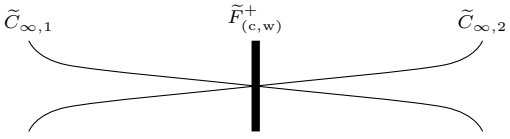
Type	Number of occurrences	Diagram
$(N,1)$	$\frac{1}{2}\rho(N,r)$	
$(2M,1)$	$\frac{1}{2}\rho(M,r)$	
	$\frac{1}{2}\rho(M,r)$	
$(d,-1)$	$\frac{1}{2}\rho(d,-r)\varphi(N/d)$	
$(2d,-1)$	$\frac{1}{2}\rho(2d,-r)\varphi(2M/d)$	
$(4d,-1)$	$\frac{1}{4}\rho(4d,-r)\varphi(M/d)$	
	$\frac{1}{4}\rho(4d,-r)\varphi(M/d)$	
	$\frac{1}{2}\varphi(N)$	

Table 3.4: The action of $\tilde{\tau}$ in a neighbourhood of the resolutions of the fixed cusps when $N = 4M \equiv 4 \pmod 8$. The integer d ranges over divisors of M such that $d \neq 1$ when the singularity is of type $(d,-1)$. In several cases the behaviour depends on the congruence class of r modulo 4, which is listed on the right.

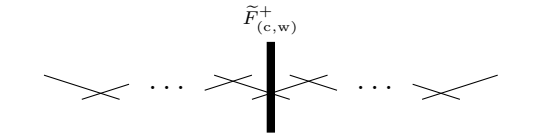
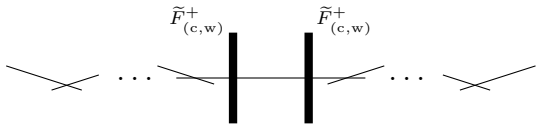
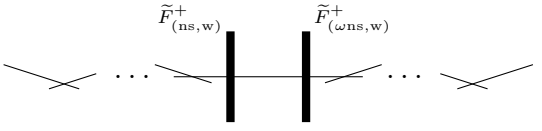
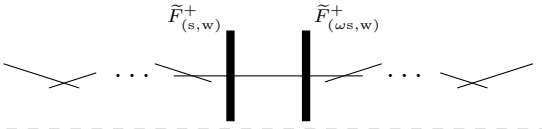
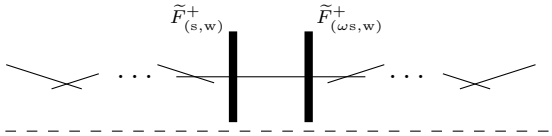
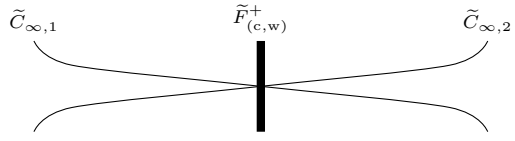
Type	Number of occurrences	Diagram	
$(N,1)$	$2\rho(M,r)$		
$(N/2,1)$	$\rho(M,r)$		$r \equiv 1 \pmod 8$
	$\rho(M,r)$		$k \geq 4$ and $r \equiv 1 \pmod 8$ $k = 3$ and $r \equiv 5 \pmod 8$
$(d,-1)$	$2^{k-2}\rho(d,-r)\varphi(M/d)$		
$(2d,-1)$	$2^{k-3}\rho(d,-r)\varphi(M/d)$		
$(4d,-1)$	$2^{k-4}\rho(4d,-r)\varphi(M/d)$		$r \equiv 3 \pmod 8$
	$2^{k-4}\rho(4d,-r)\varphi(M/d)$		$r \equiv 7 \pmod 8$
$(2^l d,-1)$	$2^{k-l-2}\rho(2^l d,-r)\varphi(M/d)$		
	$\frac{1}{2}\varphi(N)$		

TABLE 3.5: The action of $\tilde{\tau}$ in a neighbourhood of the resolutions of the fixed cusps when $N = 2^k M \equiv 0 \pmod 8$ where M is an odd integer. Here $\omega = 2^{k-1}+1$ and l ranges among integers $3 \leq l \leq k$. The integer d ranges over divisors of M such that $d \neq 1$ when the singularity is of type $(d,-1)$. In several cases the behaviour depends on the congruence class of r modulo 8, which is listed on the right.

3.4 The genera of the modular curves X_g^+

A concrete application of the results in Section 3.3 is that we are able to compute the genera of the modular curves X_g^+. There are also a number of other benefits to these calculations.

Firstly, the following results give us a convenient way of checking the (rather complicated) calculations in Sections 3.3.2 and 3.3.3. Indeed, after fixing N and choosing an element $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ it is simple to compute the genus of $X_g^+ = X(H_g^+)$ by, e.g., first computing the subgroup H_g^+ explicitly (by applying the definition in Section 2.2.7) and then using the function `GL2Genus` provided by Rouse, Sutherland, and Zureick-Brown [RSZ22, RSZ21].

Secondly, it may be possible to determine the genus of these modular curves X_g^+ by instead computing ramification indices directly, in the spirit of [Bar10, Theorems 7.2 and 7.3]. The proofs we give below allow us to avoid these calculations which would necessarily be quite complicated. We will need these genera in order to compute the Chern numbers of the surfaces $W_{N,r}$ (the surfaces $W_{N,r}$ are smooth projective surfaces birational to $Z_{N,r}^{\mathrm{sym}}$ which we construct in Section 3.6).

Finally, these results are of independent interest. A special case of Corollary 3.4.2 gives the genus of both the modular curve $X(\mathrm{s}\,p^{k+})$ and $X(\mathrm{ns}\,p^{k+})$ for every odd prime power p^k (when $p = 2$ the analogous result follows from Corollary 3.4.5). Our approach gives a uniform treatment of the split and non-split cases. More generally, Corollaries 3.4.2 and 3.4.5(i)–(ii) give explicit genus formulae for the modular curves associated to every *extended Cartan subgroup* of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (see Remark 3.4.3).

Corollaries 3.4.2–3.4.5 generalise many cases which have previously appeared in the literature. Let $\tilde{N} = N$ if N is odd, and $\tilde{N} = N/2$ if N is even.

(A) The genus of the modular curves $X(\mathrm{ns}\,p^l)$ and $X(\mathrm{ns}\,p^{l+})$ (and their fibre products) are computed by Baran in Theorems 7.2 and 7.3 of [Bar10].

(B) There is a well known isomorphism $X(\mathrm{s}\,N^2) \cong X_0(N^2)$ (see Remark 2.2.14(i)). Under this isomorphism it is simple to check that X_{s}^+ is isomorphic to $X_0^+(\tilde{N}^2)$, the quotient of $X_0(\tilde{N}^2)$ by the Fricke involution. A genus formula for these modular curves is given in e.g., [Coh91, (1.6d)].

(C) When $N = p$ is an odd prime number Hermann [Her92, (7)] gives a genus formula for the modular curve associated to the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ which treats both the split and non-split cases simultaneously.

We recover (A) from Corollaries 3.4.2–3.4.5. Note that when p^l is an odd prime power and $-r$ is a quadratic non-residue we have an isomorphism $X_{\mathrm{w}}^+ \cong X(\mathrm{ns}\,p^{\tilde{l}+})$. We similarly recover (B) from Corollaries 3.4.2–3.4.5. If $-r$ is a square modulo N, then if N is odd we have an isomorphism $X_{\mathrm{w}}^+ \cong X_0^+(\tilde{N}^2)$. Restricting the result in Corollary 3.4.2 to the case when $N = p$ is an odd prime number we recover Hermann's result (C), giving the genera of the modular curve associated to the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

The genera of these modular curves will follow immediately by combining the following lemma with Propositions 3.3.17 and 3.3.20.

Lemma 3.4.1. *Let $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be chosen so that $\widetilde{F}_g^+$ is a component of $\boldsymbol{F}_{\tilde{Z}}$. Then the elliptic points of order 2 and 3 on X_g^+ are in bijective correspondence with intersection points of $\widetilde{F}_g^+$ with the resolutions of quotient singularities of type $(2,1)$ and $(3,1)$ respectively.*

Proof. First note that the elliptic points of order 2 (resp. 3) on a modular curve X are exactly the points in the fibre of the morphism $X \to X(1)$ above $j = 1728$ (resp. $j = 0$) for which this morphism is unramified.

Let $\mathfrak{D}$ be the diagonal in $Z_1 = X(1) \times X(1)$. Note that F_g^+ has at worst nodal singularities (this may be seen from Propositions 3.3.17 and 3.3.20), in particular since $\widetilde{F}_g^+$ is non-singular the normalisation morphism $\widetilde{F}_g^+ \to F_g^+$ is unramified. Consider a point $\mathfrak{z} = (E, E, \phi) \in F_g^+$, let G be the image of $\mathrm{Aut}(E) \to \mathrm{Aut}(E[N])$, and let $\mathrm{P}G = G/\{\pm 1\}$.

If $\mathfrak{Z} \in X(N) \times X(N)$ is a pre-image of $\mathfrak{z}$, then the morphism $F_g^+ \to \mathfrak{D}$ is unramified at $\mathfrak{z}$ if and only if the diagonal of $\mathrm{P}G \times \mathrm{P}G$ fixes $\mathfrak{Z}$. It follows from Lemma 3.3.13 that $\mathfrak{z}$ is a cyclic quotient singularity of type $(d, 1)$ where $d = |\mathrm{P}G|$. The elliptic points of order 2 and 3 on $X_g^+ \cong \widetilde{F}_g^+$ are therefore in one-to-one correspondence with the points which map to the singular points of type $(2, 1)$ and $(3, 1)$ above $j = 1728$ and 0 respectively. □

Corollary 3.4.2. *Let N be an odd integer and let r be coprime to N. Let φ denote Euler's totient function and let $\rho(N, m)$ be the function defined in* (3.1)*. Define*

$$\begin{aligned}
e_2(N, r) &= \rho(N, r), \\
e_3(N, r) &= \rho(N, 3r), \\
e_\infty(N, r) &= \prod_{p|N} \left(\varphi(p^{v_p(N)}) + \sum_{l=0}^{v_p(N)-1} \left(1 + \left(\frac{-r}{p}\right)\right) \varphi(p^l) \right), \\
\mu(N, r) &= N^2 \prod_{p|N} \left(1 + \frac{1}{p}\left(\frac{-r}{p}\right)\right)
\end{aligned}$$

(cf. [Bar10, Theorem 7.2] in the non-split case when $-r$ is a quadratic non-residue modulo p). We further define

$$\begin{aligned}
e_2^+(N, r) &= \frac{1}{2} e_2(N, r) + h(-4N^2), & e_3^+(N, r) &= \frac{1}{2} e_3(N, r), \\
e_\infty^+(N, r) &= \frac{1}{2} e_\infty(N, r), & \mu^+(N, r) &= \frac{1}{2} \mu(N, r).
\end{aligned}$$

If $N \neq 1$ the degree of the morphism $X_{\mathrm{w}}^+ \to X(1)$ is equal to $\mu^+(N, r)$ and the genus of the modular curve X_{w}^+ is given by

$$1 + \frac{1}{12}\left(\mu^+(N, r) - 3e_2^+(N, r) - 4e_3^+(N, r) - 6e_\infty^+(N, r)\right).$$

Remark 3.4.3. We note once again that Corollary 3.4.2 gives a formula for the genus of both modular curves $X(\mathrm{s}p^{k+})$ and $X(\mathrm{ns}p^{k+})$. Indeed, appropriately choosing $-r$ to be a quadratic residue or non-residue modulo all primes $p|N$ we obtain a genus formula for the modular curve associated to each *extended Cartan subgroup* of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (see Remark 2.2.14 or [LMFDB, `https://www.lmfdb.org/knowledge/show/gl2.cartan`]). In particular Corollary 3.4.2 specialises, when $-r$ is a quadratic residue modulo p for every prime $p|N$ (resp. when $-r$ is a quadratic non-residue modulo p for every prime $p|N$), to a formula for the genus of the modular curve attached to the extended split[5] (resp. non-split[6]) Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Proof. For $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ let ν_2^+ and ν_3^+ be the number of elliptic points of order 2 and 3 on X_g^+ respectively and let ν_∞^+ be the number of cusps and $\eta^+ = [\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : H_g^+]$. A general

[5] See `https://www.lmfdb.org/knowledge/show/modcurve.xsp_plus`.
[6] See `https://www.lmfdb.org/knowledge/show/modcurve.xns_plus`.

result for modular curves (which follows, from the Riemann–Hurwitz formula, see e.g., [DS05, Theorem 3.1.1]) gives that $p_g(X_g^+) = 1 + \frac{1}{12}\eta^+ - \frac{1}{4}\nu_2^+ - \frac{1}{3}\nu_3^+ - \frac{1}{2}\nu_\infty^+$.

Let $g_{\mathrm{w}} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the element from Lemma 3.3.8. When $g = g_{\mathrm{w}}$ the number of elliptic points of order 2 and 3 follow immediately from Lemma 3.4.1 and Proposition 3.3.20. The number of cusps follows from Proposition 3.3.17. It remains to compute the index η^+. But this is equal to the number of points on F_{w}^+ above a general point on the diagonal in $X(1)\times X(1)$. By construction this is exactly one half of the number of elements of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which are conjugate to g_{w}. Each such element is of the form $\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ where $a^2 + bc = -r$, and there are therefore $\mu(N,r)$ such elements. □

If $N = 2^k M$ and $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ the index $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : H_g^+]$ is equal to half the order of the $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$-conjugacy class of g. This latter number is a multiplicative function of N, so in particular $[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : H_g^+] = \mu^+(M,r)\mu'$ where μ' denotes the order of the $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$-conjugacy class of g modulo 2^k. A counting argument yields the following corollaries.

Corollary 3.4.4. *Let $N = 2M$ where M is an odd integer and let r be coprime to N. The degree of the morphism $X_{(\mathrm{c,w})}^+ \to X(1)$ is equal to $3\mu^+(N,r)$ and the genus of the modular curve $X_{(\mathrm{c,w})}^+$ is given by*

$$1 + \frac{1}{12}\left(3\mu^+(M,r) - 3e_2^+(g) - 6\cdot 2e_\infty^+(M,r)\right).$$

The modular curve $X_{(I,\mathrm{w})}^+$ is isomorphic to the modular curve X_{w}^+.

Corollary 3.4.5. *Let $N = 2^k M$ where M is an odd integer and $k \geq 2$. Let r be coprime to N. Then:*

(i) *the degree of the morphism $X_{(\mathrm{ns,w})}^+ \to X(1)$ is equal to $2^{2k-3}\mu^+(N,r)$ and the genus of the modular curve $X_{(\mathrm{ns,w})}^+$ is given by*

$$1 + \frac{1}{12}\left(2^{2k-3}\mu^+(M,r) - 3h(-4(N/2)^2) - 4\cdot 2e_3^+(g) - 6\cdot 2^{k-2}e_\infty^+(M,r)\right),$$

(ii) *the degree of the morphism $X_{(\mathrm{s,w})}^+ \to X(1)$ is equal to $3\cdot 2^{2k-3}\mu^+(N,r)$ and the genus of the modular curve $X_{(\mathrm{s,w})}^+$ is given by*

$$1 + \frac{1}{12}\left(3\cdot 2^{2k-3}\mu^+(M,r) - 3h(-4(N/2)^2) - 6\cdot 3\cdot 2^{k-2}e_\infty^+(M,r)\right),$$

(iii) *the degree of the morphism $X_{(\mathrm{c,w})}^+ \to X(1)$ is equal to $2^{2k-2}\mu^+(N,r)$ and the genus of the modular curve $X_{(\mathrm{c,w})}^+$ is given by*

$$\begin{cases} 1 + \frac{1}{12}\left(3\cdot 2^{2k-2}\mu^+(M,r) - 3\rho(N,1) - 6\cdot 2^k e_\infty^+(M,r)\right) & \text{if } r \equiv 1 \pmod 4 \\ 1 + \frac{1}{12}\left(3\cdot 2^{2k-2}\mu^+(M,r) - 3h(-4N^2) - 6\cdot 2^k e_\infty^+(M,r)\right) & \text{if } r \equiv 3 \pmod 4. \end{cases}$$

3.5 Intersection numbers on the surface $\widetilde{Z}_{N,r}$

Let $\boldsymbol{F}_{\tilde{Z}} := \widetilde{\boldsymbol{F}}_Z$ denote the one dimensional component of the locus of fixed points of $\tilde{\tau}$, and recall that we write $K_{\tilde{Z}}$ for a canonical divisor of $\widetilde{Z}_{N,r}$.

To understand the intersection theory of the images of the modular curves $\widetilde{F}_{m,\lambda}$ on (a smooth model for) $Z_{N,r}^{\mathrm{sym}}$ we need to control the intersections $\widetilde{F}_{m,\lambda} \cdot \boldsymbol{F}_{\tilde{Z}}$. The following result is a direct generalisation of [Her92, Satz 3][7] in the case when $N = p$.

Lemma 3.5.1. *Let $N \geq 5$ be an integer. If $m > 1$ is an integer coprime to N then $\widetilde{F}_{m,\lambda} \cdot \boldsymbol{F}_{\tilde{Z}} \geq f(m)$ where*

$$f(m) = \begin{cases} h(-4m) + h(-m) & \text{if } m \equiv 3 \pmod 4 \\ h(-4m) & \text{otherwise.} \end{cases}$$

Proof. The Fricke involution, w_m, on $X_0(m)$ induces an involution on the non-singular points of $F_{m,\lambda}$ which agrees with τ except possibly at those points above $j, j' \in \{0, 1728, \infty\}$. Suppose $m > 4$. It is well known that a point $(E, \phi) \in X_0(m)$ is fixed by w_m if and only if it is non-cuspidal, E has complex multiplication, and $\phi^2 = -m$. This occurs only when E has CM by an order of discriminant $D = -m$ or $-4m$ (the former only occurring if $m \equiv 3 \pmod 4$). The number of j-invariants of such elliptic curves is given by the formula in the statement.

When $m \in \{2, 3, 4\}$ by Lemma 3.2.4 the curves $F_{m,\lambda}$ are (-1)-curves. Applying Lemma 3.3.16 exactly one of the two fixed points of $\tilde{\tau}$ on $\widetilde{F}_{m,\lambda}$ is a transversal intersection of $\widetilde{F}_{m,\lambda}$ and $\boldsymbol{F}_{\tilde{Z}}$. The claim follows. □

Similarly, to understand the self-intersection of a canonical divisor on (our smooth birational model for) $Z_{N,r}^{\mathrm{sym}}$ we will need the following lemma.

Lemma 3.5.2. *Let M be an odd integer. If $M \neq 1$ on $\widetilde{Z}_{M,r}$ we have*

$$K_{\tilde{Z}} \cdot \widetilde{F}_{\mathrm{w}}^{+} = \frac{1}{3}\mu^{+}(M, r) - 2e_{\infty}^{+}(M, r) - \frac{1}{3}e_{3}^{+}(M, r).$$

Let $k \geq 1$ be an integer and let $N = 2^k M$. Then on $\widetilde{Z}_{N,r}$ we have

$$K_{\tilde{Z}} \cdot \widetilde{F}_{\lambda(\mathrm{b},I)}^{+} = -1.$$

If $k = 1$ then on $\widetilde{Z}_{N,r}$ we have

$$\begin{aligned} K_{\tilde{Z}} \cdot \widetilde{F}_{(I,\mathrm{w})}^{+} &= \frac{1}{3}\mu^{+}(M, r) - e_{\infty}^{+}(M, r) - \frac{1}{3}e_{3}^{+}(M, r), \\ K_{\tilde{Z}} \cdot \widetilde{F}_{(\mathrm{c},\mathrm{w})}^{+} &= \mu^{+}(M, r) - 3e_{\infty}^{+}(M, r). \end{aligned}$$

If $k \geq 2$ then we have

$$\begin{aligned} K_{\tilde{Z}} \cdot \widetilde{F}_{(\omega\mathrm{ns},\mathrm{w})}^{+} &= \frac{2^{2k-3}}{3}\mu^{+}(M, r) - 2^{k-2}e_{\infty}^{+}(M, r) - \frac{2}{3}e_{3}^{+}(M, r), \\ K_{\tilde{Z}} \cdot \widetilde{F}_{(\omega\mathrm{s},\mathrm{w})}^{+} &= 2^{2k-3}\mu^{+}(M, r) - 3 \cdot 2^{k-2}e_{\infty}^{+}(M, r), \\ K_{\tilde{Z}} \cdot \widetilde{F}_{(\mathrm{c},\mathrm{w})}^{+} &= 2^{2k-2}\mu^{+}(M, r) - 3 \cdot 2^{k-1}e_{\infty}^{+}(M, r). \end{aligned}$$

Proof. Recall that by (3.2) we have a numerical equivalence of divisors

$$K_{\widetilde{Z}} \sim \frac{1}{6}\widetilde{C}_{\star} - D_{\infty} - \frac{1}{3}E_{3,1}$$

where $\widetilde{C}_{\star}$, D_{∞}, and $E_{3,1}$ are the divisors defined in Section 3.2 (see Table 3.1).

[7] Satz 3 of [Her92] contains a typographical error, the curve $\widetilde{F}_1$ must be excluded. The curves $\widetilde{F}_1$ and $\widetilde{F}_{\mathrm{w}}^{+}$ (which in their notation are the curves F_1 and F_{p^2}) do not meet by Corollary 3.3.5 and $\widetilde{F}_1^2 = -1$.

In general, by the projection formula for a modular curve F on $Z_{N,r}$ (i.e., the curves $F_{m,\lambda}$ or F_g^+) we have $C_\star \cdot F = 2\,[\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) : H]$ where $H \subset \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is the subgroup (unique up to conjugacy) such that $-I \in H$ and F is birational (as a cover of $X(1)$) to $X(H)$. In the cases in the lemma these indices are computed in Corollaries 3.4.2, 3.4.4, and 3.4.5. The intersection numbers $D_\infty \cdot \widetilde{F}$ and $E_{3,1} \cdot \widetilde{F}$ are simple to compute from Propositions 3.3.17 and 3.3.20. □

3.6 A non-singular model for $Z_{N,r}^{\mathrm{sym}}$

Recall that if $S/\mathbb{C}$ is a smooth, projective, algebraic surface we define the irregularity $q(S) = p_g(S) - p_a(S) = h^1(S, \mathcal{O}_S) = h^0(S, \Omega_S^1)$, where Ω_S^1 is the sheaf of holomorphic 1-forms on S. We recall from [Her91, Satz 1] and [KS97, Theorem 1] that the surface $\widetilde{Z}_{N,r}$ is *regular* i.e., $q(\widetilde{Z}_{N,r}) = 0$ (this is the case for any Hilbert modular group, see the discussion after Proposition VI.6.2 in [vdG88]).

Let $N = 2^k M$ where $k \geq 0$ and M is an odd integer. Let r be coprime to N. We suppose from now that and that $\widetilde{Z}_{N,r}$ is *not* a rational surface. Since $\widetilde{Z}_{N,r}$ is regular and not rational, no two (-1)-curves on (any smooth surface birational to) $\widetilde{Z}_{N,r}$ may intersect by Lemma 2.4.4. We may therefore construct a non-singular surface, which we denote by $Z_{N,r}^\circ$, from $\widetilde{Z}_{N,r}$ by sequentially blowing down:

1. the $\frac{1}{2}\rho(N,r)$ configurations consisting of $\widetilde{F}_{1,\lambda}$, a (-2)-curve, and a (-3)-curve,
2. the $\frac{1}{2}\rho(N,2r)$ configurations consisting of $\widetilde{F}_{2,\lambda}$ and a (-2)-curve,
3. the $\frac{1}{2}\rho(N,3r)$ (-1)-curves $\widetilde{F}_{3,\lambda}$,
4. the $\frac{1}{2}\rho(N,4r)$ (-1)-curves $\widetilde{F}_{4,\lambda}$,
5. if $k \geq 1$ the $\frac{1}{2}\rho(N,r)$ configurations consisting of $\widetilde{F}^+_{\lambda(\mathrm{b},I)}$ and a (-2)-curve,
6. if $k \geq 1$ the $\frac{1}{2}\rho(N/2,r)$ (-1)-curves $\widetilde{F}^+_{\lambda(I^\sharp,I)}$,
7. if $k = 2$ and $r = 3 \pmod 4$ the $\frac{1}{2}\rho(M,r)$ (-1)-curves $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$,
8. if $k = 3$ and $r \equiv 5 \pmod 8$ the $\rho(M,r)$ (-1)-curves $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$, and
9. if $k \geq 4$ and $r \equiv 1 \pmod 8$ the $\rho(M,r)$ (-1)-curves $\widetilde{F}^+_{\lambda(\mathrm{b}^\sharp,I)}$.

By construction the involution $\tilde{\tau}$ induces an involution τ° on $Z_{N,r}^\circ$. By Propositions 3.3.17 and 3.3.20 (see also Figures 3.2–3.4 and Tables 3.2–3.5) the action of τ° on the surface $Z_{N,r}^\circ$ has no isolated fixed points. Define the surface $W_{N,r}$ to be the quotient of $Z_{N,r}^\circ$ by τ°. We have:

Theorem 3.6.1. *The surface $W_{N,r}$ is a non-singular, regular (i.e., $q(W_{N,r}) = 0$) projective, algebraic surface which is birational to $Z_{N,r}^{\mathrm{sym}}$.*

Proof. Since τ° acts without isolated fixed points the quotient $W_{N,r}$ is non-singular. Let $\pi\colon Z_{N,r}^\circ \to W_{N,r}$ be the quotient morphism. The pull back of a non-zero holomorphic 1-form on $W_{N,r}$ is non-zero. Since both $W_{N,r}$ and $Z_{N,r}$ are smooth, the sequence $0 \to \pi^*\Omega^1_{W/\mathbb{C}} \to \Omega^1_{Z^\circ/\mathbb{C}} \to \Omega^1_{Z^\circ/W} \to 0$ is exact. Because the irregularity of the surface $Z_{N,r}^\circ$ is zero taking global sections we see that $q(W_{N,r}) = h^0(W_{N,r}, \Omega^1_W) = 0$ as required. □

3.6.1 The numerical invariants

Let $\pi\colon Z^{\circ}_{N,r} \to W_{N,r}$ be the quotient morphism. Given a divisor $D \subset \widetilde{Z}_{N,r}$ we write D° for the image of D under the blow-down $\widetilde{Z}_{N,r} \to Z^{\circ}_{N,r}$. If D is a divisor on $Z_{N,r}$ we write $D^{\circ} := \widetilde{D}^{\circ}$. If C is a divisor on $Z^{\circ}_{N,r}$ we write $\widetilde{C}$ for the strict transform of C on $\widetilde{Z}_{N,r}$. Similarly if $D \subset Z^{\circ}_{N,r}$ is a divisor, we write D^{*} for the image of D under π. If C is a curve on either $Z_{N,r}$ or $\widetilde{Z}_{N,r}$ we write $C^{*} := (C^{\circ})^{*}$.

Let $\boldsymbol{F}_{Z^{\circ}} \subset Z^{\circ}_{N,r}$ denote the divisor consisting of points fixed by τ° (i.e., $\boldsymbol{F}_{Z^{\circ}} = (\boldsymbol{F}_{\tilde{Z}})^{\circ}$). Note that $\widetilde{\boldsymbol{F}}_{Z^{\circ}}$ is the divisor on $\widetilde{Z}_{N,r}$ given by removing $\widetilde{F}_{1,\lambda}$ and $\widetilde{F}^{+}_{\lambda(\mathrm{b},I)}$ from $\boldsymbol{F}_{\tilde{Z}}$, for each $\lambda \in \{x \in (\mathbb{Z}/N\mathbb{Z})^{\times} : x^2 = r\}/\{\pm 1\}$.

Let $K_{Z^{\circ}}$ and K_W be canonical divisors for $Z^{\circ}_{N,r}$ and $W_{N,r}$ respectively. Recall that we write $K_{\tilde{Z}}$ for a canonical divisor for $\widetilde{Z}_{N,r}$. The following lemma follows immediately from the definition of $Z^{\circ}_{N,r}$ and $W_{N,r}$, together with the projection formula Proposition 2.4.2.

Lemma 3.6.2. *Let $N = 2^k M$ where M is an odd integer, and let r be an integer coprime to N such that $\widetilde{Z}_{N,r}$ is not a rational surface. We have the following*

$$K_{\tilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^{\circ}} - K_{Z^{\circ}} \cdot \boldsymbol{F}_{Z^{\circ}} = \begin{cases} \frac{3}{2}\rho(N,r) + \rho(N,2r) + \frac{1}{2}\rho(N,3r) & \text{if } k = 0, \\ 2\rho(M,r) + \frac{1}{2}\rho(M,3r) & \text{if } k = 1, \\ 3\rho(M,r) & \text{if } k = 2 \text{ and } r \equiv 1 \pmod 4, \\ \rho(M,r) + \rho(M,3r) & \text{if } k = 2 \text{ and } r \equiv 3 \pmod 4, \\ 6\rho(M,r) & \text{if } k = 3 \text{ and } r \equiv 1 \pmod 8, \\ 2\rho(M,3r) & \text{if } k \geq 3 \text{ and } r \equiv 3 \pmod 8, \\ 2\rho(M,r) & \text{if } k = 3 \text{ and } r \equiv 5 \pmod 8, \\ 8\rho(M,r) & \text{if } k \geq 4 \text{ and } r \equiv 1 \pmod 8, \\ 0 & \text{otherwise.} \end{cases}$$

We are now able to prove the following theorem which generalises a result of Hermann when $N = p$ is a prime number [Her92, (10)].

Theorem 3.6.3. *Let $N = 2^k M$ be an odd integer where $k \geq 0$ and M is an odd integer such that $N \geq 5$. Let r be an integer coprime to N such that $\widetilde{Z}_{N,r}$ is not rational. The geometric genus of $W_{N,r}$ is given as follows:*

(i) *If $k = 0$ the geometric genus is given by*

$$2p_g(W_{N,r}) = p_g(Z_{N,r}) + \frac{1}{4}\left(\frac{3}{2}\rho(N,r) + \rho(N,2r) + \frac{2}{3}\rho(N,3r) - \frac{1}{3}\mu^{+}(N,r) + 2e^{+}_{\infty}(N,r)\right) - 1.$$

(ii) *If $k = 1$ the geometric genus is given by*

$$2p_g(W_{N,r}) = p_g(Z_{N,r}) + \frac{1}{4}\left(2\rho(M,r) + \frac{2}{3}\rho(M,3r) - \frac{4}{3}\mu^{+}(M,r) + 4e^{+}_{\infty}(M,r)\right) - 1.$$

(iii) *If $k = 2$ and $r \equiv 1 \pmod 4$ the geometric genus is given by*

$$2p_g(W_{N,r}) = p_g(Z_{N,r}) + \frac{1}{4}\left(3\rho(M,r) + 6e_\infty^+(M,r) - 4\mu^+(M,r)\right) - 1.$$

(iv) *If* $k = 2$ *and* $r \equiv 3 \pmod 4$ *the geometric genus is given by*

$$2p_g(W_{N,r}) = p_g(Z_{N,r}) + \frac{1}{4}\left(\rho(M,r) + \frac{4}{3}\rho(M,3r) + 10e_\infty^+(M,r) - \frac{20}{3}\mu^+(M,r)\right) - 1.$$

(v) *If* $k \geq 3$ *and* $r \equiv 1 \pmod 8$ *the geometric genus is given by*

$$2p_g(W_{N,r}) = \begin{cases} p_g(Z_{N,r}) + \frac{1}{4}\left(6\rho(M,r) + 3\cdot 2^{k-1}e_\infty^+(M,r) - 2^{2k-2}\mu^+(M,r)\right) - 1 & \text{if } k = 3 \\ p_g(Z_{N,r}) + \frac{1}{4}\left(8\rho(M,r) + 3\cdot 2^{k-1}e_\infty^+(M,r) - 2^{2k-2}\mu^+(M,r)\right) - 1 & \text{if } k \geq 4. \end{cases}$$

(vi) *If* $k \geq 3$ *and* $r \equiv 3 \pmod 8$ *the geometric genus is given by*

$$2p_g(W_{N,r}) = p_g(Z_{N,r}) + \frac{1}{4}\left(\frac{8}{3}\rho(M,3r) + 2^{k+1}e_\infty^+(M,r) - \frac{2^{2k}}{3}\mu^+(M,r)\right) - 1.$$

(vii) *If* $k \geq 3$ *and* $r \equiv 5 \pmod 8$ *the geometric genus is given by*

$$2p_g(W_{N,r}) = \begin{cases} p_g(Z_{N,r}) + \frac{1}{4}\left(2\rho(M,r) + 3\cdot 2^{k-1}e_\infty^+(M,r) - 2^{2k-2}\mu^+(M,r)\right) - 1 & \text{if } k = 3 \\ p_g(Z_{N,r}) + \frac{1}{4}\left(3\cdot 2^{k-1}e_\infty^+(M,r) - 2^{2k-2}\mu^+(M,r)\right) - 1 & \text{if } k \geq 4. \end{cases}$$

(viii) *If* $k \geq 3$ *and* $r \equiv 7 \pmod 8$ *the geometric genus is given by*

$$2p_g(W_{N,r}) = p_g(Z_{N,r}) + \frac{1}{4}\left(2^{k+1}e_\infty^+(M,r) - 2^{2k-1}\mu^+(M,r)\right) - 1.$$

Proof. Recall that we assumed $\widetilde{Z}_{N,r}$ is not a rational surface, in particular no (-1)-curves intersect on $\widetilde{Z}_{N,r}$ by Lemma 2.4.4. By [Hir73a, Section 3, (16)] the Euler characteristics of the structure sheaves of $W_{N,r}$ and $Z^\circ_{N,r}$ are related by

$$2\chi(W_{N,r}) = \chi(Z^\circ_{N,r}) - \frac{1}{4}K_{Z^\circ}\cdot \boldsymbol{F}_{Z^\circ}.$$

We proved in Theorem 3.6.1 that the surface $W_{N,r}$ is regular and therefore we have a relation of geometric genera

$$2p_g(W_{N,r}) = p_g(Z^\circ_{N,r}) - \frac{1}{4}K_{Z^\circ}\cdot \boldsymbol{F}_{Z^\circ} - 1.$$

The claim follows immediately from Lemmas 3.5.2 and 3.6.2. □

Similarly, from the explicit formula for the class of $K_{\tilde{Z}}$ in (3.2) we are able to compute the self-intersection of K_W.

Lemma 3.6.4. *Suppose that* $W_{N,r}$ *is not a rational surface (e.g., if* $p_g(W_{N,r}) > 0$*). The Chern*

number $c_1^2(W_{N,r}) = K_W^2$ *is given by*

$$2K_W^2 - K_{\widetilde{Z}}^2 + 2K_{\widetilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ} - \widetilde{\boldsymbol{F}}_{Z^\circ}^2 = \begin{cases} \frac{13}{2}\rho(N,r) + 4\rho(N,2r) + 2\rho(N,3r) & \text{if } k = 0, \\ 9\rho(M,r) + 2\rho(M,3r) & \text{if } k = 1, \\ 14\rho(M,r) & \text{if } k = 2 \text{ and } r \equiv 1 \pmod 4, \\ 4\rho(M,r) + 4\rho(M,3r) & \text{if } k = 2 \text{ and } r \equiv 3 \pmod 4, \\ 28\rho(M,r) & \text{if } k = 3 \text{ and } r \equiv 1 \pmod 8, \\ 8\rho(M,3r) & \text{if } k \geq 3 \text{ and } r \equiv 3 \pmod 8, \\ 8\rho(M,r) & \text{if } k = 3 \text{ and } r \equiv 5 \pmod 8, \\ 36\rho(M,r) & \text{if } k \geq 4 \text{ and } r \equiv 1 \pmod 8, \\ 0 & \text{otherwise.} \end{cases}$$

where $c_1^2(\widetilde{Z}_{N,r}) = K_{\widetilde{Z}}^2$ *is given in [KS98, Theorem 2.6] and* $\widetilde{\boldsymbol{F}}_{Z^\circ}$ *denotes the strict transform of* $\boldsymbol{F}_{Z^\circ}$ *under the blowup* $\widetilde{Z}_{N,r} \to Z^\circ_{N,r}$.

Proof. By the projection formula and the fact that $\pi^* K_W = K_{Z^\circ} - \boldsymbol{F}_{Z^\circ}$, it follows that

$$2K_W^2 = K_{\widetilde{Z}}^2 - 2K_{\widetilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ} + \widetilde{\boldsymbol{F}}_{Z^\circ}^2 + (K_{Z^\circ}^2 - K_{\widetilde{Z}}^2) + 3(K_{\widetilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ} - K_{Z^\circ} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ}). \tag{3.4}$$

By repeatedly applying Lemma 2.4.3 we note that the difference $K_{Z^\circ}^2 - K_{\widetilde{Z}}^2$ is equal to the number of irreducible components of the exceptional divisor of $\widetilde{Z}_{N,r} \to Z^\circ_{N,r}$. Combining Lemma 3.6.2 and (3.4) the claim follows. □

3.6.1.1 Explicit computations of $p_g(W_{N,r})$ and K_W^2

We note that with the formulae in Theorem 3.6.3 and Lemma 3.6.4 we may compute $p_g(W_{N,r})$ and $c_1^2(W_{N,r}) = K_W^2$ for any given pair (N,r).

For $p_g(W_{N,r})$ this is easy to see. Kani–Schanz [KS98, Theorem 2] give an explicit formula for $p_g(\widetilde{Z}_{N,r})$ which may be computed for any given pair (N,r). By Theorem 3.6.3 we may compute $p_g(W_{N,r})$ from $p_g(\widetilde{Z}_{N,r})$ using only the functions $\rho(N,r)$, $\rho(N,2r)$, $\rho(N,3r)$, $\mu^+(N,r)$, and $e_\infty^+(N,r)$ all of which can be computed directly from the definitions for any given pair (N,r).

Similarly K_W^2 may be computed from Lemma 3.6.4. Again Kani–Schanz [KS98, Theorem 2] give an explicit formula for $K_{\widetilde{Z}}^2$. It remains to show that we may compute $2K_{\widetilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ} - \widetilde{\boldsymbol{F}}_{Z^\circ}^2$. Define

$$S = \mathrm{Supp}(\widetilde{\boldsymbol{F}}_{Z^\circ}) = \begin{cases} \mathrm{Supp}(\boldsymbol{F}_{\widetilde{Z}}) & \text{if } r \text{ is not a square modulo } N, \\ \mathrm{Supp}(\boldsymbol{F}_{\widetilde{Z}}) \setminus \left\{ \widetilde{F}_{1,\lambda} \right\}_\lambda & \text{if } N \text{ is odd and } r \text{ is a square modulo } N, \text{ or} \\ \mathrm{Supp}(\boldsymbol{F}_{\widetilde{Z}}) \setminus \left\{ \widetilde{F}_{1,\lambda}, \widetilde{F}^+_{\lambda(\mathrm{b},I)} \right\}_\lambda & \text{if } N \text{ is even and } r \text{ is a square modulo } N. \end{cases}$$

to be the support of the divisor $\widetilde{\boldsymbol{F}}_{Z^\circ}$, where λ ranges over $\{x \in \mathbb{Z}/N\mathbb{Z} : x^2 = r\}/\{\pm 1\}$. By Corollary 3.3.5 the components of $\boldsymbol{F}_{\widetilde{Z}}$ do not intersect and therefore

$$2K_{\widetilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ} - \widetilde{\boldsymbol{F}}_{Z^\circ}^2 = \sum_{F \in S} (2K_{\widetilde{Z}} \cdot F - F^2).$$

By the adjunction formulae we compute

$$2K_{\tilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ} - \widetilde{\boldsymbol{F}}^2_{Z^\circ} = \sum_{F \in S} (3K_{\tilde{Z}} \cdot F - 2p_g(F) + 2). \tag{3.5}$$

But for each $F \in S$ the genus $p_g(F)$ is computed in Corollaries 3.4.2–3.4.5 and $K_{\tilde{Z}} \cdot F$ is computed in Lemma 3.5.2.

For the convenience of the reader, we have prepared an accompanying `Magma` [BCP97] script in [Fre23b, `geometry/verify`] which may be used to compute $p_g(\widetilde{Z}_{N,r})$, $p_g(W_{N,r})$, $K^2_{\tilde{Z}}$, and K^2_W using the above descriptions. For each $15 \leq N \leq 40$ we include these invariants in the tables in Appendix B.

3.6.2 Bounds on $p_g(W_{N,r})$ and K^2_W and the proof of Theorem 1.0.4

In order to place the surfaces $W_{N,r}$ within the Enriques–Kodaira classification we need some loose bounds on the geometric genus and second Chern class of $W_{N,r}$. We now give bounds on $p_g(W_{N,r})$ and $c_1^2(W_{N,r}) = K^2_W$ for sufficiently large N.

Theorem 1.0.4 follows immediately from the following lemma, together with the computations of $p_g(W_{N,r})$ for $N \leq 40$ which are recorded in Appendix B.

Lemma 3.6.5. *For each $N \geq 9$ we have*

$$\begin{aligned} 2p_g(W_{N,r}) &\geq p_g(\widetilde{Z}_{N,r}) - \frac{1}{4} \cdot 2^{2k-1}\mu^+(M,r) - 1 \\ &> \frac{1}{480}N(N-1)(N-23) - \frac{\zeta(2)}{16}N^{5/2} - 1 \end{aligned}$$

and in particular $p_g(W_{N,r}) \geq 3$ except for those (N,r) appearing in cases (i)–(iii) *of Theorem 1.0.4.*

Proof. The first claim is immediate from Theorem 3.6.3. By [KS98, Proposition 2.9] for each $N \geq 9$ we have the inequality $p_g(\widetilde{Z}_{N,r}) > \frac{1}{480}N(N-1)(N-23)$. To prove the second claim it therefore suffices to show that $2^{2k}\mu(M,r) \leq \zeta(2)N^{5/2}$. To see this, note that

$$2^{2k}\mu(M,r) \leq 2^{2k}M^2 \prod_{p|M}\left(1 + \frac{1}{p}\right) = 2^{2k}\frac{M^3}{\varphi(M)}\prod_{p|M}\left(1 - \frac{1}{p^2}\right).$$

Certainly $\prod_{p|M}\left(1 - 1/p^2\right) < \prod_p \left(1 - 1/p^2\right) = \zeta(2)$. Moreover, since M is odd, we have

$$\varphi(M) = \prod_{p|M} p^{v_p(M)}\left(1 - \frac{1}{p}\right) \geq \prod_{p|M} p^{v_p(M)/2} = M^{1/2}.$$

Since $2^{2k}M^{5/2} \leq N^{5/2}$ we have

$$2^{2k}\mu(M,r) < \zeta(2)N^{5/2} \tag{3.6}$$

and the second claim follows.

Define $f(N) = \frac{1}{2}\left(\frac{1}{480}N(N-1)(N-23) - \frac{\zeta(2)}{16}N^{5/2} - 1\right) - 3$. Note that $f(2500) > 0$, and for $N \geq 2500$ the function f is increasing. Thus $p_g(W_{N,r}) > 3$ for each $N > 2500$, and with the aid of a computer we check that

$$\frac{1}{2}\left(\frac{1}{480}N(N-1)(N-23) - \frac{1}{4} \cdot 2^{2k-1}\mu^+(M,r) - 1\right) \geq 3$$

for each $67 \leq N \leq 2500$. The result follows by computing $p_g(W_{N,r})$ for each $N < 67$ and $r \in (\mathbb{Z}/N\mathbb{Z})^\times$. That is, using Theorem 3.6.3 together with the formula for $p_g(\widetilde{Z}_{N,r})$ given in [KS98, Theorem 2], as described in Section 3.6.1.1. □

Lemma 3.6.6. *For each $N \geq 5$ such that $W_{N,r}$ is not rational we have*

$$\begin{aligned} 2K_W^2 &\geq K_{\tilde{Z}}^2 - 3 \cdot 2^{2k-1}\mu^+(M,r) - 6 \\ &> \frac{1}{60}N(N-1)(N-30) - \frac{3}{4}\zeta(2)N^{5/2} - 6, \end{aligned}$$

so in particular $K_W^2 > 0$ for all $N > 105$.

Proof. From Lemma 3.6.4 we see that $2K_W^2 \geq K_{\tilde{Z}}^2 - 2K_{\tilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ} + \widetilde{\boldsymbol{F}}_{Z^\circ}^2$. Hence by (3.5) we have

$$2K_W^2 \geq K_{\tilde{Z}}^2 + \sum_F (2p_g(F) - 2) - 3K_{\tilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ}$$

where the sum ranges over irreducible components of $\widetilde{\boldsymbol{F}}_{Z^\circ}$. But $\widetilde{\boldsymbol{F}}_{Z^\circ}$ has at most three components hence

$$2K_W^2 \geq K_{\tilde{Z}}^2 - 3K_{\tilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ} - 6.$$

We compute from Lemma 3.5.2 that $K_{\tilde{Z}} \cdot \widetilde{\boldsymbol{F}}_{Z^\circ} \leq 2^{2k-1}\mu^+(M,r)$ and the first claim follows.

By Lemma 3.6.5 when $N > 24$ the surface $W_{N,r}$ is not rational, and by [KS98, Proposition 2.8] for $N \geq 5$ we have $K_{\tilde{Z}}^2 > \frac{1}{60}N(N-1)(N-30)$. As in Lemma 3.6.5, the second claim then follows from (3.6).

Finally, the function $f(N) = \frac{1}{60}N(N-1)(N-30) - \frac{3}{4}\zeta(2)N^{5/2} - 6$ is increasing for $N > 6000$ and noting that $f(6000) > 0$ is sufficient to see that $K_W^2 > 0$ for all $N \geq 6000$. With the aid of a computer we check that

$$\frac{1}{60}N(N-1)(N-30) - 3 \cdot 2^{2k-1}\mu^+(M,r) - 6 > 0$$

for each $106 \leq N \leq 6000$. □

3.7 Modular curves on $W_{N,r}$

To prove Theorem 1.0.6 we use the criteria given in Section 2.4.1. Each of these criteria relies on us being able to produce (-1) and (-2)-curves on $W_{N,r}$. We have three sources for producing such curves. Firstly the irreducible components of the exceptional divisors of the resolution of singularities $\widetilde{Z}_{N,r} \to Z_{N,r}$, secondly the modular curves $F_{m,\lambda}$ defined on $W_{N,r}$ via Hecke correspondences, and finally the diagonal Hirzebruch–Zagier divisors F_g^+ defined in Section 3.3.1.

As we have already seen, when N is divisible by 2 or 3 some adjustments must be made to correctly compute the action of $\tilde{\tau}$. In fact, there are a number of additional phenomena which mean that we must treat these cases more subtly. To this end, in Sections 3.7.2 and 3.7.3 we define additional modular curves on the surfaces $Z_{N,r}$ (either by constructing them from $F_{m,\lambda}$ or by defining carefully chosen elements $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$).

Recall that for a curve $D \subset Z_{N,r}$ we write D° for the image of $\widetilde{D}$ under the morphism $\widetilde{Z}_{N,r} \to Z_{N,r}^\circ$. We write D^* for the image of D° under the quotient morphism $\pi\colon Z_{N,r}^\circ \to W_{N,r}$. Also note that $\pi^* K_W = K_{Z^\circ} - \boldsymbol{F}_{Z^\circ}$.

3.7.1 Rational modular curves on $W_{N,r}$

Let $m \geq 2$ be an integer coprime to N, such that rm is a square modulo N. The modular curve $F^\circ_{m,\lambda}$ is naturally birational to the modular curve $X_0(m)$, and the action on $F^\circ_{m,\lambda}$ induced by τ° agrees with the Fricke involution on $X_0(m)$. It follows that for any pair (m,λ) the image $F^*_{m,\lambda}$ is birational to $X_0^+(m)$ – the quotient of $X_0(m)$ by the Fricke involution. The genus of $X_0^+(m)$ is well known (see e.g., [Coh93, (1.6d)] or [FH99, Remark 2]). For our purposes it will be sufficient to recall (from [Hel73, p. 178]) that $X_0^+(m)$, and therefore $F^*_{m,\lambda}$, is a rational curve if and only if

$$m \in \left\{ \begin{matrix} 2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21, \\ 23,24,25,26,27,29,31,32,35,36,39,41,47,49,50,59,71 \end{matrix} \right\}. \tag{3.7}$$

Combining Lemma 3.2.4 and Lemma 3.5.1 we have:

Lemma 3.7.1. *Let $m \geq 5$ be an integer such that rm is a square modulo N. Then*

$$K_W \cdot F^*_{m,\lambda} \leq \frac{1}{3}\psi(m) - \nu_\infty(m) - \frac{1}{3}\nu_3(m) - \mathfrak{e}(N,m) - f(m)$$

and equality holds if $\widetilde{F}_{m,\lambda}$ is a smooth curve (e.g., if $m < N$). Here $\psi(m)$, $\nu_\infty(m)$, $\nu_3(m)$, and $\mathfrak{e}(N,m)$ are defined in Lemma 3.2.4 and $f(m)$ is defined in Lemma 3.5.1.

3.7.2 The lifted $X_0(2)$ when $N \equiv 2 \pmod 4$

Let $N = 2M$ be an integer, where M is odd, and let r be coprime to N. Suppose that $2r$ is a square modulo M. Consider the modular curve $F_{2,\lambda} \subset Z_{M,r}$ and let $\alpha\colon Z_{N,r} \to Z_{M,r}$ denote the natural forgetful map. The irreducible components of $\alpha^{-1}F_{2,\lambda}$ are modular curves (with unusual moduli interpretations). We now give an explicit description of a component, $\mathcal{F}_{2,\lambda}$, of $\alpha^{-1}F_{2,\lambda}$. We will see that $\mathcal{F}^*_{2,\lambda}$ is often a (-1)-curve on $W_{N,r}$.

Let $X_0^{\sqrt{\Delta}}(2)$ denote the modular curve attached to the subgroup $\left\langle \left(\begin{smallmatrix}3&1\\2&3\end{smallmatrix}\right), \left(\begin{smallmatrix}3&3\\2&1\end{smallmatrix}\right) \right\rangle \subset \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ (this is the modular curve with LMFDB label `4.6.0.d.1`). Explicitly, the non-cuspidal K-rational points on $X_0^{\sqrt{\Delta}}(2)$ parametrise elliptic curves E/K admitting a 2-isogeny $E \to E'$ (defined over K) and such that $\Delta(E) \equiv \Delta(E') \pmod{(K^\times)^2}$. But any such elliptic curves are necessarily 2-congruent over K. To see this, choose Weierstrass equations $y^2 = xf(x)$ and $y^2 = xf'(x)$ for E/K and E'/K, then $K(E[2]) = K(\alpha)$ and $K(E'[2]) = K(\beta)$ where α and β are roots of $f(x)$ and $f'(x)$ respectively. Therefore E and E' are 2-congruent over K if and only if the discriminant of $f(x)$ and $f'(x)$ are equal up to a square.

As in Section 2.3.5, fix an integer $a \in \mathbb{Z}$ such that $r = 2a^2 \pmod M$. Let $\mathcal{E}/\mathbb{Q}(X_0^{\sqrt{\Delta}}(2))$ be a generic curve, and let $\Phi\colon \mathcal{E} \to \mathcal{E}'$ be a 2-isogeny defined over $\mathbb{Q}(X_0^{\sqrt{\Delta}}(2))$. Choose a 2-congruence $\Psi\colon \mathcal{E}[2] \to \mathcal{E}'[2]$, then for each $\lambda \in \{x \in \mathbb{Z}/M\mathbb{Z} : x^2 = 1\}/\{\pm 1\}$ we obtain a point $(\mathcal{E}, \mathcal{E}', \Psi \times (a\lambda\Phi)|_{\mathcal{E}[M]})$ on $Z_{N,r}$. Letting $\mathcal{F}_{2,\lambda}$ denote the Zariski closure of this point, we obtain a birational map $X_0^{\sqrt{\Delta}}(2) \dashrightarrow \mathcal{F}_{2,\lambda}$.

Lemma 3.7.2. *Suppose that $N = 2M$ where M is an odd integer. If $W_{N,r}$ is not a rational surface, then $\mathcal{F}^*_{2,\lambda}$ is a (-1)-curve on $W_{N,r}$ which intersects a single component of $E^*_{2,1}$.*

Proof. Intersecting with the class in (3.2) we have $K_{\tilde{Z}} \cdot \widetilde{\mathcal{F}}_{2,\lambda} \leq 0$. Note that $\widetilde{\mathcal{F}}_{2,\lambda}$ meets $\boldsymbol{F}_{\tilde{Z}}$ at two distinct points (corresponding to the two pre-images of the CM point of discriminant -8 on $X_0(2)$). Therefore $K_W \cdot \mathcal{F}^*_{2,\lambda} \leq -1$ and $\mathcal{F}^*_{2,\lambda}$ is a (-1)-curve by Lemma 2.4.4.

The curve $\widetilde{\mathcal{F}}_{2,\lambda}$ meets the component of $E_{2,1}$ given by resolving the singular point $(E, E, \phi) \in Z_{N,r}$ and its image under τ. Here E is an elliptic curve with $j(E) = 1728$ and $\phi = a\left(\begin{smallmatrix} 1 & -1 \\ 1 & M+1 \end{smallmatrix}\right)$. The claim follows. □

Remark 3.7.3. The curves $\mathcal{F}_{2,\lambda}$ are natural choices to consider since they are in fact the irreducible components of $\alpha^{-1}F_{2,\lambda}$ on $Z_{N,r}$ with the smallest genus. One could similarly define such curves on the surface $Z_{N,r}$ for any integer N and divisor $d|N$ with $\gcd(d, d/N) = 1$.

3.7.3 The exceptional $(F_g^+)^*$ when $N \equiv 3 \pmod 9$

Suppose that $N = 3Q$ where $Q \neq 1$ is an integer coprime to 3. Suppose that r is a square modulo Q and choose a coprime to N such that $r \equiv a^2 \pmod Q$. Fix an isomorphism $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/Q\mathbb{Z})$.

In addition to the matrices g_{s}, g_{ns}, and $g_{\mathrm{b}} \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ defined in Definition 3.3.6 we define the matrix

$$g_{\overline{\mathrm{ns}}} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}).$$

Let ω and λ be elements of $(\mathbb{Z}/N\mathbb{Z})^\times$ representing elements of $\{x \in (\mathbb{Z}/Q\mathbb{Z})^\times : x^2 = r\}/\{\pm 1\}$ and $\{x \in (\mathbb{Z}/N\mathbb{Z})^\times : x^2 = r\}/\{\pm 1\}$ respectively. The $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$-conjugacy classes of the elements $\lambda(g_{\mathrm{b}}, I)$, $\lambda(g_{\overline{\mathrm{ns}}}, I)$, $\omega(g_{\mathrm{s}}, I)$, and $\omega(g_{\mathrm{ns}}, I)$ are distinct.

Notation 3.7.4. Let $N = 3Q$ where Q is an integer coprime to 3. Let $g_\bullet \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and $g_\blacksquare \in \mathrm{GL}_2(\mathbb{Z}/Q\mathbb{Z})$ be elements with labels "$\bullet$" and "$\blacksquare$" respectively. Similarly to Notation 3.3.9, if $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$ we write $X^+_{\alpha[\bullet,\blacksquare]} := X^+_{\alpha(g_\bullet, g_\blacksquare)}$ and $F^+_{\alpha[\bullet,\blacksquare]} := F^+_{\alpha(g_\bullet, g_\blacksquare)}$.

For each such ω and λ we therefore have distinct curves $F^+_{\lambda[\mathrm{b},I]}$, $F^+_{\omega[\mathrm{ns},I]}$, $F^+_{\lambda[\overline{\mathrm{ns}},I]}$, and $F^+_{\omega[\mathrm{s},I]}$ on $Z_{N,r}$. There are:

- $\frac{1}{2}\rho(3,r)\rho(Q,r)$ curves $F^+_{\lambda[\mathrm{b},I]}$,
- $\frac{1}{4}\rho(3,r)\rho(Q,r)$ curves $F^+_{\omega[\mathrm{ns},I]}$,
- $\frac{1}{2}\rho(3,2r)\rho(Q,r)$ curves $F^+_{\lambda[\overline{\mathrm{ns}},I]}$, and
- $\frac{1}{4}\rho(3,2r)\rho(Q,r)$ modular curves $F^+_{\omega[\mathrm{s},I]}$.

Over $\mathbb{Q}(\zeta_3)$, the modular curves $F^+_{\lambda[\mathrm{b},I]}$ have two irreducible components each birational to $X_1(3)$. The curves $F^+_{\omega[\mathrm{ns},I]}$ are birational to $X(\mathrm{ns}\,3)$ and each curve $F^+_{\lambda[\overline{\mathrm{ns}},I]}$ is birational to $X(\mathrm{ns}\,3^+)$. The curves $F^+_{\omega[\mathrm{s},I]}$ are birational to $X(\mathrm{s}\,3)$. Here $X(\mathrm{ns}\,3)$ and $X(\mathrm{s}\,3)$ denote the modular curves attached to Cartan subgroups *not* their normalisers.

Lemma 3.7.5. *If $W_{N,r}$ is not rational, then $(F^+_{\lambda[\mathrm{b},I]})^*$, $(F^+_{\omega[\mathrm{ns},I]})^*$, $(F^+_{\lambda[\overline{\mathrm{ns}},I]})^*$, and $(F^+_{\omega[\mathrm{s},I]})^*$ are (geometrically irreducible) (-1)-curves.*

Proof. First note that for each $g \in \{(g_{\mathrm{b}}, I), (g_{\mathrm{ns}}, I), (g_{\overline{\mathrm{ns}}}, I), (g_{\mathrm{s}}, I)\}$ the matrix rg^{-1} is conjugate to g, so τ restricts to an involution on $F^+_{\lambda g}$. Intersecting with the canonical class (3.2) and applying Lemma 2.4.4 we see that the two components of $\widetilde{F}^+_{\lambda[\mathrm{b},I]}$ are (-1)-curves which are swapped by $\tilde{\tau}$. Similarly, for each $g \in \{(g_{\mathrm{ns}}, I), (g_{\overline{\mathrm{ns}}}, I), (g_{\mathrm{s}}, I)\}$ we have $K_{\tilde{Z}} \cdot \widetilde{F}^+_{\lambda g} \leq 0$ and $\widetilde{F}^+_{\lambda g}$ meets $\boldsymbol{F}_{\tilde{Z}}$ at two distinct points. Therefore $K_W \cdot (\widetilde{F}^+_{\lambda g})^* \leq -1$ and the claim follows from Lemma 2.4.4. □

3.8 The Kodaira dimension and Theorem 1.0.6

To prove Theorem 1.0.6 it remains to study the cases when $W_{N,r}$ is rational or of general type (the cases when $N = 17, 19$ having been studied by Hermann [Her92] who showed that $W_{17,r}$ and $W_{19,r}$ are (blown-up) elliptic K3 and properly elliptic surfaces respectively).

3.8.1 The rational cases

We first prove Theorem 1.0.6(i), which we re-state as the following proposition.

Proposition 3.8.1. *The symmetric Hilbert modular surface $W_{N,r}$ is rational if and only if either $N \leq 14$ or $(N, r) \in \{(15,1), (15,2), (15,11), (16,1), (16,3), (16,7), (18,5), (20,11), (24,23)\}$.*

Proof. A smooth rational surface $S/\mathbb{C}$ has geometric genus $p_g(S) = 0$. In particular, by Theorem 1.0.4, the surfaces $W_{N,r}$ may only be rational for those (N, r) in the statement of the proposition.

To see that whenever $p_g(W_{N,r}) = 0$ the surface $W_{N,r}$ is rational, we argue as follows. We first compute from the projection formula

$$K_W \cdot C_\infty^* = \begin{cases} \widetilde{C}_{\infty,1} \cdot (K_{\tilde{Z}} - \boldsymbol{F}_{\tilde{Z}}) + \frac{1}{2}\rho(N,r) & \text{if } N \equiv 1 \pmod 2, \\ \widetilde{C}_{\infty,1} \cdot (K_{\tilde{Z}} - \boldsymbol{F}_{\tilde{Z}}) + \rho(N,r) & \text{if } N \equiv 0 \pmod 2. \end{cases}$$

Note that on $\widetilde{Z}_{N,r}$ for each $d|N$ the resolution divisors $E_{\infty,d,-1}$ (as defined in Section 3.2, see Table 3.1) consist of $\frac{1}{2}\rho(d,-r)\varphi(N/d)$ disjoint chains of (-2)-curves linking $\widetilde{C}_{\infty,1}$ and $\widetilde{C}_{\infty,2}$. The divisors $E_{\infty,d,1}$ meet the fixed locus $\boldsymbol{F}_{\tilde{Z}}$ in the configurations given by Proposition 3.3.20. Moreover, none of the curves blown down in forming $Z_{N,r}^\circ$ meet $E_{\infty,d,-1}$. It follows that $E_{\infty,d,-1}^*$ consists of $\frac{1}{2}\rho(d,-r)\varphi(N/d)$ disjoint chains of $\lfloor d/2 \rfloor$ smooth rational curves. The first $\lfloor d/2 \rfloor - 1$ of which are (-2)-curves and the last is a (-1)-curve. The first curve in each chain meets C_∞^*. Such chains can therefore be successively blown down to form a surface $\overline{W}_{N,r}$ and if $K_{\overline{W}}$ is a canonical divisor we have

$$K_{\overline{W}} \cdot \overline{C}_\infty = K_W \cdot C_\infty^* - \frac{1}{2} \sum_{d|N, d\neq 1} \rho(d,-r)\varphi(N/d),$$

where here $\overline{C}_\infty$ denotes the image of C_∞^* on $\overline{W}_{N,r}$. By Proposition 3.3.20 we have $\widetilde{C}_{\infty,1} \cdot \boldsymbol{F}_{\tilde{Z}} = \frac{1}{2}\varphi(N)$ and

$$\widetilde{C}_{\infty,1}^2 = -\frac{1}{2} \sum_{\nu=1}^{N-1} \varphi(\gcd(\nu, N)) \left\langle \frac{\nu^2 r}{N \gcd(\nu, N)} \right\rangle$$

by [KS98, Proposition 2.5] (cf. [Her91, Hilfssatz 5], note the missing factor of $\frac{1}{2}$ in [KS98, Proposition 2.5]). Here $\langle x \rangle = x - \lfloor x \rfloor$ denotes the fractional part of x. The genus of $\widetilde{C}_{\infty,1} \cong X_1(N)$ is well known (e.g., [KS98, Remark 1.4]) and $K_{\tilde{Z}} \cdot \widetilde{C}_{\infty,1}$ can be computed the adjunction formula (Proposition 2.4.1).

Suppose that (N, r) is one of the pairs in the statement of the proposition. We compute that if $N \leq 10$ we have $K_{\overline{W}} \cdot \overline{C}_\infty \leq -2$. Moreover, if $N \geq 11$ except for the cases $(N, r) = (12, 1)$, $(14, 1)$, $(15, 1)$, $(16, 1)$, and $(24, 23)$ then $K_{\overline{W}} \cdot \overline{C}_\infty \leq -1$. In particular, by Lemma 2.4.4(ii) in each of these cases $W_{N,r}$ is rational. We consider the remaining cases separately:

The case $(N,r)=(12,1)$. Consider the divisor $E_{\infty,2,1}$ on $\widetilde{Z}_{12,1}$. Its image $E^*_{\infty,2,1}$ on $W_{12,1}$ consists of a single (-1)-curve for which $E^*_{\infty,2,1}\cdot(F^+_{(\mathrm{c,w})})^*=2$. By the projection formula

$$K_W\cdot\left(F^+_{(\mathrm{c,w})}\right)^*=\left(K_{Z^\circ}-\left(F^+_{(\mathrm{c,w})}\right)^\circ\right)\cdot\left(F^+_{(\mathrm{c,w})}\right)^\circ$$

and combining Corollary 3.4.5 and Lemmas 3.5.1 and 3.6.2 we see that $K_W\cdot(F^+_{(\mathrm{c,w})})^*=0$. Thus $K_{\overline{W}}\cdot\overline{F^+_{(\mathrm{c,w})}}=-2$ and again we see that $W_{12,1}$ is rational.

The case $(N,r)=(14,1)$. Note that the modular curve $\widetilde{F}_{11,1}$ meets the cusp resolutions only at the divisors $E_{\infty,14,9}$ and $E_{\infty,14,11}$, which are exchanged by $\tilde{\tau}$. These are $(-2,-3,-2,-2,-2)$ and $(-2,-2,-2,-3,-2)$-chains respectively, and by Lemma 3.2.2 the multiplicities of each component in $(\tilde{\mathrm{j}})^*(\infty)$ are $(9,4,3,2,1)$ and $(11,8,5,2,1)$ respectively.

By the projection formula $\widetilde{F}_{11,1}\cdot(\tilde{\mathrm{j}})^*(\infty)=[\mathrm{GL}_2(\mathbb{Z}/11\mathbb{Z}):G(\mathrm{b}\,11)]=12$ and it follows that $\widetilde{F}_{11,1}$ meets these resolutions at the last and first components respectively (this may also be seen from Lemma 3.2.4). On $\overline{W}_{14,1}$ we blow down the image of $F^*_{11,1}$ (which does not meet the exceptional divisor of $W_{14,1}\to\overline{W}_{14,1}$) followed by the first component of the image of $E^*_{\infty,14,9}$ (which meets $\overline{C}_\infty$). Since on $\overline{W}_{14,1}$ we have $K_{\overline{W}}\cdot\overline{C}_\infty=0$ the surface $W_{14,1}$ is rational.

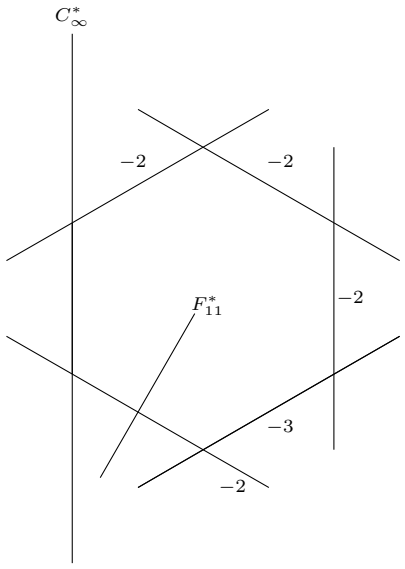


FIGURE 3.6: A configuration of curves on $W_{14,1}$ in a neighbourhood of $E^*_{\infty,14,11}$.

The case $(N,r)=(15,1)$. We consider the curves $\widetilde{F}_{4,\lambda}$ and $\widetilde{F}_{16,\lambda}$ on $\widetilde{Z}_{15,1}$. By Lemmas 3.2.2 and 3.2.4, together with the projection formula, it follows that $\widetilde{F}_{4,\lambda}$ and $\widetilde{F}_{16,\lambda}$ meet $E_{\infty,4,1}$ as depicted in Figure 3.7. Since the curves $\widetilde{F}_{4,\lambda}$ are blown down in forming $Z^\circ_{15,1}$, the components of $E^\circ_{\infty,15,4}$ are each (-3)-curves, meeting $\boldsymbol{F}_{Z^\circ}$ transversally at a point. Thus $E^*_{\infty,15,4}$ consists of a pair of (-2)-curves intersecting transversally at a single point.

From Lemma 3.7.1 it follows that $K_W\cdot F^*_{16,\lambda}\leq-1$. If either $F^*_{16,\lambda}$ is singular, or if equality does not hold, then it follows that $W_{15,1}$ is rational by Lemma 2.4.4. Otherwise, $F^*_{16,\lambda}$ is a (-1)-curve on $W_{15,1}$ which we may assume does not meet another (-1)-curve (else again $W_{15,1}$ is rational). In this case, the (-1)-curves $F^*_{16,1}$ and $F^*_{16,4}$ on $W_{15,1}$ do not intersect, hence each meets a separate component of $E^*_{\infty,15,4}$ at one point. But (after blowing down each $F^*_{16,\lambda}$) the components of $E^*_{\infty,15,4}$, which are now exceptional, intersect. Thus $W_{15,1}$ is rational.

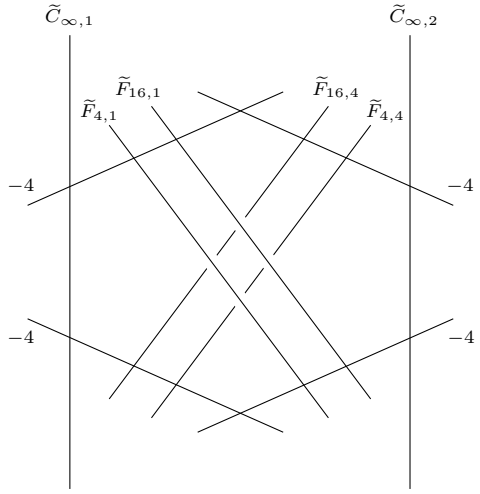


FIGURE 3.7: Configuration of curves on $\widetilde{Z}_{15,1}$ in a neighbourhood of $E_{\infty,15,4}$. We do not claim anything about the intersections of $\widetilde{F}_{4,\lambda}$ and $\widetilde{F}_{16,\lambda}$.

The case $(N,r) = (16,1)$. The curves $\widetilde{F}_{9,\lambda}$ meet the cusp resolutions at the divisors $E_{\infty,16,1}$ and $E_{\infty,16,9}$. These divisors each consist of a pair of (-16) and $(-2,-5,-2)$-chains respectively with multiplicities in $(\tilde{\mathrm{j}})^*(\infty)$ of (1) and $(9,2,1)$. The curves $\widetilde{F}_{9,\lambda}$ each have 4 cusps and by the projection formula $\widetilde{F}_{9,1} \cdot (\tilde{\mathrm{j}})^*(\infty) = 12$.

Define $g_{\mathrm{b}4^\sharp} \in \mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z})$ to be the matrix $g_{\mathrm{b}4^\sharp} = \left(\begin{smallmatrix} 3 & 4 \\ 0 & 11 \end{smallmatrix}\right)$. The modular curve $\widetilde{F}^+_{\mathrm{b}4^\sharp}$ is a rational. Indeed, $H^+_{\mathrm{b}4^\sharp}$ is the pre-image in $\mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z})$ of the largest subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ contained in $G(\mathrm{b}\,4)$ which is trivial mod 2 (this subgroup has LMFDB label `4.12.0.b.1`). Moreover $\widetilde{F}^+_{\mathrm{b}4^\sharp}$ is smooth since it is fixed by the involution on $Z_{16,1}$ induced by $\omega\tau$, where $\omega\colon Z_{16,1} \to Z_{16,1}\colon (E,E',\phi) \mapsto (E,E',9\phi)$. We compute from (3.2) that $K_{\tilde{Z}} \cdot \widetilde{F}^+_{\mathrm{b}4^\sharp} = 0$.

Since $g_{\mathrm{b}4^\sharp}$ is conjugate to its inverse, τ acts as an involution on $F^+_{\mathrm{b}4^\sharp}$. Therefore by Lemma 3.3.16 the involution $\tilde{\tau}$ either has two isolated fixed points on $\widetilde{F}^+_{\mathrm{b}4^\sharp}$ or $\widetilde{F}^+_{\mathrm{b}4^\sharp}$ meets $\widetilde{F}^+_{\mathrm{c}}$ transversally at two points. The former cannot occur, so $(F^+_{\mathrm{b}4^\sharp})^*$ is a (-1)-curve.

In a neighbourhood of $E^*_{\infty,16,9}$ we have a configuration as in Figure 3.8. Blowing down sequentially $(F_{9,\lambda})^*$ and the (-2)-curves in $E^*_{\infty,16,9}$, we see that the image of $E^*_{\infty,16,9}$ is a (-1)-curve which intersects the (-1)-curve $(F^+_{\mathrm{b}4^\sharp})^*$.

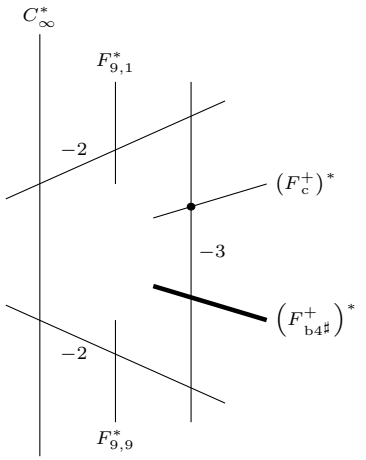


FIGURE 3.8: Configuration of curves on $W_{16,1}$. Lines and points in bold are fixed by the Atkin–Lehner involution on $W_{16,1}$ induced by $\tau\omega$ where $\omega\colon Z_{16,1} \to Z_{16,1}\colon (E,E',\phi) \mapsto (E,E',9\phi)$.

The case $(N, r) = (24, 23)$. On $Z_{24,23}$ each curve $F_{23,\lambda}$ meets exactly one of the singular points of type $(24, 23)$. The smooth curve $\widetilde{F}_{23,\lambda}$ meets the resolution of this singularity transversally at two points, each with multiplicity one (in fact, as above, one can show that $F_{23,\lambda}$ meets the resolution curves which intersect $\widetilde{C}_\infty$). Moreover by Lemma 3.7.1 we have $K_W \cdot F^*_{23,\lambda} = 0$. But then the image of $F^*_{23,\lambda}$ on $\overline{W}_{24,23}$ is a (-1)-curve. Since $K_{\overline{W}} \cdot \overline{C}_\infty = 0$, blowing down the images of the curves $F^*_{23,\lambda}$ (for the four $\lambda \in (\mathbb{Z}/24\mathbb{Z})^\times/((\mathbb{Z}/24\mathbb{Z})^\times)^2$), it follows from Lemma 2.4.4(ii) that $W_{24,23}$ is rational (the intersection number of the image of $\overline{C}_\infty$ with a canonical divisor is -4).

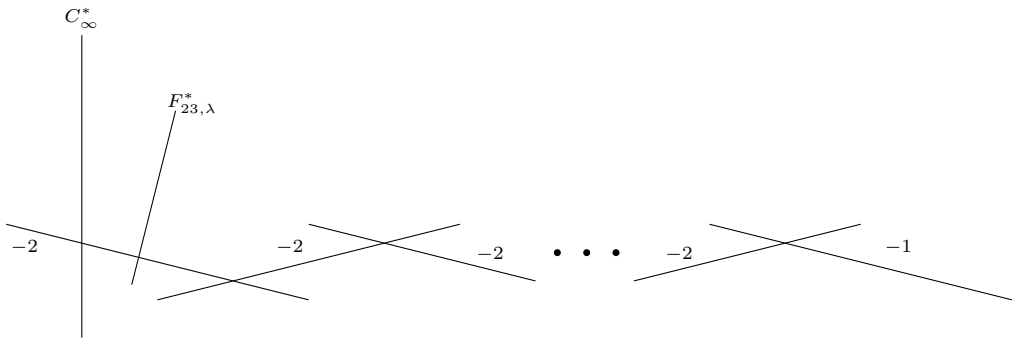


FIGURE 3.9: Configuration of curves on $W_{24,23}$. □

3.8.2 The cases of general type

We now suppose, in light of Proposition 3.8.1, that $W_{N,r}$ is not a rational surface. Recall that we write

$$s_{2,1}(N,r) = \begin{cases} \frac{1}{2}h(-4N^2) & \text{if } N \not\equiv 0 \pmod 4, \\ h(-4N^2) & \text{if } N \equiv 0 \pmod 4 \text{ and } r \equiv 3 \pmod 4, \text{ and} \\ 0 & \text{if } N \equiv 0 \pmod 4 \text{ and } r \equiv 1 \pmod 4, \end{cases}$$

and

$$s_{3,2}(N,r) = \begin{cases} \frac{1}{2}h(-3N^2) & \text{if } N \not\equiv 0 \pmod 3, \\ h(-3N^2) & \text{if } N \equiv 0 \pmod 3 \text{ and } r \equiv 2 \pmod 3, \text{ and} \\ 0 & \text{if } N \equiv 0 \pmod 3 \text{ and } r \equiv 1 \pmod 3. \end{cases}$$

Also define

$$\rho_2(N,r) = \begin{cases} \rho(N/2, r) & \text{if } N \equiv 2 \pmod 4, \text{ and} \\ 0 & \text{otherwise,} \end{cases}$$

$$\rho_3(N,r) = \begin{cases} \rho(N/3, r) & \text{if } N \equiv 3 \pmod 9, \text{ and} \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\mathfrak{m}(N,r) = \frac{1}{2}\sum_m \rho(N, mr),$$

where in the definition of $\mathfrak{m}(N,r)$ the sum ranges over those $m \geq 5$ for which $F^*_{m,\lambda}$ is rational (see (3.7)) and $K_W \cdot F^*_{m,\lambda} \leq -1$ (see Lemma 3.7.1).

We define a smooth, projective surface, which we denote $W^{\circ}_{N,r}$, by successively blowing down:

1. the $s_{3,2}(N,r)$ components of $E^*_{3,2}$ and the $s_{2,1}(N,r)$ components of $E^*_{2,1}$ whose strict transforms meet $\boldsymbol{F}_{\tilde{Z}}$,
2. the components of $E^*_{\infty,d,-1}$ for each $d|N$ with $d \neq 1$ (there are $\frac{1}{2}\lfloor d/2 \rfloor \rho(d,-1)\varphi(N/d)$ components),
3. the $\mathfrak{m}(N,r)$ rational modular curves $F^*_{m,\lambda}$ for which $K_W \cdot F^*_{m,\lambda} \leq -1$ (hence equal by Lemma 2.4.4),
4. the $\frac{1}{2}\rho(N,3r)$ components of $E^*_{3,1}$ whose strict transforms on $\widetilde{Z}_{N,r}$ met $\widetilde{F}_{3,\lambda}$,
5. the $\frac{1}{2}\rho_2(N,r)$ components of $E^*_{3,1}$ whose strict transforms on $\widetilde{Z}_{N,r}$ met $\widetilde{F}^+_{\lambda(I^\sharp,I)}$,
6. the $\frac{1}{2}\rho(N,5r)$ components of $E^*_{2,1}$ which meet the curves $F^*_{5,\lambda}$,
7. the $\frac{1}{2}\rho_2(N,2r)$ modular curves $\mathcal{F}^*_{2,\lambda}$ together with the components of $E^*_{2,1}$ which they meet,
8. the $\frac{3}{2}\rho_3(N,r)$ curves $(F^+_{\lambda[\bullet,I]})^*$ from Lemma 3.7.5.

It is then simple to compute the self-intersection of a canonical divisor for $W^{\circ}_{N,r}$ using the projection formula, as follows.

Lemma 3.8.2. *Let K_{W° be a canonical divisor for $W^{\circ}_{N,r}$. We have*

$$K^2_{W^\circ} = K^2_W + \sum_{d|N,\, d\neq 1} \frac{\lfloor d/2 \rfloor \rho(d,-r)\varphi(N/d)}{2} + s_{2,1}(N,r) + s_{3,2}(N,r) + \mathfrak{m}(N,r) + \frac{1}{2}\rho(N,3r) + \frac{1}{2}\rho(N,5r) + \frac{1}{2}\rho_2(N,r) + \rho_2(N,2r) + \frac{3}{2}\rho_3(N,r).$$

In particular if (N,r) are as in Theorem 1.0.6(iv) we have $K^2_{W^\circ} > 0$.

Proof. The first claim follows immediately from the construction. Noting that $K^2_{W^\circ} > K^2_W$ it follows from Lemma 3.6.6 that $K^2_{W^\circ} > 0$ for each $N > 105$. The remaining cases follow from a calculation, where we compute K^2_W by applying Lemma 3.6.4 as described in Section 3.6.1.1. □

Remark 3.8.3. The surface $W^{\circ}_{N,r}$ is a generalisation of the surface which Hermann denotes W^{ν}_p [Her92, p. 177]. We take this opportunity to correct a small mistake in [Her92] where it is claimed there that no known curves (i.e., modular curves and curves arising from the resolution of singularities on $Z_{N,r}$) are exceptional on W^{ν}_p. However in their construction of W^{ν}_p they do not contract the component of $E^*_{2,1}$ which meets F^*_5 when $5r$ is a square modulo p.

From Lemma 3.8.2 we are now able to deduce Theorem 1.0.6(iv), which (in particular) proves that the surface $W_{N,r}$ is of general type whenever $N \geq 25$.

Proposition 3.8.4. *If (N,r) is as in Theorem 1.0.6(iv) then $W_{N,r}$ is a surface of general type.*

Proof. By Lemma 2.4.7 if $K^2_{W^\circ} > 0$, then $W_{N,r}$ is a surface of general type. The claim then follows immediately from Lemma 3.8.2. □

Chapter 4

Congruences between quadratic twists of elliptic curves

Recall from Definition 1.0.14 that we say an elliptic curve $E/\mathbb{Q}$ admits a *quadratic twist-type* (N, r)*-congruence* if there exists a non-trivial quadratic twist $E^d/\mathbb{Q}$ of E such that E and E^d are (N, r)-congruent. We say that such a quadratic twist-type congruence is *non-trivial* if E and E^d are not isogenous over $\mathbb{Q}$. In this chapter we study quadratic twist-type congruences and, in particular, we prove Theorems 1.0.15 and 1.0.16.

In Section 4.1 we prove our main technical results. By adapting the proofs of Cremona–Freitas [CF22, Theorem 2.4] and Halberstadt [Hal98, Section 2.1] we give a necessary and sufficient condition for an elliptic curve to admit a quadratic twist-type N-congruence for $N > 2$, in terms of the mod N image of Galois (see Lemma 4.1.1). We first use this to extend [CF22, Theorem 2.4] to odd prime powers (see Proposition 4.1.4). We then classify quadratic twist-type $(2^k, r)$-congruences of non-CM elliptic curves as an application of Rouse and Zureick-Brown's [RZ15a] classification of the possible 2-adic images of the Galois representation attached to an elliptic curve $E/\mathbb{Q}$ without CM.

In Section 4.2 we show that an elliptic curve $E/\mathbb{Q}$ is isogenous to a non-trivial quadratic twist if and only if E has CM (see Lemma 4.2.1). By classifying all non-trivial quadratic twist-type congruences between elliptic curves, $E/\mathbb{Q}$, with CM (see Proposition 4.2.2) we deduce Theorem 1.0.15 when N is a prime power.

In Section 4.3 we construct modular curves which parametrise elliptic curves which admit quadratic twist-type N-congruences for composite N. By computing the genera of these modular curves and computing explicit models for those with genus ≤ 1 we conclude the proof of Theorem 1.0.15 in Section 4.4.

In Section 4.5 we give evidence for Conjecture 1.0.17. Specifically we compute explicit models for modular curves of genus ≤ 4 whose points give rise to quadratic twist-type congruences. By searching for rational points on these modular curves we prove Theorem 1.0.16 and a conditional form of Conjecture 1.0.17 (see Theorem 4.5.1).

Finally in Section 4.6.1 we perform a detailed analysis of quadratic twist-type $(15, 7)$-congruences (equivalently $(30, 7)$-congruences). We use elliptic Chabauty to find all the rational points on a genus 2 curve whose Jacobian has rank 2 and admits a Richelot isogeny. It follows that $E_{(30,7)}/\mathbb{Q}$ is (up to a quadratic twist) the only elliptic curve over $\mathbb{Q}$ admitting a non-trivial quadratic twist-type $(15, 7)$-congruence. As a corollary we obtain a new proof of the class number 1 problem in Section 4.6.1.1.

In this chapter we make extensive use of Rouse, Sutherland, and Zureick-Brown's package `gl2.m` (see [RSZ21]) which is based on the techniques in [RSZ22]. In particular we found this package especially useful for computing genera of modular curves and manipulating subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

4.1 Quadratic twist-type p^l-congruences of elliptic curves

The idea for the following lemma is due to Cremona–Freitas [CF22, Lemma 2.2 and Theorem 2.4] and Halberstadt [Hal98, Section 2.1]. We provide a generalisation to composite N.

Let K be a field of characteristic zero. For an elliptic curve E/K we let E^d/K denote the quadratic twist of E by $d \in K^\times$.

Lemma 4.1.1. *Let E/K be an elliptic curve with $j(E) \notin \{0, 1728\}$ and let $N > 2$ be an integer. Let $H^+ = \bar{\rho}_{E,N}(G_K)$ be the image of the mod N Galois representation $\bar{\rho}_{E,N}$. Then E admits a quadratic twist-type N-congruence if and only if there exists an index 2 subgroup $H \subset H^+$ and a matrix $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that*

$$g^{-1}hg = h \quad \text{for all } h \in H \qquad \text{and} \qquad g^{-1}hg = -h \quad \text{for all } h \in H^+ \setminus H. \tag{4.1}$$

More explicitly, let $d \in K^\times$ be such that $\bar{\rho}_{E,N}^{-1}(H) = G_{K(\sqrt{d})}$. Then E is N-congruent to E^d and the power of the congruence is $\det(g)$.

Proof. By Proposition 2.2.11 such a quadratic twist type N-congruence exists if and only if there exists $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that H^+ is contained in H_g^+. Moreover, in this case $d \in K^\times$ is such that $\bar{\rho}_{E,N}^{-1}(H) = G_{K(\sqrt{d})}$ where $H = H^+ \cap H_g$. But by assumption a quadratic twist type N-congruence is between E and a *non-trivial* quadratic twist. This is the case if and only if H has index 2 in H^+. The condition in (4.1) follows from the definition of H_g and H_g^+. □

Remark 4.1.2. Note that the assumption that $N > 2$ in Lemma 4.1.1 is necessary. An elliptic curve E/K is 2-congruent to every quadratic twist, so there may exist $d \in K^\times$ such that E is 2-congruent to E^d but $\bar{\rho}_{E,2}(G_K) = \bar{\rho}_{E,2}(G_{K(\sqrt{d})})$.

Remark 4.1.3. Taking traces in (4.1) shows that for any $h \in H^+ \setminus H$ we have $2\,\mathrm{tr}(h) = 0$ and $2\,\mathrm{tr}(g) = 0$. If N is odd then $\mathrm{tr}(g) = 0$, and the Cayley–Hamilton theorem implies that $g^2 = -\det(g)$.

4.1.1 Quadratic twist-type p^l-congruences

Lemma 4.1.1 allows us to extend [CF22, Theorem 2.4] to powers of odd primes (while also ensuring we avoid their condition **(S)**). For an odd prime p let ξ be a quadratic non-residue modulo p.

Proposition 4.1.4. *Let E/K be an elliptic curve with $j(E) \notin \{0, 1728\}$, let p be an odd prime, and let $l \geq 1$ be an integer. Then E admits a quadratic twist-type $(p^l, -1)$-congruence if and only if there exists a choice of basis for $E[p^l]$ such that the image of the mod p^l Galois representation, $\bar{\rho}_{E,p^l}(G_K)$, is contained in $G(\mathrm{s}\,p^{l+})$, but not the subgroup $G(\mathrm{s}\,p^l)$. More explicitly, let $d \in K^\times$ be such that $\bar{\rho}_{E,p^l}(G_{K(\sqrt{d})}) = \bar{\rho}_{E,p^l}(G_K) \cap G(\mathrm{s}\,p^l)$. Then E is $(p^l, -1)$-congruent to E^d.*

Similarly E admits a quadratic twist-type $(p^l, -\xi)$-congruence if and only if there exists a choice of basis for $E[p^l]$ such that the image of the mod p^l Galois representation, $\bar{\rho}_{E,p^l}(G_K)$, is contained in $G(\mathrm{ns}\,p^{l+})$, but not the subgroup $G(\mathrm{ns}\,p^l)$. More explicitly, let $d \in K^\times$ be such that $\bar{\rho}_{E,p^l}(G_{K(\sqrt{d})}) = \bar{\rho}_{E,p^l}(G_K) \cap G(\mathrm{ns}\,p^l)$. Then E is $(p^l, -\xi)$-congruent to E^d.

Proof. By Lemma 4.1.1 and Remark 4.1.3 the elliptic curve E admits a quadratic twist-type p^l-congruence if and only if there exists an element $g \in \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ such that $g^2 = -\det(g)$, $\bar{\rho}_{E,p^l}(G_K) \subset H_g^+$, and $\bar{\rho}_{E,p^l}(G_{K(\sqrt{d})}) = \bar{\rho}_{E,p^l}(G_K) \cap H_g$ is a proper subgroup of $\bar{\rho}_{E,p^l}(G_K)$.

By Lemma 3.3.7 there exists a scalar $u \in (\mathbb{Z}/p^l\mathbb{Z})^\times$ such that the matrix ug is conjugate to either g_{s} or $g_{\mathrm{ns}} \in \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ (as defined in Section 2.2.7). The claim follows immediately from Lemma 2.2.12. □

4.1.2 Quadratic twist-type 2^k-congruences

It is clear that an elliptic curve E/K is 2-congruent to any quadratic twist E^d/K for $d \in K^\times$. Furthermore, it was shown in [BD11, Corollary 7.4] that any elliptic curve is $(4,3)$-congruent to its quadratic twist by its discriminant. Taking $k = 1$ in the following proposition removes the hypothesis on the image of G_K (since $G(\mathrm{ns}\,2^+) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$) and we recover [BD11, Corollary 7.4]. In fact, we also recover their proof.

Proposition 4.1.5. *Let E/K be an elliptic curve with $j(E) \notin \{0, 1728\}$ and let $k \geq 1$ be an integer. Suppose that there exists a choice of basis for $E[2^k]$ such that the image of the mod 2^k Galois representation, $\bar{\rho}_{E,2^k}(G_K)$, is contained in the subgroup $G(\mathrm{ns}\,2^{k^+}) \subset \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$. Then E is $(2^{k+1}, 3)$-congruent to its quadratic twist by its discriminant $\Delta := \Delta(E)$.*

Similarly, if there exists a choice of basis for $E[2^k]$ such that the image of the mod 2^k Galois representation, $\bar{\rho}_{E,2^k}(G_K)$, is contained in the subgroup[1] $G(\mathrm{s}\,2^{k^+}) \subset \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ then E is $(2^{k+1}, -1)$-congruent to its quadratic twist by its discriminant.

Proof. First note that if E is given by a Weierstrass equation $y^2 = f(x)$ then Δ is equal to the discriminant of $f(x)$ up to a square factor. Now $G(\mathrm{ns}\,2)$ is the unique index 2 subgroup of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, so $\bar{\rho}_{E,2}(G_{K(\sqrt{\Delta})}) = G(\mathrm{ns}\,2) \cap \bar{\rho}_{E,2}(G_K)$. For any $k \geq 1$ the image of $G(\mathrm{s}\,2^k)$ (respectively $G(\mathrm{ns}\,2^k)$) under the projection $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is $G(\mathrm{s}\,2)$ (respectively $G(\mathrm{ns}\,2)$). Since $G(\mathrm{s}\,2) \subset G(\mathrm{ns}\,2)$, if $\bar{\rho}_{E,2^k}(G_K)$ is contained in either $G(\mathrm{s}\,2^k)$ or $G(\mathrm{ns}\,2^k)$ the discriminant, Δ, is a square in K. The claim follows immediately from Lemma 2.2.12 and Lemma 4.1.1 by taking g to be either g_{s} or $g_{\mathrm{ns}} \in \mathrm{GL}_2(\mathbb{Z}/2^{k+1}\mathbb{Z})$ (as defined in Section 2.2.7). □

Now suppose $K = \mathbb{Q}$. We wish to give a classification of quadratic twist-type $(2^k, r)$-congruences of elliptic curves over $\mathbb{Q}$ in terms of the image of their mod 2^k Galois representations, mimicking that given by Proposition 4.1.4 in the case of odd prime powers.

By analysing rational points on modular curves of level 2^k, Rouse and Zureick-Brown [RZ15a] have classified all possible images of the 2-adic Galois representations attached to elliptic curves $E/\mathbb{Q}$ without CM. Specifically Rouse and Zureick-Brown determine a list of 1208 open subgroups $G_i \subset \mathrm{GL}_2(\mathbb{Z}_2)$ for which there exists an elliptic curve $E/\mathbb{Q}$ without CM such that the image of the 2-adic Galois representation, $\rho_{E,2}(G_{\mathbb{Q}})$, is conjugate to G_i.

It will be more convenient for us to refer to subgroups of $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ than to their inverse images in $\mathrm{GL}_2(\mathbb{Z}_2)$ and in Table 4.1 we introduce 11 subgroups of $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ which give rise to *all* quadratic twist-type $(2^k, r)$-congruences of non-CM elliptic curves over $\mathbb{Q}$. The labelling we use for these subgroups corresponds to that of Rouse and Zureick-Brown in the following way: a subgroup $G_i \subset \mathrm{GL}_2(\mathbb{Z}_2)$ labelled by Rouse–Zureick-Brown is equal to the inverse image under the projection $\mathrm{GL}_2(\mathbb{Z}_2) \to \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ of the subgroup we label G_i.

It will often be convenient for us to refer to such an index 2 subgroup $H \subset H^+ = \bar{\rho}_{E,2^k}(G_K)$ in terms of H^+ and E. We therefore define the following notation. Let $d \in K^\times$ be such that $K(\sqrt{d})/K$ is the quadratic extension cut out by $\bar{\rho}^{-1}_{E,2^k}(H)$. Then we denote H by $H^+(\sqrt{d})$ (note that d may depend on E).

[1] Recall from Section 2.2.5 that $G(\mathrm{s}\,2^{k^+})$ is defined to be the subgroup generated by $G(\mathrm{s}\,2^k)$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ *not* as the normaliser of $G(\mathrm{s}\,2^k)$ in $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$.

Since Lemma 4.1.1 is stated purely in terms of the mod N Galois representation of an elliptic curve, the classification of Rouse and Zureick-Brown allows us to give a complete description of *non-CM* elliptic curves defined over $\mathbb{Q}$ admitting a $(2^k, r)$-congruence of quadratic twist-type.

In particular we have:

Proposition 4.1.6. *Let $E/\mathbb{Q}$ be an elliptic curve without CM and let $k \geq 2$ be an integer. Then E is $(2^k, r)$-congruent to a non-trivial quadratic twist E^d if and only if there exists a choice of basis for $E[2^k]$ such that the image of the mod 2^k Galois representation, $\bar{\rho}_{E,2^k}(G_{\mathbb{Q}})$, is contained in one of the subgroups $H^+ \subset \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ listed in Table 4.1, but not the corresponding subgroup H, and $\bar{\rho}_{E,2^k}(G_{\mathbb{Q}(\sqrt{d})}) = \bar{\rho}_{E,2^k}(G_{\mathbb{Q}}) \cap H$.*

$(2^k, r)$	The subgroup H^+ of $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$			The index 2 subgroup $H \subset H^+$		Quadratic Twist
	Generators	Index	Label	Generators	Label	
$(4,1)$	$\left\{\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}3&0\\2&1\end{smallmatrix}\right)\right\}$	6	G_9	$\left\{\left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\right\}$	$G_9(\sqrt{-1})$	-1
	$\left\{\left(\begin{smallmatrix}1&0\\2&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}3&1\\2&1\end{smallmatrix}\right)\right\}$	6	G_{11}	$\left\{\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&3\\2&3\end{smallmatrix}\right)\right\}$	$G_{11}(\sqrt{-1})$	-1
$(4,3)$	$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$	1	G_1	$\pi_2^{-1}G(\mathrm{ns}\,2)$	–	$\Delta(E)$
	$\left\{\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}3&0\\2&1\end{smallmatrix}\right)\right\}$	6	G_9	$\left\{\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\2&1\end{smallmatrix}\right)\right\}$	$G_9(\sqrt{-\Delta})$	$-\Delta(E)$
	$\left\{\left(\begin{smallmatrix}1&0\\2&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}3&1\\2&1\end{smallmatrix}\right)\right\}$	6	G_{11}	$\left\{\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}3&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}3&0\\0&3\end{smallmatrix}\right)\right\}$	$G_{11}(\sqrt{-\Delta})$	$-\Delta(E)$
$(8,1)$	$\left\{\left(\begin{smallmatrix}1&3\\0&7\end{smallmatrix}\right), \left(\begin{smallmatrix}1&3\\2&7\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\6&3\end{smallmatrix}\right)\right\}$	24	G_{97}	$\left\{\left(\begin{smallmatrix}3&4\\0&3\end{smallmatrix}\right), \left(\begin{smallmatrix}5&6\\4&1\end{smallmatrix}\right), \left(\begin{smallmatrix}5&1\\6&7\end{smallmatrix}\right)\right\}$	$G_{97}(\sqrt{-1})$	-1
$(8,3)$	$\pi_4^{-1}G(\mathrm{ns}\,4^+)$	4	G_7	$\pi_4^{-1}G(\mathrm{ns}\,4)$	–	$\Delta(E)$
	$\left\{\left(\begin{smallmatrix}1&3\\6&7\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\4&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2\\0&5\end{smallmatrix}\right)\right\}$	24	G_{90}	$\left\{\left(\begin{smallmatrix}3&4\\0&3\end{smallmatrix}\right), \left(\begin{smallmatrix}3&3\\4&1\end{smallmatrix}\right), \left(\begin{smallmatrix}5&6\\0&1\end{smallmatrix}\right)\right\}$	$G_{90}(\sqrt{-\Delta})$	$-\Delta(E)$
$(8,5)$	$\left\{\left(\begin{smallmatrix}1&2\\2&7\end{smallmatrix}\right), \left(\begin{smallmatrix}1&3\\2&7\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\6&3\end{smallmatrix}\right)\right\}$	24	G_{63}	$\left\{\left(\begin{smallmatrix}3&4\\0&3\end{smallmatrix}\right), \left(\begin{smallmatrix}5&6\\4&1\end{smallmatrix}\right), \left(\begin{smallmatrix}5&1\\6&7\end{smallmatrix}\right)\right\}$	$G_{63}(\sqrt{-1})$	-1
$(8,7)$	$\pi_4^{-1}G(\mathrm{s}\,4^+)$	12	G_{23}	$\pi_4^{-1}G(\mathrm{s}\,4)$	–	$\Delta(E)$
	$\left\{\left(\begin{smallmatrix}1&3\\0&7\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\2&7\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2\\0&5\end{smallmatrix}\right)\right\}$	24	G_{91}	$\left\{\left(\begin{smallmatrix}3&4\\0&3\end{smallmatrix}\right), \left(\begin{smallmatrix}1&7\\0&7\end{smallmatrix}\right), \left(\begin{smallmatrix}7&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}5&6\\0&1\end{smallmatrix}\right)\right\}$	$G_{91}(\sqrt{-\Delta})$	$-\Delta(E)$
$(16,3)$	$\pi_8^{-1}G(\mathrm{ns}\,8^+)$	16	G_{55}	$\pi_8^{-1}G(\mathrm{ns}\,8)$	–	$\Delta(E)$
$(32,3)$	$\pi_{16}^{-1}G(\mathrm{ns}\,16^+)$	64	G_{441}	$\pi_{16}^{-1}G(\mathrm{ns}\,16)$	–	$\Delta(E)$

TABLE 4.1: Subgroups of $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ which give rise to quadratic twist-type $(2^k, r)$-congruences over $\mathbb{Q}$. Here π_{2^k} denotes the natural reduction map $\mathrm{GL}_2(\mathbb{Z}/2^{k+1}\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$. The modular curves $X(H^+)$ all have genus 0 except $X(\mathrm{ns}\,16^+)$ which has genus 2.

Proof. This is a brute force calculation in `Magma` using the classification of Rouse and Zureick-Brown [RZ15a] and Lemma 4.1.1. □

Example 4.1.7 (A 32-Congruence)**.** Heegner [Hee52], Baran [Bar10] and Rouse–Zureick-Brown [RZ15a] determined the rational points on the genus 2 curve $X(\mathrm{ns}\,16^+)$ (see [RZ15a, Remark 1.5] for a discussion). There are *exactly* two non-CM j-invariants for which there are rational points in the fibre of $X(\mathrm{ns}\,16^+) \to X(1)$ above j, namely:

$$\frac{-2^{18} \cdot 3 \cdot 5^3 \cdot 13^3 \cdot 41^3 \cdot 107^3}{17^{16}} \quad \text{and} \quad \frac{-2^{21} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13^3 \cdot 23^3 \cdot 41^3 \cdot 179^3 \cdot 409^3}{79^{16}}.$$

The elliptic curves $E_{(32,3)a}/\mathbb{Q}$ and $E_{(32,3)b}/\mathbb{Q}$ from the statement of Theorem 1.0.16 are the minimal twists with the j-invariants above. By Proposition 4.1.5 the elliptic curves $E_{(32,3)a}$ and $E_{(32,3)b}$ admit $(32,3)$-congruences with their quadratic twists by their discriminants. In fact, these are the only j-invariants of elliptic curves admitting non-trivial quadratic twist-type 32-congruences over $\mathbb{Q}$ (see Proposition 4.2.4).

4.2 Trivial quadratic twist-type congruences and CM

Let p be an odd prime and let $l \geq 1$ be an integer. Recall that if $E/\mathbb{Q}$ has CM by an imaginary quadratic order $\mathcal{O}$ of discriminant $-D$ and p is unramified in $\mathcal{O}$ then $\bar{\rho}_{E,p^l}(G_{\mathbb{Q}})$ is contained in the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ and the inverse image of the corresponding Cartan subgroup is $G_{\mathbb{Q}(\sqrt{-D})}$. Moreover the Cartan subgroup is non-split if and only if p is inert in $\mathbb{Q}(\sqrt{-D})$ (see [Ser97, A.5] or [Bar10, Proposition 4.1]). It then follows from Proposition 4.1.4 that CM elliptic curves admit quadratic twist-type p^l-congruences for all odd prime numbers p unramified in the CM field. In fact, quadratic twist-type congruences are trivial if and only if they arise in this way:

Lemma 4.2.1. *An elliptic curve $E/\mathbb{Q}$ admits an isogeny with a non-trivial quadratic twist if and only if E has CM. More precisely if E has CM by an imaginary quadratic order, $\mathcal{O}$, of discriminant $-D$ then E is D-isogenous to its quadratic twist by $-D$. Moreover if 4 divides D then we may take the isogeny to have degree $D/4$.*

Proof. Suppose that an elliptic curve $E/\mathbb{Q}$ admits an isogeny with a non-trivial quadratic twist $E^d/\mathbb{Q}$ (where $d \in \mathbb{Z}$ is possibly positive). Composing the isogeny with the $\mathbb{Q}(\sqrt{d})$-isomorphism $E^d \to E$ gives rise to an endomorphism of E defined over $\mathbb{Q}(\sqrt{d})$ but not over $\mathbb{Q}$ (hence is not multiplication by m). Thus E has CM by an order in $\mathbb{Q}(\sqrt{d})$ (by [Sil09, Theorem VI.6.1(b)]).

Conversely, if 4 divides D (i.e., if $-D \in \{-4, -8, -12, -16, -28\}$) let $D' = D/4$ and let $D' = D$ otherwise. Note that $\sqrt{-D'} \in \mathcal{O}$. Composing the $\mathbb{Q}(\sqrt{-D'})$-isomorphism $E \to E^{-D'}$ with the endomorphism $\sqrt{-D'}$ gives an isogeny $E \to E^{-D'}$ defined over $\mathbb{Q}$. The degree of the isogeny is D', since the endomorphism $\sqrt{-D'}$ has degree D'. □

It is, however, possible that a CM elliptic curve $E/\mathbb{Q}$ may admit an N-congruence with a quadratic twist E^d which is not isomorphic to E^{-D}. For later discussions (in particular when we give evidence for Conjecture 1.0.17) it will be convenient to avoid CM elliptic curves since, for example, they do not satisfy Serre's open image theorem.

We use the classification of images of the mod p Galois representation for CM elliptic curves $E/\mathbb{Q}$ (see [Zyw15a, Propositions 1.14–1.16]) and Lemma 4.1.1 to classify non-trivial quadratic twist-type p-congruences between elliptic curves with CM (this is similar to the arguments of Cremona–Freitas [CF22, Theorem 2.4 and Corollary 2.5]). We will also need to consider 2^k-congruences. The image of the adelic Galois representation attached to a CM elliptic curve $E/\mathbb{Q}$ has been considered in [LR22] and [DLM23, Section 5] and it would be interesting to complete the proof using these results. We find it easiest to argue using the curves $X_E^r(2^k)$ defined in Section 2.2.9.

Proposition 4.2.2. *Let $N > 2$ be an integer and let $E/\mathbb{Q}$ be an elliptic curve with CM by an imaginary quadratic order of discriminant $-D$.*

Let $d \in \mathbb{Z}$ be squarefree and suppose that $d \neq 1$ and $d \neq -1$ if $j(E) = 1728$ (i.e., suppose that E is not isomorphic to E^d over $\mathbb{Q}$). Then E is (N, r)-congruent to E^d if and only if either

(i) *d is equal to $-D$ up to a square factor (i.e., the congruence is trivial), or*

(ii) *E is isomorphic to a quadratic twist of one of the elliptic curves appearing in Table 4.2 and d and (N, r) appear in the corresponding row.*

In particular no CM elliptic curve $E/\mathbb{Q}$ admits a non-trivial quadratic twist-type (N, r)-congruence when $N > 8$ and $N \neq 10, 14$.

$-D$	Weierstrass equation for E	d	(N, r)
-3	$y^2 = x^3 + 1$	-1	$(4, 1)$
		3	$(4, 3)$
	$y^2 = x^3 + 10$	5	$(10, 1)$
		-15	$(10, 2)$
	$y^2 = x^3 + 98$	21	$(14, 1)$
		-7	$(14, 3)$
-4	$y^2 = x^3 + ax$	a	$(4, 3)$
	$y^2 = x^3 + 2x$	2	$(8, 3)$
	$y^2 = x^3 - 2x$	2	$(8, 7)$
-7	$y^2 + xy = x^3 - x^2 - 2x - 1$	-1	$(4, 1)$
		7	$(4, 3)$
-8	$y^2 = x^3 + 4x^2 + 2x$	-3	$(6, 1)$
		6	$(6, 5)$
		2	$(4, 3)$
-11	$y^2 + y = x^3 - x - 7x + 10$	-3	$(6, 1)$
		33	$(6, 5)$
-12	$y^2 = x^3 - 15x + 22$	-1	$(4, 1)$
		3	$(4, 3)$
-16	$y^2 = x^3 - 11x + 14$	2	$(4, 3)$
-28	$y^2 = x^3 - 595x + 5586$	-1	$(4, 1)$
		7	$(4, 3)$

TABLE 4.2: All pairs (E, d) where $E/\mathbb{Q}$ is an elliptic curve (defined up to quadratic twist) with CM by an imaginary quadratic order of discriminant $-D$ such that E is non-trivially (N, r)-congruent with its quadratic twist by d.

Proof. It will suffice to consider the cases when $N = p$ is an odd prime and $N = 2^k$ for $k \geq 2$.

Let p be an odd prime. By Proposition 4.1.4 and [Lan76, Theorem XI.2.3] if E is p-congruent to a non-trivial quadratic twist E^d, then the image, $\mathbb{P}\bar{\rho}_{E,p}(G_{\mathbb{Q}})$, of $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$ in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is dihedral and $\mathbb{P}\bar{\rho}_{E,p}(G_{\mathbb{Q}(\sqrt{d})})$ is a cyclic subgroup of index 2. In particular if $\mathbb{P}\bar{\rho}_{E,p}(G_{\mathbb{Q}})$ is dihedral of order > 4 then it contains a unique cyclic subgroup of index 2, in which case E is p-congruent to a unique quadratic twist.

Suppose that $j(E) \neq 0$. By [Zyw15a, Proposition 1.14] for each odd prime p not dividing D we have that $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$ is *equal* to the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ (which is split if and only if $-D$ is a quadratic residue modulo p) and $\bar{\rho}_{E,p}(G_{\mathbb{Q}(\sqrt{-D})})$ is the corresponding Cartan subgroup. Therefore unless $p = 3$ and $-D \equiv 1 \pmod 3$ the image of $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$ in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is dihedral of order > 4 hence E is p-congruent to exactly one quadratic twist, namely E^{-D}, except when $D = 8$ or 11 and $p = 3$.

When $D = 8$ or 11 the image of the mod 3 Galois representation, $\bar{\rho}_{E,3}(G_{\mathbb{Q}})$, is equal to the normaliser of a split Cartan subgroup and has exactly 3 distinct index 2 subgroups satisfying Lemma 4.1.1. In particular E is non-trivially $(3, 1)$-congruent to its quadratic twist by -3 and

$(3,2)$-congruent to its quadratic twist by $3D$ (and no other quadratic twists). For both $D = 8$ and 11 the traces of Frobenius at $\ell = 17$ of E, E^{-3}, and E^{-3D} are not congruent modulo 9. Since the traces of Frobenius of N-congruent elliptic curves at good primes are congruent modulo N, none of these 3-congruences are 9-congruences.

If p divides D then by [Zyw15a, Proposition 1.14(iii)] $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$ in not contained in the normaliser of a Cartan subgroup, so by Proposition 4.1.4 E is not p-congruent to a non-trivial quadratic twist.

Now suppose that $j(E) = 0$. Let $p \geq 5$ be a prime number. If $p = 5$ suppose that E is not isomorphic to a quadratic twist of the elliptic curve $y^2 = x^3 + 10$ and if $p = 7$ suppose that E is not isomorphic to a quadratic twist of the elliptic curve $y^2 = x^3 + 98$. It follows from [Zyw15a, Proposition 1.16(i)–(iv)] that the image of $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$ in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is dihedral of order > 4 hence E is p-congruent to a unique quadratic twist – namely its 3-isogenous quadratic twist E^{-3}.

In the remaining two cases the image of the mod p Galois representation, $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$, (described in [Zyw15a, Proposition 1.16(ii)–(iii)]) contains exactly three index 2 subgroups, H, satisfying the conditions of Lemma 4.1.1. In particular the elliptic curve with Weierstrass equation $y^2 = x^3 + 10$ is $(5,1)$-congruent with its quadratic twist by 5 and $(5,2)$-congruent with its quadratic twist by -15. Similarly the elliptic curve with Weierstrass equation $y^2 = x^3 + 98$ is $(7,3)$-congruent with its quadratic twist by -7 and $(7,1)$-congruent with its quadratic twist by 21. In each of these cases by comparing traces of Frobenius at $\ell = 13$ we see that these p-congruences are not p^2-congruences.

By [Zyw15a, Proposition 1.16(v)] and Proposition 4.1.4 if an elliptic curve E with j-invariant 0 is 3-congruent to a non-trivial quadratic twist, then $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$ is contained in a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and E is isomorphic to a quadratic twist of the elliptic curve with Weierstrass equation $y^2 = x^3 + 2$. In this case E is both $(3,1)$ and $(3,2)$-congruent with its 3-isogenous quadratic twist E^{-3}.

We now determine the non-trivial quadratic twist-type 2^k-congruences between CM elliptic curves $E/\mathbb{Q}$ where $k \geq 2$ using the curves $X_E^r(2^k)$. Silverberg [Sil97] and Fisher [Fis12] computed equations for $X_E^r(4)$ and Z. Chen [Che18] computed equations for $X_E^r(8)$.

When $j(E) \notin \{0, 1728\}$ we may take simultaneous quadratic twists of E and E^d so that E is given by the corresponding Weierstrass equation in [Sil94, A.3]. Similarly when $j(E) = 1728$ (i.e., $-D = -4$) we may assume that E is given by the Weierstrass equation $y^2 = x^3 + ax$ where $a \in \mathbb{Z}$ is squarefree, and when $j(E) = 0$ (i.e., $-D = -3$) we may assume that E is given by the Weierstrass equation $y^2 = x^3 + a$ where $a \in \mathbb{Z}$ is cubefree and $a > 0$.

In each case, by determining the rational points in the fibres of the maps $X_E^r(4) \to X(1)$ above $j(E)$ we see that the only non-trivial quadratic twist-type $(4,r)$-congruences between CM elliptic curves are those appearing in Table 4.2. For each such rational point $P \in X_E^r(4)(\mathbb{Q})$ giving rise to a non-trivial quadratic twist-type $(4,r)$-congruence we compute the rational points in the fibre of the forgetful map $X_E^{r'}(8) \to X_E^r(4)$ above P for each $r' \equiv r \pmod 4$. We conclude that the only non-trivial quadratic twist-type $(8,r')$-congruences between CM elliptic curves are those in Table 4.2 (i.e., where E is a quadratic twist of one of the elliptic curves $y^2 = x^3 \pm 2x$). In both of these cases comparing traces of Frobenius at $\ell = 29$ shows that the congruence is not a 16-congruence.

We illustrate this calculation in the case where $j(E) = 0$ and $r = 1$. The other cases are verified in `Magma` (for details see [Fre23b, `qtt-congruences/verify/2-2-prop.m`]). Let E be given by the Weierstrass equation $y^2 = x^3 + a$ where $a \in \mathbb{Z}$ is cubefree and $a > 0$. From Fisher's equations for $X_E^1(4) \cong \mathbb{P}^1$ [Fis12] an elliptic curve is $(4,1)$-congruent to E if and only if it is isomorphic to an

elliptic curve with Weierstrass equation

$$y^2 = x^3 + 36ast(27s^3 - 8at^3)(27s^3 + at^3)x + a(729s^6 + 8a^2t^6)(729s^6 - 2376as^3t^3 - 8a^2t^6)$$

for some point $(s : t) \in \mathbb{P}^1(\mathbb{Q})$.

If $a \neq 1$ the only rational points in the fibre of the j-map $X_E^1(4) \to X(1)$ above 0 (i.e., where $st(27s^3 - 8at^3)(27s^3 + at^3) = 0$) are the points $(1 : 0)$ and $(0 : 1)$. The congruent elliptic curves corresponding to these points are E itself and the elliptic curve with Weierstrass equation $y^2 = x^3 - a^5$ respectively. Note that the elliptic curve given by the Weierstrass equation $y^2 = x^3 - a^5$ is not a quadratic twist of E when $a \neq 1$. Hence E does not admit any quadratic twist-type $(4, 1)$-congruences.

Now suppose that $a = 1$. The rational points in the fibre of the map $X_E^1(4) \to X(1)$ above 0 are the points $(1 : 0)$, $(-1 : 3)$, $(0 : 1)$, and $(2 : 3)$. The first two points correspond to E itself and the last two correspond to the quadratic twist of E by -1.

The elliptic curve $E : y^2 = x^3 + 1$ is $(8, 1)$-congruent to its quadratic twist by -1 if and only if there exists a rational point on the curve $X_E^1(8)$ which maps to either $(0 : 1)$ or $(2 : 3)$ on $X_E^1(4)$. By [Che18, Theorem 1.1] the curve $X_E^1(8)$ is isomorphic over $\mathbb{Q}$ to the curve in $\mathbb{P}^4$ given by the equations

$$\begin{aligned} 2x_1x_3 + x_2^2 + 2x_4^2 &= 0, \\ x_3^2 - 2x_1x_2 - 2x_0x_4 &= 0, \\ 2x_2x_3 - x_1^2 + x_0^2 &= 0, \end{aligned}$$

and with the forgetful map $X_E^1(8) \to X_E^1(4)$ given by $(x_0 : x_1 : x_2 : x_3 : x_4) \mapsto (x_0 : 3x_4)$. From these equations it is simple to check that there exist no rational points in the fibre of the map $X_E^1(8) \to X_E^1(4)$ above the points $(0 : 1)$ and $(2 : 3)$.

Therefore for each $k \geq 2$ the only non-trivial quadratic twist-type $(2^k, 1)$-congruences between elliptic curves of j-invariant 0 are those recorded in Table 4.2.

In the general case, write $N = p_1^{l_1}...p_n^{l_n}$ as a product of prime powers, where the primes p_i are distinct. The claim follows immediately since an N-congruence between E and a quadratic twist E^d gives rise to a $p_i^{l_i}$-congruence between E and E^d for each $i = 1, ..., n$. □

Remark 4.2.3. We proved in Proposition 4.2.2 that the elliptic curve E with Weierstrass equation $y^2 = x^3 + 2$ is 3-congruent and 3-isogenous to E^{-3}. This congruence does not arise from the restriction of the isogeny to the 3-torsion. By considering the p-adic images of the Galois representation attached to CM elliptic curves, it may be possible to classify the N-congruences between a (CM) elliptic curve and its isogenous quadratic twist which do not arise from the restriction of an isogeny. We do not pursue this.

Combining Proposition 4.2.2 with the results of Section 4.1 we deduce the case of Theorem 1.0.15 when N is a prime power. For an odd prime p let ξ be a quadratic non-residue modulo p.

Proposition 4.2.4. *Let p be a prime number and $l \geq 1$ be an integer. Let $\mathcal{S}$ be the set defined in Theorem 1.0.15. Then there are infinitely many j-invariants of elliptic curves $E/\mathbb{Q}$ admitting non-trivial quadratic twist-type (p^l, r)-congruences (hence $(2p^l, r)$-congruences if p is odd) if and only if $(p^l, r) \in \mathcal{S}$.*

Furthermore, suppose that $(p^l, r) \notin \mathcal{S}$ and $E/\mathbb{Q}$ is an elliptic curve admitting a non-trivial quadratic twist-type (p^l, r)-congruence. Then either E is a quadratic twist of $E_{(32,3)a}$ or $E_{(32,3)b}$

(see Theorem 1.0.16) and $(p^l, r) = (32, 3)$*, or* $p^l \geq 19$ *is odd,* $r = -\xi$ *and* $j(E)$ *is an exceptional* j*-invariant for* $X(\mathrm{ns}\, p^{l+})$.

Proof. When p is odd and $p^l \geq 13$ the modular curve $X(\mathrm{ns}\, p^{l+})$ has genus ≥ 2 (see [Bar10, Section 5] or Corollary 3.4.2). Hence by Faltings' Theorem and Proposition 4.1.4, when $p^l \geq 13$ there are at most finitely many j-invariants of elliptic curves $E/\mathbb{Q}$ admitting a quadratic twist-type $(p^l, -\xi)$-congruence.

By [BPR13, Theorem 1.1], [RSZ22], and [BDM$^+$19] there are no exceptional points on $X(\mathrm{s}\, p^{l+})$ for $p^l \geq 9$. Moreover it is shown in [BDM$^+$19] and [BDM$^+$23] that $X(\mathrm{ns}\, 13^+)$ and $X(\mathrm{ns}\, 17^+)$ have no exceptional points. Therefore by Propositions 4.1.4 and 4.2.2 there are no elliptic curves $E/\mathbb{Q}$ admitting a non-trivial quadratic twist-type $(9, 2)$, $(11, 2)$, $(13, 1)$, $(13, 2)$, $(17, 1)$, $(17, 3)$, or $(p^l, -1)$-congruence where $p^l \geq 19$. Moreover, if $E/\mathbb{Q}$ admits a non-trivial quadratic twist-type $(p^l, -\xi)$-congruence with $p^l \geq 19$ then there exists an exceptional point in the fibre of the j-map $X(\mathrm{ns}\, p^{l+}) \to X(1)$ above $j(E)$.

Similarly suppose that $p = 2$ and $(p^l, r) \notin \mathcal{S}$. Recall that the only exceptional points on $X(\mathrm{ns}\, 16^+)$ have j-invariants equal to $j(E_{(32,3)a})$ or $j(E_{(32,3)b})$ (this is due to Rouse and Zureick-Brown [RZ15a], see the discussion in Example 4.1.7). By Propositions 4.1.6 and 4.2.2 if $E/\mathbb{Q}$ admits a non-trivial quadratic twist-type (p^l, r)-congruence then E is a quadratic twist of either $E_{(32,3)a}$ or $E_{(32,3)b}$ and $(p^l, r) = (32, 3)$.

Conversely suppose that $(p^l, r) \in \mathcal{S}$. By Propositions 4.1.4 and 4.1.6 there exists a subgroup $H^+ \subset \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ and $d \in \mathbb{Q}(X(H^+))$ such that for each rational point $P \in X(H^+)$ (except possibly for the finitely many zeroes and poles of d and points above $j = \infty, 0, 1728$) an elliptic $E_P/\mathbb{Q}$ with j-invariant $j(P)$ is (p^l, r)-congruent to its quadratic twist by $d(P) \in \mathbb{Q}^\times$.

Note that exactly one of the following holds:

(i) the fibre of the degree 2 map $X(H) \to X(H^+)$ above P has a $\mathbb{Q}$-rational point (equivalently $d(P)$ is a square),

(ii) the curve E_P is isogenous over $\mathbb{Q}$ to $E_P^{d(P)}$,

(iii) the curve E_P admits a non-trivial quadratic twist-type (p^l, r)-congruence with $E_P^{d(P)}$.

When $p = 2$ Rouse and Zureick-Brown [RZ15a] showed that each of the modular curves $X(H^+)$ (i.e., those corresponding to subgroups listed in Table 4.1, except $X(\mathrm{ns}\, 16^+)$) are isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1$. When p is odd each of the modular curves $X(H^+)$ are isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1$, except $X(\mathrm{ns}\, 11^+)$ which is an elliptic curve of rank 1 (see e.g., [SZ17]).

When the curve $X(H^+)$ is isomorphic to $\mathbb{P}^1$ Hilbert's Irreducibility Theorem (see [Ser97, Chapter 9]) implies that there are infinitely many rational points $P \in X(H^+)(\mathbb{Q})$ such that case (i) does not occur. The modular curve $X(\mathrm{ns}\, 11)$ has genus 4 – so case (i) occurs for at most finitely many rational points $P \in X(\mathrm{ns}\, 11^+)(\mathbb{Q})$ by Faltings' Theorem.

By Lemma 4.2.1 case (ii) may only occur if E_P has CM. But there are only finitely many j-invariants of elliptic curves over $\mathbb{Q}$ with CM, so (ii) occurs for finitely many rational points $P \in X(H^+)$.

Thus (iii) holds for infinitely many rational points $P \in X(H^+)$. Since $X(H^+) \to X(1)$ has finite degree these correspond to infinitely many j-invariants, as required. □

4.3 Double covers of modular curves and composite level quadratic twist-type congruences

Let p_1 and p_2 be distinct odd primes and let $l_1, l_2 \geq 1$ be integers. We wish to construct elliptic curves admitting quadratic twist-type $p_1^{l_1}p_2^{l_2}$-congruences over $\mathbb{Q}$.

It is natural to consider the modular curve $X(H_1^+, H_2^+)$, where $H_1^+ \subset \mathrm{GL}_2(\mathbb{Z}/p_1^{l_1}\mathbb{Z})$ and $H_2^+ \subset \mathrm{GL}_2(\mathbb{Z}/p_2^{l_2}\mathbb{Z})$ are the normalisers of Cartan subgroups. A noncuspidal point $P \in X(H_1^+, H_2^+)(K)$ gives rise to an elliptic curve E/K admitting quadratic twist-type $p_1^{l_1}$ and $p_2^{l_2}$-congruences by Proposition 4.1.4. However these congruences may be with non-isomorphic quadratic twists. We therefore consider a double cover of $X(H_1^+, H_2^+)$, which corresponds to requiring that the quadratic twists are indeed isomorphic. We make this formal in the following way:

Let $N_1, N_2 > 2$ be coprime integers. Let $H_1^+ \subset \mathrm{GL}_2(\mathbb{Z}/N_1\mathbb{Z})$ and $H_2^+ \subset \mathrm{GL}_2(\mathbb{Z}/N_2\mathbb{Z})$ be subgroups, and suppose that there exist index 2 subgroups $H_i \subset H_i^+$ and $g_i \in \mathrm{GL}_2(\mathbb{Z}/N_i\mathbb{Z})$ satisfying the conditions of Lemma 4.1.1.

Let ι_1 and ι_2 be the involutions giving the quotients $X(H_1) \to X(H_1^+)$ and $X(H_2) \to X(H_2^+)$. Note that while the involutions ι_i depend upon the groups H_i^+ containing H_i, in all the cases we consider, the subgroup H^+ is implicit in the notation for H. More precisely, if p is a prime number and H is a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$, then H^+ will be its normaliser. When $H^+ \subset \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ is one of the subgroups listed in Table 4.1 we write $H = H^+(\sqrt{d})$.

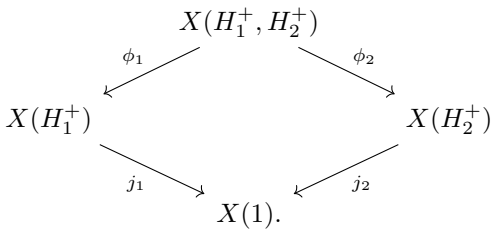
Let $j_1 \colon X(H_1^+) \to X(1)$ and $j_2 \colon X(H_2^+) \to X(1)$ be the j-invariant maps. Let $\mathcal{E}_1/\mathbb{Q}(X(H_1^+))$ and $\mathcal{E}_2/\mathbb{Q}(X(H_2^+))$ be elliptic curves with j-invariants j_1 and j_2 respectively. By Lemma 4.1.1, there exist rational functions $d_1 \in \mathbb{Q}(X(H_1^+))^\times$ and $d_2 \in \mathbb{Q}(X(H_2^+))^\times$ (depending on the index 2 subgroup H_i) such that $\mathcal{E}_i$ is N_i-congruent to its quadratic twist $\mathcal{E}_i^{d_i}$.

Remark 4.3.1. Let $F = \mathbb{Q}(X(H^+))$. For the computations in Sections 4.4 and 4.5 it will be necessary to explicitly compute these rational functions $d \in F^\times$ when $H^+ \subset \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is the normaliser of a Cartan subgroup and p is an odd prime number.

Suppose that E/K is an elliptic curve admitting (p, r)-congruence with its quadratic twist by $d \in K^\times$. Then for $p \in \{3, 5, 7, 11\}$ we can find d from the equations for $X_E^r(p)$ by computing K-rational points on the fibre of the j-map $X_E^r(p) \to X(1)$ above $j(E)$ (equations for $X_E^r(p)$ and its j-invariant maps may be found in [RS95] and [Fis12] when $p = 3, 5$ and in [HK03], [PSS07], and [Fis14] when $p = 7$ and [Fis14] when $p = 11$).

However, since the genus of $X_E^r(p)$ grows quickly with p it will instead be more convenient to note that by Proposition 4.1.4, $d \in F^\times/(F^\times)^2$ is the unique element such that the degree 2 extension $\mathbb{Q}(X(H))/F$ is given by adjoining $\sqrt{d}$ to F.

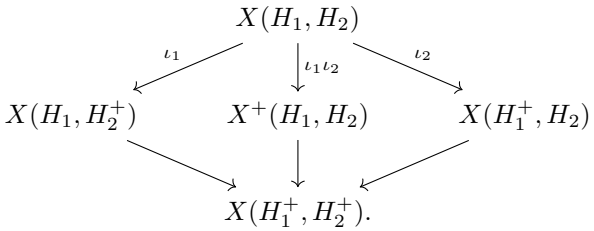
We have the natural projections from $X(H_1^+, H_2^+)$, which give the commutative diagram



We define $\psi \colon \mathcal{C} \to X(H_1^+, H_2^+)$ to be the double cover such that the corresponding extension of function fields is given by adjoining $\sqrt{\phi_1^*(d_1)\phi_2^*(d_2)}$ to the function field $\mathbb{Q}(X(H_1^+, H_2^+))$ (note

that $\mathcal{C}$ depends on the subgroups H_1 and H_2). Let $j\colon \mathcal{C} \to X(1)$ be the j-invariant map, and let $\mathcal{E}/\mathbb{Q}(\mathcal{C})$ be an elliptic curve with j-invariant j. Then $\mathcal{E}$ is N_1-congruent to its quadratic twist by $(\phi_1 \circ \psi)^*(d_1)$ and N_2-congruent to its quadratic twist by $(\phi_2 \circ \psi)^*(d_2)$. But $(\phi_1 \circ \psi)^*(d_1)$ and $(\phi_2 \circ \psi)^*(d_2)$ are equal up to a square factor, so $\mathcal{E}$ is N_1N_2-congruent to its quadratic twist by $(\phi_1 \circ \psi)^*(d_1)$.

Remark 4.3.2. Note that the curve $\mathcal{C}$ is modular. The involutions ι_1 and ι_2 induce quotients $X(H_1, H_2) \to X(H_1^+, H_2)$ and $X(H_1, H_2) \to X(H_1, H_2^+)$. Then the quotient $X^+(H_1, H_2) = X(H_1, H_2)/(\iota_1\iota_2)$ is isomorphic to $\mathcal{C}$. That is, we have a commutative diagram



Remark 4.3.3. When the integers N_i are prime powers and the subgroups $H_i \subset \mathrm{GL}_2(\mathbb{Z}/N_i\mathbb{Z})$ are Cartan subgroups the modular curve $X^+(H_1, H_2)$ is the modular curve associated to the *extended Cartan subgroup* of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (for further discussion on these modular curves, see Lemma 2.2.13 and Remark 2.2.14). More generally, if $H_i = H_{g_i}$ and $H_i^+ = H_{g_i}^+$ for some $g_i \in \mathrm{GL}_2(\mathbb{Z}/N_i\mathbb{Z})$, then the modular curve $X^+(H_1, H_2)$ is isomorphic to the modular curve X_g^+ defined in Section 2.2.7, where $g = (g_1, g_2) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

The following lemma is very closely related to Proposition 2.2.11 but also allows us to identify when a point on $X^+(H_1, H_2)$ does not correspond to a quadratic twist-type congruence (i.e., when the quadratic twist in question is trivial).

Lemma 4.3.4. *Let $P \in X^+(H_1, H_2)$ be a non-cuspidal K-rational point. Let $\mathcal{E}_P$ be the specialisation of $\mathcal{E}$ at the point P and suppose that $j(\mathcal{E}_P) \neq 0, 1728$. Then exactly one of the following holds:*

(i) *the fibre of the degree 2 map $X(H_1, H_2) \to X^+(H_1, H_2)$ above P has a K-rational point,*

(ii) *the elliptic curve $\mathcal{E}_P$ admits a quadratic twist-type N_1N_2-congruence.*

Conversely, suppose that E/K is N_1N_2-congruent to a non-trivial quadratic twist by $d \in K^\times$ and $j(E) \neq 0, 1728$. For each $i = 1, 2$ let $H_i^+ = \bar{\rho}_{E,N_i}(G_K)$ and let $H_i = \bar{\rho}_{E,N_i}(G_{K(\sqrt{d})})$. Then there exists a K-rational point in the fibre of the map $X^+(H_1, H_2) \to X(1)$ above $j(E)$ which does not lift to a K-rational point on $X(H_1, H_2)$.

Proof. From Lemma 2.2.7 and the preceding discussion (and by specialising) we see that $\mathcal{E}_P$ is N_1N_2-congruent to its quadratic twist by $(\phi_1 \circ \psi)^*(d_1)(P)$. Recall that by convention we say that $\mathcal{E}_P$ admits a quadratic twist-type N_1N_2-congruence if the quadratic twist is non-trivial. That is, if $(\phi_1 \circ \psi)^*(d_1)(P)$ is not a square in K.

The result then follows by noting that on the level of function fields the double cover

$$X(H_1, H_2) \to X^+(H_1, H_2)$$

is given by adjoining the square root of $(\phi_1 \circ \psi)^*(d_1)$.

The converse follows from Lemma 2.2.7 and the construction of the curve $\mathcal{C} \cong X^+(H_1, H_2)$, noting that the quadratic twists are equal up to a square factor. □

Corollary 4.3.5. *Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) \neq 0, 1728$. Let p_1 and p_2 be distinct odd primes. Write $N = p_1p_2$, and suppose that r is an integer coprime to N. For each $i = 1, 2$ let $H_i \subset \mathrm{GL}_2(\mathbb{Z}/p_i\mathbb{Z})$ be a Cartan subgroup which is split if and only if $-r$ is a quadratic residue modulo p_i.*

Then E admits a quadratic twist-type (N, r)-congruence if and only if there exists a rational point in the fibre of the j-map $X^+(H_1, H_2) \to X(1)$ above $j(E)$ which does not lift to a rational point on $X(H_1, H_2)$.

Moreover the congruence is non-trivial if and only if E does not have CM.

Proof. The first claim follows from Proposition 4.1.4 and Lemma 4.3.4. The second claim follows from Lemma 4.2.1 and Proposition 4.2.2. □

Corollary 4.3.6. *Let $E/\mathbb{Q}$ be an elliptic curve without CM. Let p be an odd prime, and let $l \geq 1$ and $k \geq 2$ be integers. Write $N = 2^k p^l$ and suppose that r is an integer coprime to N. Let $H_2 \subset \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ be a Cartan subgroup which is split if and only if $-r$ is a quadratic residue modulo p.*

Then E admits a quadratic twist-type (N, r)-congruence if and only if there exists a rational point in the fibre of the j-map $X^+(H_1, H_2) \to X(1)$ above $j(E)$ which does not lift to a rational point on $X(H_1, H_2)$, where $H_1 \subset \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ is one of the subgroups, H, listed in Table 4.1 which corresponds to the pair $(2^k, r)$.

Proof. This follows from Propositions 4.1.4 and 4.1.6, and Lemma 4.3.4. □

4.4 Computing modular curves of genus 0 or 1

Let p be an odd prime, and let $k \geq 2$ and $l \geq 1$ be integers. By Corollary 4.3.6 if an elliptic curve $E/\mathbb{Q}$ without CM admits a quadratic twist-type $2^k p^l$-congruence then E gives rise to a rational point on a modular curve $X^+(H_1, H_2)$ where $H_1 \subset \mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ is one of the subgroups, H, listed in Table 4.1 and $H_2 \subset \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ is a Cartan subgroup.

To complete the proof of Theorem 1.0.15 we compute explicit models for the modular curves $X^+(H_1, H_2)$ of genus 0 or 1. That is, those curves which (by Faltings' Theorem) could possibly give rise to infinite families of quadratic twist-type congruences over $\mathbb{Q}$.

It is useful to note that if $H \subset \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ is a Cartan subgroup then for each $k \geq 1$ and we have the commutative diagram

$$\begin{array}{ccc} X^+(\mathrm{ns}\, 2^{k+1}, H) & \longrightarrow & X(\mathrm{ns}\, 2^{k+1^+}) \\ \downarrow & & \downarrow \\ X^+(\mathrm{ns}\, 2^k, H) & \longrightarrow & X(\mathrm{ns}\, 2^{k^+}) \end{array}$$

which realises $X^+(\mathrm{ns}\, 2^{k+1}, H)$ as a fibre product.

Remark 4.4.1. Since we compute equations by taking fibre products, we naturally obtain the j-maps, these may be accessed from the corresponding electronic data [Fre23b, `qtt-congruences/models`].

Lemma 4.4.2. *The curves $X^+(\mathrm{ns}\, 2, \mathrm{ns}\, 3)$ and $X^+(\mathrm{ns}\, 4, \mathrm{ns}\, 3)$ are isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1$.*

Proof. We fix a model for $X(\mathrm{ns}\,3^+) \cong \mathbb{P}^1$ with j-invariant map given by t^3 (see [Hal21, Théorème III.3.3]). Let $\mathcal{E}/\mathbb{Q}(t)$ be an elliptic curve with j-invariant t^3. Now $\mathcal{E}$ is $(3,1)$-congruent to its quadratic twist by

$$-3(t^2+12t+144), \tag{4.2}$$

this may be seen from the discussion in Remark 4.3.1 and the remark following Théorème III.3.5 in [Hal21, p. 505].

Now $-3(t^2+12t+144)\Delta(\mathcal{E}) \equiv -3(t-12)$ up to squares. Therefore $X^+(\mathrm{ns}\,2, \mathrm{ns}\,3)$ is given by $s^2 = -3(t-12)$. After replacing s by $6s$ we see that $X^+(\mathrm{ns}\,2, \mathrm{ns}\,3)$ is isomorphic to $\mathbb{P}^1$ with j-invariant map

$$1728\left(1-s^2\right)^3. \tag{4.3}$$

We fix a model (taken from [RZ15a]) for $X(\mathrm{ns}\,4^+) \cong \mathbb{P}^1$ with j-invariant $(32t_4-4)/t_4^4$. Recalling that $X(\mathrm{ns}\,2^+) = X(1)$ the modular curve $X^+(\mathrm{ns}\,4, \mathrm{ns}\,3)$ is birational to the curve given by

$$\frac{32t_4-4}{t_4^4} = 1728(1-s^2)^3.$$

Putting $t_4 = \frac{u}{6(s^2-1)}$ gives a model for $X^+(\mathrm{ns}\,4, \mathrm{ns}\,3)$ as

$$3s^2 = (u+1)^2(u^2-2u+3)$$

in $\mathbb{A}^2$. This curve has genus 0, and we parametrise by setting

$$(s,u) = \left(\frac{3(t^2-2)(t^2+2)}{(t^2-2t-2)^2}, \frac{2(t-1)(t+2)}{t^2-2t-2}\right).$$

This gives a model for $X^+(\mathrm{ns}\,4, \mathrm{ns}\,3) \cong \mathbb{P}^1$ with forgetful map to $X(\mathrm{ns}\,4^+)$ given by

$$t_4 = \frac{(t^2-2t-2)^3}{24(t^3-4)(t^3+2)}. \tag{4.4}$$

□

Lemma 4.4.3. *We have the following:*

(i) *The curve $X^+(\mathrm{ns}\,2, \mathrm{s}\,3)$ is isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1$.*

(ii) *The curve $X^+(\mathrm{ns}\,4, \mathrm{s}\,3)$ has genus 1 and is isomorphic over $\mathbb{Q}$ to the elliptic curve with LMFDB label* `48.a4`*, which has rank 0.*

Moreover the only rational points on $X^+(\mathrm{ns}\,4, \mathrm{s}\,3)$ are CM points which correspond to the discriminants -3 and -11.

Proof. We fix a model (see [Hal21, Théorème III.3.6(d)]) for $X(\mathrm{s}\,3^+) \cong \mathbb{P}^1$ with j-invariant map given by

$$\left(\frac{3t(t+4)}{t+3}\right)^3 \tag{4.5}$$

and let $\mathcal{E}/\mathbb{Q}(t)$ be an elliptic curve with this j-invariant. By Remark 4.3.1 and [Hal21, Théorème III.3.6(b)] we see that $\mathcal{E}$ is $(3,2)$-congruent to its quadratic twist by

$$t^2 - 12. \tag{4.6}$$

We have $(t^2-12)\Delta(\mathcal{E}) \equiv 3(t+3)$ up to squares. Then by setting $3s^2 = t+3$ we obtain an isomorphism over $\mathbb{Q}$ between $X^+(\mathrm{ns}\,2, \mathrm{s}\,3)$ and $\mathbb{P}^1$ with j-invariant map $\left(\frac{3(s^2-1)(3s^2+1)}{s^2}\right)^3$.

Therefore $X^+(\mathrm{ns}\,4, \mathrm{s}\,3)$ is birational to the curve given by

$$\frac{32t_4 - 4}{t_4^4} = \left(\frac{3(s^2-1)(3s^2+1)}{s^2}\right)^3.$$

Setting $t_4 = \frac{2s^2}{3(s^2-1)(3s^2+1)}u$ we obtain a birational model for $X^+(\mathrm{ns}\,4, \mathrm{s}\,3)$ defined by

$$4s^2u(u^3-4) = -3(s^2-1)(3s^2+1)$$

in $\mathbb{A}^2$. `Magma` verifies that

$$(s,u) = \left(\frac{6x^3 + x^2y + 14x^2 + 12xy - 8x + 8y - 16}{(x+4)^2(2x+y+2)}, \frac{6(x^2+3x+y+2)}{(x+4)(2x+y+2)}\right)$$

gives an explicit isomorphism from the elliptic curve with Weierstrass equation $y^2 = x^3+x^2-4x-4$ and LMFDB label `48.a4` to $X^+(\mathrm{ns}\,4, \mathrm{s}\,3)$.

The Mordell-Weil group of the elliptic curve `48.a4` is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. From the j-maps above it is simple to check that each rational point on $X^+(\mathrm{ns}\,4, \mathrm{s}\,3)$ corresponds to an elliptic curve with CM by an order of discriminant -3 or -11. □

Lemma 4.4.4. *The curve $X^+(\mathrm{ns}\,2, \mathrm{ns}\,5)$ is isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1$.*

Proof. We fix a model (see [Hal21, Théorème III.5.13]) for $X(\mathrm{ns}\,5^+) \cong \mathbb{P}^1$ with j-invariant map given by

$$\frac{5^3(t+1)(2t+1)^3(2t^2-3t+3)^3}{(t^2+t-1)^5} \tag{4.7}$$

and let $\mathcal{E}/\mathbb{Q}(t)$ be an elliptic curve with this j-invariant. By Remark 4.3.1 and the proof of Théorème III.5.18 in [Hal21, p. 568] we see that $\mathcal{E}$ is $(5,2)$-congruent to its quadratic twist by

$$-(8t^2 - 12t + 7). \tag{4.8}$$

We have $-(8t^2-12t+7)\Delta(\mathcal{E}) \equiv -(t^2+t-1)$ up to squares. Therefore $X^+(\mathrm{ns}\,2, \mathrm{ns}\,5)$ is given by $s^2 = -(t^2+t-1)$ in $\mathbb{A}^2$. We parametrise this conic by setting $(s,t) = (\frac{-u^2+u+1}{u^2+1}, \frac{-u^2-2u}{u^2+1})$ to obtain a model of $X^+(\mathrm{ns}\,2, \mathrm{ns}\,5) \cong \mathbb{P}^1$ with j-invariant

$$\frac{-5^3(2u-1)(4u^2+u+1)^3(2u^2+3u+3)^3(u^2+4u-1)^3}{(u^2-u-1)^5}. \tag{4.9}$$

□

Lemma 4.4.5. *The curve $X^+(\mathrm{ns}\,2, \mathrm{s}\,5)$ is isomorphic over $\mathbb{Q}$ to the elliptic curve with LMFDB label `20.a3`, which has rank 0. Moreover the only noncuspidal rational points on $X^+(\mathrm{ns}\,2, \mathrm{s}\,5)$ are CM points which correspond to the discriminants -4, -11, and -19.*

Proof. We fix a model (see [Hal21, Théorème III.5.9]) for $X(\mathrm{s}\,5^+) \cong \mathbb{P}^1$ with j-invariant map given by

$$\frac{(t+3)^3(t^2+t+4)^3(t^2-4t-1)^3}{(t^2+t-1)^5} \tag{4.10}$$

and let $\mathcal{E}/\mathbb{Q}(t)$ be an elliptic curve with this j-invariant. By Remark 4.3.1 and the discussion in [Hal21, p. 548] we see that $\mathcal{E}$ is $(5,1)$-congruent to its quadratic twist by

$$t^2-4t-16. \tag{4.11}$$

We have $(t^2-4t-16)\Delta(\mathcal{E}) \equiv t(t^2+t-1)$ up to squares. Setting $x=t$ shows that $X^+(\mathrm{ns}\,2, \mathrm{s}\,5)$ is isomorphic to the elliptic curve with Weierstrass equation $y^2 = x^3+x^2-x$ and LMFDB label `20.a3`.

The Mordell-Weil group of the elliptic curve `20.a3` has order 6. From the j-maps above it is simple to check that each point is either a cusp or a CM point corresponding to an elliptic curve with CM by an order of discriminant -4, -11, or -19. □

Lemma 4.4.6. *The curves $X^+(\mathrm{ns}\,2, \mathrm{ns}\,7)$ and $X^+(\mathrm{ns}\,2, \mathrm{s}\,7)$ are both isomorphic over $\mathbb{Q}$ to the elliptic curve with LMFDB label* `196.a2`*, which has rank* 1*.*

Proof. We fix a model (see [Hal21, Théorème III.7.30]) for $X(\mathrm{ns}\,7^+) \cong \mathbb{P}^1$ with j-invariant map given by

$$\frac{(3t+1)^3(t^2+3t+4)^3(t^2+10t+4)^3(4t^2+5t+2)^3}{(t^3+t^2-2t-1)^7} \tag{4.12}$$

and let $\mathcal{E}/\mathbb{Q}(t)$ be an elliptic curve with this j-invariant. By Remark 4.3.1 and [Hal21, Théorème III.7.32] we see that $\mathcal{E}$ is $(7,1)$-congruent to its quadratic twist by

$$-(16t^4+68t^3+111t^2+62t+11). \tag{4.13}$$

We have $-(16t^4+68t^3+111t^2+62t+11)\Delta(\mathcal{E}) \equiv -(t^3+t^2-2t-1)$ up to squares. Setting $x=-t$ shows that $X^+(\mathrm{ns}\,2, \mathrm{ns}\,7)$ is isomorphic to the elliptic curve with Weierstrass equation $y^2 = x^3-x^2-2x+1$ and LMFDB label `196.a2`.

To compute a model for $X^+(\mathrm{ns}\,2, \mathrm{s}\,7)$ we fix a model (see [Hal21, Théorème III.7.19]) for $X(\mathrm{s}\,7^+) \cong \mathbb{P}^1$ with j-invariant map given by

$$\frac{(1-t)(t-2)^3(t^2+3t-3)^3(t^2+3t+4)^3(t^4+t^3-t^2+2t+4)^3}{(t^3+t^2-2t-1)^7} \tag{4.14}$$

and let $\mathcal{E}/\mathbb{Q}(t)$ be an elliptic curve with this j-invariant. By Remark 4.3.1 and [Hal21, Proposition III.7.24] we see that $\mathcal{E}$ is $(7,6)$-congruent to its quadratic twist by

$$(t^4+6t^3+3t^2-18t-19). \tag{4.15}$$

We have $(t^4+6t^3+3t^2-18t-19)\Delta(\mathcal{E}) \equiv -(t^3+t^2-2t-1)$ up to squares. Setting $x=-t$ shows that $X^+(\mathrm{ns}\,2, \mathrm{s}\,7)$ is isomorphic to the elliptic curve with Weierstrass equation $y^2 = x^3-x^2-2x+1$ and LMFDB label `196.a2`. □

Lemma 4.4.7. *The curve $X^+(\mathrm{ns}\,2, \mathrm{ns}\,9)$ is isomorphic over $\mathbb{Q}$ to the elliptic curve with LMFDB label* `324.a2`*, which has rank* 1*.*

Proof. We fix a model (due to Baran [Bar09, Proposition 4.6]) for $X(\mathrm{ns}\,9^+) \cong \mathbb{P}^1$ with forgetful map $X(\mathrm{ns}\,9^+) \to X(\mathrm{ns}\,3^+)$ given by

$$t_3 = \frac{-3(t^3+3t^2-6t+4)(t^3+3t^2+3t+4)(5t^3-3t^2-3t+2)}{(t^3-3t+1)^3}. \tag{4.16}$$

Once again note that we may realise $X^+(\mathrm{ns}\,2, \mathrm{ns}\,9)$ as the fibre product

$$\begin{array}{ccc} X^+(\mathrm{ns}\,2, \mathrm{ns}\,9) & \longrightarrow & X(\mathrm{ns}\,9^+) \\ \downarrow & & \downarrow \\ X^+(\mathrm{ns}\,2, \mathrm{ns}\,3) & \longrightarrow & X(\mathrm{ns}\,3^+) \end{array}$$

Noting (4.3) the modular curve $X^+(\mathrm{ns}\,2, \mathrm{ns}\,9)$ is given by

$$12(1-s^2) = \frac{-3(t^3+3t^2-6t+4)(t^3+3t^2+3t+4)(5t^3-3t^2-3t+2)}{(t^3-3t+1)^3}.$$

After making the change of variables $s = \frac{3(t+1)(t^2-t+1)(t^2+2t-2)}{2(t^3-3t+1)^2}u$ we have a model for $X^+(\mathrm{ns}\,2, \mathrm{ns}\,9)$ as

$$(t+1)u^2 = (t^3-3t+1)$$

in $\mathbb{A}^2$. Then setting $x = \frac{3}{t+1}$ and $y = \frac{-3u}{t+1}$ shows that $X^+(\mathrm{ns}\,2, \mathrm{ns}\,9)$ is isomorphic to the elliptic curve with Weierstrass equation $y^2 = x^3 - 9x + 9$ and LMFDB label `324.a2`. The forgetful map $X^+(\mathrm{ns}\,2, \mathrm{ns}\,9) \to X(\mathrm{ns}\,9^+)$ is given by $t_9 = \frac{3-x}{x}$. □

Lemma 4.4.8. *We have the following:*

(i) *The curve $X^+(G_{11}(\sqrt{-1}), \mathrm{ns}\,3)$ is isomorphic over $\mathbb{Q}$ to the elliptic curve with LMFDB label* `72.a4` *and rank 0. Moreover the only rational points on $X^+(G_{11}(\sqrt{-1}), \mathrm{ns}\,3)$ are CM points corresponding to the discriminant -4.*

(ii) *The curve $X(G_9, \mathrm{ns}\,3^+)$ is isomorphic over $\mathbb{Q}$ to the elliptic curve with LMFDB label* `144.a3` *and rank 0. Moreover the only rational points on $X(G_9, \mathrm{ns}\,3^+)$ are a cusp and a CM point corresponding to the discriminant -4. In particular the curves $X^+(G_9(\sqrt{-1}), \mathrm{ns}\,3)$ and $X^+(G_9(\sqrt{-1}), \mathrm{s}\,3)$ have no exceptional points.*

Proof. (i) To compute a model for $X^+(G_{11}(\sqrt{-1}), \mathrm{ns}\,3)$ we fix a model (computed by Rouse and Zureick-Brown [RZ15a]) for $X(G_{11}) \cong \mathbb{P}^1$ with j-invariant map given by $\frac{(t^2-16)^3}{t^2}$. We then see that $X(G_{11}, \mathrm{ns}\,3^+)$ is given by requiring that $\frac{(t^2-16)^3}{t^2}$ is a cube. In particular setting $t = s^3$ gives an isomorphism between $X(G_{11}, \mathrm{ns}\,3^+)$ and $\mathbb{P}^1$ with forgetful map to $X(\mathrm{ns}\,3^+)$ given by

$$t_3 = \frac{(s^6-16)}{s^2}. \tag{4.17}$$

Now $3(t_3^2+12t_3+144) \equiv 3(s^2-2s+4)(s^2+2s+4)$ up to a square factor. By (4.2) the modular curve $X^+(G_{11}(\sqrt{-1}), \mathrm{ns}\,3)$ is birational to the curve

$$u^2 = 3(s^2-2s+4)(s^2+2s+4)$$

in $\mathbb{A}^2$. Taking

$$(s,u) = \left(\frac{-2(3x+y+15)}{3x-y+15}, \frac{12(x-1)(x+5)(x+11)}{(3x-y+15)^2}\right)$$

gives an explicit isomorphism from the elliptic curve with Weierstrass equation $y^2 = x^3 - 39x - 70$ and LMFDB label `72.a4` to $X^+(G_{11}(\sqrt{-1}), \mathrm{ns}\,3)$. The elliptic curve `72.a4` has Mordell-Weil group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. From the j-maps above it is simple to check that all the rational points on $X^+(G_{11}(\sqrt{-1}), \mathrm{ns}\,3)$ correspond to an elliptic curve with CM by an order of discriminant -4.

(ii) To compute a model for $X(G_9, \mathrm{ns}\,3^+)$ we fix a model for $X(G_9) \cong \mathbb{P}^1$ (computed by Rouse and Zureick-Brown [RZ15a]) with j-invariant map given by $\frac{(t^2+48)^3}{t^2+64}$. We then see that $X(G_9, \mathrm{ns}\,3^+)$ is given by requiring that $\frac{(t^2+48)^3}{t^2+64}$ is a cube. Therefore $X(G_9, \mathrm{ns}\,3^+)$ is birational to the curve given by

$$t^2 + 64 = s^3$$

in $\mathbb{A}^2$. Setting $t = 8y$ and $s = 4x$ we see that $X(G_9, \mathrm{ns}\,3^+)$ is isomorphic to the elliptic curve with Weierstrass equation $y^2 = x^3 - 1$ and LMFDB label `144.a3`. The elliptic curve `144.a3` has Mordell-Weil group isomorphic to $\mathbb{Z}/2\mathbb{Z}$. From the j-invariant maps above it is simple to check that one point on $X(G_9, \mathrm{ns}\,3^+)$ is a cusp and the other corresponds to an elliptic curve with CM by an order of discriminant -4.

The curve $X^+(G_9(\sqrt{-1}), \mathrm{ns}\,3)$ is a double cover of $X(G_9, \mathrm{ns}\,3^+)$ and $X^+(G_9(\sqrt{-1}), \mathrm{s}\,3)$ is a degree 4 cover of $X(G_9, \mathrm{ns}\,3^+)$ via the factorisation

$$X^+(G_9(\sqrt{-1}), \mathrm{s}\,3) \to X(G_9(\sqrt{-1}), \mathrm{s}\,3^+) \to X(G_9, \mathrm{ns}\,3^+).$$

In particular, the only rational points on the curves $X^+(G_9(\sqrt{-1}), \mathrm{ns}\,3)$ and $X^+(G_9(\sqrt{-1}), \mathrm{s}\,3)$ are CM points and cusps. □

Remark 4.4.9. We have omitted calculating models for the modular curves $X^+(G_9(\sqrt{-\Delta}), \mathrm{ns}\,3)$, $X^+(G_9(\sqrt{-\Delta}), \mathrm{s}\,3)$, $X^+(G_{11}(\sqrt{-\Delta}), \mathrm{ns}\,3)$ and $X^+(G_{11}(\sqrt{-\Delta}), \mathrm{s}\,3)$ because in Lemma 4.4.2 and Lemma 4.4.3 we showed that $X^+(\mathrm{ns}\,2, \mathrm{ns}\,3)$ and $X^+(\mathrm{ns}\,2, \mathrm{s}\,3)$ have infinitely many rational points. By Corollary 4.3.6 each of these curves may only give rise to quadratic twist-type $(12, 7)$ or $(12, 11)$-congruences.

$(2^k p^l, r)$	Modular curve	Genus	LMFDB label	Rank	Lemma
$(12, 1)$	$X^+(G_9(\sqrt{-1}), \mathrm{ns}\,3)$	1	`144.a*`	0	4.4.8
	$X^+(G_{11}(\sqrt{-1}), \mathrm{ns}\,3)$	1	`72.a4`	0	4.4.8
$(12, 5)$	$X^+(G_9(\sqrt{-1}), \mathrm{s}\,3)$	1	`144.a*`	0	4.4.8
$(12, 7)$	$X^+(\mathrm{ns}\,2, \mathrm{ns}\,3)$	0			4.4.2
$(12, 11)$	$X^+(\mathrm{ns}\,2, \mathrm{s}\,3)$	0			4.4.3
$(20, 3)$	$X^+(\mathrm{ns}\,2, \mathrm{ns}\,5)$	0			4.4.4
$(20, 11)$	$X^+(\mathrm{ns}\,2, \mathrm{s}\,5)$	1	`20.a3`	0	4.4.5
$(24, 11)$	$X^+(\mathrm{ns}\,4, \mathrm{s}\,3)$	1	`48.a4`	0	4.4.3
$(24, 19)$	$X^+(\mathrm{ns}\,4, \mathrm{ns}\,3)$	0			4.4.2
$(28, 3)$	$X^+(\mathrm{ns}\,2, \mathrm{s}\,7)$	1	`196.a2`	1	4.4.6
$(28, 11)$	$X^+(\mathrm{ns}\,2, \mathrm{ns}\,7)$	1	`196.a2`	1	4.4.6
$(36, 19)$	$X^+(\mathrm{ns}\,2, \mathrm{ns}\,9)$	1	`324.a2`	1	4.4.7

Table 4.3: Modular curves of genus ≤ 1 which parametrise quadratic twist-type $(2^k p^l, r)$-congruences of elliptic curves where $k \geq 2$, $l \geq 1$ and p is an odd prime.

With these explicit models we now conclude the proof of Theorem 1.0.15.

Proof of Theorem 1.0.15. We have already proved the case where N is a prime power in Proposition 4.2.4. It therefore suffices to consider the case where N is divisible by two or more distinct primes. When $N = 2p^l$ and p is an odd prime, the claim follows immediately from Proposition 4.2.4 (an elliptic curve is 2-congruent to all of its quadratic twists).

First suppose that (N, r) is not in the set $\mathcal{S}$ in the statement of Theorem 1.0.15. Suppose that N is divisible by distinct *odd* prime numbers p_1 and p_2. If an elliptic curve $E/\mathbb{Q}$ with $j(E) \neq 0, 1728$ admits a quadratic twist-type N-congruence then by Corollary 4.3.5 there exists a rational point on one of the 4 modular curves $X^+(H_1, H_2)$ above $j(E)$, where $H_i \subset \mathrm{GL}_2(\mathbb{Z}/p_i\mathbb{Z})$ is a Cartan subgroup. Table B.1 lists the genera of the modular curves $X^+(H_1, H_2)$ whenever $X(H_i^+)$ has infinitely many rational points. It follows from Faltings' Theorem that for each such N there are at most finitely j-invariants of elliptic curves $E/\mathbb{Q}$ admitting a quadratic twist-type N-congruence.

Now suppose that N is divisible by $2^k p^l$ where p is an odd prime and $l \geq 1$ and $k \geq 2$ are integers. Table B.2 records the genera of the modular curves $X^+(H_1, H_2)$ from Corollary 4.3.6 whenever $X(H_i^+)$ has infinitely many rational points. It follows from Faltings' Theorem that if there exist infinitely many j-invariants of elliptic curves admitting quadratic twist-type (N, r)-congruences then $(N, r) \in \mathcal{S}$ or there are infinitely many points on one of the modular curves $X^+(G_{11}(\sqrt{-1}), \mathrm{ns}\,3)$, $X^+(G_9(\sqrt{-1}), \mathrm{ns}\,3)$, $X^+(G_9(\sqrt{-1}), \mathrm{s}\,3)$, $X^+(\mathrm{ns}\,2, \mathrm{s}\,5)$, or $X^+(\mathrm{ns}\,4, \mathrm{s}\,3)$. But each of these curves has finitely many rational points (see Table 4.3).

Conversely, the modular curves $X^+(\mathrm{ns}\,2, \mathrm{ns}\,3)$, $X^+(\mathrm{ns}\,2, \mathrm{s}\,3)$, $X^+(\mathrm{ns}\,4, \mathrm{ns}\,3)$, $X^+(\mathrm{ns}\,2, \mathrm{ns}\,5)$, $X^+(\mathrm{ns}\,2, \mathrm{ns}\,7)$, $X^+(\mathrm{ns}\,2, \mathrm{s}\,7)$, and $X^+(\mathrm{ns}\,2, \mathrm{ns}\,9)$ have infinitely many rational points (as recorded in Table 4.3).

For a rational point P on one of these modular curves (not lying above $j = \infty, 0, 1728$) let $E_P/\mathbb{Q}$ be an elliptic curve with j-invariant $j(P)$. Then exactly one of the following holds:

(i) the fibre of the degree 2 map $X(\mathrm{ns}\,2^k, H) \to X^+(\mathrm{ns}\,2^k, H)$ above P has a $\mathbb{Q}$-rational point (equivalently $\Delta(E_P)$ is a square),

(ii) the curve E_P is isogenous over $\mathbb{Q}$ to $E_P^{\Delta(E_P)}$,

(iii) the curve E_P admits a non-trivial quadratic twist-type congruence with $E_P^{\Delta(E_P)}$.

In the cases where the modular curve $X^+(\mathrm{ns}\,2^k, H)$ has genus 0, Hilbert's Irreducibility Theorem (see [Ser97, Chapter 9]) implies that for infinitely many rational points P case (i) does not occur. In the cases $X^+(\mathrm{ns}\,2, \mathrm{ns}\,7)$, $X^+(\mathrm{ns}\,2, \mathrm{s}\,7)$, and $X^+(\mathrm{ns}\,2, \mathrm{ns}\,9)$ the corresponding double cover in (i) has genus 5, 5, and 7 respectively - so case (i) occurs for at most finitely many rational points by Faltings' Theorem.

By Lemma 4.2.1 (ii) may only occur if E_P has CM. But there are only finitely many j-invariants of elliptic curves over $\mathbb{Q}$ with CM, so (ii) occurs for at most finitely many points $P \in X(H^+)$.

Therefore (iii) occurs for infinitely many rational points $P \in X^+(\mathrm{ns}\,2^k, H)$. Hence when $(N, r) \in \mathcal{S}$ it follows from Corollary 4.3.6 that there exist infinitely many j-invariants of elliptic curves admitting non-trivial quadratic twist-type (N, r)-congruences over $\mathbb{Q}$, as required. □

4.5 Evidence for Conjecture 1.0.17

This section is motivated by two goals. First we wish to construct examples of non-trivial quadratic twist-type (N, r)-congruences for some $(N, r) \notin \mathcal{S}$ (in particular we wish to prove Theorem 1.0.16, see Examples 4.5.8 and 4.5.13). Second we provide evidence for Conjecture 1.0.17.

By Proposition 4.2.4, the prime power case of Conjecture 1.0.17 is equivalent to the conjecture that there exist no exceptional points on the modular curve $X(\mathrm{ns}\,p^{l+})$ for all odd prime powers $p^l \geq 19$ (see e.g., [RSZ22, Conjecture 1.5]). This is our "Assumption (A)" in Theorem 4.5.1.

If we assume (A) then by Propositions 4.2.2 and 4.2.4 when N is not a prime power (or twice an odd prime power) and $(N, r) \notin \mathcal{S}$, non-trivial quadratic twist-type (N, r)-congruences may only arise from exceptional points on the modular curves $X^+(H_1, H_2)$ in Corollaries 4.3.5 and 4.3.6 where $X(H_i^+)$ has infinitely many rational points. These curves, and their genera, are listed in Tables B.1 and B.2.

We therefore compute explicit models for the modular curves $X^+(H_1, H_2)$ in Tables B.1 and B.2 of genus ≤ 4 whose noncuspidal rational points give rise to elliptic curves admitting an (N, r)-congruence with a quadratic twist, where $(N, r) \notin \mathcal{S}$. Each such curve is listed (together with their known exceptional j-invariants) in Table 4.4.

This allows us to prove the following conditional form of Conjecture 1.0.17:

Theorem 4.5.1. *Assume the following:*

(A) *There are no exceptional points on the modular curves $X(\mathrm{ns}\,p^{l+})$ for all odd prime powers $p^l \geq 19$,*

(B) *There are no (non-CM) points of canonical height $\geq 10^{15}$ on the genus 1 modular curves in Table 4.5 lifting to rational points on the double cover $X^+(H_1, H_2)$,*

(C) *There are no exceptional points on the modular curves in Tables B.1 and B.2 of genus ≥ 5.*

Then Conjecture 1.0.17 holds.

(N, r)	Modular curve	Exceptional j-invariants	Reference
$(12, 1)$	$X^+(G_9(\sqrt{-1}), \mathrm{ns}\,3)$		Lemma 4.4.8
	$X^+(G_{11}(\sqrt{-1}), \mathrm{ns}\,3)$		Lemma 4.4.8
$(12, 5)$	$X^+(G_9(\sqrt{-1}), \mathrm{s}\,3)$		Lemma 4.4.8
	$X^+(G_{11}(\sqrt{-1}), \mathrm{s}\,3)$		Lemma 4.5.3
$(20, 11)$	$X^+(\mathrm{ns}\,2, \mathrm{s}\,5)$		Lemma 4.4.5
$(24, 7)$	$X^+(\mathrm{s}\,4, \mathrm{ns}\,3)$		Lemma 4.5.5
$(24, 11)$	$X^+(\mathrm{ns}\,4, \mathrm{s}\,3)$		Lemma 4.4.3
$(30, 1)$	$X^+(\mathrm{ns}\,3, \mathrm{s}\,5)$		Assumption (B)
$(30, 7)$	$X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$	$\frac{-3^3 \cdot 5^6 \cdot 199^3 \cdot 809^3 \cdot 5059^3}{61^{15}}$	Proposition 4.6.2
$(40, 3)$	$X^+(\mathrm{ns}\,4, \mathrm{ns}\,5)$		Lemma 4.5.6
$(42, 1)$	$X^+(\mathrm{ns}\,3, \mathrm{ns}\,7)$		Assumption (B)
$(44, 3)$	$X^+(\mathrm{ns}\,2, \mathrm{ns}\,11)$		Assumption (B)
$(48, 19)$	$X^+(\mathrm{ns}\,8, \mathrm{ns}\,3)$	$\frac{2^{15} \cdot 3^3 \cdot 5^3 \cdot 31^3 \cdot 41^3 \cdot 47^3 \cdot 83^3 \cdot 293^3}{23^{24}}$	Assumption (B)

Table 4.4: Exceptional j-invariants for the modular curves $X^+(H_1, H_2)$ in Tables B.1 and B.2 with genus ≤ 4 and whose exceptional points give rise to elliptic curves admitting an (N, r)-congruence with a quadratic twist, where $(N, r) \notin \mathcal{S}$.

Modular curve	Affine equation in $\mathbb{A}^3$	Genus 1 modular curve	LMFDB label	Lemma
$X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$	$v^2+v=u^3+1$ $w^2=3(3u^2-2u-4v+3)(9u^2-10u+5)$	$X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+)$	225.c2	4.5.7
$X^+(\mathrm{ns}\,3, \mathrm{s}\,5)$	$v^2+v=u^3+1$ $w^2=-(3v+3u^3-12u^2+12u-6)$	$X(\mathrm{ns}\,3^+, \mathrm{s}\,5^+)$	225.c2	4.5.9
$X^+(\mathrm{ns}\,3, \mathrm{ns}\,7)$	$v^2+v=u^3+12$ $w^2=4u^3+21u^2-42u+49$	$X(\mathrm{ns}\,3^+, \mathrm{ns}\,7^+)$	441.d2	4.5.10
$X^+(\mathrm{ns}\,2, \mathrm{ns}\,11)$	$v^2+v=u^3-u^2-7u+10$ $w^2=(-3u^2+24u-37)v-u^4+5u^3+18u^2-95u+94$	$X(\mathrm{ns}\,11^+)$	121.b2	4.5.11
$X^+(\mathrm{ns}\,8, \mathrm{ns}\,3)$	$v^2=u^3+8$ $w^2=3(3u^3+3u^2+2uv-8u+8)$	$X(\mathrm{ns}\,8^+, \mathrm{ns}\,3^+)$	576.e4	4.5.12

TABLE 4.5: Affine models for the modular curves in Table 4.4 which naturally arise as a double cover of a modular curve of genus 1 and rank 1. The double covers are given by $(u, v, w) \mapsto (u, v)$.

Remark 4.5.2. Assumption (A) in Theorem 4.5.1 would follow from [RSZ22, Conjecture 1.5] together with [BDM$^+$19, Corollary 1.3] and [BDM$^+$23, Theorem 1.4]. In Proposition 4.6.2 we prove that the only rational points on the curve $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ are those listed in Table 4.6, so assumption (B) may be weakened slightly to exclude $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$.

4.5.1 Computing modular curves of genus ≤ 4

We first show that the modular curves in Table 4.4 which do not appear in Table 4.5 arise naturally as a double cover of a modular curve with no exceptional points. Note that the curves in Table 4.4 of genus ≤ 1 were computed in Section 4.4.

Lemma 4.5.3. *The curve $X(G_{11}, \mathrm{s}\,3^+)$ is isomorphic over $\mathbb{Q}$ to the elliptic curve with LMFDB label* 48.a4 *and rank* 0. *Moreover the modular curves $X(G_{11}, \mathrm{s}\,3^+)$ and $X^+(G_{11}(\sqrt{-1}), \mathrm{s}\,3)$ have no noncuspidal rational points.*

Proof. Recalling (4.5) we see that the double cover $X(\mathrm{s}\,3^+) \to X(\mathrm{ns}\,3^+)$ is given on the level of function fields by setting $\frac{3t(t+4)}{t+3} = t_3$. In particular by (4.17) the modular curve $X(G_{11}, \mathrm{s}\,3^+)$ is birational to the curve given by

$$\frac{3t(t+4)}{t+3} = \frac{(s^6-16)}{s^2}$$

in $\mathbb{A}^2$. By setting $t = \frac{(s-2)(s+2)(s^2+2)^2u+(s^4-2s^2+4)}{6s^2}$ we see that $X(G_{11}, \mathrm{s}\,3^+)$ is birational to the curve $u^2 = (s^2-2s+4)(s^2+2s+4)$ in $\mathbb{A}^2$. Setting $u = 4(x^2+2x+4)/(x^2-4)$ and $s = 4y/(x^2-4)$ shows that $X(G_{11}, \mathrm{s}\,3^+)$ is isomorphic over $\mathbb{Q}$ to the elliptic curve with Weierstrass equation $y^2 = x^3+x^2-4x-4$ and LMFDB label 48.a4.

The elliptic curve 48.a4 has Mordell-Weil group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. From the j-maps above it is simple to check that each of these points on $X(G_{11}, \mathrm{s}\,3^+)$ is a cusp. In particular the double cover $X^+(G_{11}(\sqrt{-1}), \mathrm{s}\,3)$ has no noncuspidal rational points. □

As a corollary we may deduce the level 12 part of Conjecture 1.0.17.

Corollary 4.5.4. *There exist no elliptic curves $E/\mathbb{Q}$ admitting a non-trivial quadratic twist-type $(12, 1)$ or $(12, 5)$-congruence.*

Proof. By Proposition 4.2.2 no CM elliptic curve $E/\mathbb{Q}$ admits a non-trivial quadratic twist-type 12-congruence. Hence if $E/\mathbb{Q}$ admits a non-trivial quadratic twist-type $(12, 1)$ or $(12, 5)$-congruence then by Corollary 4.3.6 the elliptic curve E gives rise to an exceptional point on one of the four modular curves $X^+(G_9(\sqrt{-1}), \mathrm{ns}\,3)$, $X^+(G_{11}(\sqrt{-1}), \mathrm{ns}\,3)$, $X^+(G_9(\sqrt{-1}), \mathrm{s}\,3)$, and $X^+(G_{11}(\sqrt{-1}), \mathrm{s}\,3)$. But by Lemmas 4.4.8 and 4.5.3 each of these curves has only rational cusps and CM points. □

Lemma 4.5.5. *The curve $X(\mathrm{s}\,4^+, \mathrm{ns}\,3^+)$ is isomorphic over $\mathbb{Q}$ to the elliptic curve with LMFDB label* `36.a4` *and rank* 0*. Moreover the only rational points on the modular curve $X(\mathrm{s}\,4^+, \mathrm{ns}\,3^+)$ are cusps and CM points corresponding to the discriminants -4 and -7. In particular the modular curve $X^+(\mathrm{s}\,4, \mathrm{ns}\,3)$ has no exceptional points.*

Proof. To compute a model for $X(\mathrm{s}\,4^+, \mathrm{ns}\,3^+)$ we fix a model (computed by Rouse and Zureick-Brown [RZ15a]) for $X(\mathrm{s}\,4^+) \cong \mathbb{P}^1$ with j-invariant map given by $\frac{-64(t^2-3)^3(t^2+1)^3}{(t^2-1)^4}$. We then see that $X(\mathrm{s}\,4^+, \mathrm{ns}\,3^+)$ is given by requiring that (t^2-1) is a cube. In particular $X(\mathrm{s}\,4^+, \mathrm{ns}\,3^+)$ is isomorphic over $\mathbb{Q}$ the curve

$$t^2 = s^3 + 1$$

in $\mathbb{A}^2$. This is a Weierstrass equation for the elliptic curve with LMFDB label `36.a4` and rank 0.

The elliptic curve `36.a4` has Mordell-Weil group isomorphic to $\mathbb{Z}/6\mathbb{Z}$. Of these points on $X(\mathrm{s}\,4^+, \mathrm{ns}\,3^+)$ three are cusps, two correspond to a curve with CM by an order of discriminant -7, and one corresponds to a curve with CM by an order of discriminant -4. Since $X^+(\mathrm{s}\,4, \mathrm{ns}\,3)$ is a double cover of $X(\mathrm{s}\,4^+, \mathrm{ns}\,3^+)$ it has no exceptional points. □

Lemma 4.5.6. *The modular curve $X^+(\mathrm{ns}\,4, \mathrm{ns}\,5)$ has no exceptional points.*

Proof. Baran showed that the genus 2 curve $X(\mathrm{ns}\,4^+, \mathrm{ns}\,5^+)$ has no exceptional points (see [Bar10, Table 5.1]). Hence $X^+(\mathrm{ns}\,4, \mathrm{ns}\,5)$ has no exceptional points. □

We now show that the remaining modular curves in Table 4.4 arise as a double cover of an elliptic curve of rank 1. The models which we compute are recorded in Table 4.5. In the cases where we find an exceptional point (i.e., $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ and $X^+(\mathrm{ns}\,8, \mathrm{ns}\,3)$) we also compute a canonical model. Canonical models for the other curves are not recorded here but may be found in the electronic data [Fre23b, `qtt-congruences/models`].

Lemma 4.5.7. *We have:*

(i) *The modular curve $X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+)$ is isomorphic to the elliptic curve with Weierstrass equation $v^2 + v = u^3 + 1$ and LMFDB label* `225.c2`*.*

(ii) *The modular curve $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ is birational to the curve in $\mathbb{A}^3$ given by*

$$v^2 + v = u^3 + 1 \qquad \text{and} \qquad w^2 = 3(3u^2 - 2u - 4v + 3)(9u^2 - 10u + 5) \tag{4.18}$$

with forgetful map to the model of $X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+)$ in (i) *given by $(u, v, w) \mapsto (u, v)$.*

(iii) *The modular curve $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ is a hyperelliptic curve of genus 2 which is isomorphic over $\mathbb{Q}$ to the curve with Weierstrass equation*

$$y^2 + y = x^6 + 3x^5 - 5x^3 + 3x. \tag{4.19}$$

Proof. (i) We begin by computing equations for $X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+)$. Recall the models for $X(\mathrm{ns}\,3^+)$ and $X(\mathrm{ns}\,5^+)$ with j-invariants given by t^3 and equation (4.7). It follows that $X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+)$ is birational to the curve given by

$$s^3 = \frac{5^3(t+1)(2t+1)^3(2t^2-3t+3)^3}{(t^2+t-1)^5}$$

in $\mathbb{A}^2$. Therefore $X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+)$ is isomorphic to the elliptic curve with Weierstrass equation $v^2 + v = u^3 + 1$ and LMFDB label `225.c2`. The forgetful maps $X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+) \to X(\mathrm{ns}\,3^+)$ and $X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+) \to X(\mathrm{ns}\,5^+)$ are given by

$$t_3 = \frac{-5u(v+3)(8v^2+23v+17)}{(v^2+v-1)^2} \qquad \text{and} \qquad t_5 = \frac{-(v+2)}{(v+1)}.$$

(ii) Now $3(t_3^2 + 12t_3 + 144)(8t_5^2 - 12t_5 + 7)$ is equal to $3(3u^2 - 2u - 4v + 3)(9u^2 - 10u + 5)$ up to a square factor in $\mathbb{Q}(X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+))$. In particular, noting (4.2) and (4.8), $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ is birational to the curve, $\mathcal{C}$, given by (4.18).

(iii) `Magma` verifies that taking

$$u = \frac{x^4 + 2x^3 - x + 3y + 4}{(x-1)^2(x+2)^2},$$

$$v = \frac{x^6 + 3x^5 + 6x^4 + 7x^3 + 3x^2y - 6x^2 + 3xy - 9x + 3y + 16}{(x-1)^3(x+2)^3},$$

$$w = \frac{3(2x+1)(x^6 + 3x^5 + 21x^4 + 37x^3 + 6x^2y - 27x^2 + 6xy - 45x + 15y + 64)}{(x-1)^4(x+2)^4}$$

gives a birational map between the hyperelliptic curve with Weierstrass equation (4.19) and $\mathcal{C}$. □

Example 4.5.8 (A 30-Congruence)**.** The curve $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ with model given by (4.19) has the rational point $(3, 36)$ which lies in the fibre of the non-CM j-invariant

$$\frac{-3^3 \cdot 5^6 \cdot 199^3 \cdot 809^3 \cdot 5059^3}{61^{15}}.$$

The minimal twist with this j-invariant is the elliptic curve $E_{(30,7)}/\mathbb{Q}$ from the statement of Theorem 1.0.16 with conductor $61 \cdot 214663^2$. By Corollary 4.3.5 the elliptic curve $E_{(30,7)}$ admits a non-trivial $(30, 7)$-congruence with its quadratic twist by -214663.

Lemma 4.5.9. *We have:*

(i) *The modular curve $X(\mathrm{ns}\,3^+, \mathrm{s}\,5^+)$ is isomorphic to the elliptic curve with Weierstrass equation $v^2 + v = u^3 + 1$ and LMFDB label `225.c2`.*

(ii) *The modular curve $X^+(\mathrm{ns}\,3, \mathrm{s}\,5)$ is birational to the curve in $\mathbb{A}^3$ given by*

$$v^2 + v = u^3 + 1 \qquad \text{and} \qquad w^2 = -(3v + 3u^3 - 12u^2 + 12u - 6) \tag{4.20}$$

with forgetful map to the model of $X(\mathrm{ns}\,3^+, \mathrm{s}\,5^+)$ in (i) *given by $(u, v, w) \mapsto (u, v)$.*

Proof. (i) Recall the model for $X(\mathrm{s}\,5^+)$ with j-invariant given by equation (4.10). Then the curve $X(\mathrm{ns}\,3^+, \mathrm{s}\,5^+)$ is birational to the curve given by

$$s^3 = \frac{(t+3)^3(t^2+t+4)^3(t^2-4t-1)^3}{(t^2+t-1)^5}$$

in $\mathbb{A}^2$. It follows that $X(\mathrm{ns}\,3^+, \mathrm{s}\,5^+)$ is also isomorphic to the elliptic curve with Weierstrass equation $v^2+v = u^3+1$ and LMFDB label `225.c2`. The forgetful maps $X(\mathrm{ns}\,3^+, \mathrm{s}\,5^+) \to X(\mathrm{ns}\,3^+)$ and $X(\mathrm{ns}\,3^+, \mathrm{s}\,5^+) \to X(\mathrm{s}\,5^+)$ are given by

$$t_3 = \frac{-u(v-2)(v^2+v+4)(v^2+6v+4)}{(v^2+v-1)^2} \qquad \text{and} \qquad t_5 = -(v+1).$$

(ii) Now $-3(t_3^2+12t_3+144)(t_5^2-4t_5-16)$ is equal to $-(3v+3u^3-12u^2+12u-6)$ up to a square factor in $\mathbb{Q}(X(\mathrm{ns}\,3^+,\mathrm{s}\,5^+))$. In particular, noting (4.2) and (4.11), $X^+(\mathrm{ns}\,3,\mathrm{s}\,5)$ is birational to the curve given by (4.20). □

Lemma 4.5.10. *We have:*

(i) *The modular curve $X(\mathrm{ns}\,3^+,\mathrm{ns}\,7^+)$ is isomorphic to the elliptic curve with Weierstrass equation $v^2+v=u^3+12$ and LMFDB label* `441.d2`.

(ii) *The modular curve $X^+(\mathrm{ns}\,3,\mathrm{ns}\,7)$ is birational to the curve in $\mathbb{A}^3$ given by*

$$v^2+v=u^3+12 \qquad \text{and} \qquad w^2=4u^3+21u^2-42u+49 \tag{4.21}$$

with forgetful map to the model of $X(\mathrm{ns}\,3^+,\mathrm{ns}\,7^+)$ in (i) *given by $(u,v,w)\mapsto(u,v)$.*

Proof. (i) Recall the model for $X(\mathrm{ns}\,7^+)\cong\mathbb{P}^1$ with j-invariant given by equation (4.12). Then $X(\mathrm{ns}\,3^+,\mathrm{ns}\,7^+)$ is birational to the curve given by

$$s^3=\frac{(3t+1)^3(t^2+3t+4)^3(t^2+10t+4)^3(4t^2+5t+2)^3}{(t^3+t^2-2t-1)^7}$$

in $\mathbb{A}^2$. It follows that $X(\mathrm{ns}\,3^+,\mathrm{ns}\,7^+)$ is isomorphic to the elliptic curve with Weierstrass equation $v^2+v=u^3+12$ and LMFDB label `441.d2` (see also [Bar10, Equation 5.5]). The forgetful map $X(\mathrm{ns}\,3^+,\mathrm{ns}\,7^+)\to X(\mathrm{ns}\,7^+)$ is given by

$$t_7=\frac{6u^2-uv-11u-7v+70}{3u^2-uv+10u-7v-77}.$$

Let the forgetful map $X(\mathrm{ns}\,3^+,\mathrm{ns}\,7^+)\to X(\mathrm{ns}\,3^+)$ be given by $(u,v)\mapsto t_3$.

(ii) Now $3(t_3^2+12t_3+144)(16t_7^4+68t_7^3+111t_7^2+62t_7+11)$ is equal to $4u^3+21u^2-42u+49$ up to a square factor in $\mathbb{Q}(X(\mathrm{ns}\,3^+,\mathrm{ns}\,7^+))$. In particular, noting (4.2) and (4.13), we see that $X^+(\mathrm{ns}\,3,\mathrm{ns}\,7)$ is birational to the curve given by (4.21). □

Lemma 4.5.11. *We have:*

(i) *The modular curve $X(\mathrm{ns}\,11^+)$ is isomorphic to the elliptic curve with Weierstrass equation $v^2+v=u^3-u^2-7u+10$ and LMFDB label* `121.b2`.

(ii) *The modular curve $X^+(\mathrm{ns}\,2,\mathrm{ns}\,11)$ is birational to the curve in $\mathbb{A}^3$ given by*

$$v^2+v=u^3-u^2-7u+10 \qquad \text{and} \qquad w^2=(-3u^2+24u-37)v-u^4+5u^3+18u^2-95u+94 \tag{4.22}$$

with forgetful map to the model of $X(\mathrm{ns}\,11^+)$ in (i) *given by $(u,v,w)\mapsto(u,v)$.*

Proof. (i) This is [CC04, Theorem 1.1], [Hal98], [Hal21, Théorème III.13.18], or [Lig77, Proposition 4.3.8.1]. The j-invariant map is given by

$$\frac{(f_1f_2f_3f_4)^3}{f_5^2f_6^{11}}$$

where

$$\begin{aligned}
f_1 &= u^2 + 3u + 6,\\
f_2 &= 11(u^2-5)v + (2u^4 + 23u^3 - 72u^2 - 28u + 127),\\
f_3 &= 6v + 11u - 19,\\
f_4 &= 22(u-2)v + (5u^3 + 17u^2 - 112u + 120),\\
f_5 &= 11v + (2u^2 + 17u - 34),\\
f_6 &= (u-4)v - (5u - 9).
\end{aligned}$$

(ii) Let $\mathcal{E}/\mathbb{Q}(X(\mathrm{ns}\,11^+))$ be an elliptic curve with this j-invariant. By Remark 4.3.1 and [Hal21, Proposition III.13.25] we see that $\mathcal{E}$ is $(11,1)$-congruent to its quadratic twist by $d = d_1d_2d_3$ where

$$\begin{aligned}
d_1 &= 3619v - (108u^5 + 168u^4 - 641u^3 - 1007u^2 - 3769u + 9670),\\
d_2 &= 48(3u+5)v - (276u^2 - 452u + 185),\\
d_3 &= 16v + 28u - 49.
\end{aligned}$$

Now $d\Delta(\mathcal{E})$ is equal to $(-3u^2 + 24u - 37)v - u^4 + 5u^3 + 18u^2 - 95u + 94$ up to a square factor in $\mathbb{Q}(X(\mathrm{ns}\,11^+))$ so $X^+(\mathrm{ns}\,2, \mathrm{ns}\,11)$ is birational to the curve given by (4.22). □

Lemma 4.5.12. *We have:*

(i) *The modular curve $X(\mathrm{ns}\,8^+, \mathrm{ns}\,3^+)$ is isomorphic to the elliptic curve with Weierstrass equation $v^2 = u^3 + 8$ and LMFDB label* `576.e4`.

(ii) *The modular curve $X^+(\mathrm{ns}\,8, \mathrm{ns}\,3)$ is birational to the curve in $\mathbb{A}^3$ given by*

$$v^2 = u^3 + 8 \qquad \text{and} \qquad w^2 = 3(3u^3 + 3u^2 + 2uv - 8u + 8) \tag{4.23}$$

with forgetful map to the model of $X(\mathrm{ns}\,8^+, \mathrm{ns}\,3^+)$ in (i) *given by $(u,v,w) \mapsto (u,v)$.*

(iii) *The modular curve $X^+(\mathrm{ns}\,8, \mathrm{ns}\,3)$ is a non-hyperelliptic curve of genus 3 which may be canonically embedded in $\mathbb{P}^2$ over $\mathbb{Q}$ as the curve*

$$\begin{aligned}
2X^3Y - 2X^3Z + X^2Y^2 - 2X^2YZ - 2X^2Z^2 - 2XY^3 + 2XY^2Z\\
+2XYZ^2 - 2XZ^3 - Y^4 + 2Y^3Z + Y^2Z^2 - 2YZ^3 = 0.
\end{aligned} \tag{4.24}$$

Proof. (i) We fix a model for $X(\mathrm{ns}\,8^+) \cong \mathbb{P}^1$ so that the j-invariant map is given by

$$\frac{-2^{15}(t-2)t^3(t^2-2t-2)^3(t^2-2t+2)^3}{(t^2-2)^8},$$

this is the model from [RZ15a] obtained after replacing t by $1/t$.

Then $X(\mathrm{ns}\,8^+, \mathrm{ns}\,3^+)$ is birational to the curve given by

$$s^3 = \frac{-2^{15}(t-2)t^3(t^2-2t-2)^3(t^2-2t+2)^3}{(t^2-2)^8}$$

in $\mathbb{A}^2$. It follows that $X(\mathrm{ns}\,8^+, \mathrm{ns}\,3^+)$ is isomorphic to the elliptic curve with Weierstrass equation $v^2 = u^3 + 8$ and LMFDB label `576.e4`. The forgetful maps $X(\mathrm{ns}\,8^+, \mathrm{ns}\,3^+) \to X(\mathrm{ns}\,8^+)$ and

$X(\mathrm{ns}\,8^+, \mathrm{ns}\,3^+) \to X(\mathrm{ns}\,3^+)$ are given by

$$t_8 = \frac{2(v-2)}{v-4} \qquad \text{and} \qquad t_3 = \frac{64u(v-2)(v^2-12v+24)(v^2-4v+8)}{(v^2-8)^3}.$$

(ii) Let $\mathcal{E}/\mathbb{Q}(X(\mathrm{ns}\,8^+, \mathrm{ns}\,3^+))$ be an elliptic curve with j-invariant t_3^3. Then $-3(t_3^2+12t_3+144)\Delta(\mathcal{E})$ is equal to $3(3u^3+3u^2+2uv-8u+8)$ up to a square factor in $\mathbb{Q}(X(\mathrm{ns}\,8^+, \mathrm{ns}\,3^+))$. Therefore, recalling (4.2), $X^+(\mathrm{ns}\,8, \mathrm{ns}\,3)$ is birational to the curve $\mathcal{C}$ given by (4.23).

(iii) `Magma` verifies that taking

$$u = \frac{2(XY+Y^2-XZ-YZ-Z^2)}{Z^2},$$

$$v = \frac{2(2X^2Y+2XY^2-2X^2Z-3XYZ-Y^2Z-2XZ^2+YZ^2)}{Z^3},$$

$$w = \frac{2(X+2Y-Z)(2XY+2Y^2-2XZ-2YZ-3Z^2)}{Z^3}$$

gives a birational map between the curve given by (4.24) and $\mathcal{C}$. □

Example 4.5.13 (A 48-Congruence)**.** The model for $X^+(\mathrm{ns}\,8, \mathrm{ns}\,3)$ given by (4.24) has the rational point $(4:-7:1)$ which lies in the fibre of the non-CM j-invariant

$$\frac{2^{15}\cdot 3^3\cdot 5^3\cdot 31^3\cdot 41^3\cdot 47^3\cdot 83^3\cdot 293^3}{23^{24}}.$$

The minimal twist with this j-invariant is the elliptic curve $E_{(48,19)}/\mathbb{Q}$ from the statement of Theorem 1.0.16. The conductor of $E_{(48,19)}$ is $19^2\cdot 23\cdot 43^2\cdot 39451^2$ and its discriminant is $-19^3\cdot 23^{24}\cdot 43^3\cdot 39451^3$.

By Corollary 4.3.6 the elliptic curve $E_{(48,19)}$ admits a non-trivial $(48,19)$-congruence with its quadratic twist by its discriminant, which (up to a square factor) is equal to $-19\cdot 43\cdot 39451$.

4.5.2 A review of the Mordell-Weil sieve

In order to search for points on the modular curves in Table 4.5 and prove Theorem 4.5.1 we briefly recall the Mordell-Weil sieve (see also [RSZ22, Section 10]).

Let $\phi\colon C \to E$ be a morphism defined over $\mathbb{Q}$ where $E/\mathbb{Q}$ is an elliptic curve and $C/\mathbb{Q}$ has genus ≥ 2. Let $P_1, ..., P_n \in E(\mathbb{Q})$ be generators for the Mordell-Weil group of E. For any good prime p for both C and E we have a commutative diagram

$$\begin{array}{ccccc} C(\mathbb{Q}) & \xrightarrow{\phi} & E(\mathbb{Q}) & \twoheadleftarrow & \mathbb{Z}^n \\ \downarrow & & \downarrow{\scriptstyle \mathrm{red}_p} & & \downarrow \\ \widetilde{C}(\mathbb{F}_p) & \xrightarrow{\widetilde{\phi}} & \widetilde{E}(\mathbb{F}_p) & \longleftarrow & \prod_{i=1}^n \mathbb{Z}/N_{p,i}\mathbb{Z} \end{array}$$

where $N_{p,i}$ is the order of $\mathrm{red}_p(P_i)$ in $\widetilde{E}(\mathbb{F}_p)$, and $\widetilde{C}$, $\widetilde{E}$, $\widetilde{\phi}$ are the reductions of C, E, and ϕ modulo p respectively. If there exists a rational point in the fibre of ϕ above $Q \in E(\mathbb{Q})$ then the fibre of $\widetilde{\phi}$ above $\mathrm{red}_p(Q)$ is non-empty. Writing $Q = \sum_{i=1}^n a_i P_i$ we obtain a set of congruence conditions on $a = (a_1, ..., a_n)$ in $\prod_{i=1}^n \mathbb{Z}/N_{p,i}\mathbb{Z}$.

Repeating this for a (finite) set of primes of good reduction for E and C allows us to give an (often large) bound, $B > 0$, such that every rational point on C is either known to us, or lies in the fibre above a point $Q = \sum_{i=1}^n a_i P_i$ such that $\max\{|a_i|\}_{i=1}^n > B$.

We are now able to prove Theorem 4.5.1.

Proof of Theorem 4.5.1. Suppose that an elliptic curve $E/\mathbb{Q}$ admits a non-trivial quadratic twist-type (N, r)-congruence. If N is a prime power, assumption (A) together with Proposition 4.2.4 shows that either $(N, r) \in \mathcal{S}$ or E is a quadratic twist of either $E_{(32,3)a}$ or $E_{(32,3)b}$.

It therefore suffices to consider the case where N is divisible by two or more distinct primes. If p is odd, the case when $N = 2p^l$ follows immediately. Otherwise by assumptions (A) and (C), together with Propositions 4.2.2 and 4.2.4, and Corollaries 4.3.5 and 4.3.6, if $(N, r) \notin \mathcal{S}$ then there exists an exceptional point on one of the 13 curves in Table 4.4 above $j(E)$.

We proved in Lemmas 4.4.3, 4.4.5, 4.4.8, 4.5.3, 4.5.5, and 4.5.6 that the modular curves appearing in Table 4.4 but not Table 4.5 have no exceptional points. Hence $j(E)$ must be an exceptional j-invariant for one of the 5 curves in Table 4.5.

The Mordell-Weil sieve shows that, except for the points on $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ and $X^+(\mathrm{ns}\,8, \mathrm{ns}\,3)$ above $j(E_{(30,7)})$ and $j(E_{(48,19)})$, the only exceptional points on these 5 curves lie in the fibre of $X^+(H_1, H_2) \to X(H_1^+, H_2^+)$ above a point of canonical height $\geq 10^{15}$. □

4.6 2-cover descent on genus 2 curves admitting a Richelot isogeny

We now study the rational points on the modular curve $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ in detail. In particular we will show that (up to a quadratic twist) $E_{(30,7)}$ is the only elliptic curve over $\mathbb{Q}$ admitting a non-trivial quadratic twist-type $(15, 7)$-congruence. The key observation is that since the Jacobian of $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ admits a Richelot isogeny we may use elliptic Chabauty to determine the rational points on $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$.

Let $C/\mathbb{Q}$ be a hyperelliptic curve of genus 2 given by a Weierstrass equation $y^2 = f(x)$, where $f(x) \in \mathbb{Q}[x]$ has degree 6. Further suppose that there exists an extension $K/\mathbb{Q}$ such that $f(x)$ factors as a product $f_1(x)f_2(x)$ over K where $f_1(x)$ has degree 4 and $f_2(x)$ has degree 2.

We consider the family of genus 3 double covers $C_d \to C$ over K, where C_d is given by

$$dy_1^2 = f_1(x)$$
$$dy_2^2 = f_2(x).$$

for some $d \in K^\times$. Let S be the union of the infinite places of K, the primes of K lying above 2 and the bad primes of C. We write

$$K(S, 2) = \{a \in K^\times/(K^\times)^2 : v_\mathfrak{p}(a) \equiv 0 \pmod 2 \text{ for each (finite) place } \mathfrak{p} \text{ of } K \text{ not in } S\}$$

where $v_\mathfrak{p} \colon K_\mathfrak{p} \to \mathbb{Z}$ is the normalised discrete valuation.

By étale descent (see e.g., [Bru03, Lemma 3.1]), for each point $P \in C(K)$ there exists a $d \in K(S, 2)$ such that P lifts to a K-point on C_d. However, a rational point $P \in C(\mathbb{Q})$ lifts to a point on $C_d(K)$ with rational x-coordinate. We therefore consider the family of genus 1 curves C'_d/K given by

$$C'_d : dy^2 = f_1(x).$$

Thus, to determine the x-coordinates supporting a rational point on C it suffices to determine the set of $P \in C'_d(K)$ such that $x(P) \in \mathbb{Q}$. If C'_d has a K-point then the method of elliptic

Chabauty provides a solution to this problem under the hypothesis that $\operatorname{rank} C'_d(K) \leq [K : \mathbb{Q}]$ (this has been implemented in `Magma`, see [Bru03] and [Bru06]).

Now $\mathrm{Jac}(C)$ admits a Richelot isogeny over $\mathbb{Q}$ if and only if there exists a degree 3, étale, $\mathbb{Q}$-algebra $L/\mathbb{Q}$ such that $f(x)$ admits such a factorisation $f(x) = \mathrm{Norm}_{L[x]/\mathbb{Q}[x]} Q(x)$ for some quadratic polynomial $Q(x) \in L[x]$ (see [BD11, Lemma 4.1]). In particular, for each number field L' appearing in the factorisation of L we obtain a factorisation $f(x) = f_1(x)f_2(x)$ defined over L' (but not over any proper subfields).

Remark 4.6.1. In the file `qtt-congruences/functions/twocover.m` in the supporting electronic data [Fre23b] we have implemented the above method for genus 2 curves $C/\mathbb{Q}$ given by a Weierstrass equation $y^2 = f(x)$ where $f(x)$ is irreducible and $\mathrm{Jac}(C)$ admits a Richelot isogeny.

4.6.1 The rational points on $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$

To illustrate, we study the rational points on the modular curve $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$. In particular we will show that (up to a quadratic twist) $E_{(30,7)}$ is the only elliptic curve over $\mathbb{Q}$ admitting a non-trivial quadratic twist-type $(15, 7)$-congruence. The key observation is that since the Jacobian of $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ admits a Richelot isogeny we may use elliptic Chabauty to determine the rational points on $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$. We have:

Proposition 4.6.2. *The rational points on the model for $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ given by (4.19) are exactly those listed in Table 4.6. In particular the only non-trivial quadratic twist-type $(15, 7)$-congruence over $\mathbb{Q}$ (up to taking quadratic twists) is between the elliptic curve $E_{(30,7)}$ (see Theorem 1.0.16) and its quadratic twist by -214663.*

j-invariant	Points	Quadratic twist	CM
0	$(1,1), (-2,1)$	-3	-3
$-3^3 \cdot 5^3$	$(-1,0), (0,0)$	-7	-7
$3^3 \cdot 5^3 \cdot 17^3$	$(1,-2), (-2,-2)$	-7	-28
$-2^{18} \cdot 3^3 \cdot 5^3$	$+\infty, -\infty$	-43	-43
$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	$(-1,-1), (0,-1)$	-67	-67
$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	$(3,-37), (-4,-37)$	-163	-163
$-\frac{3^3 \cdot 5^6 \cdot 199^3 \cdot 809^3 \cdot 5059^3}{61^{15}}$	$(3,36), (-4,36)$	-214663	

Table 4.6: All rational points on the model for $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ given by (4.19).

Proof. Let C be the genus 2 curve with short Weierstrass equation

$$y^2 = f(x) = 4x^6 + 12x^5 - 20x^3 + 12x + 1,$$

and note that replacing y by $2y + 1$ gives an isomorphism from the model for $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$ given by (4.19) to C. The `Magma` function `RankBounds` verifies that $J = \mathrm{Jac}(C)$ has rank 2. In particular Chabauty's method is not immediately applicable since $\operatorname{rank} J(\mathbb{Q}) = \dim J$.

Let θ be a root of $x^3 + x^2 - 3x + 3$ and let K be the cubic number field $\mathbb{Q}(\theta)$. Over K, $f(x)$ factors as a product of a quartic and quadratic polynomial $f_1(x)$ and $f_2(x)$, where

$$f_1(x) = 4x^4 + 8x^3 + (-2\theta^2 - 2\theta)x^2 + (-2\theta^2 - 2\theta - 4)x + \theta^2 - 2\theta + 1$$
$$f_2(x) = x^2 + x + (\theta^2 + \theta - 4)/2.$$

Let S be the union of the set of infinite places of K and set of places of K lying above $2, 3$, or 5. We consider the family of 64 genus 3 double covers $C_d \to C$ over K indexed by $d \in K(S,2)$, and the corresponding family of genus 1 curves C'_d.

Of these 64 genus 1 curves, 60 have a local obstruction at a place $v \in S$ - that is $C'_d(K_v) = \emptyset$ for some $v \in S$. The remaining four curves are when $d \in \{1, \theta^2+2\theta-1, \theta^2+\theta-3, 2\theta^2+2\theta-3\}$. Each of these four curves C'_d have a K-rational point and have Mordell-Weil rank ≤ 2 - in particular elliptic Chabauty may be applied (implemented in `Magma` as the function `Chabauty`). We find that the x-coordinates supporting a rational point on C are contained in the set $\{-4, -2, -1, -1/2, 0, 1, 3, \infty\}$. Each of these x-coordinates, except $-1/2$, gives rise to a rational point on C. Proposition 4.6.2 then follows from an elementary calculation. □

4.6.1.1 A solution to the class number 1 problem

It was conjectured by Gauss that the only orders in an imaginary quadratic field with class number 1 are those with discriminants -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, and -163. It is well know that there is a bijective correspondence between orders, $\mathcal{O}$, in an imaginary quadratic field with class number 1 and j-invariants of elliptic curves $E/\mathbb{Q}$ with CM by $\mathcal{O}$ (see [Sil94, Chapter 2]). In this case $j(E)$ is an integer (see [Sil94, Chapter 2 Section 6]).

Since CM elliptic curves give rise to rational points on the modular curve $X(\operatorname{ns} {p^l}^+)$ for suitable p^l (see [Bar10, Section 4] and [Ser97, A.5]) this suggests that to prove the class number 1 problem it is enough to find all the integral points (that is, points lying above j-invariants which are integers) on $X(\operatorname{ns} {p_1^{l_1}}^+, ..., \operatorname{ns} {p_n^{l_n}}^+)$ where $p_1, ..., p_n$ are distinct prime numbers. This approach has successfully been used to give a solutions to the class number one problem in all cases where the genus of $X(\operatorname{ns} {p_1^{l_1}}^+, ..., \operatorname{ns} {p_n^{l_n}}^+)$ is ≤ 2 (see [Bar10], [Ser97, p. 197], and the references therein).

We now discuss a slightly different (but closely related) approach to the class number 1 problem via the modular curves $X^+(\operatorname{ns} p^l, \operatorname{ns} q^k)$ constructed in Section 4.3. We are careful not to quote the results from Section 4.2 since they rely upon the classification of elliptic curves $E/\mathbb{Q}$ with CM.

Suppose that an elliptic curve $E/\mathbb{Q}$ with $j(E) \neq 0, 1728$ has CM by an order in an imaginary quadratic field K. Let $-D$ be the discriminant of K, where D is a positive integer. Let p be a prime number and let $l \geq 1$ be an integer. If p is inert in K then $\bar{\rho}_{E,p^l}(G_{\mathbb{Q}})$ is contained in the normaliser of a non-split Cartan subgroup and $\bar{\rho}_{E,p^l}(G_{\mathbb{Q}(\sqrt{-D})})$ is contained in the corresponding Cartan subgroup (see [Bar10, Proposition 4.1] and [Ser97, A.5]). By Proposition 4.1.4 E is therefore $(p^l, -\xi)$-congruent to its quadratic twist by $-D$.

Each prime number $p < \frac{1+D}{4}$ is inert in K (see the discussion following Proposition 4.10 in [Bar10] and [Ser97, p. 190]). Hence if an elliptic curve $E/\mathbb{Q}$ has CM by an order in an imaginary quadratic field K of discriminant $-D \leq -4p$, then E is $(p^l, -\xi)$-congruent to its quadratic twist by $-D$.

Now fix a pair of prime powers p^l, q^k. By the preceding discussion if $E/\mathbb{Q}$ has CM by an order in an imaginary quadratic field K of discriminant $-D \leq \min\{-4p, -4q\}$ then there exists a integral point in the fibre of the j-map $X(\operatorname{ns} {p^l}^+, \operatorname{ns} {q^k}^+) \to X(1)$ above $j(E)$.

But as we observed, E is $p^l q^k$-congruent to E^{-D}. Therefore by Lemma 4.3.4 there exists a integral point on $X^+(\operatorname{ns} p^l, \operatorname{ns} q^k)$ above $j(E)$.

In Proposition 4.6.2 we determined all the rational (hence integral) points on $X^+(\operatorname{ns} 3, \operatorname{ns} 5)$. By taking $p^l = 3$ and $q^k = 5$ in the above discussion it follows from Proposition 4.6.2 that the only imaginary quadratic fields with class number 1 and discriminant ≤ -20 have discriminant -43, -67, and -167. Hence we have a solution to the class number one problem.

Remark 4.6.3. Level 15 proofs of the class number 1 problem have previously been given by Siegel [Sie68] and I. Chen [Che99] by analysing integral points on the rank 1 elliptic curve $X(\mathrm{ns}\,3^+, \mathrm{ns}\,5^+)$. We have instead analysed the rational points on the double cover $X^+(\mathrm{ns}\,3, \mathrm{ns}\,5)$.

Chapter 5

Families of (N, r)-congruent elliptic curves

The primary goal of this chapter is to prove Theorems 1.0.9–1.0.12 from the introduction.

We begin in Section 5.1 by using invariant theoretic techniques to find simple (symmetric) conditions for a pair of elliptic curves to be 2, 3, or 4-congruent in Theorem 5.1.4 (note that our condition for 2-congruence was already proved by Fisher, see [Fis20, Lemma 3.5]). We also compute symmetric equations for the surfaces $Z_{5,2}$ and $Z_{7,1}$ (such equations are given for $Z_{5,1}$ and $Z_{7,2}$ by Kumar [Kum15]).

In Section 5.2 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. We employ this description to compute explicit models for the surfaces $Z_{N,r}$ in Theorem 1.0.9 in Section 5.3.

In Section 5.4 we identify the modular curves in Section 2.3.5 on our models for the surfaces $Z_{N,r}$. We prove Theorem 1.0.10 in Section 5.5 by finding curves with infinitely many rational points (and which do not arise as Hecke correspondences) on our models for $Z_{N,r}$. 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 5.5.1, 5.5.3, and 5.5.4) and similarly we find such an example of $(14, 1)$-congruent elliptic curves over $\mathbb{Q}(t)$ in Example 5.5.5. In Example 5.5.2 we give an example of a pair of geometrically non-isogenous $(12, 5)$-congruent elliptic curves defined over $\mathbb{Q}(\mathcal{C})$ where $\mathcal{C}/\mathbb{Q}$ is an elliptic curve of rank 1.

We conclude in Sections 5.6 and 5.7 by giving further examples of rational points and curves on our models for $Z_{N,r}$. In particular, we prove Theorems 1.0.11 and 1.0.12.

For notational simplicity in this chapter we use $W_{N,r}$ to denote (a smooth surface birational to) the symmetric Hilbert modular surface $Z_{N,r}/\tau$ defined in Section 2.3.6.

5.1 Symmetric equations for families of N-congruent elliptic curves

Several approaches have been applied to parametrising (universal) families of 2, 3, 4, 5 and 7-congruent elliptic curves.

Equations for $X_E^1(N)$ when $N = 2$, 3, 4, and 5 were computed by Rubin and Silverberg (see [RS95, Sil97, RS01]). Using a direct approach Lario–Rio computed equations for $X_E^r(3)$ when $r = 1$ and 2 (see [LR95, Section 3]).

Fisher [Fis12] described how when $N = 2$, 3, 4, and 5 the curve $X_E^r(N)$ is related to the Hessian of a genus one model of degree N, and hence computed explicit equations for $X_E^r(N)$ using classical invariant theory. When $N = 3$ similar approaches have been employed in [Kuw12] and [ATT18]. 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 [Kum15] (for every $N \leq 11$), Bröker–Howe–Lauter–Stevenhagen [BHLS15] (when $N = 3$), and Bruin–Doerksen [BD11] (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'.

Equations for the twist $X_E^r(7)$ have been computed by Halberstadt–Kraus [HK03] and Poonen–Schaefer–Stoll [PSS07] when $r = 1$ and 3 respectively (see also [Fis14]). Chen computed a parametrisation for $Z_{7,1}$ and gave a fibration for the elliptic K3 surface $Z_{7,3}$ [Che16, Section 8.2] (see also [Fis20]).

Our approach is to use Proposition 2.3.10 to compute models for the surfaces $Z_{N,r}$ for each $(N, r) = (2, 1)$, $(3, 1)$, $(3, 2)$, $(4, 1)$, $(4, 3)$, $(5, 2)$, and $(7, 1)$. 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 Theorem 5.1.4). Indeed, it is this observation which makes it practical for us to compute (birational) models for $Z_{N,r}$ via fibre products.

5.1.1 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 Υ_N. The method we describe has been successfully employed by Fisher to compute birational models for $Z_{13,r}$ and $Z_{17,r}$ (see [Fis19] and [Fis21]).

Recall that when $N \neq 2$ we write $\Upsilon'_N = \Upsilon_N$ and when $N = 2$ we write Υ'_2 for the unique non-split extension of Υ_2. Suppose that we have the data of:

- an embedding $X(N) \hookrightarrow \mathbb{P}^n$ for some $n \geq 1$, and
- a representation $\rho\colon \Upsilon'_N \to \mathrm{GL}_{n+1}(\overline{K})$ such that the induced projective representation is G_K-equivariant and gives the action of Υ_N on $X(N)$.

Let $\Lambda_r \subset \mathrm{im}(\rho) \times \mathrm{im}(\rho)$ denote the pre-image of $(\bar{\rho} \times \bar{\rho})(\mathbf{\Delta}_r)$. Let $f(x_0, ..., x_n, x'_0, ..., x'_n)$ be a polynomial which is homogeneous of degrees m and m' in the two sets of variables.

Definition 5.1.1. We say that f is an *r–bi-invariant* if f is invariant under the action of Λ_r on the polynomial ring $K[x_0, ..., x_n, x'_0, ..., x'_n]$. If $f(x_0, ..., x_n, x'_0, ..., x'_n) = f(x'_0, ..., x'_n, x_0, ..., x_n)$ we say that f is *symmetric*.

The action of $\mathbf{\Delta}_r$ on $X(N) \times X(N)$ induces an action on $Y(N) \times Y(N) = \operatorname{Spec} R$. By Proposition 2.3.10 the surface $Z_{N,r}$ is birational to $\operatorname{Spec} R^{\mathbf{\Delta}_r}$. To compute a birational model for $Z(N, r)$ it is enough to compute generators and relations for the K-algebra $R^{\mathbf{\Delta}_r}$, 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 $S \subset R^{\mathbf{\Delta}_r}$ is the subalgebra of elements invariant under the natural involution on $Y(N) \times Y(N)$, then $W_{N,r}$ is birational to $\operatorname{Spec} S$.

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

If $A \subset K[x_0, ..., x_n, x'_0, ..., x'_n]$ 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 $Z_{N,r} \dashrightarrow \operatorname{Spec} R^{\mathbf{\Delta}_r} \dashrightarrow \operatorname{Proj} A$. Moreover if $B \subset A$ is the subalgebra of symmetric r–bi-invariants, then we have a rational map $W_{N,r} \dashrightarrow \operatorname{Spec} S \dashrightarrow \operatorname{Proj} B$.

Consider non-zero r–bi-invariants $w_0, ..., w_k \in K[x_0, ..., x_n, x'_0, ..., x'_n]$ 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). Consider the rational map

$$\varphi_{N,r} \colon X(N) \times X(N) \to \mathbb{P}^k$$

given by $([x_0 : ... : x_n], [x'_0 : ... : x'_n]) \mapsto [w_0 : ... : w_k]$. Since $w_0, ..., w_k$ are symmetric and invariant under the action of Λ_r we obtain a factorisation

$$\begin{array}{ccc} X(N) \times X(N) & & \\ \downarrow & \overset{\varphi_{N,r}}{\searrow} & \\ W_{N,r} & \overset{\psi_{N,r}}{\dashrightarrow} & \mathrm{im}(\varphi_{N,r}). \end{array}$$

When $N = 2$, 3, 4, 5, and 7 we will carefully choose symmetric r–bi-invariants $w_0, ..., w_k$ so that $\psi_{N,r}$ is birational.

5.1.2 Symmetric bi-invariants

We now give choices of r–bi-invariants such that the map $\psi_{N,r}$ is birational for each $N = 2$, 3, 4, 5, and 7. We consider the action of Υ'_N on $X(N) \cong \mathbb{P}^1$ via the representation ρ in Section 2.2.1.

Remark 5.1.2. Note that in the case when $N = 4$ the actions of Λ_1 and Λ_3 on $K[x_0, x_1, x'_0, x'_1]$ via ρ 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 [BD11, Corollary 7.4] or Proposition 4.1.5 for a more general statement). In particular, if E and E' are $(4, 1)$-congruent, then the quadratic twist of E by its discriminant $E^{\Delta(E)}$ 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 $D = D(x_0, ..., x_n)$, $c_4 = c_4(x_0, ...x_n)$, and $c_6 = c_6(x_0, ..., x_n)$ defined in Section 2.2.1. We let $D' = D(x'_0, ..., x'_n)$, $c'_4 = c_4(x'_0, ..., x'_n)$, and $c'_6 = c_6(x'_0, ..., x'_n)$. By Lemma 2.2.2 the forgetful map $X(N) \times X(N) \to Z_1$ is given by $([x_0 : ... : x_n], [x'_0 : ... : x'_n]) \mapsto (j, j')$ where $j = c_4^3/D^N$ and $j' = c_4'^3/D'^N$. We write $J = j/1728$ (similarly $J' = j'/1728$).

5.1.2.1 Case $(N, r) = (2, 1)$

Define the bi-invariant form $I_{1,1} = 192x_0x'_0 + x_1x'_1$. We let

$$w_0 = I_{1,1}^3, \quad w_1 = 2I_{1,1}c_4c'_4, \quad \text{and} \quad w_2 = 1728DD'.$$

First note that $c_6c'_6 = 4w_0 - \frac{3}{2}w_1 - w_2$. In particular we have

$$JJ' = \frac{w_1^3}{8w_0w_2^2},$$

$$(J-1)(J'-1) = \left(\frac{4w_0 - \frac{3}{2}w_1 - w_2}{w_2}\right)^2.$$

Let $S_{2,1} = \mathbb{P}^2$ with coordinates w_0, w_1, w_2. Then there is a commutative diagram

$$\begin{array}{ccc} W_{2,1} & \overset{\psi_{2,1}}{\dashrightarrow} & S_{2,1} \\ & \searrow & \downarrow \\ & & W_1 \end{array}$$

where the map $S_{2,1} \dashrightarrow W_1$ is given by the rational functions JJ' and $(J-1)(J'-1)$ above.

5.1.2.2 Case $(N, r) = (4, r)$

Consider the r-bi-invariant forms

$$\begin{aligned} I_{2,2} &= 16(x_0x_1' - x_1x_0')^2, \\ I_{4,4} &= 256x_0^4x_0'^4 + 16x_0^4x_1'^4 + 192x_0^2x_1^2x_0'^2x_1'^2 + 16x_1^4x_0'^4 + x_1^4x_1'^4, \end{aligned}$$

and define

$$w_0 = I_{4,4}^3, \quad w_1 = 2I_{4,4}c_4c_4', \quad w_2 = 3I_{2,2}^2I_{4,4}^2, \quad \text{and} \quad w_3 = 72I_{2,2}I_{4,4}DD'.$$

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 $\varphi_{4,r} \colon X(4) \times X(4) \dashrightarrow \mathbb{P}^3$ is the quadric surface

$$S(4, r) = \{192w_0^2 - 96w_0w_1 + 128w_0w_3 + 48w_0w_2 - w_2^2 = 0\} \subset \mathbb{P}^3.$$

Let $H = \ker\left(\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})\right)$, 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_4c_4', and $(DD')^2$ are invariant under the action of $H \times H$. In particular w_0, w_1 and w_3^2/w_2 are invariant under $H \times H$ and we have the relation $c_6c_6' = 4w_0 - \frac{3}{2}w_1 - (w_3^2/w_2)$.

Using the equations for the forgetful map $X(4) \to X(2)$ given in Section 2.2.1 we see that the diagram

$$\begin{array}{ccc} W_{4,r} & \overset{\psi_{4,r}}{\dashrightarrow} & S_{4,r} \\ \downarrow & & \downarrow \\ W_{2,1} & \overset{\psi_{2,1}}{\dashrightarrow} & S_{2,1} \end{array}$$

commutes, where the map $S_{4,r} \dashrightarrow S_{2,1}$ is given by $[w_0 : w_1 : w_2 : w_3] \mapsto [w_0 : w_1 : w_3^2/w_2]$.

5.1.2.3 Case $(N, r) = (3, 1)$

We consider the r-bi-invariant forms

$$\begin{aligned} I_{2,2} &= 3(54x_0^2x_0'^2 + x_0x_1x_1'^2 + x_1^2x_0'x_1'), \\ I_{6,6} &= 3^6(x_0x_1' - x_1x_0')^6, \end{aligned}$$

and define

$$w_0 = 12I_{6,6}, \quad w_1 = 4I_{2,2}^3, \quad w_2 = c_6c_6', \quad \text{and} \quad w_3 = 144DD'.$$

The image of the rational map $\varphi_{3,1}\colon X(3) \times X(3) \dashrightarrow \mathbb{P}^3$ is the cubic surface

$$S_{3,1} = \{8w_0^2w_1 - 60w_0w_1^2 + 12w_0w_1w_2 + 36w_0w_1w_3 - 9w_1^3 + 27w_1^2w_3 - 27w_1w_3^2 + 9w_3^3 = 0\} \subset \mathbb{P}^3.$$

Additionally there are the relations:

$$JJ' = \frac{w_1 A(w_0, w_1, w_2)}{36w_3^3},$$

$$(J-1)(J'-1) = \frac{w_1 w_2^2}{4w_3^3},$$

where

$$\begin{aligned} A(w_0, w_1, w_2) = {} & 4w_0^2 - 192w_0w_1 + 12w_0w_2 + 72w_0w_3 + 603w_1^2 - 144w_1w_2 \\ & - 918w_1w_3 + 9w_2^2 + 108w_2w_3 + 351w_3^2. \end{aligned}$$

We therefore have a commutative diagram

$$\begin{array}{ccc} W_{3,1} & \overset{\psi_{3,1}}{\dashrightarrow} & S_{3,1} \\ & \searrow & \downarrow \\ & & W_1 \end{array}$$

where the morphism $S_{3,1} \dashrightarrow W_1$ is given by the rational functions JJ' and $(J-1)(J'-1)$ above.

5.1.2.4 Case $(N, r) = (3, 2)$

Define the r-bi-invariant $I_{2,2} = (18x_0x_0' + x_1x_1')^2$ and let

$$w_0 = \tfrac{3}{2}(3I_{2,2}^2 - c_4c_4' - 144DD'), \quad w_1 = c_4c_4', \quad \text{and} \quad w_2 = 144DD'.$$

Let $S_{3,2} = \mathbb{P}^2$. The bi-invariants w_0, w_1, and w_2 are linearly independent, so the rational map $\varphi_{3,2}\colon X(3) \times X(3) \dashrightarrow S_{3,2}$ is surjective. We have the relations

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

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

Therefore there is a commutative diagram

$$\begin{array}{ccc} W_{3,2} & \overset{\psi_{3,2}}{\dashrightarrow} & S_{3,2} \\ & \searrow & \downarrow \\ & & W_1 \end{array}$$

where the map $S_{3,2} \dashrightarrow W_1$ is given by the rational functions JJ' and $(J-1)(J'-1)$ above.

5.1.2.5 Case $(N, r) = (5, 2)$

Consider the following r–bi-invariants:

$$I_{4,4} = x_0^4 x_0' x_1'^3 - x_0^3 x_1 x_0'^4 + 3x_0^2 x_1^2 x_0'^2 x_1'^2 + x_0 x_1^3 x_1'^4 - x_1^4 x_0'^3 x_1',$$
$$I_{7,1} = x_0^7 x_1' + 7x_0^5 x_1^2 x_0' + 7x_0^2 x_1^5 x_1' - x_1^7 x_0'$$

and define the symmetric r–bi-invariants

$$w_0 = I_{4,4}^5, \quad w_1 = c_4 c_4', \quad w_2 = I_{4,4} I_{7,1} I_{1,7}, \quad \text{and} \quad w_3 = 12 I_{4,4}^2 DD',$$

where $I_{1,7}$ denotes the form obtained from $I_{7,1}$ under the involution swapping the roles of $[x_0 : x_1]$ and $[x_0' : x_1']$. Let $S_{5,2}$ denote the image of the induced rational map $\varphi_{5,2} \colon X(5) \times X(5) \dashrightarrow \mathbb{P}^3$. We define a rational map $\mathbb{A}^2 \dashrightarrow \mathbb{P}^3$ by $(a, b) \mapsto [\Phi_0 : \Phi_1 : \Phi_2 : \Phi_3]$, where

$$\begin{aligned}
\Phi_0 &= b, \\
\Phi_1 &= -16(a^4 + 4a^3 - 10a^2 b + 6a^2 - 24ab^2 - 5ab + 4a + 16b^2 + 14b + 1), \\
\Phi_2 &= 4b(a-3)^2, \\
\Phi_3 &= 12b(2a - b + 1).
\end{aligned}$$

Using `Magma` we check that the bi-invariants w_i satisfy the equation for (closure of) the image of this map in $\mathbb{P}^3$. We therefore obtain a rational map $\Phi_{5,2} \colon \mathbb{A}^2 \dashrightarrow S_{5,2}$ given by $(a, b) \mapsto [\Phi_0 : \Phi_1 : \Phi_2 : \Phi_3]$. Using `Magma` we check that $\Phi_{5,2}$ is in fact birational.

It is clear that $JJ' = \frac{w_0^2 w_1^3}{12 w_3^5}$. Similarly we may express $(J-1)(J'-1)$ as a rational function whose numerator and denominator have degree 7 in w_i. It is simple to check with computer algebra that (after pulling back along $\Phi_{5,2}$) we have

$$JJ' = \frac{\boldsymbol{A}_{(5,2)}^3}{\boldsymbol{D}_{(5,2)}}$$

$$(J-1)(J'-1) = \frac{\boldsymbol{B}_{(5,2)}^2}{\boldsymbol{D}_{(5,2)}}$$

where the polynomials $\boldsymbol{A}_{(5,2)}$, $\boldsymbol{B}_{(5,2)}$, and $\boldsymbol{D}_{(5,2)} \in \mathbb{Z}[a, b]$ are given in Appendix A.1.

5.1.2.6 Case $(N, r) = (7, 1)$

Consider the embedding $X(7) \hookrightarrow \mathbb{P}^2$ as the Klein quartic with Υ_7 acting linearly as described in Section 2.2.1. Define the following r–bi-invariants

$$\begin{aligned}
I_{2,2} &= x_0^2 x_0' x_1' + x_0 x_1 x_0'^2 + x_0 x_2 x_2'^2 + x_1^2 x_1' x_2' + x_1 x_2 x_1'^2 + x_2^2 x_0' x_2', \\
I_{3,1} &= x_0^3 x_1' + 3x_0^2 x_1 x_0' + 3x_0 x_2^2 x_2' + x_1^3 x_2' + 3x_1^2 x_2 x_1' + x_2^3 x_0', \\
I_{3,3} &= x_0^3 x_0'^2 x_2' - x_0^2 x_1 x_1' x_2'^2 + x_0^2 x_2 x_0'^3 - x_0^2 x_2 x_1'^2 x_2' - x_0 x_1^2 x_0' x_2'^2 + x_0 x_1^2 x_1'^3 - 4x_0 x_1 x_2 x_0' x_1' x_2' \\
&\quad - x_0 x_2^2 x_0' x_1'^2 + x_1^3 x_0' x_1'^2 - x_1^2 x_2 x_0'^2 x_2' - x_1 x_2^2 x_0'^2 x_1' + x_1 x_2^2 x_2'^3 + x_2^3 x_1' x_2'^2.
\end{aligned}$$

Now consider the symmetric r–bi-invariants

$$w_0 = I_{2,2}^3, \quad w_1 = I_{3,3}^2, \quad w_2 = I_{3,1} I_{1,3} I_{2,2}, \quad \text{and} \quad w_3 = DD',$$

where $I_{1,3}$ is the bi-invariant obtained by swapping the roles of x_i and x_i' in $I_{3,1}$. It is simple to check with computer algebra that the bi-invariants w_0, w_1, w_2, and w_3 satisfy the single relation $Q = 3w_0^2 + 2w_0w_1 - w_0w_2 + w_0w_3 - w_1w_2 = 0$ modulo the ideal $I(X(7) \times X(7))$. In particular, the image of the map $\varphi_{7,1} \colon X(7) \times X(7) \dashrightarrow \mathbb{P}^3$ is the quadric surface $S_{7,1}$ given by the vanishing of Q. Let $\Phi_{7,1} \colon \mathbb{A}^2 \dashrightarrow S_{7,1}$ be the birational map given by

$$(a, b) \mapsto [(b-1)^2 : b^2 - 1 : (b-1)(4a + 3b - 1) : (8ab + b^2 + 4b - 1)].$$

Then, modulo $I(X(7) \times X(7))$, we have

$$JJ' = \frac{\boldsymbol{A}_{(7,1)}^3}{\boldsymbol{D}_{(7,1)}}$$

$$(J-1)(J'-1) = \frac{\boldsymbol{B}_{(7,1)}^2}{\boldsymbol{D}_{(7,1)}}$$

where the polynomials $\boldsymbol{A}_{(7,1)}$, $\boldsymbol{B}_{(7,1)}$, and $\boldsymbol{D}_{(7,1)} \in \mathbb{Z}[a, b]$ are given in Appendix A.1.

The relations above are too complicated to check naively, even with the assistance of computer algebra. Instead we use the following consequence of Bezout's theorem, which is directly analogous to [Fis19, Lemma 6.2].

Lemma 5.1.3. *Let $f \in \mathbb{Q}[x_0, x_1, x_2, x_0', x_1', x_2']$ be a bi-invariant under the action of Δ_1 on $X(7) \times X(7)$. Let $\mathcal{S} \subset X(7)(\mathbb{C})$ be a set of n points. Suppose that f has homogeneous bi-degree (m, m) and vanishes at every point $(P, Q) \in \mathcal{S} \times \mathcal{S}$. If $n > 4m$, then f vanishes modulo $I(X(7) \times X(7))$.*

5.1.3 Symmetric conditions for 2, 3, and 4-congruences

We now prove Theorem 5.1.4. 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 [Fis12] and of Rubin and Silverberg [RS95, Sil97, RS01], the conditions in Theorem 5.1.4 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 [Fis20, Lemma 3.5] with a different (computational) proof using the equations for $X_E^1(2)$. It is also possible to verify Theorem 5.1.4 using the equations of Fisher and of Rubin and Silverberg for $X_E^r(N)$ (the necessary transformations are recorded in the electronic data [Fre23b]). We opt for a more geometric approach which explains how we found these conditions.

Theorem 5.1.4. *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, Δ and c_4', c_6', Δ' 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 α and β satisfy the conditions of* (i) *and*

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

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

where $\delta = 3(JJ' - (\alpha+1)^2)$.

(iii) *If $J \neq J'$ and $(\sqrt[3]{J}+1)(\sqrt[3]{J'}+1) \neq 1$ (for all choices of cube roots) then E and E' are $(3,1)$-congruent if and only if there exists $\alpha, \beta, \tau \in K$ such that*

$$\alpha^3 - 3JJ'\alpha - JJ'(J+J') = 0,$$

$$\beta^4 - 6(J-1)(J'-1)\beta^2 - 8(J-1)^2(J'-1)^2\beta - 3(4\alpha+1)(J-1)^2(J'-1)^2 = 0,$$

$$\tau^2 = 3c_6c_6'\delta,$$

where

$$\delta = -6\left(\frac{2\beta^3 - (5\alpha+2)\beta^2 - 10(J-1)(J'-1)\beta + 3(J-1)(J'-1)(13\alpha - 2 + 6(J+J'))}{\beta^3 - 3(J-1)(J'-1)\beta - 2(J-1)^2(J'-1)^2}\right).$$

(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*

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

$$\beta^4 - 6(\alpha+1)(J-1)(J'-1)\beta^2 - 8(J-1)^2(J'-1)^2\beta - 3(\alpha-1)^2(J-1)^2(J'-1)^2 = 0,$$

$$\tau^2 = \begin{cases} 3c_6c_6'\beta & \text{if } \beta \neq 0, \\ -2c_6c_6' & \text{if } \beta = 0. \end{cases}$$

Remark 5.1.5. Note that in Theorem 5.1.4:

(i) The conditions on α are convenient ways of writing the conditions that $\Delta\Delta'$ is a square when $N = 2, 4$, that Δ/Δ' is a cube when $(N,r) = (3,1)$, and that $\Delta\Delta'$ is a cube when $(N,r) = (3,2)$.

When $N = 4$ the term δ is equal to Δ (and Δ') up to a square factor (modulo squares we have $\delta/\Delta \equiv 3\delta(J-1) \equiv (\alpha - (J-1))^2$). The conditions on τ are therefore equivalent to the fact that Δ/Δ' 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 α in Theorem 5.1.4 may have more than one root in K. Indeed, the theorem would be false if we required the existence of a β (and γ, τ) *for a fixed choice of α (and β).* 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 β has no root when the negative root α is chosen. When α is chosen to be positive the polynomial in β splits, but the polynomial in γ has a root for only one of the possible choices of β.

When $(N,r)=(3,1)$ a similar example is given over $\mathbb{Q}(\zeta_3)$ by the pair `15.a1` and `15.a5` and when $(N,r)=(3,2)$ by the pair `11.a1` and `11.a2`.

(iii) When $(N,r)=(3,1)$ the condition that $(\sqrt[3]{J}+1)(\sqrt[3]{J'}+1)\neq 1$ is necessary. The elliptic curves with LMFDB labels `245.a1` and `1323.s1` are not (quadratic twists of) $(3,1)$-congruent elliptic curves, however there do exist $\alpha,\beta\in\mathbb{Q}$ satisfying Theorem 5.1.4(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.b2` 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 5.1.4. 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 $P_\alpha\in K[J,J',\alpha]$, $P_\beta\in K[J,J',\alpha,\beta]$ (and $P_\gamma\in K[J,J',\alpha,\beta,\gamma]$ when $N=4$) be the polynomials from the statement of the theorem. Define the surface

$$\mathcal{Z}_{N,r}=\begin{cases}\operatorname{Spec}K[J,J',\alpha,\beta]/(P_\alpha,P_\beta) & \text{when } N=2,3, \text{ and}\\ \operatorname{Spec}K[J,J',\alpha,\beta,\gamma]/(P_\alpha,P_\beta,P_\gamma) & \text{when } N=4.\end{cases}$$

Similarly let

$$\mathcal{W}_{N,r}=\begin{cases}\operatorname{Spec}K[JJ',(J-1)(J'-1),\alpha,\beta]/(P_\alpha,P_\beta) & \text{when } N=2,3, \text{ and}\\ \operatorname{Spec}K[JJ',(J-1)(J'-1),\alpha,\beta,\gamma]/(P_\alpha,P_\beta,P_\gamma) & \text{when } N=4.\end{cases}$$

Write, in the notation of Section 5.1.2:

$$\begin{aligned}
&(N,r)=(2,1): && \alpha=\frac{4w_0-\frac{3}{2}w_1-w_2}{w_2} && \beta=w_1/w_2 && \\
&(N,r)=(4,r): && \alpha=\frac{4w_0-\frac{3}{2}w_1-(w_3^2/w_2)}{(w_3^2/w_2)} && \beta=\frac{w_1}{w_3^2/w_2} && \gamma=\frac{JJ'w_2}{\beta w_3}\\
&(N,r)=(3,1): && \alpha=\frac{\eta}{12w_0w_3^2} && \beta=\frac{(\frac{3}{2}(3w_1-w_3)/w_3)^2-3(\alpha+1)}{2} &&\\
&(N,r)=(3,2): && \alpha=w_1/w_2 && \beta=\frac{(w_0/w_2)^2-3(\alpha^2+\alpha+1)}{2} &&
\end{aligned}$$

where $\eta=(w_0+3w_1-3w_3)(8w_0w_1-3w_1^2+6w_1w_3-3w_3^2)$. Then these choices induce maps $S_{N,r}\dashrightarrow\mathcal{W}_{N,r}$ (where $S_{N,r}$ are the surfaces defined in Sections 5.1.2.1–5.1.2.4) and therefore maps $W_{N,r}\dashrightarrow\mathcal{W}_{N,r}$.

In particular we have a commutative diagram

$$\begin{array}{ccc} Z_{N,r} & \xrightarrow{\ \pi\ } & \mathcal{Z}_{N,r}\\ & {\scriptstyle\mathcal{J}_Z}\searrow \quad \swarrow{\scriptstyle\mathcal{J}_{\mathcal{Z}}} & \\ & Z_1 & \end{array}$$

where $\mathcal{J}_Z$ and $\mathcal{J}_{\mathcal{Z}}$ are morphisms. The degree of the morphism $\mathcal{J}_Z$ is equal to $|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|/2$ and the degree of $\mathcal{J}_{\mathcal{Z}}$ may be read off from the degrees of the polynomials P_α, P_β, and P_γ. Since these degrees are equal for each (N,r) the map π is birational.

Write $R = K[J, J']\left[\frac{1}{JJ'(J-1)(J'-1)(J-J')\xi}\right]$ where $\xi = 1$ if $N \in \{2, 4\}$ or $(N, r) = (3, 2)$ and

$$\xi = (JJ')^3 + 3(JJ')^2(J + J') - 27(JJ')^2 + 3(JJ')(J + J')^2 + (J + J')^3$$

when $(N, r) = (3, 1)$. Letting $Z_1' = \operatorname{Spec} R$ we have a natural open immersion $Z_1' \subset Z_1$. Let $Z_{N,r}'$ and $\mathcal{Z}_{N,r}'$ be the pre-images of Z_1' under the maps $\mathcal{J}_Z$ and $\mathcal{J}_{\mathcal{Z}}$ respectively.

Explicitly $Z_{N,r}'$ and $\mathcal{Z}_{N,r}'$ are the surfaces given by deleting the points on $Z_{N,r}$ and $\mathcal{Z}_{N,r}$ above the loci:

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

We next show that π extends to an isomorphism $\widetilde{\pi}\colon Z_{N,r}' \to \mathcal{Z}_{N,r}'$. Note that the morphism $Z_{N,r}' \to Z_1'$ is finite étale since $X(N) \to X(1)$ is finite étale away from $j = 0, 1728, \infty$.

When $N = 2, 3$ we see that the finite morphism $\mathcal{Z}_{N,r}' \to Z_1'$ factors via

$$\mathcal{Z}_{N,r}' = \operatorname{Spec} R[\alpha, \beta]/(P_\alpha, P_\beta) \longrightarrow \operatorname{Spec} R[\alpha]/(P_\alpha) \longrightarrow Z_1'.$$

and similarly when $N = 4$ with an extra factor accounting for the polynomial in γ. In particular when $N = 2, 3$, to show that $\mathcal{Z}_{N,r}' \to Z_1'$ 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 `Magma` and using the fact that 2, 3, J, J', $J - 1$, $J' - 1$, $J - J'$, and ξ are units in R shows that the ideals $\left(P_\alpha, \frac{\partial P_\alpha}{\partial\alpha}\right)$, $\left(P_\alpha, P_\beta, \frac{\partial P_\beta}{\partial\beta}\right)$, and $\left(P_\alpha, P_\beta, P_\gamma, \frac{\partial P_\gamma}{\partial\gamma}\right)$ contain 1. In particular, the morphisms $\mathcal{Z}_{N,r}' \to Z_1'$ are finite étale.

Applying the following lemma with $X = \mathcal{Z}_{N,r}'$, $Y = Z_{N,r}'$, and $S = Z_1'$ shows that π extends to an isomorphism $\widetilde{\pi}\colon \mathcal{Z}_{N,r}' \to Z_{N,r}'$.

Lemma 5.1.6. *Let X, Y, and S be integral K-varieties. Suppose that S is smooth and that there exists a commutative diagram*

$$\begin{array}{ccc} X & \overset{\pi}{\dashrightarrow} & Y \\ & {\scriptstyle p_X}\searrow \quad \swarrow{\scriptstyle p_Y} & \\ & S & \end{array}$$

where p_X and p_Y are finite étale morphisms and π is birational. Then π extends uniquely to an isomorphism $\widetilde{\pi}\colon X \to Y$.

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

By assumption S is integral and non-singular, 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 [Stacks, Lemma 0BQG] noting the proof of [Stacks, Lemma 0BQI]). In particular the isomorphism $\pi|_U\colon U \to V$ extends uniquely to a morphism $\widetilde{\pi}\colon X \to Y$. A symmetrical argument shows that the inverse of $\pi|_U$ extends uniquely to a morphism $Y \to X$. Therefore by uniqueness $\widetilde{\pi}$ is an isomorphism. □

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 α, β (and γ if $N = 4$) are (N, r)-congruent *up to quadratic twist*. When $N = 3, 4$ it remains to show that the condition on τ 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 5.1.7 (cf. [FK22, Proposition 4.18])**.** *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 $L = K^{\mathrm{ur}}(E[N])$ and $L' = K^{\mathrm{ur}}(E'[N])$. 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 [ST68, §2 Corollary 3]). Since E has good reduction over K we have $L' = L = K^{\mathrm{ur}}$. Therefore E' has good reduction over K. □

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

Let $\mathscr{E} \to \mathcal{Z}'_{N,r}$ be given by the Weierstrass equation

$$y^2 = x^3 - 27\frac{j}{j-1728}x - 54\frac{j}{j-1728} \tag{5.1}$$

and let $\mathscr{E}' \to \mathcal{Z}'_{N,r}$ be given by the Weierstrass equation

$$y^2 = x^3 - 27d^2\frac{j'}{j'-1728}x - 54d^3\frac{j'}{j'-1728} \tag{5.2}$$

where

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

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 δ and α are units in $R[\alpha, \beta, \gamma]/(P_\alpha, P_\beta, P_\gamma)$. Similarly when $(N, r) = (3, 1)$ the function δ is a unit in $R[\alpha, \beta]/(P_\alpha, P_\beta)$. Computing the discriminants of the Weierstrass equations in (5.1) and (5.2) we see that the fibres of $\mathscr{E}, \mathscr{E}' \to \mathcal{Z}'_{N,r}$ are non-singular except when $(N, r) = (3, 2)$ and $\beta = 0$.

The generic fibres of $\mathscr{E}, \mathscr{E}' \to \mathcal{Z}'_{N,r}$ 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 that $\mathcal{E}$ 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 5.1.7 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 λ 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 δ when $N = 4$.

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

Note that $3c_6c_6'\alpha$ 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 $3c_6c_6'\delta\alpha$ 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 β 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. □

5.1.4 Parametrisations of $W_{N,r}$ for $N \leq 5$ and $N = 7$

In order to compute models for $W_{12,r}$, $W_{14,r}$, and $W_{15,r}$ we will first need explicit parametrisations $\mathbb{A}^2 \dashrightarrow W_{N,r}$ for each $N \leq 5$ and $N = 7$. Such models are given by Kumar [Kum15] in the case when $r = -1$, we extend these to the case when $r \neq 1$. These parametrisations were found by first parametrising the surfaces $S_{N,r}$ constructed in Section 5.1.2.

Proposition 5.1.8. *For each $2 \leq N \leq 5$ and $N = 7$ the surface $W_{N,r}$ is $\mathbb{Q}$-birational to $\mathbb{A}^2$ and we have a commutative diagram*

$$\begin{array}{ccc} W_{N,r} & \dashrightarrow & \mathbb{A}^2 \\ \downarrow & & \vdots \\ W_1 & \xrightarrow{\sim} & W_1 \end{array}$$

where the map on the right is given by $(a,b) \mapsto (JJ', (J-1)(J'-1))$, the horizontal maps are birational and

$$JJ' = \frac{\boldsymbol{A}_{(N,r)}^3}{\boldsymbol{D}_{(N,r)}}, \qquad (J-1)(J'-1) = \frac{\boldsymbol{B}_{(N,r)}^2}{\boldsymbol{D}_{(N,r)}}.$$

The rational functions $\boldsymbol{A}_{(N,r)}$, $\boldsymbol{B}_{(N,r)}$, and $\boldsymbol{D}_{(N,r)} \in \mathbb{Q}(a,b)$ are given in Appendix A.2.

Proof. As in the proof of Theorem 5.1.4, for each $N \leq 4$, let $\mathcal{W}_{N,r}$ be the affine surface defined by the polynomials in Theorem 5.1.4 in the variables JJ', $(J-1)(J'-1)$, α, β (and γ if $N = 4$). We check in `Magma` that the rational maps $\mathbb{A}^2 \dashrightarrow \mathcal{W}_{N,r}$ given by taking JJ' and $(J-1)(J'-1)$ as in the statement of the proposition (and solving for α, β, and γ) are birational.

When $N = 5$ or 7 the models we reproduce in the proposition for $W_{5,1}$ and $W_{7,3}$ are given by Kumar [Kum15]. In the remaining cases we follow an argument of Fisher [Fis19, Remark 6.3].

Let $(N,r) = (5,2)$ or $(7,1)$. By Proposition 2.3.10 there exists a birational map $Z_{N,r} \dashrightarrow \boldsymbol{\Delta}_r \backslash (X(N) \times X(N))$ and we therefore have a factorisation

$$X(N) \times X(N) \dashrightarrow W_{N,r} \dashrightarrow S_{N,r} \dashrightarrow W_1.$$

Since in both cases $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ is a simple group the subgroup $\mathbf{\Delta}_r \subset \Upsilon_N \times \Upsilon_N$ is maximal, in particular either the second or the third map must be birational. In each case the latter map is not birational since w_0/w_3 is not $\Upsilon_N \times \Upsilon_N$-invariant, so $S_{N,r}$ and $W_{N,r}$ are birational. When $(N, r) = (5, 2)$ and $(7, 1)$ the claim follows immediately from the discussion in Sections 5.1.2.5 and 5.1.2.6. □

Finally, to compute models for $Z_{15,r}$ we will need the following lemma, which is a generic version of the condition on the c_6-invariants in Theorem 5.1.4, but in the case when $N = 5$.

Lemma 5.1.9. *Let $\mathcal{E}/\mathbb{Q}(Z_{5,r})$ and $\mathcal{E}'/\mathbb{Q}(Z_{5,r})$ be $(5, r)$-congruent elliptic curves with j-invariants $1728J$ and $1728J'$ respectively. Let $c_6 = c_6(\mathcal{E})$ and $c_6' = c_6(\mathcal{E}')$ and identify $\mathbb{Q}(a, b)$ with a subfield of $\mathbb{Q}(Z_{5,r})$ via the isomorphism $\mathbb{Q}(a, b) \cong \mathbb{Q}(W_{5,r}) \subset \mathbb{Q}(Z_{5,r})$ given in Proposition 5.1.8. Then there exists $\tau \in \mathbb{Q}(Z_{5,r})$ such that $\tau^2 = 3c_6c_6'\delta$, where*

$$\begin{aligned}\delta =& 3(-64a^3 - 24(187b^2 + 102b - 2)a^2 - 12(46b^4 - 1173b^3 - 391b^2 - 207b + 1)a \\ &+ (b^2 + 1)(b^4 + 522b^3 - 10006b^2 - 522b + 1))\end{aligned}$$

when $r = 1$, and

$$\begin{aligned}\delta =& 6(8a^6 + 48a^5 - 120(b - 1)a^4 + 4(144b^2 - 75b + 40)a^3 + 12(29b^2 - 42b + 10)a^2 \\ &- 12(150b^3 - 109b^2 + 49b - 4)a - (216b^4 + 1540b^3 + 489b^2 + 264b - 8))\end{aligned}$$

when $r = 2$.

Proof. We follow a similar approach to the proof of Theorem 5.1.4. When $r = 1$ the rational function $(J - J')^2$ is equal to

$$P_{5,1}(a, b) = -64a^3 + a^2b^2 + 152a^2b + 48a^2 - 2ab^3 - 110ab^2 - 166ab - 12a + b^4 + 22b^3 + 119b^2 - 22b + 1$$

up to a square factor. It follows that $Z_{5,r}$ is birational to the cubic surface $z^2 = P_{5,1}(a, b)$, which we parametrise by taking

$$a = \frac{(2s^2 + 15st - 9s + 12t^2 + 11t - 11)(12s^2 + 15st + 11s + 2t^2 - 9t - 11)}{4(s + 2t - 1)(2s + t - 1)(2s + 3t + 1)(3s + 2t + 1)},$$

$$b = \frac{-4(s + t + 2)^2(3s^2 + 2s + 3t^2 + 2t - 2)}{(s + 2t - 1)(2s + t - 1)(2s + 3t + 1)(3s + 2t + 1)},$$

$$z = \frac{(s - t)(s + t + 2)(4s + 7t - 1)(7s + 4t - 1)(9s^2 + 20st + 2s + 9t^2 + 2t - 2)}{(s + 2t - 1)^2(2s + t - 1)^2(2s + 3t + 1)(3s + 2t + 1)}.$$

Similarly, when $r = 2$ the rational function $(J - J')^2$ is equal to

$$P_{5,2}(a, b) = 16a^4 + 64a^3 - 360a^2b + 96a^2 + 216ab^2 - 80ab + 64a + 81b^2 + 24b + 16$$

up to a square factor. The surface $Z_{5,r}$ is birational to the affine surface $z^2 = P_{5,r}(a, b)$, which we parametrise by taking

$$a = -\frac{1}{32}(3st + 7s + 7t + 27),$$

$$b = \frac{(9st - 27s + 21t + 1)(9st + 21s - 27t + 1)}{2^6 3^3(3s + 3t + 10)},$$

$$z = \frac{(s-t)(3t+7)(3s+7)(3st+7s+7t+123)}{2^8(3s+3t+10)}.$$

Now consider the elliptic curves $\mathcal{E}/\mathbb{Q}(s,t)$ and $\mathcal{E}'/\mathbb{Q}(s,t)$ given by the Weierstrass equations

$$\mathcal{E} : y^2 = x^3 - 27\frac{j}{j-1728}x - 54\frac{j}{j-1728}$$
$$\mathcal{E}' : y^2 = x^3 - 27d^2\frac{j}{j-1728}x - 54d^3\frac{j}{j-1728}$$

where

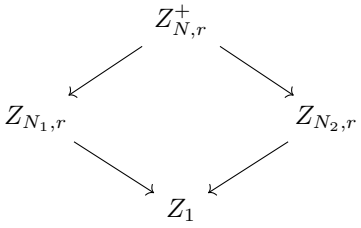
$$d = \frac{3\delta jj'}{(j-1728)(j'-1728)}.$$

By Lemma 5.1.7, after choosing models for $\mathcal{E}$ and $\mathcal{E}'$ with coefficients in $\mathbb{Z}[s,t]$, it suffices to show that $\mathcal{E}$ and $\mathcal{E}^D$ are not $(5,r)$-congruent for each $D \neq 1$ dividing $\Delta(\mathcal{E})\Delta(\mathcal{E}')$. Specialising at a small number of $s,t \in \mathbb{Q}$ and comparing traces of Frobenius concludes the proof. □

Remark 5.1.10. Notice that the parametrisations of $Z_{5,r}$ in Lemma 5.1.9 are symmetric in the variables (s,t). That is, the involution $\tau\colon Z_{5,r} \to Z_{5,r}$ is given on this birational model by $(s,t) \mapsto (t,s)$. In the electronic data [Fre23b] we record such symmetric families of (N,r)-congruent elliptic curves over $\mathbb{Q}(s,t)$ for each $N \leq 4$.

5.2 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



and similarly for $W^+_{N,r}$.

Remark 5.2.1. 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 $j(P), j'(P) \notin \{0, 1728\}$ 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_i, 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 5.2.2. 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 5.1.2) and the isomorphism respects the maps $Z_{4,r} \to Z_1$.

Remark 5.2.3. In this setting the surface $Z^+_{N,r}$ is playing a similar role to the fibre product $X(H_1, H_2)$ plays in the construction of $X^+(H_1, H_2)$ in Chapter 4. Indeed, both parametrise pairs of elliptic curves that are N_1N_2-congruent after a quadratic extension.

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 $N_i \neq 2$ for $i = 1, 2$. By the above discussion if $\mathcal{E}/\mathbb{Q}(Z^+_{N,r})$ is an elliptic curve with j-invariant j then there exists a pair of elliptic curves $\mathcal{E}_1'/\mathbb{Q}(Z^+_{N,r})$ and $\mathcal{E}_2'/\mathbb{Q}(Z^+_{N,r})$ with j-invariant j' such that $\mathcal{E}$ and $\mathcal{E}_i'$ are (N_i, r)-congruent. Let $d \in \mathbb{Q}(Z_{N,r})$ be such that $\mathcal{E}_1'$ is isomorphic to the quadratic twist of $\mathcal{E}_2'$ 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 $\mathbb{Q}(Z_{N,r})$.

5.3 Computing the surfaces $Z_{N,r}$

We now prove Theorem 1.0.9 by applying Theorem 5.1.4 to compute the fibre products described in Section 5.2.

The most straightforward case is when $N = 14$. In this case we use Theorem 5.1.4(i) to construct the covers $Z_{14,r} \to Z_{7,r}$, and utilise the methods outlined in Section 2.5 to simplify their birational models. Extending this approach, to compute the surfaces $Z_{12,r}$ for $r = 1, 7$ we use Theorem 5.1.4(i)–(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 5.1.4(iv) to construct the covers $Z_{12,r} \to Z_{4,r}$. Similarly we use Theorem 5.1.4(iv) to view $Z_{15,r}$ as an explicit cover of $Z_{5,r}$.

Remark 5.3.1. It is also possible to compute $Z_{12,r}$ for $r = 1, 7$ by using Theorem 5.1.4(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 5.1.4(i)–(ii) to construct the covers $Z_{12,r} \to Z_{3,2}$.

The transformations in this section were arrived at by utilising the techniques described in Section 2.5. Firstly, we simplify the equations for each cover by applying minimisation as described in Section 2.5.1. Secondly, after finding a parametrisation of this simplified model, we applied repeated Cremona transformations described in Section 2.5.2 to simplify the parametrisation. The calculations in this section are supported by supplementary `Magma` files verifying the algebra (see [Fre23b, `ZNr-eqns/verify`]).

5.3.1 Computing models for $Z_{12,1}$ and $Z_{12,7}$

We will use Theorem 5.1.4 to compute a model for the fibre product $W^+_{12,r}$.

The surface $W_{3,1}$ is birational to $\mathbb{A}^2$ with the forgetful map $\mathbb{A}^2 \dashrightarrow W_1$ given in Proposition 5.1.8. 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 the surface given by

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

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

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

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

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

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

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

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

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

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 5.1.4(ii) the surface $W_{12,1}^+$ (which by Remark 5.2.2 is isomorphic to $W_{12,7}^+$) is birational to the surface given by

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

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

$$\gamma_4 = \frac{(2p^3q+12p^2q^2+18pq^3+9q^4+24pq^2+24q^3-24pq-8q^2-32q+16)^2}{64(p+4q-4)(p+q+2)^3}\gamma_4'$$
$$q = \frac{\left((\gamma_4')^2-3p+4\gamma_4'-8\right)q' - 2p\gamma_4' - 4p + 4\gamma_4' - 16}{6\gamma_4'}$$

we find that $W_{12,1}^+$ is birational to the quadric surface

$$3(q')^2 - 2\gamma_4'q' + 8q' + p + 4 = 0$$

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

$$(p,q',\gamma_4') = \left(\frac{-4(s-3)(s+1)(3s-2t-1)^2}{3(s-1)^2(s-2t-1)(3s+2t+1)}, \frac{8s(t-1)}{3(s-1)(s-2t-1)}, \frac{4s(s-3)(3s-2t-1)}{(s-1)(s-2t-1)(3s+2t+1)}\right).$$

The forgetful map $W^+_{12,1} \to W_{6,1}$ is given by $(s,t) \mapsto (p,q)$.

5.3.1.1 The surface $Z_{12,1}$

The α_4, β_4, and γ_4 are elements of $\mathbb{Q}(W^+_{12,1})$ which satisfy the conditions of Theorem 5.1.4(ii). Let $\delta_4 = 3(JJ' - (\alpha_4+1)^2)$ be as in Theorem 5.1.4(ii). By construction there exist $\alpha_3, \beta_3, \delta_3 \in \mathbb{Q}(W^+_{12,1})$ which satisfy Theorem 5.1.4(iii).

As in Section 5.2 let $\mathcal{E}/\mathbb{Q}(Z^+_{12,1})$ be an elliptic curve with j-invariant $1728J$. Let $\mathcal{E}'_1/\mathbb{Q}(Z^+_{12,1})$ and $\mathcal{E}'_2/\mathbb{Q}(Z^+_{12,1})$ be elliptic curves with j-invariant $1728J'$ which are $(3,1)$ and $(4,1)$-congruent to $\mathcal{E}$ respectively.

It follows from Theorem 5.1.4(ii) and (iii) that up to square factors $c_6(\mathcal{E})$ is equal to both $3\delta_3 c_6(\mathcal{E}'_1)$ and $3\alpha_4\delta_4 c_6(\mathcal{E}'_2)$. In particular $\mathcal{E}'_1$ is isomorphic to the quadratic twist of $\mathcal{E}'_2$ by $\alpha_4\delta_4\delta_3$.

Therefore by the discussion in Section 5.2 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

$$(s,t,w') = \left(\frac{-2u^2-uv^2-u+4v^2}{uv^2+u+4v^2}, \frac{2u^2v^2-4u^2+uv^4-6uv^2-3u-8v^4}{(2u+v^2+3)(uv^2+u+4v^2)}, \right.$$
$$\left. \frac{36v(u+2)(u+v^2+1)(u+2v^2)(2u^2+uv^2+u-4v^2)^2}{(2u+v^2+3)^2(uv^2+u+4v^2)^3}\right).$$

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 $P_{12,1}(u,v)$ be the polynomial from the statement of Theorem 1.0.9, recorded in Appendix A. It follows immediately that $Z_{12,1}$ is birational to the affine surface given by the equation

$$z^2 = P_{12,1}(u,v)$$

since $(J-J')^2$ is equal to $P_{12,1}(u,v)$ up to a square factor.

5.3.1.2 The surface $Z_{12,7}$

By Theorem 5.1.4 the surface $W_{12,5}$ 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 $3(t-1)(-9s^3+12s^2t+4st^2+15s^2+4st-12t^2+s-12t-3)$ up to a square factor. Therefore the surface $W_{12,5}$ is birational to the affine surface given by

$$(w')^2 = 3(t-1)(-9s^3+12s^2t+4st^2+15s^2+4st-12t^2+s-12t-3).$$

We parametrise this surface by setting

$$(s,t,w') = \left(\frac{(u-1)(u^2-v^2+4u+1)}{u^3+u^2-uv^2-3u-v^2+1}, \frac{u^3-uv^2+7u^2-v^2+9u+1}{u^3+u^2-uv^2-3u-v^2+1}, \right.$$
$$\left. \frac{36uv(u+2)(u^2+4u-v^2+1)}{(u^3+u^2-uv^2-3u-v^2+1)^2}\right).$$

Hence $W_{12,5}$ is birational to $\mathbb{A}^2$ and the forgetful map $W_{12,5} \to W_{12,1}^+$ is given by $(u,v) \mapsto (s,t)$.

Let $P_{12,7}(u,v)$ be the polynomial from the statement of Theorem 1.0.9, recorded in Appendix A. It follows immediately that $Z_{12,7}$ is birational to the affine surface given by the equation

$$z^2 = P_{12,7}(u,v)$$

since $(J-J')^2$ is equal to $P_{12,7}(u,v)$ up to a square factor.

5.3.2 Computing models for $Z_{12,5}$ and $Z_{12,11}$

For each $r = 1, 3$, the surface $W_{4,r}$ is birational to $\mathbb{A}^2$ with the forgetful map $\mathbb{A}^2 \dashrightarrow W_1$ given in Proposition 5.1.8. 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

$$\alpha_3^3 - JJ' = 0$$

in $\mathbb{A}^3$. By making a change of coordinates $\alpha_3 = \frac{2(-2ab+b^2+2a+2b)}{3(b-1)(-a+b+1)^2}\alpha_3'$ 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 $(c,d) \mapsto (a,b)$.

By Theorem 5.1.4(iv) the surface $W_{12,5}^+$ (which by Remark 5.2.2 is isomorphic to $W_{12,11}^+$) is birational to the surface given by

$$\beta_3^4 - 6(\alpha_3+1)(J-1)(J'-1)\beta_3^2 - 8((J-1)(J'-1))^2\beta_3 - 3((\alpha_3-1)(J-1)(J'-1))^2 = 0$$

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 $\mathbb{A}^2_{\mathbb{Q}(c,d)}$. By using minimisation over the base ring $\mathbb{Z}[c,d]$ as described in Section 2.5, we arrive at the change of coordinates

$$\theta = \frac{g_3(c,d)^2(g_1(c,d)\theta' + g_2(c,d)\beta_3' + 2(2d^3+1)g_2(c,d))}{3(\beta_3' + 2(2d^3+1))},$$
$$\beta_3 = \frac{g_3(c,d)\left(-3(d^2c+4(2d^3+1))\beta_3' + 2(2d^3+1)(2c^2-3(d^2+4)c+6(2d^3+1)\right)}{3(\beta_3'+2(2d^3+1))}$$

where

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

$$g_2(c,d) = (3d^4 - 8d^3 - 4)c^2 + 24(d^2+1)(2d^3+1)c + 12(2d^3+1)^2,$$
$$g_3(c,d) = \frac{d^6c^3 - 8(2d^3+1)^2c^2 + 48(2d^3+1)^2c - 8(2d^3+1)^3}{c^4d^8}.$$

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

$$2(\beta_3')^2 - 2\beta_3'\theta' - (\theta')^2 + \left(-8d^3 - 4\right)\beta_3' + \left(-8d^3 - 4\right)\theta' + c^2d^4 - 8cd^5 - 4cd^2 = 0,$$
$$-3(\beta_3')^2 + 3(\theta')^2 - 6cd^2\beta_3' - 3c^2d^4 + 8c^2d^3 - 48cd^3 + 4c^2 - 24c = 0$$

in $\mathbb{A}^4$. We parametrise this surface by setting

$$(c, d, \beta_3', \theta') = \left(\frac{6(s+t)h_1(s,t)}{h_3(s,t)}, \frac{t}{s+t+2}, \frac{2h_1(s,t)h_2(s,t)}{(s+t+2)^2h_3(s,t)}, \frac{-4(s-1)(s^2+st+s+2t+1)h_1(s,t)}{(s+t+2)^2h_3(s,t)}\right)$$

where

$$h_1(s,t) = s^3 + (3t+6)\,s^2 + \left(3t^2+12t+12\right)s + 3t^3 + 6t^2 + 12t + 8,$$
$$h_2(s,t) = 4s^3 + 4s^2t - 3st^2 - 2st - 6s - 3t^3 - 2t + 2,$$
$$h_3(s,t) = 2s^4 + (4t+4)\,s^3 + \left(5t^2+18t+12\right)s^2 + \left(6t^3+20t^2+24t+10\right)s + 3t^4 + 6t^3 + 11t^2 + 8t - 1.$$

Therefore $W^+_{12,5}$ is birational to $\mathbb{A}^2$ and the forgetful map $W^+_{12,5} \to W^{\sqrt[3]{\Delta\Delta'}}_{4,1}$ is given by $(s,t) \mapsto (c,d)$.

5.3.2.1 The surface $Z_{12,5}$

Note that $\alpha_3, \beta_3 \in \mathbb{Q}(W^+_{12,5})$ satisfy the conditions of Theorem 5.1.4(iv). By construction there exist elements α_4, β_4, γ_4 of $\mathbb{Q}(W^+_{12,1})$ which satisfy Theorem 5.1.4(i)–(ii). Let $\delta_4 = 3(JJ' - (\alpha_4+1)^2)$ be as in Theorem 5.1.4(ii)

By Theorem 5.1.4 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

$$(s, t, w') = \left(\frac{-u^2 + v^2 + 2u - 2}{u^2 - 2u - v^2}, \frac{2u-2}{u^2-2u-v^2}, \frac{2v}{u^2-2u-v^2}\right).$$

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 $P_{12,5}(u,v)$ be the polynomial from the statement of Theorem 1.0.9, recorded in Appendix A. It follows immediately that $Z_{12,5}$ is birational to the affine surface given by the equation

$$z^2 = P_{12,5}(u,v)$$

since $(J - J')^2$ is equal to $P_{12,5}(u,v)$ up to a square factor.

5.3.2.2 The surface $Z_{12,11}$

By Theorem 5.1.4 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 $P_{12,11}(u,v)$ be the polynomial from the statement of Theorem 1.0.9, recorded in Appendix A. It follows immediately that $Z_{12,11}$ is birational to the affine surface given by the equation

$$z^2 = P_{12,11}(u,v)$$

since $(J-J')^2$ is equal to $P_{12,11}(u,v)$ up to a square factor.

5.3.3 Computing models for $Z_{14,1}$ and $Z_{14,3}$

5.3.3.1 The surface $Z_{14,1}$

The surface $W_{7,1}$ is birational to $\mathbb{A}^2$ with the forgetful map $\mathbb{A}^2 \dashrightarrow W_1$ given in Proposition 5.1.8. The surface $W_{7,1}^{\sqrt{\Delta\Delta'}}$ is birational to the surface in $\mathbb{A}^3$ given by

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

After making the change of coordinates

$$\alpha = \frac{\boldsymbol{B}_{7,1}}{27(b+1)^2(8ab+b^2+4b-1)^4}\alpha'$$

the surface $W_{7,1}^{\sqrt{\Delta\Delta'}}$ is birational to the surface given by in $\mathbb{A}^3$ by

$$(b-1)(\alpha')^2 - (b+1)(8ab+b^2+4b-1) = 0. \tag{5.3}$$

We parametrise the cubic surface in (5.3) by setting $(a,b,\alpha') = \left(\frac{-c^2d+c^2+d^3-3d^2-5d-1}{8d(d+1)}, \frac{1}{d}, \frac{c}{d}\right)$. By Theorem 5.1.4(i) the surface $W_{14,1}$ is birational to the triple cover of $\mathbb{A}^2_{c,d}$ given in $\mathbb{A}^3$ by

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

Let β' be given by the Möbius transformation

$$\beta = \frac{d^6\boldsymbol{A}_{(7,1)}}{2^4 3^3 c^7(d-1)^3} \cdot \frac{h_1(c,d)\beta' + h_2(c,d)}{h_3(c,d)\beta' + h_4(c,d)} \tag{5.4}$$

where in (5.4) we take

$$h_1(c,d) = -(d-1)^3c^7 + (d-1)^2(d^2+38d+41)c^6 + (d-1)(d+1)(3d^3+225d^2+353d+123)c^5$$

$$
\begin{aligned}
&- (d+1)(3d^5 + 339d^4 + 2d^3 - 278d^2 + 459d + 499)c^4 - (d+1)^2(3d^5 + 453d^4 - 14d^3 \\
&+ 1246d^2 + 1019d - 1299)c^3 + (d+1)^2(3d^6 + 570d^5 - 155d^4 + 2812d^3 + 4397d^2 \\
&- 1558d - 2229)c^2 + (d+1)^3(d^6 + 228d^5 - 139d^4 + 2584d^3 + 1315d^2 - 1596d - 1305)c \\
&- (d+1)^3(d^7 + 267d^6 - 191d^5 + 4155d^4 + 4395d^3 - 775d^2 - 3245d - 2559),
\end{aligned}
$$

$$
\begin{aligned}
h_2(c,d) = &-(d-1)^3c^7 + (d-1)^2(d+1)(17d+23)c^6 + (d-1)(d+1)(3d^3 + 189d^2 + 337d + 175)c^5 \\
&- (d+1)^2(51d^4 - 462d^3 + 68d^2 + 726d + 129)c^4 - (d+1)^2(3d^5 + 381d^4 + 626d^3 \\
&+ 526d^2 + 251d - 123)c^3 + (d+1)^3(51d^5 - 891d^4 + 802d^3 + 4334d^2 - 37d - 2211)c^2 \\
&+ (d+1)^3(d^6 + 192d^5 + 481d^4 + 1088d^3 - 725d^2 - 640d + 819)c - (d+1)^4(17d^6 \\
&- 440d^5 + 705d^4 + 4400d^3 - 645d^2 - 3960d + 1011),
\end{aligned}
$$

$$h_3(c,d) = (d-1)c^3 - (d^2 - 10d - 7)c^2 - (d+1)(d^2 - 20d - 9)c + (d+1)(d^3 - 29d^2 - 37d + 1),$$

$$h_4(c,d) = (d-1)c^3 + (d+1)(7d+1)c^2 - (d+1)(d^2 - 8d - 13)c - 7(d+1)^2(d^2+3).$$

A calculation with computer algebra shows that $W_{14,1}$ is birational to the surface given by

$$2(c-d+1)(\beta')^3 + 2(c-d-1)(\beta')^2 - (d+1)(c+d+3)\beta' - (d+1)(c+d+1) = 0 \tag{5.5}$$

in $\mathbb{A}^3$. We parametrise the quartic surface given in (5.5) by setting

$$
\begin{aligned}
c &= \frac{-2v(u-1)(u^2v - u^2 - uv^2 + uv - u + v^2)}{(uv - u - v - 1)(u^2 - uv + u + v)}, \\
d &= \frac{-(u^3v - u^3 + u^2v^2 + u^2v - 2u^2 - 2uv^2 - uv - u + v^2 - v)}{(uv - u - v - 1)(u^2 - uv + u + v)}, \quad \text{and} \\
\beta' &= \frac{-v(u-1)}{uv - u - v - 1}.
\end{aligned}
$$

In particular $W_{14,1}$ is rational over $\mathbb{Q}$. Finally, the surface $Z_{14,1}$ is birational to the double cover of $W_{14,1}$ given by $z^2 - (J - J')^2 = 0$. Theorem 1.0.9 follows in the case when $(N, r) = (14, 1)$ by noting that $P_{14,1}(u,v)(J-J')^2$ is a square in $\mathbb{Q}(W_{14,1})$ (here $P_{14,1}(u,v)$ is the polynomial recorded in Appendix A).

5.3.3.2 The surface $Z_{14,3}$

The surface $W_{7,3}$ is birational to $\mathbb{A}^2$ with the forgetful map $\mathbb{A}^2 \dashrightarrow W_1$ given in Proposition 5.1.8 (these are the formulae given by Kumar [Kum15]). We define the surface $W_{7,3}^{\sqrt{\Delta\Delta'}}$ to be the affine surface given by the vanishing of $\alpha^2 - (J-1)(J'-1)$ in $\mathbb{A}^3$. After making the change of variables

$$\alpha = \frac{\boldsymbol{B}_{(7,3)}}{2^6 3^3 a^3 b^3 (b+1)^2 (ab + a - 1)^4} \alpha'$$

it follows that $W_{7,3}^{\sqrt{\Delta\Delta'}}$ is birational to the cubic surface

$$b(\alpha')^2 - a(ab + a - 1) = 0$$

which we parametrise by setting $(a, b, \alpha') = \left(\frac{-d+1}{c^2 - d^2 + d}, d - 1, \frac{c}{c^2 - d^2 + d}\right)$.

It follows from Theorem 5.1.4(i) that the surface $W_{14,3}$ is birational to the degree 3 cover of $W_{7,3}^{\sqrt{\Delta\Delta'}}$ given by

$$\beta^3 - 3JJ'\beta - 2JJ'(\alpha - 1) = 0.$$

Let β' be given by the Möbius transformation

$$\beta = \frac{(c^2-d^2+d)^4 \boldsymbol{A}_{(7,3)}}{2^6 3^3 c^7 d^2 (d-1)^4} \cdot \frac{h_1(c,d)\beta' + h_2(c,d)}{h_3(c,d)\beta' + h_4(c,d)}$$

where

$$\begin{aligned}
h_1(c,d) &= -c^6 + 2(9d+1)c^5 - (15d^2+d+15)c^4 - 2^2(9d^3+10d^2-12d+1)c^3 + (33d^4+98d^3 \\
&\quad - 253d^2 - 54d + 33)c^2 + 2(9d^5+55d^4-39d^3-99d^2+83d+1)c - (17d^6+169d^5 \\
&\quad - 310d^4 - 395d^3 + 790d^2 - 271d + 17), \\
h_2(c,d) &= c^7 - dc^6 - (3d^2+23d+5)c^5 + (3d^3-19d^2-7d+18)c^4 + (3d^4-38d^3+113d^2 \\
&\quad - 18d + 7)c^3 - (3d^5-122d^4+317d^3-642d^2+19d+36)c^2 - (d^6-61d^5+408d^4 \\
&\quad - 289d^3 - 280d^2 + 239d + 3)c + (d^7-103d^6+696d^5-1525d^4+740d^3+347d^2 \\
&\quad - 141d + 18), \\
h_3(c,d) &= c^2 + (6d-2)c - 7(d^2-d+1), \\
h_4(c,d) &= -c^3 + dc^2 + (d^2-7d+3)c - (d+2)(d^2-3d-3).
\end{aligned}$$

It is then a calculation to see that $W_{14,3}$ is birational to the surface in $\mathbb{A}^3$ given by the equation

$$(\beta')^3 - (c+d+4)(\beta')^2 + (2c+3d+5)(\beta') + cd - c + d^2 - 3d - 2 = 0. \tag{5.6}$$

We parametrise the affine surface in (5.6) by setting

$$(c,d,\beta') = \left(\frac{-(u^2+2uv^2+2u-2v^3+v^2+4v+1)}{4(v-1)(v+1)}, \frac{(u-v-1)(u-v+3)}{4(v-1)(v+1)}, \frac{-(u-3v+5)}{2(v-1)} \right).$$

As above it follows that $W_{14,3}$ is a rational over $\mathbb{Q}$. Similarly, the surface $Z_{14,3}$ is birational to the double cover of $W_{14,3}$ given by $z^2 - (J-J')^2 = 0$. Theorem 1.0.9 follows in the case when $(N,r) = (14,3)$ by noting that $P_{14,3}(u,v)(J-J')^2$ is a square in $\mathbb{Q}(W_{14,3})$ (here $P_{14,3}(u,v)$ is the polynomial recorded in Appendix A).

5.3.4 Computing models for $Z_{15,2}$ and $Z_{15,11}$

5.3.4.1 The surface $Z_{15,2}$

The surface $W_{5,2}$ is birational to $\mathbb{A}^2$ with the forgetful map $\mathbb{A}^2 \dashrightarrow W_1$ given in Proposition 5.1.8. Let $\Delta = \Delta(\mathcal{E})$ and $\Delta' = \Delta(\mathcal{E}')$ be the discriminants of elliptic curves $\mathcal{E}/\mathbb{Q}(Z_{5,2})$ and $\mathcal{E}'/\mathbb{Q}(Z_{5,2})$ with j-invariants $1728J$ and $1728J'$ respectively. Write $W_{5,2}^{\sqrt[3]{\Delta\Delta'}}$ for the degree 3 cover of $Z_{5,2}$ whose function field is given by adjoining $\sqrt[3]{\Delta\Delta'}$ to $\mathbb{Q}(Z_{5,2})$. Then $W_{5,2}^{\sqrt[3]{\Delta\Delta'}}$ is birational to the surface given by

$$\alpha^3 - JJ' = 0$$

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

$$\alpha = \frac{\boldsymbol{A}_{(5,1)}}{2^2 3^2 b(2a-b+1)^2} \alpha'$$

we see that $W_{5,2}^{\sqrt[3]{\Delta\Delta'}}$ is birational to the affine surface given by the vanishing of $(\alpha')^3 + 2a - b + 1$ in $\mathbb{A}^3$. We parametrise this cubic surface by setting $(a,b,\alpha') = ((c-1)/2, c+d^3, d)$.

By Theorem 5.1.4(iv) the surface $W^+_{15,2}$ is therefore birational to the degree 4 cover of $W^{\sqrt[3]{\Delta\Delta'}}_{5,2}$ given by

$$\beta^4 - 6(\alpha+1)(J-1)(J'-1)\beta^2 - 8((J-1)(J'-1))^2\beta - 3((\alpha-1)(J-1)(J'-1))^2 = 0.$$

Let η be given by the relation

$$\beta = \frac{\boldsymbol{B}_{(5,2)}}{2^5 3^4 d^{10}(c+d^3)^2}\eta$$

and let $\theta = \eta^2$. We define η' and θ' by the $\mathrm{PGL}_3(\mathbb{Q}(c,d))$ change of coordinates

$$\eta = \frac{g_1(c,d)\eta' + g_2(c,d)\theta' + g_3(c,d)}{g_7(c,d)\eta' + g_8(c,d)\theta' + g_9(c,d)}, \quad \text{and} \quad \theta = \frac{g_4(c,d)\eta' + g_5(c,d)\theta' + g_6(c,d)}{g_7(c,d)\eta' + g_8(c,d)\theta' + g_9(c,d)}$$

where the polynomials $g_i(a,b) \in \mathbb{Z}[a,b]$ are too complicated to reproduce here, but may be found in the accompanying electronic data [Fre23b]. It follows that $W^+_{15,2}$ is birational to the affine surface given by the vanishing of

$$\begin{aligned}
Q_1 &= 2\eta'^2 + \eta'\theta' + (3c - 4d - 11)\eta' + (c - 2d - 3)\theta' + c^2 - 2cd - 7c + 10d + 15,\\
Q_2 &= (2d+5)\eta'^2 + (3d+5)\eta'\theta' + (cd + 7c + 7d^2 - 2d - 24)\eta' + (d+1)\theta'^2 + (cd + 4c\\
&\quad + 5d^2 - 6d - 13)\theta' + 2c^2 + 2cd^2 + 6cd - 18c + 6d^3 - 19d^2 - 12d + 28
\end{aligned}$$

in $\mathbb{A}^4$. We parametrise this surface by setting

$$\begin{aligned}
(c, d, \eta', \theta') = \Bigg(&\frac{-(s^2t + 5st - s + t^2 + 4t - 1)h_1(s,t)}{(s^2+s+t)(s^2t - 3st + s + t^2)^2}, \frac{(s^2t + st + t^2 - 4t + 1)}{s^2t - 3st + s + t^2},\\
&\frac{h_2(s,t)}{(s^2+s+t)(s^2t - 3st + s + t^2)^2}, \frac{h_3(s,t)}{(s^2+s+t)(s^2t - 3st + s + t^2)^2}\Bigg)
\end{aligned}$$

where

$$\begin{aligned}
h_1(s,t) &= s^4t + 2s^3t + 2s^2t^2 + s^2t + 2st^2 + t^3 - 16t^2 + 8t - 1,\\
h_2(s,t) &= 5t^2s^6 - t(13t-7)s^5 + (15t^3 + 15t^2 - 16t + 4)s^4 - (26t^3 - 87t^2 + 45t - 7)s^3 + (15t^4\\
&\quad - 9t^3 + 34t^2 - 19t + 3)s^2 - (13t^4 + 41t^3 - 36t^2 + 10t - 1)s + (5t^5 - 24t^4 - 54t^3\\
&\quad + 47t^2 - 12t + 1),\\
h_3(s,t) &= -5t^2s^6 + 3(t)(3t-2)s^5 - (15t^3 - 5t^2 - 7t + 3)s^4 + (18t^3 - 97t^2 + 56t - 9)s^3 - 3(5t^4\\
&\quad - 19t^3 + 30t^2 - 14t + 2)s^2 + t(3t-2)(3t^2 - 8t + 2)s - (5t^5 - 52t^4 - 43t^3 + 46t^2\\
&\quad - 12t + 1).
\end{aligned}$$

Let $\mathcal{E}/\mathbb{Q}(Z^+_{15,2})$ and $\mathcal{E}'/\mathbb{Q}(Z^+_{15,2})$ be $(5,2)$-congruent elliptic curves with j-invariants $1728J$ and $1728J'$ respectively and let $c_6 = c_6(\mathcal{E})$ and $c'_6 = c_6(\mathcal{E}')$. By Theorem 5.1.4(iv) (and the discussion in Section 5.2) it follows that $W_{15,2}$ is birational to the double cover of $W^+_{15,2}$ given by

$$w^2 = 3c_6c'_6\beta.$$

Applying Lemma 5.1.9 we check with the aid of computer algebra that $3c_6c'_6\beta$ is equal to $-4t+1$ up to a square factor, and hence $W_{15,2}$ is birational to the affine surface given by $(w')^2 = -4t + 1$

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

$$(s,t,w') = \left(\frac{uv^2-u-v^2}{v(v-1)}, \frac{-u(v-1)(uv-u-v)}{v^2}, \frac{2uv-2u-v}{v}\right).$$

It then follows immediately that $Z_{15,2}$ is birational to the surface $z^2 = P_{15,2}(u,v)$ given in Theorem 1.0.9 since $(J-J')^2$ is equal to $P_{15,2}$ up to a square factor (here $P_{15,2}(u,v)$ is the polynomial recorded in Appendix A).

5.3.4.2 The surface $Z_{15,11}$

Kumar [Kum15] gave a birational model for the surface $W_{5,1}$ with the forgetful map $\mathbb{A}^2 \dashrightarrow W_1$ given in Proposition 5.1.8. Let $\Delta = \Delta(\mathcal{E})$ and $\Delta' = \Delta(\mathcal{E}')$ be the discriminants of elliptic curves $\mathcal{E}/\mathbb{Q}(Z_{5,1})$ and $\mathcal{E}'/\mathbb{Q}(Z_{5,2})$ with j-invariants $1728J$ and $1728J'$ respectively. Again write $W_{5,1}^{\sqrt[3]{\Delta\Delta'}}$ for the degree 3 cover of $Z_{5,1}$ whose function field is given by adjoining $\sqrt[3]{\Delta\Delta'}$ to $\mathbb{Q}(Z_{5,1})$. Then $W_{5,1}^{\sqrt[3]{\Delta\Delta'}}$ is birational to the surface given by

$$\alpha^3 - JJ' = 0$$

in $\mathbb{A}^3$. Let c be such that

$$\alpha = \frac{\boldsymbol{A}_{(5,1)}}{2^4 3^6 b^3 a^6}\alpha'$$

then it follows that $W_{5,1}^{\sqrt[3]{\Delta\Delta'}}$ is birational to the affine cubic surface $(\alpha')^3 - ab = 0$, which we parametrise by setting $(a,b,\alpha') = (1/(c^2d), d/c, 1/c)$.

By Theorem 5.1.4(iv) the surface $W_{15,11}^{+}$ is therefore birational to the degree 4 cover of $W_{5,2}^{\sqrt[3]{\Delta\Delta'}}$ given by

$$\beta^4 - 6(\alpha+1)(J-1)(J'-1)\beta^2 - 8((J-1)(J'-1))^2\beta - 3((\alpha-1)(J-1)(J'-1))^2 = 0.$$

Let η be given by the relation

$$\beta = \frac{\boldsymbol{B}_{(5,2)}}{2^5 3^4 d^{10}(c+d^3)^2}\eta$$

and let $\theta = \eta^2$. We define η' and θ' by the $\mathrm{PGL}_3(\mathbb{Q}(c,d))$ change of coordinates

$$\eta = \frac{g_1(c,d)\theta' + g_2(c,d)}{g_6(c,d)\theta' + g_7(c,d)}, \quad \text{and} \quad \theta = \frac{g_3(c,d)\eta' + g_4(c,d)\theta' + g_5(c,d)}{g_6(c,d)\theta' + g_7(c,d)}$$

where

$$\begin{aligned}
g_1(c,d) =& -d(dc^3 - d(119d-12)c^2 + (187d^3 - 132d^2 - 4)c - (17d^4 + 12d^3 - 32d + 12)),\\
g_2(c,d) =& 2(59d^2c^3 + d(714d^2 - 265d + 7)c^2 + d(323d^3 + 990d^2 - 462d - 68)c + (12d^5 - 85d^4\\
&- 77d^3 - 576d^2 + 160d - 28)),\\
g_3(c,d) =& 48(d^3c^4 - 22d^4c^3 + d^2(119d^3 - 3)c^2 + 2d^3(11d^3 + 4)c + d(d^6 - 47d^3 + 1)),\\
g_4(c,d) =& d(d^2c^5 + d^2(235d + 24)c^4 + 2d(1045d^3 - 924d^2 - 4)c^3 + 2d(1615d^4 + 8568d^3 - 184d\\
&- 60)c^2 - (1595d^6 - 4488d^5 + 1976d^3 - 1200d^2 - 144d - 16)c + (7d^7 + 264d^6 + 1456d^4\\
&- 9720d^3 + 1008d^2 + 112d + 96),\\
g_5(c,d) =& 2(25d^3c^5 + d^2(5700d^2 - 1835d - 7)c^4 + 2d^2(6175d^3 + 5610d^2 + 462d + 152)c^3\\
&- 2d(2850d^5 + 4445d^4 + 15169d^3 + 6588d^2 - 2240d - 28)c^2 + d(25d^6 + 8580d^5
\end{aligned}$$

$$\begin{aligned}
&- 10164d^4 + 2848d^3 - 7680d^2 - 96d - 776)c - 7(5d+1)(d^6 + 24d^5 + 208d^3 - 744d^2\\
&+ 144d + 16)),\\
g_6(c,d) &= d(c+7d),\\
g_7(c,d) &= 2(25cd - 35d - 7).
\end{aligned}$$

It follows that $Z^+_{15,11}$ is birational to the surface given by the vanishing of

$$\begin{aligned}
Q_1 &= \eta'^2 + 4\eta'\theta' - d(3c+d-4)\theta'^2 + 2(32cd + 14c - d^2 + 18d - 32)\theta' - 49c^2 + 214cd\\
&\quad - 364c - d^2 + 32d - 256,\\
Q_2 &= 2d(c+7d)\eta'\theta' + 4(25cd - 35d - 7)\eta' + 2d(10cd - 5d^2 + 30d - 3)\theta'^2 + 2d(7c^2 + 118cd - 16c\\
&\quad - 17d^2 + 88d - 440)\theta' - 4(119c^2d + 191cd^2 + 645cd + 49c + 6d^3 - 85d^2 + 173d - 994)
\end{aligned}$$

in $\mathbb{A}^4$. We parametrise this affine surface by setting

$$(c,d,\eta',\theta') = \left(\frac{-h_1(s,t)(s^3 - s^2 - st^2 - st - t^2)}{(s-t-1)(st-s+1)h_4(s,t)}, \frac{-(s-t-1)^2(s-t+3)}{h_4(s,t)}, \right.$$
$$\left. \frac{-h_2(s,t)}{(s-t-1)(st-s+1)h_4(s,t)h_5(s,t)}, \frac{-2h_3(s,t)}{(s-t-1)h_5(s,t)}\right)$$

where

$$\begin{aligned}
h_1(s,t) &= s^3 - 2s^2 - st^2 - st + s - t^3 + t^2 + t,\\
h_2(s,t) &= -7s^8 - 7(t-3)s^7 + 2(77t^2 - 97t + 34)s^6 - (149t^3 + 20t^2 - 672t + 473)s^5 - (79t^4\\
&\quad - 86t^3 + 310t^2 + 710t - 981)s^4 + (108t^5 - 44t^4 - 323t^3 + 103t^2 + 398t - 953)s^3 - (20t^6\\
&\quad - 160t^5 - 65t^4 - 361t^3 + 164t^2 + 429t - 438)s^2 - (72t^6 - 213t^5 - 241t^4 + 125t^3\\
&\quad - 267t^2 - 357t + 75)s - t(7t^5 + 44t^4 - 161t^3 - 206t^2 + 30t + 87),\\
h_3(s,t) &= 4s^3 - 6s^2t + 2s^2 - 19st^2 + 14st - 9s - 4t^2 - 15t + 3,\\
h_3(s,t) &= s^2 - st^2 + st - s + t^3 - 2t^2 - 2t,\\
h_4(s,t) &= s^2 - 4st + 5s + t - 6.
\end{aligned}$$

Let $\mathcal{E}/\mathbb{Q}(Z^+_{15,1})$ and $\mathcal{E}'/\mathbb{Q}(Z^+_{15,1})$ be $(5,1)$-congruent elliptic curves with j-invariants $1728J$ and $1728J'$ respectively and let $c_6 = c_6(\mathcal{E})$ and $c'_6 = c_6(\mathcal{E}')$. By Theorem 5.1.4(iv) (and the discussion in Section 5.2) it follows that $W_{15,1}$ is birational to the double cover of $W^+_{15,1}$ given by

$$w^2 = 3c_6c'_6\beta.$$

Applying Lemma 5.1.9 it follows that $3c_6c'_6\beta$ is equal to $(s-t-1)(s-t+3)$ up to a square factor, and hence $W_{15,11}$ is birational to the surface given by $(w')^2 = (s-t-1)(s-t+3)$ in $\mathbb{A}^3$. We parametrise this quadric surface by setting

$$(s,t,w') = \left(\frac{(u^2v + u^2 + 2uv^2 + 2uv + 2u + v^3 + v^2 + 2v + 1)}{(v+1)(u+v)(u+v+1)}, \frac{-(uv - u + v^2)}{(v+1)(u+v)(u+v+1)}, \right.$$
$$\left. \frac{2u + 2v + 1}{(u+v)(u+v+1)}\right).$$

It then follows immediately that $Z_{15,11}$ is birational to the surface $z^2 = P_{15,11}(u,v)$ given in Theorem 1.0.9 since $(J - J')^2$ is equal to $P_{15,11}$ up to a square factor (here $P_{15,11}(u,v)$ is the

polynomial recorded in Appendix A).

5.4 Modular curves on $W_{N,r}$

5.4.1 The Hecke correspondences $F_{m,\lambda}$

We now list the modular curves $F_{m,\lambda}$ which appear on the models for $Z_{N,r}$ computed in Section 5.3, ignoring those with $m \leq 4$ (since by Lemma 3.2.4 these define (-1)-curves on $\widetilde{Z}_{N,r}$). For several small values of m the modular curves in question have been blown down, we list these first in Table 5.1. When $N = 14$ and $m = 15, 19$ and when $N = 15$ and $m = 11, 14$ we have not yet been able to identify all the modular curves $F_{m,\lambda}$.

In Tables 5.2–5.9 the modular curves $F^*_{m,\lambda} \subset W_{N,r}$ are each birational to $X_0^+(m)$, the quotient of $X_0(m)$ by the Fricke involution. The modular curves $F_{m,\lambda} \subset Z_{N,r}$ are the pre-images of the curves $F^*_{m,\lambda}$ under the map $Z_{N,r} \to W_{N,r}$.

(N,r)	m	Equation for the curve $F_{m,\lambda}$ on a blowup of $Z_{N,r}$
$(12,5)$	5	$z^2 = \widetilde{P}_{12,5}\left(\frac{1}{2}(3-\varepsilon), \frac{1}{2}(\pm 1 \pm \varepsilon + \varepsilon^2 t), 1\right) = \frac{1}{4}\left(-t^2 \mp 44t + 16\right)\varepsilon^4 + O(\varepsilon^5)$
$(12,7)$	7	$z^2 = \widetilde{P}_{12,7}(-\varepsilon, \pm 1 \pm \varepsilon + \varepsilon^2 t, 1) = (4t^2 \pm 52t - 27)\varepsilon^4 + O(\varepsilon^5)$
$(14,1)$	9	$z^2 = \widetilde{P}_{14,1}(\varepsilon, -\varepsilon + \varepsilon^2 t, 1) = (t^2 - 16t - 44)\varepsilon^4 + O(\varepsilon^5)$
	11	$z^2 = \widetilde{P}_{14,1}(1 + \varepsilon^2 t, 1, \varepsilon) = (t^4 + 12t^3 - 40t^2 + 28t - 8)\varepsilon^8 + O(\varepsilon^9)$
$(14,3)$	5	$z^2 = \widetilde{P}_{14,3}(\frac{1}{2}\varepsilon, 1 + \frac{1}{4}\varepsilon^2 t, 1) = (-16t^2 + 88t + 4)\varepsilon^4 + O(\varepsilon^5)$
	13	$z^2 = \widetilde{P}_{14,3}(-4 + \frac{1}{4}\varepsilon, -1 + \frac{1}{12}\varepsilon + \frac{1}{4}\varepsilon t, 1) = -t^2(477t^2 + 48t - 1)\varepsilon^4 + O(\varepsilon^5)$
	17	$z^2 = \widetilde{P}_{14,3}(\frac{1}{4}\varepsilon, -1 + \frac{1}{4}\varepsilon t, 1) = -(t^4 - 16t^3 + 9t^2 - 2t + 4)\varepsilon^4 + O(\varepsilon^5)$
$(15,2)$	8	$\begin{cases} z^2 = \widetilde{P}_{15,2}(\varepsilon, -\varepsilon + \varepsilon^2 t, 1) = (t^2 - 22t - 7)\varepsilon^4 + O(\varepsilon^5) \\ z^2 = \widetilde{P}_{15,2}(\varepsilon^2 t, 1, \varepsilon) = (t^2 - 24t + 16)\varepsilon^4 + O(\varepsilon^5) \end{cases}$
	17	$z^2 = \widetilde{P}_{15,2}(1, \varepsilon + \varepsilon^2 + \varepsilon^3 t, \varepsilon) = -(16t^4 - 92t^3 + 207t^2 - 208t + 76)\varepsilon^{14} + O(\varepsilon^{15})$
$(15,11)$	11	$z^2 = \widetilde{P}_{15,11}(-1 + \varepsilon^2 t, 1, \varepsilon) = (t^4 - 12t^3 - 40t^2 - 28t - 8)\varepsilon^8 + O(\varepsilon^9)$

TABLE 5.1: The modular curves $F_{m,\lambda}$ on $Z_{N,r}$ which have been blown down. Here $\widetilde{P}_{N,r}(x_0, x_1, x_2)$ is a homogeneous polynomial such that $\widetilde{P}_{N,r}(u, v, 1) = P_{N,r}(u, v)$. The two cases when $N = 12, 15$ correspond to the two choices $\lambda \in \{x \in (\mathbb{Z}/N\mathbb{Z})^\times : x^2 = 1\}/\{\pm 1\}$ (note that one of the two curves $F_{17,\lambda}$ has not been blown down when $(N,r) = (15,2)$).

m	Equation for $F^*_{m,\lambda}$ on $W_{12,1}$
13	$\pm v + 1$
25	$2u + v^2 \pm 2v + 1$
37	$2u^2 + (v^2 \pm 2v + 1)u \pm v^3 - 3v^2 \pm 3v - 1$
49	$4u^2 + 2(3v^2 \pm 2v + 3)u + v^4 \pm 4v^3 + 6v^2 \pm 4v + 1$
61	$4u^3 + 2(v^2 \pm 2v + 5)u^2 + (-v^4 \pm 6v^3 - 4v^2 \pm 10v + 5)u \pm v^5 - 5v^4 \pm 10v^3 - 10v^2 \pm 5v - 1$

TABLE 5.2: Modular curves on $W_{12,1}$. The choice of sign corresponds to the two choices of $\lambda \in \{1, 5\}$.

m	Equation for $F^*_{m,\lambda}$ on $W_{12,5}$
17	$u \pm v$
29	$u^2 + 2u - v^2 \pm 2v - 4$
41	$u^3 - (\pm v - 2)u^2 + (-v^2 - 12)u \pm v^3 - 2v^2 \pm 4v + 8$
53	$u^4 - (2v^2 \pm 4v)u^2 + (\pm 8v - 16)u + v^4 \pm 4v^3 + 8v^2 + 16$

Table 5.3: Modular curves on $W_{12,5}$. The choice of sign corresponds to the two choices of $\lambda \in \{1, 5\}$.

m	Equation for $F^*_{m,\lambda}$ 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	$(v^2 \mp 6v + 1)u^2 + (-2v^2 \pm 4v - 2)u - v^4 \mp 2v^3 \pm 2v + 1$

Table 5.4: Modular curves on $W_{12,7}$. The choice of sign corresponds to the two choices of $\lambda \in \{1, 5\}$.

m	Equation for $F^*_{m,\lambda}$ 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	$(\pm 3v^3 + 2v^2 \pm 3v)u + v^4 \pm v^3 + 4v^2 \pm v + 1$
59	$(-3v^4 \pm 3v^3 - v^2 \pm v)u \pm v^5 + 8v^4 \pm 7v^3 + 11v^2 \pm 4v + 1$
71	$(\pm 7v^5 \pm 10v^3 \mp v)u + v^6 \mp v^5 + 15v^4 \pm 10v^3 + 15v^2 \pm 7v + 1$

Table 5.5: Modular curves on $W_{12,11}$. The choice of sign corresponds to the two choices of $\lambda \in \{1, 5\}$.

m	Equation for F^*_m on $W_{14,1}$
25	$u - v + 1$
29	$(v - 1)u - 1$
37	$(v - 1)u^2 - (v^2 + 1)u + v^2$
39	$u^2 - vu + v$
43	$(v - 1)u^2 - v^2u + v^2 + 1$
51	$(v - 1)u^3 - (v^2 - 2v + 2)u^2 - (v^2 - v + 1)u + v^2$
53	$(v - 1)u^2 - v(v - 1)u + v^2 - v + 1$
57	$(v - 1)u^3 - (2v^2 - 3v + 2)u^2 + (v^3 + v - 1)u - v(v^2 - v + 1)$
71	$(v - 1)u^3 - vu^2 + u + v$
81	$(v - 1)u^4 - (v^2 - v + 2)u^3 + (v^2 + v - 1)u^2 + vu - v^2$

Table 5.6: Modular curves on $W_{14,1}$.

m	Equation for F^*_m on $W_{14,3}$
27	$u + v^2 - v + 2$
31	$u + v(v + 1)$
33	$u^2 + (v^2 + 3)u - (v + 1)(v^2 + v - 4)$
41	$(v + 3)u - (v - 1)(v + 5)$
45	$u^2 + (v - 1)^2u - (v + 1)(v^2 - 5v - 2)$
47	$u^2 + (v + 1)^2u - (v - 2)(v + 1)^2$
55	$u^2 + (v^2 - 4v - 1)u - (v + 1)(v^2 - 7v + 4)$
59	$(v^2 + 3)u - (v + 1)(v^2 - 4v - 1)$
61	$u^2 + (v + 1)^2u - v^3 - 4v^2 + 11v - 2$

Table 5.7: Modular curves on $W_{14,3}$.

m	Equation for $F^*_{m,\lambda}$ on $W_{15,2}$	
17	$v-1$	
23	v	∞
32	$u+v^2-v$	$v(v-1)u-2v^2+2v-1$
38	$(v-1)u^2-(2v-1)u-v^2+2v-1$	$(v-1)u^2-uv^2+v(v^2-v+1)$
47	$u+v-1$	$(v-1)u-v^2+v-1$
53	$(v-1)u^2-v(v+1)u+v$	$(v-1)^2u^2-(v-1)^2u-v(v^2-v+1)$

TABLE 5.8: Modular curves on $W_{15,2}$. The two columns correspond to the two choices $\lambda \in \{1,4\}$. Note that when $N=17$ one of the curves $F^*_{m,\lambda}$ has been blown down, and when $N=23$ one of the curves is the line at infinity in $\mathbb{P}^2$.

m	Equation for $F^*_{m,\lambda}$ on $W_{15,11}$	
26	u	$uv+v^2+v+1$
29	$uv+1$	$uv+v+1$
41	$u+v$	$u+v+1$
44	$u^2v+(v^2+1)u-1$	$u^2v+(v^2+2v+1)u+v+1$
56	$u^2v+(2v^2+v+1)u+v$	$u^2v^2+v^2(v+1)u-v-1$
59	$uv+u+1$	$v(v+1)u+v^3+v^2+2v+1$
71	$uv+u+v$	$v(v+1)u+v^3+2v^2+v+1$

TABLE 5.9: Modular curves on $W_{15,11}$. The two columns correspond to the two choices $\lambda \in \{1,4\}$.

(N,r)	Component of $\boldsymbol{F}_Z$	Equation on $Z_{N,r}$
$(12,1)$	$F^+_{(\mathrm{c,ns})}$	$P_{12,1}(u,v)$
$(12,5)$	$F^+_{(\mathrm{c,s})}$	$P_{12,5}(u,v)$
$(12,7)$	$F^+_{(\mathrm{ns,ns})}$	$P_{(\mathrm{ns,ns})}(u,v)$
	$F^+_{(\mathrm{s,ns})}$	$P_{(\mathrm{s,ns})}(u,v)$
	$F^+_{(\mathrm{c,ns})}$	$P_{(\mathrm{c,ns})}(u,v)$
$(12,11)$	$F^+_{(\mathrm{ns,s})}$	$P_{(\mathrm{ns,s})}(u,v)$
	$F^+_{(\mathrm{s,s})}$	$P_{(\mathrm{s,s})}(u,v)$
	$F^+_{(\mathrm{c,s})}$	$P_{(\mathrm{c,s})}(u,v)$
$(14,1)$	$F^+_{(I,\mathrm{ns})}$	$P_{(I,\mathrm{ns})}(u,v)$
	$F^+_{(\mathrm{c,ns})}$	$P_{(\mathrm{c,ns})}(u,v)$
$(14,3)$	$F^+_{(I,\mathrm{s})}$	$P_{(I,\mathrm{s})}(u,v)$
	$F^+_{(\mathrm{c,s})}$	$P_{(\mathrm{c,s})}(u,v)$
$(15,2)$	$F^+_{(\mathrm{s,ns})}$	$P_{15,2}(u,v)$
$(15,11)$	$F^+_{(\mathrm{s,s})}$	$P_{15,11}(u,v)$

TABLE 5.10: The components of $\boldsymbol{F}_Z$ on our model for $Z_{N,r}$. Here the factors $P_{(\bullet,\blacksquare)}(u,v) \in \mathbb{Z}[u,v]$ are the factors of $P_{N,r}(u,v)$ defined in Appendix A.1.

5.4.2 The modular curves F_g^+

When $N = 12$, 14, and 15 we identify the components of the fixed point locus $\boldsymbol{F}_Z$ defined in Section 3.3.1. By Corollary 3.3.11 when $N = 12$ the divisor $\boldsymbol{F}_Z$ consists of either 5 components (when $r = 1$), 3 components (when $r = 7, 11$), or 1 component (when $r = 5$). Similarly when $N = 14$ the divisor $\boldsymbol{F}_Z$ consists of 4 components $r = 1$ and 2 components when $r = 3$. However, when $r = 1$, the components $F_{1,\lambda}$ and $F^+_{\lambda(\mathrm{b},I)}$ are blown down on our models and we do not attempt to identify them on a blow-up.

5.5 Families of congruences and Theorem 1.0.10

To prove Theorem 1.0.10 we find curves $C \subset Z_{N,r}$ of genus 0 or 1 with infinitely many rational points. In Lemma 5.5.6 we prove that by specialising along the resulting families of (N, r)-congruent elliptic curves (which are defined over the function field of C) we are able to find infinitely many examples of (N, r)-congruences, and if a single such example does not come from an isogeny then the same is true for infinitely many examples. We first give the curves $C \subset Z_{N,r}$ explicitly in terms of our models for $Z_{N,r}$ when $(N, r) = (12, r)$ and $(14, 1)$.

5.5.1 Families of 12-congruences

Example 5.5.1 (A family of $(12, 1)$-congruences)**.** Examples of pairs of $(12, 1)$-congruent elliptic curves over $\mathbb{Q}(t)$ have previously been given by Chen [Che16, Section 7.3] and Fisher [Fis20]. We include one here for completeness. The model $z^2 = P_{12,1}(u, v)$ has an obvious elliptic fibration over the t-line given by $y^2 = P_{12,1}(x, t)$. 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

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

Moreover the sections with x-coordinate $\frac{3(2t^8+37t^6+450t^4-27t^2+54)}{(t-3)^2}$ 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 [Fis20, 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 $\mathcal{E}_{12,1}/\mathbb{Q}(t)$ and $\mathcal{E}'_{12,1}/\mathbb{Q}(t)$ where

$$\begin{aligned} \mathcal{E}_{12,1} &: y^2 = x^3 - 3(t^2+1)(4t^2+2t+1)p(t)x - 2(t^2+1)^2(4t^2+2t+1)q(t) \\ \mathcal{E}'_{12,1} &: y^2 = x^3 - 3(t^2+1)(4t^2+2t+1)p'(t)x + 2(t^2+1)^2(4t^2+2t+1)q'(t) \end{aligned}$$

and

$$\begin{aligned} p(t) = {} & 36t^{12} + 234t^{11} + 693t^{10} + 1530t^9 + 2808t^8 + 4128t^7 + 4964t^6 + 4792t^5 + 3652t^4 + 2000t^3 \\ & + 736t^2 + 160t + 16, \\ q(t) = {} & 432t^{18} + 4320t^{17} + 20196t^{16} + 63720t^{15} + 159111t^{14} + 330453t^{13} + 581103t^{12} + 875862t^{11} \\ & + 1137762t^{10} + 1270440t^9 + 1208628t^8 + 960528t^7 + 622592t^6 + 320528t^5 + 127472t^4 \end{aligned}$$

$$
\begin{aligned}
&+ 37728t^3 + 7840t^2 + 1024t + 64,\\
p'(t) = {}& 55396t^{12} - 97238t^{11} + 230581t^{10} - 206878t^9 + 177280t^8 - 86384t^7 + 2612t^6 - 6600t^5\\
&+ 900t^4 - 1008t^3 + 288t^2 + 288t + 144,\\
q'(t) = {}& 26076112t^{18} - 62137376t^{17} + 165178492t^{16} - 207914808t^{15} + 236336753t^{14} - 163049017t^{13}\\
&+ 71325401t^{12} - 36145662t^{11} + 7345854t^{10} - 7544088t^9 + 2972844t^8 + 1350576t^7\\
&+ 531072t^6 - 137808t^5 - 17712t^4 - 4320t^3 + 14688t^2 + 6912t + 1728.
\end{aligned}
$$

Example 5.5.2 (A family of $(12,5)$-congruences)**.** Our model for the surface $Z_{12,5}$ contains the genus 1 curve given by the vanishing of $u^3 + 3u^2 - (v^2+10)u - 3v^2 + 6$. This curve is birational over $\mathbb{Q}$ to the elliptic curve $\mathcal{C}/\mathbb{Q}$ given by the Weierstrass equation

$$\mathcal{C} : \eta^2 = \xi^3 - \xi^2 - 16\xi + 16.$$

The elliptic curve $\mathcal{C}$ has LMFDB label `240.a3` 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 $\mathbb{Q}(\mathcal{C})$ in terms of ξ and η. The Weierstrass equations are too complicated to reproduce here, but we include them in the electronic data [Fre23b].

Example 5.5.3 (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 $\mathcal{E}_{12,7}/\mathbb{Q}(t)$ and $\mathcal{E}'_{12,7}/\mathbb{Q}(t)$ where

$$
\begin{aligned}
\mathcal{E}_{12,7} &: y^2 = x^3 - 3\frac{(t^2+3)(t^4-3t^2+9)p(t)}{(t^4+3)(t^4+27)}x - 2\frac{(t^2+3)(t^4-3t^2+9)q(t)}{(t^4+3)(t^4+27)}\\
\mathcal{E}'_{12,7} &: y^2 = x^3 - 3(t^2+3)(t^4-3t^2+9)(t^4+3)(t^4+27)p'(t)x\\
&\qquad - 2(t^2+3)(t^4-3t^2+9)(t^4+3)^2(t^4+27)^2q'(t)
\end{aligned}
$$

and

$$
\begin{aligned}
p(t) = {}& t^{18} - 18t^{16} + 135t^{14} - 729t^{12} + 2889t^{10} - 7533t^8 + 15093t^6 - 15795t^4 + 53946t^2 + 2187,\\
q(t) = {}& t^{26} - 27t^{24} + 309t^{22} - 2133t^{20} + 10341t^{18} - 35559t^{16} + 85158t^{14} - 109350t^{12} - 141345t^{10}\\
&+ 1337715t^8 - 3133971t^6 + 4183731t^4 + 3483891t^2 - 59049,\\
p'(t) = {}& t^{18} + 222t^{16} - 585t^{14} + 5031t^{12} - 22599t^{10} + 78003t^8 - 177147t^6 + 295245t^4 - 354294t^2\\
&+ 177147,\\
q'(t) = {}& t^{26} - 531t^{24} - 5739t^{22} + 38691t^{20} - 148635t^{18} + 141345t^{16} + 984150t^{14} - 6897798t^{12}\\
&+ 25922511t^{10} - 67847301t^8 + 125951517t^6 - 164215269t^4 + 129140163t^2 - 43046721.
\end{aligned}
$$

Example 5.5.4 (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 $\mathcal{E}_{12,11}/\mathbb{Q}(t)$ and $\mathcal{E}'_{12,11}/\mathbb{Q}(t)$ where

$$
\begin{aligned}
\mathcal{E}_{12,11} : y^2 = x^3 &- 3\frac{(25t^6+63t^4+27t^2-27)(t^6+15t^4+3t^2-27)}{(t^4-18t^2-27)(t^4+6t^2-3)}x\\
&- 2\frac{(25t^6+63t^4+27t^2-27)(5t^8-24t^6-78t^4+81)}{(t^4-18t^2-27)(t^4+6t^2-3)}
\end{aligned}
$$

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

and

$$\begin{aligned}
p'(t) &= 25t^{20} + 18t^{18} - 1971t^{16} - 16200t^{14} - 138942t^{12} - 367092t^{10} - 500526t^8 - 332424t^6 \\
&\quad - 13851t^4 + 1458t^2 + 6561, \\
q'(t) &= 3125t^{32} + 30000t^{30} + 94800t^{28} + 878688t^{26} + 25070580t^{24} + 173317968t^{22} + 693690912t^{20} \\
&\quad + 1821351744t^{18} + 3069524646t^{16} + 3140007120t^{14} + 1733188752t^{12} + 288404064t^{10} \\
&\quad - 233440380t^8 - 163447632t^6 + 7558272t^4 - 1594323.
\end{aligned}$$

5.5.2 Families of 14-congruences

Example 5.5.5 (A family of $(14, 1)$-congruences)**.** The locus on our model for the surface $Z_{14,1}$ given by the vanishing of $(v - 1)u - v^2 + v - 3$ consists of a pair of genus 0 curves. Each of these curves corresponds to the j-invariant of the elliptic curves $\mathcal{E}_{14,1}/\mathbb{Q}(t)$ and $\mathcal{E}'_{14,1}/\mathbb{Q}(t)$ given by the Weierstrass equations

$$\begin{aligned}
\mathcal{E}_{14,1} &: y^2 = x^3 - 3(t + 1)^2 x + \frac{2(3t^6 + 4t^5 + 43t^4 + 70t^3 + 109t^2 + 70t + 43)}{3t^3 - 5t^2 - 5t - 11} \\
\mathcal{E}'_{14,1} &: y^2 = x^3 - 3(t + 1)(3t^3 - 5t^2 - 5t - 11)p'(t)x + (3t^3 - 5t^2 - 5t - 11)q'(t)
\end{aligned}$$

where

$$\begin{aligned}
p'(t) &= 27t^{18} + 108t^{17} + 360t^{16} + 640t^{15} - 5268t^{14} - 32736t^{13} - 129704t^{12} - 355008t^{11} \\
&\quad - 790704t^{10} - 1421888t^9 - 2162112t^8 - 2743296t^7 - 2954816t^6 - 2641920t^5 - 1964160t^4 \\
&\quad - 1161728t^3 - 536832t^2 - 170496t - 33536, \\
q'(t) &= 486t^{30} + 3240t^{29} + 13581t^{28} + 34794t^{27} + 285807t^{26} + 1845962t^{25} + 8698045t^{24} \\
&\quad + 28851216t^{23} + 65140096t^{22} + 65237792t^{21} - 220441776t^{20} - 1513296640t^{19} \\
&\quad - 5375592848t^{18} - 14427212544t^{17} - 32026924704t^{16} - 61000786176t^{15} - 101600600256t^{14} \\
&\quad - 149504306688t^{13} - 195480630144t^{12} - 227655581184t^{11} - 236160499200t^{10} \\
&\quad - 217723224576t^9 - 177612973824t^8 - 127308136448t^7 - 79371799552t^6 - 42414931968t^5 \\
&\quad - 19022485504t^4 - 6930857984t^3 - 1947058176t^2 - 381009920t - 40738816.
\end{aligned}$$

That $\mathcal{E}_{14,1}$ and $\mathcal{E}'_{14,1}$ are $(7, 1)$-congruent may be checked using the formulae for $X_E(7)$ in [HK03] or [Fis14]. It follows by construction that $\mathcal{E}_{14,1}$ and $\mathcal{E}'_{14,1}$ are $(14, 1)$-congruent. Finally by specialising at (for example) $t = 1$ we see that $\mathcal{E}_{14,1}$ and $\mathcal{E}'_{14,1}$ are non-isogenous.

5.5.3 Proof of Theorem 1.0.10

We now complete the proof of Theorem 1.0.10. We first require a lemma which allows us to specialise a family of non-trivially N-congruent elliptic curves over a function field.

Lemma 5.5.6. *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 non-singular and do not have CM. If $j(\mathcal{E}_P)$ and $j(\mathcal{E}'_P)$ are not j-invariants of m-isogenous elliptic curves over $\mathbb{Q}$ for any integer m then for all but finitely many $Q \in C(\mathbb{Q})$ we have that $j(\mathcal{E}_Q)$ and $j(\mathcal{E}'_Q)$ are not the 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 non-singular 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 [Fis15, Theorem 1.5] which we reproduce here for completeness.

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

Let C' be the image of the map $C \to X(1) \times X(1)$ given by extending $t \mapsto (j(\mathcal{E}), j(\mathcal{E}'))$. Consider the curves, T_m, on $X(1) \times X(1)$ which are the image of the modular curves $X_0(m)$ under the graph of the Hecke correspondence. Since the curves T_m are geometrically irreducible and $j(\mathcal{E}_P)$ and $j(\mathcal{E}'_P)$ are not j-invariants of $\mathbb{Q}$-isogenous elliptic curves, the curve C' meets each T_m at finitely many points (over $\overline{\mathbb{Q}}$).

Mazur [Maz78] and Kenku [Ken82] 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 $j\colon C \to C'$ has finite degree.

(ii) We define a morphism $j\colon C \to \mathbb{P}^1 \cong X(1)$ by extending $j(\mathcal{E})$. Let $\mathcal{M}$ be the set of all maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. For each $H \in \mathcal{M}$ let $X(H)/\mathbb{Q}$ denote the modular curve whose K-points parametrise elliptic curves E/K such that $\bar{\rho}_{E,N}(G_{\mathbb{Q}})$ is contained in a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ conjugate to H (see e.g., [RSZ22, Section 2]). Let C_H be the fibre product

$$\begin{array}{ccc} C_H & \longrightarrow & X(H) \\ {\scriptstyle \phi_H}\downarrow & & \downarrow \\ C & \xrightarrow{\ j\ } & X(1) \end{array}$$

We claim that the set

$$C(\mathbb{Q}) \setminus \bigcup_{H \in \mathcal{M}} \phi_H(C_H(\mathbb{Q}))$$

is infinite.

First suppose that C has genus 0. Note that the morphisms ϕ_H have degree greater than 1 because the mod N Galois representation attached to $\mathcal{E}_P/\mathbb{Q}$ is surjective. Therefore since $\mathcal{M}$ is finite $\bigcup_{H \in \mathcal{M}} \phi_H(C_H(\mathbb{Q}))$ is a thin set in the sense of Serre. The claim follows from Hilbert's Irreducibility Theorem [Ser08, 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 ≥ 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 [Sil09, 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 $\mathcal{E}_P/\mathbb{Q}$ 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 Φ_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. □

Proof of Theorem 1.0.10. Consider the pairs of elliptic curves, $E_{12,r}/\mathbb{Q}$ and $E'_{12,r}/\mathbb{Q}$ given by specialising the pairs in Examples 5.5.1, 5.5.3, and 5.5.4 at $t = 2$ and the pair in Example 5.5.2 at the point $(\xi, \eta) = (0, 4)$. Similarly consider the pair of elliptic curves $E_{14,1}/\mathbb{Q}$ and $E'_{14,1}/\mathbb{Q}$ given by specialising the pairs in Example 5.5.5 at $t = 2$. The hypotheses of condition (i) in Lemma 5.5.6 are satisfied since for each $(N, r) = (12, 1)$, $(12, 5)$, $(12, 7)$, $(12, 11)$, and $(14, 1)$ the curve $E_{N,r}$ is alone in its $\mathbb{Q}$-isogeny class. The first claim then follows from Lemma 5.5.6(i).

Applying Zywina's algorithm [Zyw22] we check that the mod N Galois representation $\bar{\rho}_{E,N}$ is surjective for each $N = 12, 14$ and $E = E_{N,r}$. □

5.6 The proof of Theorem 1.0.12

First note that neither $E_{(15,2)}$ and $E'_{(15,2)}$ nor $E_{(15,11)}$ and $E'_{(15,11)}$ are (geometrically) isogenous. We first show that $E_{(15,2)}$ and $E'_{(15,2)}$ are $(15, 2)$-congruent over $\mathbb{Q}$. Consider the point

$$(u, v, z) = \left(\frac{-68}{65}, \frac{23}{10}, \frac{8639891337}{211250000}\right)$$

on our model for $Z_{15,2}$. It is simple to check from the moduli interpretation for $Z_{15,2}$ that this point corresponds to a pair of elliptic curves with the same j-invariants as $E_{(15,2)}$ and $E'_{(15,2)}$. In particular, $E_{(15,2)}$ is $(15, 2)$-congruent over $\mathbb{Q}$ to a quadratic twist of $E'_{(15,2)}$. By Lemma 5.1.7 such a quadratic twist must be supported on the bad primes of $E_{(15,2)}$ and $E'_{(15,2)}$ and checking traces of Frobenius modulo a few small primes for each allowable quadratic twist of $E'_{(15,2)}$ suffices to show that the quadratic twist must be trivial.

The same argument, applied to the point

$$(u, v, z) = \left(\frac{-17}{966}, \frac{7}{2}, \frac{2588569292309}{5561000352}\right)$$

on our model for $Z_{15,11}$ suffices to show that $E_{(15,11)}$ and $E'_{(15,11)}$ are $(15, 11)$-congruent over $\mathbb{Q}$. □

Remark 5.6.1. There are many ways to conclude the above proof rather than comparing traces of Frobenius across quadratic twists. For example one may compare (finitely many) traces of Frobenius using the criteria [KO92, Proposition 4] which relies on a Sturm bound (see also [CF22, Section 3.2]). It is also possible to check that $E_{(15,r)}$ and $E'_{(15,r)}$ are both 3 and 5-congruent over $\mathbb{Q}$ using Fisher's equations for $X_E^r(3)$ and $X_E^r(5)$ in [Fis12].

5.7 Further examples of N-congruences

When $N \geq 12$ and $(N, r) \neq (12, 1)$ the surfaces $Z_{N,r}$ are of general type and we would expect by the Bombieri–Lang conjecture that they contain at most finitely many curves of genus 0 or 1. In

Equation for C^*	Genus of C	Primes where C is locally insoluble	Has $\mathbb{Q}$-point	LMFDB label of the Jacobian of C	Rank
$u \pm v - 1$	0	$\{3, \infty\}$	No		
$v^2 + 1$	$0^\dagger$		No		
$-u^2 + v^2 + 2$	$0^\dagger$		No		
$u^3 + 3u^2 - (v^2 + 10)u - 3v^2 + 6$	1		Yes	240.a3	1
$-u + 2 \pm uv \mp v + v^2$	1		Yes	32.a4	0
$u^2 - 2u - v^2$	1	$\{2, \infty\}$	No	32.a3	0
$u^2 + 4u - 8 - v^2$	1	$\{3, \infty\}$	No	45.a6	0
$u^2 - 2u + 4 + 2uv - 2v + v^2$	$1^\dagger$		No		
$u^2 - 2u + 2 \pm 2uv \mp 2v + v^2$	$1^\dagger$		No		

TABLE 5.11: Examples of curves $C \subset Z_{12,5}$ of genus 0 or 1 without a known moduli interpretation.

Equation for C^*	Genus of C	Primes where C is locally insoluble	Has $\mathbb{Q}$-point	LMFDB label of the Jacobian of C	Rank
$u^2 + 3u - 2v^2 + 2$	0		Yes		
$u + 2$	$0^\dagger$		No		
$u^2 + 2u - 3 - v^2$	$0^\dagger$		No		
$u + 2 \pm 2v$	1		Yes	2898.n2	1
$u + 2 \pm v$	1		Yes	1224.h1	1
$u^2 - 2u + 3v^2 + 1$	$1^\dagger$		No		
$u^2 - 2u + v^2 + 1$	$1^\dagger$		No		
$u^2 + 2u + v^2 - 1$	1	$\{2, \infty\}$	No	64.a3	0
$u^2 - u + 2v^2$	1	$\{11, \infty\}$	No	7920.ba1	1
$u^2 \pm uv + u + v^2 \pm 2v + 1$	$1^\dagger$		No		

TABLE 5.12: Examples of curves $C \subset Z_{12,7}$ of genus 0 or 1 without a known moduli interpretation.

Equation for C^*	Genus of C	Primes where C is locally insoluble	Has $\mathbb{Q}$-point	LMFDB label of the Jacobian of C	Rank
$(9v^4 + 30v^2 + 5)u - 45v^4 - 6v^2 + 7$	0		Yes		
$u \pm 2v + 1$	1		Yes	32.a4	0

TABLE 5.13: Examples of curves $C \subset Z_{12,11}$ of genus 0 or 1 without a known moduli interpretation.

Equation for C^*	Genus of C	Primes where C is locally insoluble	Has $\mathbb{Q}$-point	LMFDB label of the Jacobian of C	Rank
$(v - 1)u - v^2 + v - 3$	0		Yes		
$u - 2v + 1$	1		Yes	64.a3	0
$v - 1$	1		Yes	36.a3	0
$uv - v - 1$	1		Yes	49.a4	0
$uv - v^2 - u + v - 1$	1		Yes	32.a4	0

TABLE 5.14: Examples of curves $C \subset Z_{14,1}$ of genus 0 or 1 without a known moduli interpretation.

Equation for C^*	Genus of C	Primes where C is locally insoluble	Has $\mathbb{Q}$-point	LMFDB label of the Jacobian of C	Rank
$v + 1$	$0^\dagger$		No		
v	1		Yes	52.a1	0
$u - v + 1$	1		Yes	40.a2	0
$u - 3v + 1$	1		Yes	24.a4	0
$u + v + 1$	1		Yes	24.a3	0

TABLE 5.15: Examples of curves $C \subset Z_{14,3}$ of genus 0 or 1 without a known moduli interpretation.

Tables 5.11–5.15 we record examples of curves of genus 0 or 1 on $Z_{N,r}$ (where $N = 12, 14$ and $(N, r) \neq (12, 1)$) 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 5.11–5.15 an irreducible curve $C \subset Z_{N,r}$ is recorded by its image C^* under the map $Z_{N,r} \to W_{N,r}$. The column "genus" records the genus of C. If C is not geometrically irreducible we write $g^\dagger$ 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 5.7.1. 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. This would answer Question 1.1.1.

By the Bombieri–Lang conjecture we expect any infinite family of rational points on $Z_{14,3}$ to be concentrated on a finite number of curves of genus 0 or 1. To answer Question 1.1.2, it would be interesting to determine whether or not there exists a curve of genus 0 or 1 with infinitely many rational points on $Z_{14,3}$ (which does not lie above $j = \infty$, $j' = \infty$, or a Hecke correspondence on Z_1).

Remark 5.7.2. It is possible to find examples of curves of genus 0 and 1 on $Z_{N,r}$ which do not arise as a Hecke correspondence $F_{m,\lambda}$ but which nevertheless map to the graph of a Hecke correspondence on Z_1. Examples are furnished by the genus 0 curve $u + 2 = 0$ 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 $N \geq 12$ and $(N, r) \neq (12, 1)$ the surfaces $Z_{N,r}$ are of general type [KS98, Theorem 4] so we expect by the Bombieri–Lang conjecture that the rational points are contained in a proper Zariski closed subvariety of $Z_{N,r}$. Except for those points which lie on a known curve of genus 0 or 1 (i.e., a modular curve, a curve recorded in Tables 5.11–5.13, or a curve above the loci $j \in \{0, 1728, \infty\}$, $j' \in \{0, 1728, \infty\}$, or $j = j'$ on Z_1) we found:

- 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,
- 8 points on $Z_{12,11}$ which correspond to 2 pairs of $(12, 11)$-congruent elliptic curves,
- 34 points on $Z_{14,1}$ which correspond to 17 pairs of $(14, 1)$-congruent elliptic curves,
- 44 points on $Z_{14,3}$ which correspond to 21 pairs of $(14, 3)$-congruent elliptic curves,
- 2 points on $Z_{15,2}$ which correspond to one pair of $(15, 2)$-congruent elliptic curves, and
- 2 points on $Z_{15,11}$ which correspond to one pair of $(15, 11)$-congruent elliptic curves.

These points are recorded (together with the corresponding congruent elliptic curves) in the electronic data attached to this thesis [Fre23b].

5.7.1 Examples of N-congruent elliptic curves with small conductor

In Table 5.16 we give examples of non-isogenous $(12, r)$ and $(14, r)$-congruent elliptic curves which have small conductor. When $N = 12, 14$ and $(N, r) \neq (12, 1)$ we list all examples which we found (up to simultaneous quadratic twist) with conductor $\leq 10^{10}$. These examples were constructed by

r	E	E'	r	E	E'
7	735.d2	24255.bh1	5	16039350*	176432850*
7	11830.x2	11830.m1	7	25860114*	336181482*
5	60450.cx2	60450.cw2	7	28594930*	2030240030*
5	76614.o1	1302438*	7	29894410*	29894410*
5	92510.w1	92510.i1	5	39160576*	39160576*
5	769515*	45401385*	7	123160716*	5788553652*
7	838240*	838240*	7	124010865*	124010865*
5	1991985*	1991985*	7	159365310*	159365310*
5	4353790*	4353790*	11	388152270*	388152270*
11	4976690*	4976690*	5	1885555650*	1885555650*
5	5144914*	5144914*	5	2016538368*	2016538368*
5	5355525*	91043925*	5	2992233426*	2992233426*
7	10691890*	10691890*	7	8900609640*	8900609640*
5	13286570*	13286570*			

TABLE 5.16: 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 [LMFDB] (i.e., of conductor $N \geq 500\,000$).

r	E	E'	r	E	E'
1	7128.c1	92664.i1	1	5443823*	397399079*
1	33033.h2	627627*	1	6743475*	6399557775*
1	33453.f1	3780189*	1	7343336*	168896728*
1	36414.r1	36414.q1	3	7535360*	128101120*
3	40362.n1	40362.o2	1	9803430*	9803430*
3	58989.g1	1002813*	3	11120109*	11120109*
3	80142.z1	5690082*	1	11712327*	5048012937*
1	89775.c1	3680775*	3	16071510*	16071510*
1	119658.s1	119658.t1	1	18961965*	18961965*
3	137984.bl1	2621696*	1	25427325*	25427325*
1	142830.bk1	142830.bj1	1	43850157*	43850157*
1	153725.h1	15526225*	1	47486145*	807264465*
1	250325.c1	115900475*	3	47700114*	47700114*
1	306456.l1	3371016*	1	50623111*	3594240881*
1	322137.b1	52508331*	1	63755384*	63755384*
3	453870.bc1	13162230*	1	97990074*	97990074*
3	486013.a1	486013.b1	1	106187939*	6477464279*
3	756150*	756150*	3	142715940*	5851353540*
1	822341*	18913843*	3	283361610*	283361610*
3	858858*	858858*	1	353119921*	6003038657*
1	899197*	38665471*	1	423150310*	423150310*
1	923362*	923362*	1	481871975*	9155567525*
1	2221800*	37770600*	1	521798550*	521798550*
1	2453880*	2453880*	1	525287490*	525287490*
1	2530866*	2530866*	3	913837925*	913837925*
1	2884637*	672120421*	1	6524160174*	6524160174*
1	4346958*	4346958*	1	7248494110*	7248494110*
1	4809679*	62525827*	1	8623259554*	8623259554*

TABLE 5.17: Known examples of pairs of geometrically non-isogenous $(14, r)$-congruent elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ (up to simultaneous quadratic twist) of conductors $\leq 10^{10}$. We write $N*$ for an elliptic curve of conductor N which does not appear in the LMFDB [LMFDB] (i.e., of conductor $N \geq 500\,000$).

searching for rational points on our models for $Z_{N,r}$. When $(N, r) = (12, 1)$ 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 [Fre23b].

We do not include examples where E and E' are quadratic twists since many such examples may be constructed by searching for points on the modular curves in Chapter 4.

Remark 5.7.3. The pair of $(12, 5)$-congruent elliptic curves `60450.cx2` and `60450.cw2` appearing in Table 5.16 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. Similarly, the pair of $(14, 3)$-congruent elliptic curves `40362.n1` and `40362.o2` appearing in Table 5.17 give rise to 4 points on $Z_{14,3}$.

Chapter 6

Elements in the Tate–Shafarevich group of genus 2 Jacobians

Let $C/\mathbb{Q}$ be a genus 2 curve and let $J = \mathrm{Jac}(C)$ be the Jacobian of C. Let $\widehat{J}$ denote the dual of J and equip J with the canonical principal polarisation $\lambda\colon J \to \widehat{J}$ arising from the theta divisor. The principal polarisation λ induces an involution on the endomorphism ring of J known as the *Rosati involution*. Precisely, if $\psi \in \mathrm{End}(J)$ then the Rosati involution is given by $\psi \mapsto \psi^\dagger = \lambda^{-1}\hat{\psi}\lambda$. Here $\hat{\psi}\colon \widehat{J} \to \widehat{J}$ denotes the dual isogeny.

If D is an integer then we say that J has *real multiplication (RM) by* $\mathbb{Z}[\sqrt{D}]$ if the Rosati-fixed subspace, $\mathrm{End}_{\mathbb{Q}}(J)^\dagger$, of the endomorphism ring of J contains a subring isomorphic to $\mathbb{Z}[\sqrt{D}]$. By abuse of terminology, if J has RM by $\mathbb{Z}[\sqrt{D}]$ we say that C has RM by $\mathbb{Z}[\sqrt{D}]$.

In this chapter we prove the following theorem, which provides examples of genus 2 curves $C/\mathbb{Q}$ such that the Tate–Shafarevich group, $Ш(J/\mathbb{Q})$, contains an element of order 7.

Theorem 6.0.1. *For each genus 2 curve $C/\mathbb{Q}$ in Table 6.1 (whose conductor is not decorated with a dagger) the Tate–Shafarevich group $Ш(J/\mathbb{Q})$ of the Jacobian $J = \mathrm{Jac}(C)$ of C contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$.*

Remark 6.0.2. In [Fre23b, `genus-2-sha/data`] we give various other examples with $Ш(J/\mathbb{Q})[7] \neq 0$ and with $\sqrt{N_J} < 10^{13}$.

Central to the proof of Theorem 6.0.1 is the notion of visibility (see e.g., [CM00]). Starting from a genus 2 curve $C/\mathbb{Q}$ with RM by $\mathbb{Z}[\sqrt{2}]$ we use visibility to relate the $(3 \pm \sqrt{2})$-Selmer group of J to the 7-Selmer group of an elliptic curve, thereby allowing us to circumvent an expensive $(3 \pm \sqrt{2})$-descent on J.

Definition 6.0.3. Let A/K and A'/K be abelian varieties. If $\psi\colon A \to B$ and $\psi'\colon A' \to B'$ are isogenies we say that A/K and A'/K are (ψ, ψ')-*congruent* if there exists a G_K-equivariant group isomorphism $\phi\colon A[\psi] \to A'[\psi']$.

Moreover, suppose that $A[\psi]$ and $A'[\psi']$ are equipped with the structure of a symplectic abelian group. We say that A and A' are (ψ, ψ', r)-congruent if there exists a (ψ, ψ')-congruence $\phi\colon A[\psi] \to A'[\psi']$ with power r.

The main technical contribution of this chapter is given in Section 6.3.2 where we describe an algorithm for determining a (p-adic approximation to) the twists of the Klein quartic $X(7)$ which parametrise elliptic curves that are $([3 \pm \sqrt{2}], [7])$-congruent to a fixed genus 2 Jacobian $J/\mathbb{Q}$ with RM by $\mathbb{Z}[\sqrt{2}]$. That is, we compute the twists of $X(7)$ described in Section 2.2.9 with the Galois module $M = J[3 \pm \sqrt{2}]$ (this is a symplectic abelian group by Lemma 6.3.1).

In Section 6.1 we give a brief overview of *visibility* of elements of the Tate–Shafarevich group. In particular, we recall [Fis16, Theorem 2.2]. This allows us to construct elements of the Shafarevich–Tate group of an abelian variety given a (ψ, ψ')-congruence (and some additional local data).

r	$f(x)$	$\sqrt{N_J}$	E
-1	$-10(x^6-4x^5-3x^4+8x^3+25x^2+20x+5)$	3200†	3200.a1
-1	$165(x^6+6x^5+27x^4-2x^3+45x^2+20)$	39325	39325.c2
-1	$-1275(x^6+6x^5+27x^4-2x^3+45x^2+20)$	93925	93925.d1
-1	$285(x^6+6x^5+27x^4-2x^3+45x^2+20)$	117325	117325.c2
-1	$-62(9x^6-12x^5+64x^4-56x^3+136x^2-60x+84)$	184512	184512.bw1
-1	$-184(x^6+6x^5-20x^4+240x^3+70x^2-84x+12)$	203136	203136.i2
-1	$-184(x^6+6x^5-20x^4+240x^3+70x^2-84x+12)$	203136	11985024*
-1	$-80(3x^6+12x^5+89x^4-56x^3-7x^2-132x+99)$	211200	211200.c1
-1	$465(9x^6-12x^5+64x^4-56x^3+136x^2-60x+84)$	216225	432450.ci1
1	$-17160(375x^6-75x^5+2525x^4-1089x^3+6140x^2-4500x+2000)$	243360†	243360.ds1
-1	$-120(11x^6-18x^5+47x^4+6x^3+71x^2+18x+27)$	244800	244800.dc1
1	$-13(x^6-2x^5+3x^4x^3-7x^2-2x+1)$	256880	51376.e1
-1	$-390(x^6+6x^5+27x^4-2x^3+45x^2+20)$	270400	270400.dc2
1	$-708(3x^6+12x^4-10x^3-12x+11)$	281961	2819610*
-1	$-22(x^6-24x^5+100x^4+102x^3-80x^2-132x-39)$	302016	302016.p1
-1	$-6(13x^6-116x^5-316x^4+58x^3+264x^2-116x+13)$	313920	313920.bb1
-1	$-55(13x^6-116x^5-316x^4+58x^3+264x^2-116x+13)$	329725	659450*
-1	$-110(x^6-4x^5-3x^4+8x^3+25x^2+20x+5)$	387200	8905600*
1	$11(x^6+6x^5+11x^4-13x^2+6x-2)$	423984	423984.by1

TABLE 6.1: Examples of genus 2 curves $C\colon y^2 = f(x)$ whose Jacobians $J/\mathbb{Q}$ have conductor $N_J < (500\,000)^2$, and such that $Ш(J/\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$. This subgroup is made visible by a $([3\pm\sqrt{2}],[7])$-congruence (with conjectural power r) between $J/\mathbb{Q}$ and an elliptic curve $E/\mathbb{Q}$. Cases whose conductor is decorated with a dagger remain conjectural (pending the computation of a Tamagawa number at 2). Explicit Weierstrass equations for the corresponding elliptic curves are given in the electronic data [Fre23b, `genus-2-sha/data`]. The curves $C/\mathbb{Q}$ were generated from the formulae of Bending [Ben99, Theorem 4.1] and conductors were computed using code of Dokchitser–Doris [DD19].

A versal family of genus 2 curves $C/\mathbb{Q}$ whose Jacobians have RM by $\mathbb{Z}[\sqrt{2}]$ are given by Bending [Ben99, Ben98], and many examples of small conductor are given in [Ben98, Appendix A]. Bending's family is given by a triple of parameters $A, P, Q \in \mathbb{Q}$. It is simple to search for further examples of small conductor (noting from [Ben98, Section 6.3] that it is often useful to specialise at $P \in \{\pm 1, \pm 1/2, \pm 1/3, \pm 1/5\}$). Combining these with the examples found in the LMFDB [LMFDB] we obtain a small (non-exhaustive) database of curves with RM by $\mathbb{Z}[\sqrt{2}]$ and whose Jacobians have conductor $\sqrt{N_J} \leq 10^{13}$ (these may be found in `genus-2-sha/rm8-examples` at [Fre23b]).

For each curve in this database we apply our algorithm to compute the associated twists of the Klein quartic. By searching for rational points on these twists, we find a number of putative examples of $([3\pm\sqrt{2}],[7])$-congruences between a genus 2 Jacobian $J/\mathbb{Q}$ and an elliptic curve $E/\mathbb{Q}$. Using an approach of Fisher [Fis16] we prove these congruences in Proposition 6.4.1. By finding examples of quadratic twists where there is a rank discrepancy between $E^d/\mathbb{Q}$ and $J^d/\mathbb{Q}$ we obtain elements of the Tate–Shafarevich group of $J^d/\mathbb{Q}$ in Theorem 6.0.1.

We conclude with several examples (and study closely an interesting non-example of Timo Keller) in Section 6.5.

6.1 Visibility

We first briefly recall some generalities about visibility of elements of Tate–Shafarevich groups of abelian varieties, following e.g., [CM00, AS02, AS05, Fis16].

Let A/K and A'/K be abelian varieties defined over a number field K. Suppose that there exist isogenies $\psi\colon A \to B$ and $\psi'\colon A' \to B'$ such that there exists an (ψ,ψ')-congruence $\phi\colon A[\psi] \to A'[\psi']$. The congruence ϕ induces an isomorphism $H^1(K, A[\psi]) \cong H^1(K, A'[\psi'])$ on Galois cohomology.

One might hope that if enough "local coincidences" occur at the bad primes of A and A' then the ψ and ψ'-Selmer groups $S^{(\psi)}(A/K)$ and $S^{(\psi')}(A'/K)$ may be isomorphic. In this case, if the order of the group $B(K)/\psi A(K)$ is smaller than the order of $B'(K)/\psi' A'(K)$ then the latter will contribute to a discrepancy between the order of $B(K)/\psi A(K)$ and $S^{(\psi)}(A/K)$ thereby "explaining" some non-trivial elements of $Ш(A/K)[\psi]$.

To make this idea precise let $\Delta \subset A \times A'$ be the graph of the congruence ϕ and consider the abelian variety $D = (A \times A')/\Delta$. Write ι for the morphism

$$\iota\colon A \to A \times A' \to D.$$

Definition 6.1.1. We say that an element (or subgroup) of $H^1(K, A)$ is *visible in* D if it is contained in the kernel of the homomorphism $\iota_*\colon H^1(K, A) \to H^1(K, D)$. We write $\mathrm{Vis}_D\, H^1(K, A)$, respectively $\mathrm{Vis}_D\, Ш(A/K)$, for the subgroup of $H^1(K, A)$, respectively $Ш(A/K)$, consisting of elements visible in D.

We will use the following theorem (which is proved in [Fis16, Theorem 2.2], see also [AS02] and [AS05, Appendix]), which we state in the case when $K = \mathbb{Q}$.

Theorem 6.1.2. *If $B(\mathbb{Q})/\phi A(\mathbb{Q}) = 0$ then the subgroup $\mathrm{Vis}_D\, H^1(\mathbb{Q}, A)$ of $H^1(\mathbb{Q}, A)$ is isomorphic to $B'(\mathbb{Q})/\phi' A'(\mathbb{Q})$. Moreover if the order, $|\Delta|$, of the subgroup Δ is odd, and*

(i) *all Tamagawa numbers of $A/\mathbb{Q}$ and $A'/\mathbb{Q}$ are coprime to $|\Delta|$, and*

(ii) *the abelian variety D has good reduction at all primes dividing $|\Delta|$*

then $\mathrm{Vis}_D\, Ш(A/\mathbb{Q}) \cong B'(\mathbb{Q})/\phi' A'(\mathbb{Q})$.

6.2 The twisting principle for $X(7)$

Let K be a field of characteristic zero and let $(M, \langle\cdot,\cdot\rangle)$ be a symplectic abelian group over K equipped with a symplectic $\overline{K}$-isomorphism $\iota\colon M \cong \mu_7 \times \mathbb{Z}/7\mathbb{Z}$. Let $X_M(7)$ denote the twist of $X(7)$ defined in Section 2.2.9. Similarly let $X_M^r(7)$ denote the twist of $X(7)$ associated to the symplectic abelian group $(M, \langle\cdot,\cdot\rangle^r)$. When $r = \pm 1$ we write $X_M^r(7) = X_M^{\pm}(7)$. Following [Fis14] we give an explicit description for the twists $X_M^{\pm}(7)$ as plane quartic curves.

Recall that we write Υ_N for the automorphism group (scheme) of the symplectic abelian group $\mu_N \times \mathbb{Z}/N\mathbb{Z}$. In Section 2.2.1 we defined a Galois equivariant representation $\rho\colon \Upsilon_7 \to \mathrm{GL}_3(\overline{K})$ following Klein [Kle78, Elk99, Fis14]. When Υ_7 acts on $\mathbb{P}^2$ via ρ the Klein quartic curve $X(7) \subset \mathbb{P}^2$ given by

$$X(7) : x_0^3 x_1 + x_1^3 x_2 + x_0 x_2^3 = 0$$

is fixed.

Let $\xi\colon G_K \to \mathrm{GL}_3(\overline{K})$ denote the cocycle obtained from ι by the twisting principle. Explicitly, let ξ be the cocycle given by $\sigma \mapsto \rho(\sigma(\iota)\iota^{-1})$. Here $\sigma(\iota)\colon M \cong \mu_7 \times \mathbb{Z}/7\mathbb{Z}$ is the $\overline{K}$-isomorphism given by $P \mapsto \sigma(\iota(\sigma^{-1}P))$.

By Hilbert's Theorem 90 the cocycle ξ is a coboundary, that is, there exists a matrix $A \in \mathrm{GL}_2(\overline{K})$ such that $\sigma(A^{-1})A = \xi(\sigma)$ for every $\sigma \in G_K$.

Lemma 6.2.1. *The curves $X_M(7)$ and $X^-_M(7)$ are isomorphic to the images of the morphisms $X(7) \to \mathbb{P}^2$ given by*

$$\mathbf{x} \mapsto A\mathbf{x} \quad \textit{and} \quad \mathbf{x} \mapsto A^{-T}\mathbf{x}$$

respectively. Here $\mathbf{x}$ is a point in $\mathbb{P}^2$ written as a column vector and A^{-T} denotes the inverse transpose of A.

Proof. The proof is identical to [Fis14, Lemma 3.2]. □

Finally, we note that it is simple to compute the moduli interpretation for a given twist of $X(7)$ following [Fis14, Section 4.1]. More explicitly, let $\mathcal{X} \subset \mathbb{P}^2$ be a twist of $X(7)$ given by the vanishing of a homogeneous quartic polynomial $\mathcal{F}(x_0, x_1, x_2)$. Define

$$D = \frac{-1}{54} \times \begin{vmatrix} \frac{\partial^2\mathcal{F}}{\partial x_0^2} & \frac{\partial^2\mathcal{F}}{\partial x_0\partial x_1} & \frac{\partial^2\mathcal{F}}{\partial x_0\partial x_2} \\ \frac{\partial^2\mathcal{F}}{\partial x_0 x_1} & \frac{\partial^2\mathcal{F}}{\partial x_1^2} & \frac{\partial^2\mathcal{F}}{\partial x_1\partial x_2} \\ \frac{\partial^2\mathcal{F}}{\partial x_0 x_2} & \frac{\partial^2\mathcal{F}}{\partial x_1\partial x_2} & \frac{\partial^2\mathcal{F}}{\partial x_2^2} \end{vmatrix}$$

and define c_4 and c_6 by analogy with the formulae in Section 2.2.1. Then, by the discussion in [Fis14], the j-invariant map $\mathcal{X} \to X(1)$ is given by $1728\frac{c_4^3}{c_4^3 - c_6^2}$.

6.3 An algorithm to compute an approximation to $X^r_{J[3\pm\sqrt{2}]}(7)$

In order to construct twists of $X(7)$ we first need to interpret $J[3 \pm \sqrt{2}]$ as a symplectic abelian group. Let K be a field of characteristic zero and let C/K be a genus 2 curve and let $J = \mathrm{Jac}(C)$ be its Jacobian. Writing $\widehat{J}$ for the dual of J, we have the N-Weil pairing $J[N] \times \widehat{J}[N] \to \mu_N$. Equipping J with the canonical principal polarisation we therefore obtain the non-degenerate pairing $e_{J,N}\colon J[N] \times J[N] \to \mu_N$ which we again refer to as the N-Weil pairing.

Lemma 6.3.1. *Let K be a field of characteristic zero and let J/K be a genus 2 Jacobian with real multiplication by $\mathbb{Z}[\sqrt{2}]$ over K. For each choice of sign the subgroup $J[3 \pm \sqrt{2}] \subset J[7]$, together with the (restriction to $J[3 \pm \sqrt{2}]$ of the) 7-Weil pairing $e_{J,7}$, is isomorphic over $\overline{K}$ to $\mu_7 \times \mathbb{Z}/7\mathbb{Z}$ (equipped with the standard pairing).*

Proof. We have a short exact sequence of G_K-modules

$$0 \to J[3 + \sqrt{2}] \to J[7] \to J[3 - \sqrt{2}] \to 0$$

where the second map is the restriction of the endomorphism $3 + \sqrt{2}$ to $J[7]$. If $P \in J[3 + \sqrt{2}]$ and $Q \in J[3 - \sqrt{2}]$ then there exists $R \in J[7]$ such that $Q = (3 + \sqrt{2})R$. In particular since $\sqrt{2}$ is fixed by the Rosati involution we have

$$e_{J,7}(P, Q) = e_{J,7}(P, (3 + \sqrt{2})R) = e_{J,7}((3 + \sqrt{2})P, R) = 1,$$

and therefore $J[7] = J[3 \pm \sqrt{2}] \oplus J[3 \pm \sqrt{2}]$ is an orthogonal decomposition with respect to $e_{J,7}$, as required. □

6.3.1 Hilbert's Theorem 90 is effective

To compute twists of $X(7)$ using Lemma 6.2.1 we will need to compute matrices which realise a given cocycle as a coboundary. Towards this, note that the standard proof of Hilbert's Theorem 90 is "nearly" effective. Indeed following [Ser79, Proposition X.3] let L/K be a finite extension of infinite fields, let $\xi \in H^1(\mathrm{Gal}(L/K), \mathrm{GL}_n(L))$ be a 1-cocycle, and choose an element $c \in \mathrm{GL}_n(L)$. Define a matrix $b \in \mathrm{M}_n(L)$ by the Poincaré series

$$b = \sum_{\sigma \in \mathrm{Gal}(L/K)} \xi(\sigma)\sigma(c).$$

Since $\xi(\sigma) = \sigma(b)^{-1}b$ it is immediate that ξ is a coboundary, provided that c is chosen so that b is invertible. If L is infinite the linear independence of field embeddings guarantees the existence of c. Indeed, for a fixed cocycle ξ, the failure of b to be invertible is a Zariski closed condition on the matrix c. In particular, for a generic choice of c, the matrix b will be invertible. The proof therefore suggests an algorithm.

Algorithm 6.1 Generating matrices which realise Hilbert's Theorem 90.

Input: A cocycle $\xi \in H^1(\mathrm{Gal}(L/K), \mathrm{GL}_n(L))$.

Output: A matrix $b \in \mathrm{GL}_n(L)$ such that $\xi(\sigma) = \sigma(b)^{-1}b$ for each $\sigma \in \mathrm{Gal}(L/K)$.

1: Choose "randomly" a matrix $c \in \mathrm{GL}_n(L)$.
2: Compute the matrix $b = \sum_\sigma \xi(\sigma)\sigma(c)$.
3: **if** $\det(b) \neq 0$ **then**
4: **return** b
5: **else**
6: Return to step 1.
7: **end if**

Remark 6.3.2. In step 1 of Algorithm 6.1 the user must choose a matrix $c \in \mathrm{GL}_n(L)$. In our application the extension $L/\mathbb{Q}$ will be a finite extension and we will have access to a LLL-reduced $\mathbb{Z}$-basis $\{l_1, ..., l_m\}$ for the ring of integers $\mathcal{O}_L \subset L$. We choose "small" elements of L by generating a tuple $x_1, ..., x_m \in \{0, \pm 1\}$ and considering the element $\sum_{i=1}^m x_i l_i \in \mathcal{O}_L$. This approach extends to choosing a matrix $c \in \mathrm{GL}_n(L)$ by choosing the n^2 entries as described (in practice, we also choose almost all x_i to be equal to zero).

Remark 6.3.3. There is no guarantee that Algorithm 6.1 terminates in finite time. In practice we have found very few instances when Algorithm 6.1 fails to terminate in one iteration.

6.3.2 The main algorithm

Fix a primitive 7^{th} root of unity ζ, and let $J/\mathbb{Q}$ be the Jacobian of a genus 2 curve $C/\mathbb{Q}$. Suppose that J has real multiplication by $\mathbb{Z}[\sqrt{2}]$. Let $\mathcal{K} = J/\{\pm 1\}$ denote the Kummer surface of J. We identify $\mathcal{K}$ with the singular quartic surface in $\mathbb{P}^3$ by the embedding in [CF96, (3.1.8)]. Let x_J denote the quotient morphism $J \to \mathcal{K}$. If $\psi \colon J \to J'$ is an isogeny we write $\mathcal{K}[\psi] = x_J(J[\psi])$.

Let $\mathfrak{p} = (3 \pm \sqrt{2})$ for some choice of sign, so that in $\mathbb{Z}[\sqrt{2}]$ we have a factorisation $(7) = \mathfrak{p}\bar{\mathfrak{p}}$ (where $\bar{\mathfrak{p}}$ denotes the conjugate of $\mathfrak{p}$). We write $L = \mathbb{Q}(\mathcal{K}[\mathfrak{p}])$. Note that for generic $J/\mathbb{Q}$, we have

an isomorphism of abstract groups $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})/\{\pm 1\}$.

By assumption $[\sqrt{2}]\colon J \to J$ is a Richelot isogeny and using the approach in [Nic18a, Section 5.7] (which is implemented in [Nic18b, `richelot/richelot_on_kummer.m`]) we determine explicit polynomials giving the morphism $[\sqrt{2}]\colon \mathcal{K} \to \mathcal{K}$ induced by the action of $\sqrt{2}$ on J. Formulae for the multiplication-by-3 map $[3]\colon \mathcal{K} \to \mathcal{K}$ are given in [CF96, Section 3.5].

Note that $\mathcal{K}[3+\sqrt{2}] \cup \mathcal{K}[3-\sqrt{2}]$ is exactly the set $\{P \in \mathcal{K} : 3P = \sqrt{2}P\}$. By taking successive resultants it is simple to compute polynomials $f_1(t), f_2(t), f_3(t) \in \mathbb{Q}[t]$ such that $\mathcal{K}[\mathfrak{p}]$ is contained in the set

$$\{(1 : \alpha_1 : \alpha_2 : \alpha_3) \in \mathcal{K} : f_1(\alpha_1) = f_2(\alpha_2) = f_3(\alpha_3) = 0\} \cup \{(0 : 0 : 0 : 1)\}.$$

We fix a prime number $p \neq 7$ not dividing the discriminant of $f_1(t)$ and at which J has good reduction. Further suppose that the minimal polynomial of ζ is irreducible over $\mathbb{F}_p$ and that L is equal to the splitting field of $f_1(t)$. Let $\mathfrak{P}$ be a prime of L dividing p and denote by $L_{\mathfrak{P}}$ and $l_{\mathfrak{P}}$ the completion and residue field of L at $\mathfrak{P}$ respectively.

Our algorithm proceeds as follows:

1. Compute the Galois group of $f_1(t)$ using `GaloisGroup` in `Magma`. This gives a group $G \subset S_n$ and a G-set $\{r_1, ..., r_n\}$ of ($\mathfrak{P}$-adic approximations to) the roots of $f_1(t)$ in $L_{\mathfrak{P}}$ such that G gives the action of $\mathrm{Gal}(L/\mathbb{Q})$ on the roots of $f_1(t)$ in L.

2. Compute a ($\mathfrak{P}$-adic approximation to an) embedding $\mathbb{Q}_p(\zeta) \hookrightarrow L_{\mathfrak{P}}$ by computing a $\mathfrak{P}$-adic approximation to ζ.

3. Compute a $\mathbb{Z}/7\mathbb{Z}$-basis $\{\bar{P}, \bar{Q}\}$ for $J(l_{\mathfrak{P}})[\mathfrak{p}]$ which is symplectic with respect to the Weil pairing (via the `Magma` intrinsic `WeilPairing`). This uniquely determines a pair $\{P, Q\} \in \mathcal{K}(L_{\mathfrak{P}})$ which reduce modulo $\mathfrak{P}$ to $x_J(\bar{P})$ and $x_J(\bar{Q})$ respectively.

4. Let $\iota\colon J[\mathfrak{p}] \cong \mu_7 \times \mathbb{Z}/7\mathbb{Z}$ be the isomorphism given by $P \mapsto (\zeta, 0)$ and $Q \mapsto (1, 1)$. Determine explicitly the 1-cocycle
$$\xi\colon \mathrm{Gal}(L/\mathbb{Q}) \cong G \to \mathrm{PGL}_3(\mathbb{Q}(\zeta)).$$

5. Compute a ($\mathfrak{P}$-adic approximation to) a matrix $A \in \mathrm{PGL}_3(L) \subset \mathrm{PGL}_3(L_{\mathfrak{P}})$ which realises ξ as a coboundary, using Algorithm 6.1.

6. Twist $X(7)$ by A and A^{-T} to obtain curves $X^{\pm} \subset \mathbb{P}^2_{L_{\mathfrak{P}}}$. By Lemma 6.2.1 these twists are $\mathfrak{P}$-adic approximations to the twists $X^{\pm}_{J[\mathfrak{p}]}(7) \subset \mathbb{P}^2_{\mathbb{Q}}$. After normalising each equation so that the first non-zero coefficient is equal to 1, the curves obtained therefore have coefficients in $\mathbb{Q}$ (up to a numerical error).

7. Recognise the coefficients of the twists $X^{\pm}$ as rational numbers using the LLL algorithm.

8. Minimise and reduce the models for $X^{\pm}$ using the algorithm of Elsenhans–Stoll [ES21], which is implemented in `Magma` as `MinRedTernaryForm`.

Remark 6.3.4. Computing the matrix $A \in \mathrm{PGL}_3(L_{\mathfrak{P}})$ must be done with some care in order to control coefficient explosion (and to minimise the $\mathfrak{P}$-adic precision we must carry throughout the calculation). In our implementation we assume that $J[\mathfrak{p}]$ is an irreducible $G_{\mathbb{Q}}$-module and (heavily) rely on the following observation:

Since the Galois module $J[\mathfrak{p}]$ is irreducible, there exists a subfield $\mathbb{Q} \subset K \subset L$ (which is unique up to conjugacy) such that $\mathcal{K}[\mathfrak{p}]$ contains a $\mathrm{Gal}(L/K)$-stable "cyclic subgroup" (or more

precisely, the image of a cyclic subgroup of $J[\mathfrak{p}]$). From the properties of the Weil pairing we have $L = \mathbb{Q}(\zeta)K$.

We first compute an LLL-reduced basis $\{1, k_1, ..., k_7\}$ for $K/\mathbb{Q}$. The elements $k\zeta^i$ form a $\mathbb{Q}$-basis for $L/\mathbb{Q}$ where $0 \leq i \leq 6$ and k ranges over the $\mathrm{Gal}(L/\mathbb{Q})$-conjugates of k_j for each $1 \leq j \leq 7$. We then apply Algorithm 6.1 noting Remark 6.3.2.

Remark 6.3.5. It would be interesting to compute the twists $X^r_{\mathcal{J}[\mathfrak{p}]}(7)$ for the Jacobian $\mathcal{J}$ of the curve $\mathcal{C}/\mathbb{Q}(Y_-(8))$ given in [Ben98, Ben99] (here, as in Chapter 2, $Y_-(8)$ denotes the Hilbert modular surface of discriminant 8 which parametrises abelian surfaces with RM by $\mathbb{Z}[\sqrt{2}]$). Unfortunately the algorithm we describe is ill suited to this task. One might hope to interpolate over twists computed for a large number of specialisations. However these twists are only defined up to the action of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{P}^2) \cong \mathrm{PGL}_3(\mathbb{Q})$ and our algorithm for generating Hilbert 90 matrices does not do so in a compatible way (it requires a choice of sign, a choice of basis for $J[\mathfrak{p}]$, and a "randomly" generated matrix).

6.4 Proving $([3 \pm \sqrt{2}], [7])$-congruences

We now prove Theorem 6.0.1, by showing the pairs (C, E) in Table 6.1 are in fact $([3 \pm \sqrt{2}], [7])$-congruent.

Proof of Theorem 6.0.1. To show that $Ш(J/\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$ first note that in each case the Tamagawa numbers of $E/\mathbb{Q}$ and $J/\mathbb{Q}$ are coprime to 7 (the orders of the component groups of J were computed using both Liu's `genus2reduction` in `Sage` [Sage] and Donnelly's `Magma` functions `ComponentGroup` and `RegularModel`). The torsion subgroups of $E/\mathbb{Q}$ and $J/\mathbb{Q}$ are trivial, the rank of $E/\mathbb{Q}$ is 2, and the rank of $J/\mathbb{Q}$ is 0 (the latter can be checked using e.g., the intrinsic `RankBounds` in `Magma` [BCP97]). The following proposition shows that J and E are $([3 \pm \sqrt{2}], [7])$-congruent, and applying Theorem 6.1.2 proves that $Ш(J/\mathbb{Q})[7]$ contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$ which is visible in $(J \times E)/\Delta$. □

Proposition 6.4.1. *For each pair (C, E) of genus 2 curve $C/\mathbb{Q}$ and elliptic curve $E/\mathbb{Q}$ in Table 6.1 we have a $([3 \pm \sqrt{2}], [7])$-congruence between $J = \mathrm{Jac}(C)$ and E for some choice of sign.*

Proof. We follow the approach taken in [Fis16, Theorem 6.3]. Let $\mathcal{K} = J/\{\pm 1\}$ be the Kummer surface of J given by the model in [CF96, Chapter 3] and let $x_J \colon J \to \mathcal{K}$. Similarly let $x_E \colon E \to E/\{\pm 1\} \cong \mathbb{P}^1$. We check in each case that the mod 7 Galois representation attached to $E/\mathbb{Q}$ is surjective using Zywina's algorithm [Zyw22]. By [Fis16, Proposition 6.1] to show that there exists a quadratic twist $E^d/\mathbb{Q}$ of $E/\mathbb{Q}$ which is $([3 \pm \sqrt{2}], [7])$-congruent to $J/\mathbb{Q}$ it therefore suffices to show that there exist points $P \in J[3 \pm \sqrt{2}]$ and $Q \in E[7]$ such that the fields $\mathbb{Q}(x_J(P))$ and $\mathbb{Q}(x_E(Q))$ are isomorphic. Using the approach detailed in [Fis16, Theorem 6.3] we give an explicit degree 24 number field $L/\mathbb{Q}$ and equations for points $x_J(P) \in \mathcal{K}(L)$ and $x_E(Q) \in \mathbb{P}^1(L)$ which generate $L/\mathbb{Q}$.

As discussed in [Fis16, (5.2)] by [FLS+01, Section 2.1] or [MS93, Lemma 3] an isomorphism of Galois modules $J[3 \pm \sqrt{2}] \cong E^d[7]$ induces a congruence

$$a_p(E^d)^2 - t_p a_p(E^d) + n_p \equiv 0 \pmod 7. \tag{6.1}$$

Here $t_p = p+1-N_1$ and $n_p = (N_1^2+N_2)/2-(p+1)N_1-p$ where $N_1 = \#C(\mathbb{F}_p)$ and $N_2 = \#C(\mathbb{F}_{p^2})$.

By the same reasoning as Lemma 5.1.7 if $d \in \mathbb{Z}$ is chosen to be squarefree then d is divisible only by bad primes of E and C. Let D be the product of the bad primes of C and E. In each

example, the congruence in (6.1) fails to hold for each divisor $d \neq 1$ dividing $\pm D$ for some p. It therefore follows that $J[3 \pm \sqrt{2}]$ and $E[7]$ are isomorphic as $G_{\mathbb{Q}}$-modules. □

6.5 Examples

6.5.1 The proof of Theorem 1.0.18

Let $C/\mathbb{Q}$ be the genus 2 curve given by the Weierstrass equation

$$C : y^2 = -10(x^6 - 10x^5 + 32x^4 - 40x^3 + 38x^2 - 20x + 4).$$

We compute with using the methods of Dokchitser–Doris [DD19] that the conductor of $J = \mathrm{Jac}(C)$ is 3200^2. Moreover, J is geometrically simple and has $\mathbb{Z}[\sqrt{2}]$-multiplication defined over $\mathbb{Q}$ (the curve C is a quadratic twist of the curve given by taking $(A, P, Q) = (-10, 1, -5)$ in [Ben99, Theorem 4.1]). By Proposition 6.4.1 for some choice of sign J is $([3 \pm \sqrt{2}], [7])$-congruent to the elliptic curve with LMFDB label `3200.a1` and Weierstrass equation

$$E : y^2 = x^3 - 100x + 400.$$

Moreover, if $\Delta \subset J \times E$ is the graph of this congruence, then by Theorem 6.0.1 the group $Ш(J/\mathbb{Q})$ contains a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$ which is visible in the abelian three-fold $(J \times E)/\Delta$.

6.5.2 A (non)-example worthy of further study

The following interesting example was provided to me by Timo Keller. Consider the genus 2 curve $C/\mathbb{Q}$ with LMFDB label `385641.a.385641.1` and Weierstrass equation

$$y^2 + (x^3 + 1)y = -6x^4 + 6x^3 + 27x^2 - 30x - 22.$$

Let $J/\mathbb{Q}$ be the Jacobian of C and let $d = -11$. We check with van Bommel's code [vB21] that the Birch and Swinnerton-Dyer conjecture predicts that $|Ш(J^d/\mathbb{Q})| = 7^2$. The algorithm in Section 6.3.2 outputs the four Klein quartic twists

$$\begin{aligned}
X_1^+ &: x_0^4 - 3x_0^3x_1 - 28x_0^3x_2 - 15x_0^2x_1^2 - 3x_0^2x_1x_2 + 39x_0^2x_2^2 - 6x_0x_1^3 - 12x_0x_1^2x_2 \\
&\quad - 6x_0x_1x_2^2 - 29x_0x_2^3 + 3x_1^4 + 9x_1^3x_2 + 30x_1^2x_2^2 - 3x_1x_2^3 - 10x_2^4 = 0, \\
X_1^- &: -4x_0^4 + 6x_0^3x_1 + 7x_0^3x_2 + 3x_0^2x_1^2 + 12x_0x_1^3 + 6x_0x_1^2x_2 - 9x_0x_1x_2^2 - x_0x_2^3 \\
&\quad - 6x_1^4 - 3x_1^3x_2 + 3x_1^2x_2^2 + 6x_1x_2^3 + x_2^4 = 0, \\
X_2^+ &: -2x_0^4 + 39x_0^3x_1 + 11x_0^3x_2 - 42x_0^2x_1^2 - 18x_0^2x_1x_2 + 20x_0x_1^3 - 6x_0x_1^2x_2 \\
&\quad + 12x_0x_1x_2^2 - 7x_0x_2^3 - 24x_1^4 + 13x_1^3x_2 + 15x_1^2x_2^2 + 9x_1x_2^3 + x_2^4 = 0, \\
X_2^- &: 2x_0^4 + 5x_0^3x_1 + 9x_0^3x_2 + 6x_0^2x_2^2 - x_0x_1^3 - 6x_0x_1^2x_2 + 12x_0x_1x_2^2 + 2x_0x_2^3 \\
&\quad - x_1^4 - 3x_1^3x_2 + 3x_1^2x_2^2 + 17x_1x_2^3 + 12x_2^4 = 0.
\end{aligned}$$

Naively searching for points on these curves (using `PointSearch` in `Magma`) yields no rational points on X_1^+, X_1^-, and X_2^+. However, there is one rational point on X_2^- which corresponds to the elliptic curve $E/\mathbb{Q}$ with LMFDB label `1242.m1`, and Weierstrass equation $y^2 + xy + y = x^3 - x^2 - 1666739x - 2448131309$.

Lemma 6.5.1. *After choosing an appropriate embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathrm{End}_{\mathbb{Q}}(J)$ the curves $X_1^{\pm}$ are isomorphic to $X^{\pm}_{J[3-\sqrt{2}]}(7)$ and the curves $X_2^{\pm}$ are isomorphic to $X^{\pm}_{J[3+\sqrt{2}]}(7)$.*

Proof. Using the equations for $X_E^{\pm}(7)$ in [HK03, PSS07, Fis14] it is simple to check that $X_2^{\pm}$ is isomorphic to $X_E^{\mp}(7)$. We showed in Proposition 6.4.1 that J and E are indeed $([3 \pm \sqrt{2}], [7], -1)$-congruent, hence (after choosing an appropriate embedding $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathrm{End}_{\mathbb{Q}}(J)$) we see that the curve $X^{\pm}_{J[3+\sqrt{2}]}(7)$ is isomorphic to $X_2^{\pm}$.

To show the analogous result for $X_1^{\pm}$ and $X^{\pm}_{J[3-\sqrt{2}]}$ we choose a pair of points on $P, P' \in X_1^+$ (by taking hyperplane section) defined over quartic number fields $K/\mathbb{Q}$ and $K'/\mathbb{Q}$ with $K \cap K' = \mathbb{Q}$. The same argument as Proposition 6.4.1 shows that these points correspond to elliptic curves F/K and F'/K' that are $([3 \pm \sqrt{2}], [7], 1)$-congruent to J. Thus over K (respectively K') the twist $X^+_{J[3-\sqrt{2}]}(7)$ is isomorphic over K to $X_F^+(7)$ (respectively isomorphic to $X_{F'}^+(7)$ over K'). Since $K \cap K' = \mathbb{Q}$ either $X^+_{J[3-\sqrt{2}]}(7)$ and X_1^+ are isomorphic over $\mathbb{Q}$, or $X^+_{J[3-\sqrt{2}]}(7)$ admits a non-trivial automorphism over the compositum KK'. All non-trivial automorphisms of $X^+_{J[3-\sqrt{2}]}(7)$ are defined over $\mathbb{Q}(J[3-\sqrt{2}])$ but not over $\mathbb{Q}$. Therefore since $\mathbb{Q}(J[3-\sqrt{2}]) \cap KK' = \mathbb{Q}$ the curve $X^+_{J[3-\sqrt{2}]}(7)$ does not admit a non-trivial automorphism over KK', and therefore is isomorphic to X_1^+ over $\mathbb{Q}$.

A symmetrical argument with $X_F^-(7)$ and $X_{F'}^-(7)$ shows the analogous claim for X_1^-. □

Searching to progressively larger heights on $X_1^{\pm}$ and $X_2^{\pm}$ yields no further examples of $([3 \pm \sqrt{2}], [7])$-congruences. However, the quadratic twist of E by -11 has trivial Mordell-Weil group, so cannot contribute to visualising the (conjectural) non-trivial elements of $Ш(J/\mathbb{Q})[7]$. This leads us to the following conjecture.

Conjecture 6.5.2. *Let $C/\mathbb{Q}$ be the genus 2 curve with LMFDB label* `385641.a.385641.1`*, let $J/\mathbb{Q}$ be its Jacobian, and let $d = -11$. There exists a subgroup isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$ contained in $Ш(J^d/\mathbb{Q})$ that is not visible in an abelian 3-fold.*

It may be possible to prove Conjecture 6.5.2 using the techniques of [PSS07] if one assumes the Birch and Swinnerton-Dyer conjecture for J. An unconditional proof would require proving that $Ш(J/\mathbb{Q})[7] \neq 0$, possibly by constructing a genus 2 Jacobian $J'/\mathbb{Q}$ which is $([3 + \sqrt{2}], [3 \pm \sqrt{2}])$-congruent to J, and applying visibility.

Appendix A

Models for $Z_{N,r}$

A.1 Equations defining $Z_{N,r}$

We record the defining equations for the models for the surfaces $Z_{N,r}$ computed in Chapter 5, and given in Theorem 1.0.9.

Defining equations for $Z_{12,r}$

We define

$$\begin{aligned}
P_{12,1}(u,v) =& -4u^4 - 2(2v^2+3)u^3 - (v^4 - 13v^2 + 3)u^2 + 2(5v^4 + 9v^2)u + v^6 - 6v^4 + 9v^2.\\
P_{12,5}(u,v) =& v^2u^8 + 4v^2u^7 + (-4v^4 - 20v^2 + 4)u^6 + (-12v^4 - 32v^2 - 8)u^5 + (6v^6 + 44v^4 + 160v^2\\
&- 76)u^4 + (12v^6 + 64v^4 - 64v^2 + 352)u^3 + (-4v^8 - 28v^6 - 204v^4 - 232v^2 - 592)u^2\\
&+ (-4v^8 - 32v^6 + 72v^4 + 224v^2 + 448)u + v^{10} + 4v^8 + 40v^6 + 52v^4 - 32v^2 - 128,\\
P_{12,7}(u,v) =& -P_{(\mathrm{ns,ns})}(u,v)P_{(\mathrm{s,ns})}(u,v)P_{(\mathrm{c,ns})}(u,v),\\
P_{12,11}(u,v) =& -P_{(\mathrm{ns,s})}(u,v)P_{(\mathrm{s,s})}(u,v)P_{(\mathrm{c,s})}(u,v).
\end{aligned}$$

Here

$$\begin{aligned}
P_{(\mathrm{ns,ns})}(u,v) =& u - 1,\\
P_{(\mathrm{s,ns})}(u,v) =& (v^2+1)u + v^2 - 1,\\
P_{(\mathrm{c,ns})}(u,v) =& u^4 + 6u^3 + (-2v^2 + 12)u^2 + (-6v^2 + 8)u + v^4 - v^2,
\end{aligned}$$

and

$$\begin{aligned}
P_{(\mathrm{ns,s})}(u,v) =& u + 1,\\
P_{(\mathrm{s,s})}(u,v) =& (v^4 + 6v^2 + 1)u - 7v^4 - 2v^2 + 1,\\
P_{(\mathrm{c,s})}(u,v) =& v^4u^4 + 8v^4u^3 + (-9v^6 + 24v^4 + 11v^2)u^2 + (-54v^6 - 36v^4 - 6v^2)u + 27v^8 + 27v^6\\
&+ 9v^4 - v^2 - 1.
\end{aligned}$$

Defining equations for $Z_{14,r}$

We define

$$\begin{aligned}
P_{14,1}(u,v) &= P_{(I,\mathrm{ns})}(u,v)P_{(\mathrm{c,ns})}(u,v),\\
P_{14,3}(u,v) &= P_{(I,\mathrm{s})}(u,v)P_{(\mathrm{c,s})}(u,v).
\end{aligned}$$

Here

$$P_{(I,\mathrm{ns})}(u,v) = (v^2-2v+1)u^2-(v^3-v^2+2v-2)u+v^3-v^2+1$$

$$\begin{aligned}P_{(\mathrm{c,ns})}(u,v) =& (v^2-2v+1)u^6-(3v^3-15v^2+12v)u^5+(3v^4-33v^3+27v^2-6v-2)u^4-(v^5\\ &-29v^4+5v^3+5v^2-10v)u^3-(9v^5+28v^4-21v^3+23v^2-8v-1)u^2+(17v^5\\ &-3v^4+12v^3+2v)u-7v^5+3v^4-8v^3+v^2,\end{aligned}$$

and

$$P_{(I,\mathrm{s})}(u,v) = (v^2+4v-1)u-v^3-5v^2+13v+1,$$

$$\begin{aligned}P_{(\mathrm{c,s})}(u,v) =& u^7+(4v^2-3v+5)u^6+6(v^4-2v^3+2v^2-v+2)u^5+2(2v^6-9v^5+10v^4+2v^3\\ &-v^2-7v+7)u^4+v(v-1)(v+1)(v^5-12v^4+28v^3+2v^2+9v+32)u^3-(v-1)\\ &(v+1)^2(3v^6-20v^5+32v^4-22v^3-5v^2-16v-16)u^2+(v-1)^2(v+1)^3(3v^5\\ &-17v^4+5v^3-29v^2-3v-13)u-(v-1)^2(v+1)^4(v^5-7v^4+3v^3+3v^2-v+3).\end{aligned}$$

Defining equations for $Z_{15,r}$

We define

$$\begin{aligned}P_{15,2}(u,v) =& -(v-1)^4(7v^2+2v+7)u^8+2(v-1)^3(5v^4+18v^3+4v^2+10v-5)u^7\\ &-(v-1)^2(11v^6+24v^5+95v^4-38v^3+39v^2-46v+11)u^6+2(v-1)(v^8+19v^7\\ &-2v^6+74v^5-71v^4+29v^3-31v^2+14v-1)u^5+(2v^{10}-12v^9-47v^8+76v^7\\ &-188v^6+232v^5-103v^4+46v^3-22v^2-2v+2)u^4-2(4v^{11}-15v^{10}+30v^9\\ &-77v^8+87v^7-84v^6+25v^5+44v^4-53v^3+40v^2-19v+4)u^3+(v^{12}+20v^{11}\\ &-80v^{10}+168v^9-270v^8+270v^7-220v^6+120v^5-57v^4+26v^3-2v^2-4v+1)u^2\\ &-2v(v^2-v+1)(12v^8-28v^7+35v^6-28v^5+4v^4+4v^3-3v^2+2v-1)u\\ &+v^2(2v-1)^4(v^2-v+1)^2,\end{aligned}$$

$$\begin{aligned}P_{15,11}(u,v) =& v^6(v+1)^2u^{10}+2v^5(v+1)(2v^3+9v^2+v+3)u^9+v^4(6v^6+68v^5+101v^4+114v^3\\ &+47v^2+14v+15)u^8+2v^3(2v^8+46v^7+106v^6+185v^5+134v^4+71v^3+6v^2\\ &+10v+10)u^7+v^2(v^{10}+58v^9+215v^8+520v^7+595v^6+446v^5+63v^4-54v^3\\ &-51v^2+30v+15)u^6+2v(7v^{11}+52v^{10}+180v^9+299v^8+305v^7+81v^6-130v^5\\ &-187v^4-90v^3-14v^2+16v+3)u^5+(19v^{12}+118v^{11}+285v^{10}+390v^9+133v^8\\ &-358v^7-734v^6-644v^5-276v^4-40v^3+29v^2+18v+1)u^4+2(v+1)(7v^{11}\\ &+21v^{10}+33v^9-16v^8-103v^7-200v^6-160v^5-81v^4+22v^3+22v^2+12v+2)u^3\\ &+(v+1)(v^{11}+9v^{10}-12v^9-56v^8-147v^7-171v^6-92v^5+42v^4+111v^3+97v^2\\ &+30v+6)u^2-2(v+1)^2(v^8+8v^7+v^6+5v^5-23v^4-21v^3-24v^2-11v-2)u\\ &+(v+1)^2(v^6+8v^5+8v^4+18v^3+8v^2+8v+1).\end{aligned}$$

A.2 j-invariant maps for $W_{N,r}$

Let $J = j/1728$ and $J' = j'/1728$. In this section we give the rational functions $\boldsymbol{A}_{(N,r)}$, $\boldsymbol{B}_{(N,r)}$, and $\boldsymbol{D}_{(N,r)} \in \mathbb{Q}(a,b)$ from Proposition 5.1.8. That is, so that the forgetful map $W_{N,r} \to W_1$ factors through the rational map $\mathbb{A}^2 \dashrightarrow W_1$ given by $(a,b) \mapsto (JJ', (J-1)(J'-1))$ where

$$JJ' = \frac{\boldsymbol{A}_{(N,r)}^3}{\boldsymbol{D}_{(N,r)}}, \quad \text{and} \quad (J-1)(J'-1) = \frac{\boldsymbol{B}_{(N,r)}^2}{\boldsymbol{D}_{(N,r)}}.$$

j-invariants for $W_{2,1}$

$$\begin{aligned}
\boldsymbol{A}_{(2,1)} &= b(2a+3b+2),\\
\boldsymbol{B}_{(2,1)} &= a(2a+3b+2)^2,\\
\boldsymbol{D}_{(2,1)} &= (2a+3b+2)^4.
\end{aligned}$$

j-invariants for $W_{3,1}$

$$\begin{aligned}
\boldsymbol{A}_{(3,1)} &= -(-2ab+b^2-4a-4b),\\
\boldsymbol{B}_{(3,1)} &= (b+2)(a^2b-2ab^2+b^3+2a^2+ab-2b^2+a+b),\\
\boldsymbol{D}_{(3,1)} &= (2b+1)^3(-ab+b^2-2a-2b)^2.
\end{aligned}$$

j-invariants for $W_{3,2}$

$$\begin{aligned}
\boldsymbol{A}_{(3,2)} &= a(3a+2b+3)\\
\boldsymbol{B}_{(3,2)} &= \tfrac{1}{2}(3a^2+3a-b^2+3)(3a+2b+3)\\
\boldsymbol{D}_{(3,2)} &= (3a+2b+3)^3.
\end{aligned}$$

j-invariants for $W_{4,r}$

$$\begin{aligned}
\boldsymbol{A}_{(4,r)} &= \tfrac{1}{3}(-2ab+b^2+2a+2b),\\
\boldsymbol{B}_{(4,r)} &= \tfrac{1}{4}(a^2b+2ab^2+b^3-a^2+b^2-2a+b+1),\\
\boldsymbol{D}_{(4,r)} &= \tfrac{1}{16}(b-1)^2(-a+b+1)^4.
\end{aligned}$$

j-invariants for $W_{5,1}$

$$\begin{aligned}
\boldsymbol{A}_{(5,1)} =& (16b^4-1824b^3+1976b^2+456b+1)a^4-4b(8b^3-476b^2+338b+55)a^3+2b^2(12b^2\\
&-268b+99)a^2-4b^3(2b-5)a+b^4,\\
\boldsymbol{B}_{(5,1)} =& (4b^2+1)(16b^4+4176b^3-40024b^2-1044b+1)a^6-6b(32b^5+5488b^4-34592b^3+3128b^2\\
&-5842b-89)a^5+3b^2(80b^4+8032b^3-29720b^2+4624b-2491)a^4-4b^3(40b^3+1908b^2\\
&-3384b+545)a^3+3b^4(2b-1)(10b+139)a^2-6b^5(2b-5)a+b^6,
\end{aligned}$$

$$\boldsymbol{D}_{(5,1)} = -2^{12}3^6a^5b^7(2a-1)^2.$$

j-invariants for $W_{5,2}$

$$\begin{aligned}
\boldsymbol{A}_{(5,2)} =& 4(a^4+4a^3-2(5b-3)a^2-(24b^2+5b-4)a+(16b^2+14b+1)),\\
\boldsymbol{B}_{(5,2)} =& 8a^6+48a^5-120(b-1)a^4+4(144b^2-75b+40)a^3+12(29b^2-42b+10)a^2-12(150b^3\\
&-109b^2+49b-4)a-(216b^4+1540b^3+489b^2+264b-8),\\
\boldsymbol{D}_{(5,2)} =& -2^6 3^6 b^3(2a-b+1)^5.
\end{aligned}$$

j-invariants for $W_{7,1}$

$$\begin{aligned}
\boldsymbol{A}_{(7,1)} =& 16((b-1)^2a^4+4(b-1)(11b^2+27b+14)a^3+\left(21b^4+23b^3+11b^2-27b-12\right)a^2+\\
&\left(14b^5+7b^4-39b^3-4b^2+25b+13\right)a+4b^6-2b^5-b^4-9b^3-3b^2+11b+4),\\
\boldsymbol{B}_{(7,1)} =& 64(b-1)^3a^6-384(b-1)^2(25b^2+45b+22)a^5+96(b-1)(73b^4-409b^3-1241b^2-1107b\\
&-308)a^4+32(203b^6-933b^5-4851b^4-3363b^3+3258b^2+4392b+1166)a^3-24(419b^7\\
&+89b^6+1586b^5+5614b^4+1907b^3-4711b^2-3944b-704)a^2-12(287b^8+533b^7-93b^6\\
&+1661b^5+3709b^4+247b^3-3295b^2-2441b-352)a-(11b^3+13b^2+7b+1)(49b^6\\
&-56b^5+179b^4-156b^3+255b^2+284b-539),\\
\boldsymbol{D}_{(7,1)} =& 3^6(b-1)(b+1)^3(8ab+b^2+4b-1)^7.
\end{aligned}$$

j-invariants for $W_{7,3}$

$$\begin{aligned}
\boldsymbol{A}_{(7,3)} =& (144b^6-48b^5-80b^4+320b^3+200b^2-8b+1)a^4+4b(96b^4+206b^3+132b^2-34b\\
&-55)a^3+2b^2(108b^3+316b^2+304b+99)a^2+4b^3(4b+5)a+b^4\\
\boldsymbol{B}_{(7,3)} =& (2b^2+2b+1)(20b^2+20b+1)(324b^4+144b^3-146b^2+34b-1)a^6-6b(432b^7+1176b^6\\
&+4240b^5+7864b^4+5382b^3+680b^2-246b+89)a^5+3b^2(2160b^6+9576b^5+15840b^4\\
&+14268b^3+11504b^2+8156b+2491)a^4+4b^3(1152b^4+4177b^3+5568b^2+3093b\\
&+545)a^3+3b^4(180b^3+516b^2+480b+139)a^2-6b^5(4b+5)a-b^6,\\
\boldsymbol{D}_{(7,3)} =& 2^{12}3^6a^5b^7(b+1)^4(ab+a-1)^7.
\end{aligned}$$

Appendix B

Tables

By Propositions 4.1.4, 4.1.6, and 4.2.4 we have a finite list of pairs of subgroups $H, H^+ \subset \mathrm{GL}_2(\mathbb{Z}/p^l\mathbb{Z})$ which give rise to nontrivial quadratic twist-type p^l-congruences where p^l is a prime power (assuming there are no exceptional points on $X(\mathrm{ns}\, p^{l+})$ for $p^l \geq 19$).

We therefore compute the genera of the modular curves $X^+(H_1, H_2)$ which give rise to nontrivial quadratic twist-type $p_1^{l_1}p_2^{l_2}$-congruences over $\mathbb{Q}$. In Table B.1 we list these genera when p_1 and p_2 are odd and in Table B.2 we list these genera in the case where $p_1 = 2$. To perform these calculations we use Rouse, Sutherland, and Zureick-Brown's function `GL2Genus` in the package `gl2.m` [RSZ21].

In Table B.3 we give an example of a quadratic twist-type (N, r)-congruence for each pair (N, r) allowed by Conjecture 1.0.17. Similarly in Table B.4 we give an example of an (N, r)-congruence between elliptic curves with surjective mod N Galois representations for each pair (N, r) where such an example is known to exist. We check surjectivity of Galois representations with Zywina's algorithm [Zyw22].

Finally, in Table B.5 we list numerical invariants for the surfaces $W_{N,r}$ which are calculated using the formulae in Chapter 3 and our implementation in [Fre23b].

H_1 \ H_2	ns 5	s 5	ns 7	s 7	ns 11
ns 3	*2*	*3*	*4*	7	17
s 3	5	8	12	17	40
ns 5			26	35	76
s 5			40	55	117
ns 7					166
s 7					225

TABLE B.1: Genera of the modular curves $X^+(H_1, H_2)$ in Corollary 4.3.5 of level pq such that $X(H_i^+)$ has infinitely many rational points for $i = 1, 2$. Models for the curves whose genera are in *italics* are computed in Section 4.5.

H_1 \ H_2	ns 3	s 3	ns 5	s 5	ns 7	s 7	ns 9	ns 11
$G_9(\sqrt{-1})$	**1**	**1**	5	7	13	17	19	41
$G_{11}(\sqrt{-1})$	**1**	*3*	7	9	15	21	21	45
$G(\text{ns}\,2)$	**0**	**0**	**0**	**1**	**1**	**1**	**1**	*4*
$G_9(\sqrt{-\Delta})$	2	3	7	10	16	21	22	46
$G_{11}(\sqrt{-\Delta})$	0	1	5	8	12	17	16	40
$G_{97}(\sqrt{-1})$	7							
$G(\text{ns}\,4)$	**0**	**1**	*3*	6	8	11	10	
$G_{90}(\sqrt{-\Delta})$	5	13						
$G_{63}(\sqrt{-1})$	7							
$G(\text{s}\,4)$	*2*	5	13	20	30	41	40	
$G_{91}(\sqrt{-\Delta})$	5	13						
$G(\text{ns}\,8)$	*3*	9						

TABLE B.2: Genera of the modular curves $X^+(H_1, H_2)$ in Corollary 4.3.6 of level $2^k p^l$ such that $X(H_i^+)$ has infinitely many rational points for $i = 1, 2$. If the image of $X^+(H_1, H_2)$ at level $2^{k-1}p^l$ is of genus ≥ 2 we leave a space. Models for the curves whose genera are in **bold** are computed in Section 4.4 and models for the curves whose genera are in *italics* are computed in Section 4.5.

(N,r)	j-invariant of an elliptic curve $E/\mathbb{Q}$ admitting a quadratic twist-type (N,r)-congruence	LMFDB label of the minimal twist of E	Quadratic twist	Modular Curve	Model
$(8,1)$	$\frac{-2^6\cdot 3^3\cdot 17^3\cdot 47^3}{7^8}$	16128.w2	-1	$X(G_{97})$	[RZ15b, X_{97}]
$(8,5)$	$\frac{2^6\cdot 17^3\cdot 19^3}{3^4}$	2400.p1	-1	$X(G_{63})$	[RZ15b, X_{63}]
$(8,7)$	$\frac{2^2\cdot 3^3\cdot 13^3}{5^4}$	40.a4	$\Delta(E)$	$X(\mathrm{s}\,4^+)$	[RZ15b, X_{23}]
$(10,1)$	$\frac{-2^9\cdot 3^3\cdot 7^3}{19^5}$	608.d1	-1	$X(\mathrm{s}\,5^+)$	[Hal21, Thm. III.5.9]
$(12,11)$	$\frac{5^3\cdot 31^3}{2^6\cdot 3^3}$	726.b2	$\Delta(E)$	$X^+(\mathrm{ns}\,4,\mathrm{s}\,3)$	Lemma 4.4.3
$(20,3)$	$\frac{-2^{18}\cdot 3\cdot 5^3\cdot 11^3\cdot 17\cdot 23^3\cdot 31^3}{61^{10}}$	475983.f1	$\Delta(E)$	$X^+(\mathrm{ns}\,4,\mathrm{ns}\,5)$	Lemma 4.4.4
$(22,1)$	$\frac{-2^9\cdot 3^3\cdot 5^3\cdot 13\cdot 71^3\cdot 181^3}{43^{11}}$	232544.i1	-1	$X(\mathrm{ns}\,11^+)$	[Hal98]
$(28,3)$	$\frac{2^{18}\cdot 3^3\cdot 5^3\cdot 7^4\cdot 37^3}{13^{14}}$	24721333*	$\Delta(E)$	$X^+(\mathrm{ns}\,2,\mathrm{ns}\,7)$	Lemma 4.4.6
$(28,11)$	$\frac{-2^{15}\cdot 5^3\cdot 11^3\cdot 17^3\cdot 29^3}{13^{14}}$	1218886357*	$\Delta(E)$	$X^+(\mathrm{ns}\,2,\mathrm{s}\,7)$	Lemma 4.4.6
$(30,7)$	$\frac{-3^3\cdot 5^6\cdot 199^3\cdot 809^3\cdot 5059^3}{61^{15}}$	2810892417709*	-214663	$X^+(\mathrm{ns}\,3,\mathrm{ns}\,5)$	Lemma 4.5.7
$(32,3)$	$\frac{-2^{18}\cdot 3\cdot 5^3\cdot 13^3\cdot 41^3\cdot 107^3}{17^{16}}$	356257899*	$\Delta(E)$	$X(\mathrm{ns}\,16^+)$	[RZ15b, X_{441}]
$(36,19)$	$\frac{-2^{24}\cdot 3^3\cdot 5^3\cdot 11^3\cdot 47^3\cdot 103^3}{17^{18}}$	21043447153673*	$\Delta(E)$	$X^+(\mathrm{ns}\,2,\mathrm{ns}\,9)$	Lemma 4.4.7
$(48,19)$	$\frac{2^{15}\cdot 3^3\cdot 5^3\cdot 31^3\cdot 41^3\cdot 47^3\cdot 83^3\cdot 293^3}{23^{24}}$	23893951694358047*	$\Delta(E)$	$X^+(\mathrm{ns}\,8,\mathrm{ns}\,3)$	Lemma 4.5.12

Table B.3: All known pairs (N,r) for which we have examples of nontrivial quadratic twist-type (N,r)-congruences. If M divides N and (N,r) appears in the above list, we do not give an example of an (M,r)-congruence. We also list the modular curve giving rise to the corresponding example. When the conductor of an elliptic curve is outside the range of the LMFDB we use a "$*$" to replace the label for the isogeny class.

(N,r)	j-invariants of a pair of elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ admitting an (N,r)-congruence	LMFDB labels of the pair of elliptic curves (E,E')	References
$(8,1)$	$\left(\frac{2^{12}\cdot 59^3}{3^{10}\cdot 19}, \frac{-2^{12}\cdot 41^3\cdot 20921^3}{3^2\cdot 19\cdot 53^8}\right)$	(57.b2, 3021.a1)	[Che16, Che18]
$(8,3)$	$\left(\frac{-19}{2^{10}}, \frac{2^{10}\cdot 149519^3}{19^3\cdot 31^8}\right)$	(152.a1, 4712.a1)	[Che16, Che18]
$(8,5)$	$\left(\frac{-2^{12}\cdot 13171^3}{3^2\cdot 19^5}, \frac{-2^{12}\cdot 41^3\cdot 20921^3}{3^2\cdot 19\cdot 53^8}\right)$	(57.b1, 3021.a1)	[Che16, Che18]
$(8,7)$	$\left(\frac{-7^2\cdot 17^3\cdot 41^3}{2^{15}\cdot 3}, \frac{7^2\cdot 2087^3\cdot 15889^3}{2\cdot 3^7\cdot 173^8}\right)$	(294.d1, 50862.v1)	[Che16, Che18]
$(9,1)$	$\left(\frac{3^3\cdot 1451^3}{17}, \frac{-3^3\cdot 7^3\cdot 13^3\cdot 1361^3}{17\cdot 29^9}\right)$	(17.a1, 493.b1)	[Fis15]
$(9,2)$	$\left(2^4\cdot 17^3, \frac{2\cdot 17^3\cdot 167^3\cdot 3637^3}{103^9}\right)$	(200.b1, 20600.e1)	[Fis15]
$(10,1)$	$\left(\frac{5^3\cdot 7\cdot 107^3}{2^{15}\cdot 11}, \frac{5^{15}\cdot 7\cdot 491^3}{2^5\cdot 11\cdot 23^{10}}\right)$	(1078.k2, 24794.bl1)	[Fis20]
$(10,3)$	$\left(\frac{769^3}{2\cdot 173}, \frac{77465469218 89^3}{2^{27}\cdot 101^{10}\cdot 173^3}\right)$	(346.b1, 34946.g1)	[Fis20]
$(11,1)$	$\left(\frac{5^3\cdot 13^3\cdot 569^3}{2^6\cdot 3\cdot 23^6}, \frac{-5^3\cdot 11^3\cdot 17^3\cdot 746058233^3}{2^5\cdot 3^8\cdot 23\cdot 127^{11}}\right)$	(138.b1, 17526.d1)	[CF22, Fis14]
$(11,2)$	$\left(\frac{2^{12}\cdot 29^3}{3^6\cdot 5^2\cdot 43}, \frac{2^{12}\cdot 31^3\cdot 1709^3\cdot 15391^3}{3^5\cdot 5^3\cdot 43^2\cdot 109^{11}}\right)$,	(645.b1, 70305.b1)	[CF22, Fis14, Kum15]
$(12,1)$	$\left(\frac{11^6}{2\cdot 7\cdot 41}, \frac{11^3\cdot 97^3\cdot 16411^3\cdot 34673^3}{2^{25}\cdot 7\cdot 19^{12}\cdot 41}\right)$	(574.b1, 10906.d1)	[Che16, Fis20], Thm. 1.0.9
$(12,5)$	$\left(\frac{29\cdot 379^3}{2^{12}\cdot 5^8\cdot 11}, \frac{-29^2\cdot 2490889^3}{2^{36}\cdot 5^4\cdot 11^5}\right)$	(92510.i1, 92510.w1)	Thm. 1.0.9

TABLE B.4: Known examples of (N,r)-congruences between geometrically non-isogenous elliptic curves over $\mathbb{Q}$ where the mod N Galois representation is *surjective*. If M divides N and (N,r) appears in the above list, we do not give an example of an (M,r)-congruence.

(N,r)	j-invariants of a pair of elliptic curves $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ admitting an (N,r)-congruence	LMFDB labels of the pair of elliptic curves (E,E')	References
$(12,7)$	$\left(\frac{-2^6\cdot 3^3\cdot 13\cdot 43^3\cdot 1987^3}{5^7\cdot 31^3}, \frac{-2^6\cdot 3^3\cdot 13\cdot 115321^3}{5\cdot 31^9}\right)$	(838240*, 838240*)	Thm. 1.0.9
$(12,11)$	$\left(\frac{131^2\cdot 60601^3}{2^{10}\cdot 5\cdot 29^8}, \frac{67^3\cdot 127^3\cdot 131}{2^2\cdot 5^{11}\cdot 29^4}\right)$	(4976690*, 4976690*)	Thm. 1.0.9
$(13,1)$	$\left(\frac{109^3\cdot 181^3}{3\cdot 5^2\cdot 23^4}, \frac{17929^3}{3^3\cdot 5^2\cdot 23\cdot 29}\right)$	(345.b1, 10005.m1)	[CF22, Fis19]
$(13,2)$	$\left(\frac{2^{14}\cdot 3^3}{13}, \frac{-2^8\cdot 3^3\cdot 151^3\cdot 2399^3}{13\cdot 19^{13}}\right)$	(52.a1, 988.c1)	[CF22, Fis19]
$(14,1)$	$\left(\frac{1319^3}{7^6\cdot 89}, \frac{-6356968276201^3}{7^{10}\cdot 59^{14}\cdot 89}\right)$	(623.a1, 36757.a1)	Thm. 1.0.9
$(14,3)$	$\left(\frac{-2^{27}}{3^2\cdot 7}, \frac{-2^{15}\cdot 31^3\cdot 6115849^3}{3^{12}\cdot 7^3\cdot 17^{14}}\right)$	(58989.g1, 1002813*)	Thm. 1.0.9
$(15,2)^\dagger$	$\left(\frac{-2^8\cdot 3^3\cdot 8326531123^3}{7^9\cdot 17^2\cdot 41^5\cdot 61}, \frac{-2\cdot 3^3\cdot 115837^3\cdot 1323779^3}{7^3\cdot 17\cdot 41^{10}\cdot 61^2}\right)$	(402380888*, 402380888*)	Thm. 1.0.12
$(15,11)^\dagger$	$\left(\frac{3^6\cdot 199\cdot 289754657821 21^3}{7\cdot 11^{10}\cdot 13^6\cdot 23^3\cdot 61^{10}}, \frac{-3^6\cdot 199^2\cdot 1146429804545 99^3}{7^{14}\cdot 11^5\cdot 13^9\cdot 23^3\cdot 61^5}\right)$	(82293302803113011 61*, 82293302803113011 61*)	Thm. 1.0.12
$(17,1)^\dagger$	$\left(\frac{3^3\cdot 47189^3\cdot 228953^3}{2^3\cdot 5^3\cdot 13\cdot 59^2}, \frac{3^3\cdot 83^3\cdot 3457^3\cdot 1474127^3}{2^{14}\cdot 5^{11}\cdot 11^{17}\cdot 13\cdot 59}\right)$	(279809270*, 3077901970*)	[Fis21]
$(17,3)^\dagger$	$\left(\frac{-5\cdot 7\cdot 11^3}{3^5}, \frac{5\cdot 7\cdot 19^3\cdot 41^3\cdot 14303^3}{3^2\cdot 13^{17}}\right)$	(3675.g1, 47775.be1)	[Bil16, CF22, Fis21]

Table B.4 (continued): Known examples of (N,r)-congruences between geometrically non-isogenous elliptic curves over $\mathbb{Q}$ where the mod N Galois representation is *surjective*. If M divides N and (N,r) appears in the above list, we do not give an example of an (M,r)-congruence. A † indicates that the example is the only one known.

N	r	$p_g(\widetilde{Z}_{N,r})$	$\kappa(\widetilde{Z}_{N,r})$	$p_g(W_{N,r})$	$K^2_{W^\circ}$	$\kappa(W_{N,r})$
15	1	4	2	0		-1
	2	6	2	0		-1
	7	8	2	2	0	1^*
	11	10	2	0		-1
16	1	4	2	0		-1
	3	7	2	0		-1
	5	8	2	1	-4	0^*
	7	11	2	0		-1
17	1	10	2	1	-2	0
	3	10	2	1	-2	0
18	1	8	2	1	-6	0^*
	5	13	2	0		-1
19	1	14	2	2	-1	1
	2	15	2	2	0	1
20	1	12	2	1	-8	0^*
	3	14	2	1	-4	0^*
	11	18	2	0		-1
	13	16	2	4	5	2
21	1	15	2	4	8	2
	2	17	2	1	-8	0^*
	5	25	2	2	-2	1^*
	10	23	2	6	12	2
22	1	17	2	2	-4	1^*
	7	23	2	3	1	2
23	1	23	2	4	5	2
	5	32	2	7	22	2
24	1	13	2	3	-4	2^*
	5	25	2	3	0	2^*
	7	25	2	3	0	2^*
	11	29	2	2	-4	1^*
	13	21	2	6	12	2
	17	25	2	3	-4	2^*
	19	25	2	6	14	2
	23	37	2	0		-1
25	1	36	2	6	13	2
	2	36	2	10	36	2
26	1	33	2	5	8	2
	5	33	2	6	12	2
27	1	42	2	13	50	2
	2	46	2	7	17	2

TABLE B.5: Numerical invariants of the surfaces $W_{N,r}$. Kodaira dimensions decorated with an asterisk are conjectural. The surface $W^\circ_{N,r}$ is defined only when $W_{N,r}$ is not rational, so the column recording $K^2_{W^\circ}$ is left empty if $W_{N,r}$ is rational.

N	r	$p_g(\widetilde{Z}_{N,r})$	$\kappa(\widetilde{Z}_{N,r})$	$p_g(W_{N,r})$	$K^2_{W^\circ}$	$\kappa(W_{N,r})$
28	1	38	2	11	36	2
	3	47	2	5	7	2
	5	43	2	10	36	2
	11	42	2	7	11	2
29	1	59	2	15	71	2
	2	59	2	16	69	2
30	1	39	2	8	16	2
	7	47	2	15	63	2
	11	57	2	4	1	2
	17	49	2	8	18	2
31	1	69	2	19	91	2
	3	78	2	22	111	2
32	1	55	2	15	59	2
	3	63	2	14	55	2
	5	67	2	20	92	2
	7	75	2	11	42	2
33	1	80	2	29	146	2
	2	88	2	17	66	2
	5	84	2	19	78	2
	7	84	2	28	154	2
34	1	78	2	18	82	2
	3	78	2	20	88	2
35	1	99	2	28	137	2
	2	103	2	37	208	2
	3	111	2	36	190	2
	6	115	2	28	140	2
36	1	74	2	26	123	2
	5	90	2	22	102	2
	7	84	2	23	104	2
	11	100	2	12	40	2
37	1	131	2	41	240	2
	2	131	2	42	240	2
38	1	108	2	30	150	2
	3	114	2	30	158	2
39	1	132	2	47	283	2
	2	136	2	35	174	2
	7	148	2	57	339	2
	14	152	2	37	194	2

Table B.5 (continued): Numerical invariants of the surfaces $W_{N,r}$. Kodaira dimensions decorated with an asterisk are conjectural. The surface $W^\circ_{N,r}$ is defined only when $W_{N,r}$ is not rational, so the column recording $K^2_{W^\circ}$ is left empty if $W_{N,r}$ is rational.

Bibliography

[ABB+23] Eran Assaf, Angelica Babei, Ben Breen, Edgar Costa, Juanita Duque-Rosero, Aleksander Horawa, Jean Kieffer, Avinash Kulkarni, Grant Molnar, Sam Schiavone, and John Voight, *A database of basic numerical invariants of Hilbert modular surfaces*, arXiv e-prints (2023), arXiv:2301.10302, To appear in Contemp. Math. ↑2

[Abe29] Neils H. Abel, *Précis d'une theorie des fonctions elliptiques*, J. Reine Angew. Math. **4** (1829), 236–277. MR1577734. ↑1

[AMRT10] Avner Ash, David Mumford, Michael Rapoport, and Yung-Sheng Tai, *Smooth compactifications of locally symmetric varieties*, second ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2010, With the collaboration of Peter Scholze. MR2590897. ↑27

[AS02] Amod Agashe and William Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185. MR1939144. ↑8, ↑155

[AS05] ———, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484, With an appendix by J. Cremona and B. Mazur. MR2085902. ↑8, ↑155

[ATT18] 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. MR3856778. ↑5, ↑115

[Bar09] Burcu Baran, *A modular curve of level 9 and the class number one problem*, J. Number Theory **129** (2009), no. 3, 715–728. MR2488598. ↑100

[Bar10] ———, *Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem*, J. Number Theory **130** (2010), no. 12, 2753–2772. MR2684496. ↑14, ↑18, ↑67, ↑68, ↑88, ↑89, ↑93, ↑105, ↑107, ↑112

[Bas85] Dieter Bassendowski, *Klassifikation Hilbertscher Modulflächen zur symmetrischen Hurwitz-Maass-Erweiterung*, Bonner Mathematische Schriften [Bonn Mathematical Publications], vol. 163, Universität Bonn, Mathematisches Institut, Bonn, 1985, Dissertation, University of Bonn, Bonn, 1984. MR817435. ↑2, ↑32, ↑49

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR1484478. ↑11, ↑75, ↑159

[BD11] 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. MR2866068. ↑5, ↑87, ↑111, ↑116, ↑117

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944. MR3961086. ↑7, ↑93, ↑104

[BDM+23] ———, *Quadratic Chabauty for modular curves: Algorithms and examples*, Compositio Mathematica **159** (2023), no. 6, 1111–1152. ↑7, ↑93, ↑104

[Bea96] Arnaud Beauville, *Complex algebraic surfaces*, second ed., London Mathematical Society Student Texts, vol. 34, Cambridge University Press, Cambridge, 1996, Translated from the 1978 French original by R. Barlow, with assistance from N. I. Shepherd-Barron and M. Reid. MR1406314. ↑34, ↑35, ↑36

[Ben98] Peter R. Bending, *Curves of genus* 2 *with* $\sqrt{2}$*-multiplication*, Ph.D. thesis, University of Oxford, 1998. ↑154, ↑159

[Ben99] ———, *Curves of genus 2 with sqrt2 multiplication*, arXiv e-prints (1999), math/9911273. ↑154, ↑159, ↑160

[BFT14] Nils Bruin, E. Victor Flynn, and Damiano Testa, *Descent via* $(3,3)$*-isogeny on Jacobians of genus 2 curves*, Acta Arith. **165** (2014), no. 3, 201–223. MR3263947. ↑8

[BHLS15] 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. MR3349314. ↑5, ↑116

[BHPV04] Wolf P. Barth, Klaus Hulek, Chris A. M. Peters, and Antonius Van de Ven, *Compact complex surfaces*, second ed., vol. 4, Springer-Verlag, Berlin, 2004. MR2030225. ↑35, ↑37

[Bil16] Nicolas Billerey, *On some remarkable congruences between two elliptic curves*, arXiv e-prints (2016), arXiv:1605.09205. ↑4, ↑171

[BKLS21] Manjul Bhargava, Zev Klagsbrun, Robert J. Lemke Oliver, and Ari Shnidman, *Elements of given order in Tate-Shafarevich groups of abelian varieties in quadratic twist families*, Algebra Number Theory **15** (2021), no. 3, 627–655. MR4261095. ↑8

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on* $X_0^+(p^r)$, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984. MR3137477. ↑7, ↑22, ↑93

[Bru03] Nils Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49. MR2011330. ↑110, ↑111

[Bru06] ———, *Some ternary Diophantine equations of signature* $(n,n,2)$, Discovering mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 63–91. MR2278923. ↑111

[BT16] Benjamin Bakker and Jacob Tsimerman, *p-torsion monodromy representations of elliptic curves over geometric function fields*, Ann. of Math. (2) **184** (2016), no. 3, 709–744. MR3549621. ↑4

[Car01] David Carlton, *Moduli for pairs of elliptic curves with isomorphic* N*-torsion*, Manuscripta Math. **105** (2001), no. 2, 201–234. MR1846618. ↑24, ↑28

[CC04] Imin Chen and Chris Cummins, *Elliptic curves with nonsplit mod 11 representations*, Math. Comp. **73** (2004), no. 246, 869–880. MR2031412. ↑107

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR1406090. ↑157, ↑158, ↑159

[CF22] John E. Cremona and Nuno Freitas, *Global methods for the symplectic type of congruences between elliptic curves*, Rev. Mat. Iberoam. **38** (2022), no. 1, 1–32. MR4382462. ↑4, ↑6, ↑85, ↑86, ↑89, ↑147, ↑170, ↑171

[CFS10] John E. Cremona, Tom Fisher, and Michael Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra Number Theory **4** (2010), no. 6, 763–820. MR2728489. ↑37, ↑39

[Che99] Imin Chen, *On Siegel's modular curve of level* 5 *and the class number one problem*, J. Number Theory **74** (1999), no. 2, 278–297. MR1671653. ↑113

[Che16] Zexiang Chen, *Congruences of elliptic curves*, Ph.D. thesis, University of Cambridge, 2016, `http://zc231.user.srcf.net/Maths/PhDThesis.pdf`. ↑5, ↑9, ↑116, ↑143, ↑170

[Che18] ———, *Families of elliptic curves with the same mod 8 representations*, Math. Proc. Cambridge Philos. Soc. **165** (2018), no. 1, 137–162. MR3811549. ↑5, ↑9, ↑91, ↑92, ↑170

[CM00] John E. Cremona and Barry Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR1758797. ↑8, ↑9, ↑153, ↑155

[Coh91] Harvey Cohn, *A numerical survey of the reduction of modular curve genus by Fricke's involutions*, Number theory (New York, 1989/1990), Springer, New York, 1991, pp. 85–104. MR1124636. ↑67

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR1228206. ↑25, ↑77

[CR03] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441. MR1972744. ↑38

[DD19] Tim Dokchitser and Christopher Doris, *3-torsion and conductor of genus 2 curves*, Math. Comp. **88** (2019), no. 318, 1913–1927. MR3925491. ↑154, ↑160

[DLM22] Valerio Dose, Guido Lido, and Pietro Mercuri, *Automorphisms of Cartan modular curves of prime and composite level*, Algebra Number Theory **16** (2022), no. 6, 1423–1461. MR4488580. ↑18

[DLM23] Harris B. Daniels, Álvaro Lozano-Robledo, and Jackson S. Morrow, *Towards a classification of entanglements of Galois representations attached to elliptic curves*, Rev. Mat. Iberoam. **39** (2023), no. 3, 803–844. ↑89

[DR73] Pierre Deligne and Michael Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1973, pp. 143–316. Lecture Notes in Math., Vol. 349. MR0337993. ↑14, ↑15, ↑23, ↑24

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR2112196. ↑69

[EK14] Noam Elkies and Abhinav Kumar, *K3 surfaces and equations for Hilbert modular surfaces*, Algebra Number Theory **8** (2014), no. 10, 2297–2411. MR3298543. ↑5, ↑24, ↑29

[Elk99] Noam D. Elkies, *The Klein quartic in number theory*, The eightfold way, Math. Sci. Res. Inst. Publ., vol. 35, Cambridge Univ. Press, Cambridge, 1999, pp. 51–101. MR1722413. ↑15, ↑155

[ES21] Andreas-Stephan Elsenhans and Michael Stoll, *Minimization of hypersurfaces*, arXiv e-prints (2021), arXiv:2110.04625, To appear in Math. Comp. ↑158

[FH99] Masahiro Furumoto and Yuji Hasegawa, *Hyperelliptic quotients of modular curves $X_0(N)$*, Tokyo J. Math. **22** (1999), no. 1, 105–125. MR1692024. ↑77

[Fis12] Tom Fisher, *The Hessian of a genus one curve*, Proc. Lond. Math. Soc. (3) **104** (2012), no. 3, 613–648. MR2900238. ↑4, ↑5, ↑9, ↑15, ↑16, ↑91, ↑94, ↑115, ↑121, ↑147

[Fis14] ———, *On families of 7- and 11-congruent elliptic curves*, LMS J. Comput. Math. **17** (2014), no. 1, 536–564. MR3356045. ↑4, ↑5, ↑9, ↑10, ↑15, ↑16, ↑94, ↑116, ↑145, ↑155, ↑156, ↑161, ↑170

[Fis15] ———, *On families of 9-congruent elliptic curves*, Acta Arith. **171** (2015), no. 4, 371–387. MR3430770. ↑5, ↑9, ↑146, ↑170

[Fis16] ———, *Visualizing elements of order 7 in the Tate-Shafarevich group of an elliptic curve*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 100–114. MR3540949. ↑8, ↑153, ↑154, ↑155, ↑159

[Fis19] ———, *On families of 13-congruent elliptic curves*, arXiv e-prints (2019), arXiv:1912.10777. ↑3, ↑5, ↑9, ↑29, ↑54, ↑116, ↑121, ↑126, ↑171

[Fis20] ———, *Explicit moduli spaces for congruences of elliptic curves*, Math. Z. **295** (2020), no. 3-4, 1337–1354. MR4125692. ↑5, ↑115, ↑116, ↑121, ↑143, ↑170

[Fis21] ———, *On pairs of 17-congruent elliptic curves*, arXiv e-prints (2021), arXiv:2106.02033. ↑3, ↑4, ↑5, ↑9, ↑116, ↑171

[FK91] Gerhard Frey and Ernst Kani, *Curves of genus 2 covering elliptic curves and an arithmetical application*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 153–176. MR1085258. ↑1

[FK22] Nuno Freitas and Alain Kraus, *On the symplectic type of isomorphisms of the p-torsion of elliptic curves*, Mem. Amer. Math. Soc. **277** (2022), no. 1361, v+105. MR4403927. ↑6, ↑125

[FLS+01] E. Victor Flynn, Franck Leprévost, Edward F. Schaefer, William A. Stein, Michael Stoll, and Joseph L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70** (2001), no. 236, 1675–1697. MR1836926. ↑159

[Fly15] E. V. Flynn, *Descent via $(5,5)$-isogeny on Jacobians of genus 2 curves*, J. Number Theory **153** (2015), 270–282. MR3327574. ↑8

[Fre95] Gerhard Frey, *On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, vol. I, Int. Press, Cambridge, MA, 1995, pp. 79–98. MR1363496. ↑1

[Fre97] ———, *On ternary equations of Fermat type and relations with elliptic curves*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 527–548. MR1638494. ↑1

[Fre22] Sam Frengley, *On* 12*-congruences of elliptic curves*, arXiv e-prints (2022), arXiv:2208.05842, To appear in Int. J. Number Theory. ↑5

[Fre23a] ———, *Congruences of elliptic curves arising from nonsurjective mod N Galois representations*, Math. Comp. **92** (2023), no. 339, 409–450. MR4496970. ↑10, ↑19, ↑52

[Fre23b] ———, *Github repository*, `https://github.com/SamFrengley/thesis.git`, 2023. ↑3, ↑5, ↑9, ↑11, ↑48, ↑49, ↑52, ↑75, ↑91, ↑96, ↑105, ↑111, ↑121, ↑128, ↑129, ↑137, ↑144, ↑149, ↑151, ↑153, ↑154, ↑167

[FS22] E. Victor Flynn and Ari Shnidman, *Arbitrarily large p-torsion in Tate-Shafarevich groups*, arXiv e-prints (2022), arXiv:2209.08088. ↑8

[Hal98] Emmanuel Halberstadt, *Sur la courbe modulaire* $X_{ndép}(11)$, Experiment. Math. **7** (1998), no. 2, 163–174. MR1677158. ↑6, ↑85, ↑86, ↑107, ↑169

[Hal21] ———, *Calculs explicites sur les courbes modulaires*, `https://hal.archives-ouvertes.fr/hal-03149641`, February 2021, Les présentes notes constituent une introduction élémentaire aux courbes modulaires. ↑22, ↑97, ↑98, ↑99, ↑107, ↑108, ↑169

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. No. 52, Springer-Verlag, New York-Heidelberg, 1977. MR463157. ↑34, ↑35

[Hau79] Wilfried Hausmann, *Kurven auf Hilbertschen Modulflächen*, Bonner Mathematische Schriften [Bonn Mathematical Publications], vol. 123, Universität Bonn, Mathematisches Institut, Bonn, 1979, Dissertation, Rheinische Friedrich-Wilhelms-Universität, Bonn, 1979. MR598814. ↑2, ↑32, ↑49, ↑55, ↑58

[Hau82] ———, *The fixed points of the symmetric Hilbert modular group of a real quadratic field with arbitrary discriminant*, Math. Ann. **260** (1982), no. 1, 31–50. MR664363. ↑2, ↑32, ↑44, ↑49, ↑55, ↑58

[Hee52] Kurt Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227–253. MR53135. ↑88

[Hel73] H. Helling, *Note über das Geschlecht gewisser arithmetischer Gruppen*, Math. Ann. **205** (1973), 173–179. MR332660. ↑77

[Her91] Carl Friedrich Hermann, *Modulflächen quadratischer Diskriminante*, Manuscripta Math. **72** (1991), no. 1, 95–110. MR1107455. ↑2, ↑24, ↑27, ↑31, ↑43, ↑44, ↑45, ↑46, ↑47, ↑48, ↑62, ↑63, ↑71, ↑79

[Her92] ———, *Symmetrische Modulflächen der Diskriminante* p^2, Manuscripta Math. **76** (1992), no. 2, 169–179. MR1174909. ↑2, ↑3, ↑32, ↑43, ↑45, ↑51, ↑54, ↑55, ↑56, ↑58, ↑67, ↑70, ↑72, ↑79, ↑83

[Hir53] Friedrich Hirzebruch, *Über vierdimensionale Riemannsche Flächen mehrdeutiger analytischer Funktionen von zwei komplexen Veränderlichen*, Math. Ann. **126** (1953), 1–22. MR62842. ↑27

[Hir71] ———, *The Hilbert modular group, resolution of the singularities at the cusps and related problems*, Séminaire Bourbaki, 23ème année (1970/1971), Lecture Notes in Math., Vol. 244, Springer, Berlin, 1971, pp. Exp. No. 396, pp. 275–288. MR0417187. ↑2, ↑27

[Hir73a] ———, *The Hilbert modular group and some algebraic surfaces*, Trudy Mat. Inst. Steklov. **132** (1973), 55–66, 264. MR0344255. ↑73

[Hir73b] ———, *Hilbert modular surfaces*, Enseign. Math. (2) **19** (1973), 183–281. MR393045. ↑2, ↑10, ↑32, ↑35, ↑43, ↑46, ↑49, ↑57, ↑58

[Hir78] ———, *Modulflächen und Modulkurven zur symmetrischen Hilbertschen Modulgruppe*, Ann. Sci. École Norm. Sup. (4) **11** (1978), no. 1, 101–165. MR498398. ↑2, ↑32

[HK03] Emmanuel Halberstadt and Alain Kraus, *Sur la courbe modulaire $X_E(7)$*, Experiment. Math. **12** (2003), no. 1, 27–40. MR2002672. ↑5, ↑94, ↑116, ↑145, ↑161

[HvdG81] Friedrich Hirzebruch and Gerard van der Geer, *Lectures on Hilbert modular surfaces*, Séminaire de Mathématiques Supérieures [Seminar on Higher Mathematics], vol. 77, Presses de l'Université de Montréal, Montreal, QC, 1981, Based on notes taken by W. Hausmann and F. J. Koll. MR639898. ↑33

[HVdV74] Friedrich Hirzebruch and Antonius Van de Ven, *Hilbert modular surfaces and the classification of algebraic surfaces*, Invent. Math. **23** (1974), 1–29. MR364262. ↑2

[HZ76] Friedrich Hirzebruch and Don Zagier, *Intersection numbers of curves on Hilbert modular surfaces and modular forms of Nebentypus*, Invent. Math. **36** (1976), 57–113. MR453649. ↑2, ↑32, ↑58

[HZ77] ———, *Classification of Hilbert modular surfaces.*, Complex analysis and algebraic geometry, (W. L. Jr Baily and T. Shioda, eds.), Cambridge University Press, 1977, pp. 43–77. MR480356. ↑2, ↑49

[Jac29] Carl Gustav Jacob Jacobi, *Fundamenta nova theoriae functionum ellipticarum*, Bornträger, 1829. ↑1

[Kan94] Ernst Kani, *Elliptic curves on abelian surfaces*, Manuscripta Math. **84** (1994), no. 2, 199–223. MR1285957. ↑3

[Kan21] ———, *Subcovers of curves and moduli spaces*, Geometry at the frontier—symmetries and moduli spaces of algebraic varieties, Contemp. Math., vol. 766, Amer. Math. Soc., [Providence], RI, 2021, pp. 229–250. MR4248056. ↑3

[Kan23] ———, *Modular curves on Humbert surfaces and on their normalizations*, In preparation. ↑3, ↑33, ↑58

[Ken82] M. A. Kenku, *On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{q}$-isogeny class*, J. Number Theory **15** (1982), no. 2, 199–202. MR675184. ↑146

[Kle78] Felix Klein, *Ueber die Transformation siebenter Ordnung der elliptischen Functionen*, Math. Ann. **14** (1878), no. 3, 428–471. MR1509988. ↑15, ↑155

[Kle56] ———, *Lectures on the icosahedron and the solution of equations of the fifth degree*, revised ed., Dover Publications, Inc., New York, N.Y., 1956, Translated into English by George Gavin Morrice. MR0080930. ↑15

[KO92] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), no. 2, 259–275. MR1166121. ↑147

[KR00] E.J. Kani and O.G. Rizzo, *Mazur's question on mod 11 representations of elliptic curves*, Preprint (2000), `https://mast.queensu.ca/~kani/papers/mazur8pl.pdf`. ↑5

[Kra03] Adolf Krazer, *Lehrbuch der thetafunktionen*, vol. 12, BG Teubner, 1903, Reprinted by Chelsea, New York, 1970. ↑1

[KS97] Ernst Kani and Wolfgang Schanz, *Diagonal quotient surfaces*, Manuscripta Math. **93** (1997), no. 1, 67–108. MR1446192. ↑27, ↑43, ↑63, ↑71

[KS98] ———, *Modular diagonal quotient surfaces*, Math. Z. **227** (1998), no. 2, 337–366. MR1609061. ↑2, ↑4, ↑24, ↑27, ↑29, ↑31, ↑43, ↑44, ↑45, ↑46, ↑55, ↑62, ↑74, ↑75, ↑76, ↑79, ↑149

[Kuh88] Robert M. Kuhn, *Curves of genus* 2 *with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988), no. 1, 41–49. MR936803. ↑1

[Kum15] Abhinav Kumar, *Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields*, Res. Math. Sci. **2** (2015), Art. 24, 46. MR3427148. ↑3, ↑5, ↑9, ↑10, ↑24, ↑25, ↑26, ↑29, ↑115, ↑116, ↑126, ↑135, ↑138, ↑170

[Kuw12] Masato Kuwata, *Constructing families of elliptic curves with prescribed mod 3 representation via Hessian and Cayleyan curves*, arXiv e-prints (2012), arXiv:1112.6317. ↑5, ↑115

[Lan76] Serge Lang, *Introduction to modular forms*, Grundlehren der Mathematischen Wissenschaften, No. 222, Springer-Verlag, Berlin-New York, 1976. MR0429740. ↑90

[Leg28] Adrien-Marie Legendre, *Traité des fonctions elliptiques et des intégrales eulériennes*, Huzard-Courcier (Paris), 1828. ↑1

[Lig77] Gérard Ligozat, *Courbes modulaires de niveau* 11, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), 1977, pp. 149–237. Lecture Notes in Math., Vol. 601. MR0463118. ↑107

[LMFDB] The LMFDB Collaboration, *The L-functions and modular forms database*, `http://www.lmfdb.org`, [Online; accessed November 2023]. ↑4, ↑9, ↑19, ↑22, ↑49, ↑68, ↑150, ↑154

[LR95] Joan C. Lario and Anna Rio, *An octahedral-elliptic type equality in* $\mathrm{Br}_2(k)$, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 1, 39–44. MR1340079. ↑115

[LR22] Álvaro Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplication*, Algebra Number Theory **16** (2022), no. 4, 777–837. MR4467123. ↑89

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR482230. ↑146

[McM07] Curtis T. McMullen, *Foliations of Hilbert modular surfaces*, Amer. J. Math. **129** (2007), no. 1, 183–215. MR2288740. ↑10, ↑25, ↑31

[MS93] J. R. Merriman and N. P. Smart, *Curves of genus* 2 *with good reduction away from 2 with a rational Weierstrass point*, Math. Proc. Cambridge Philos. Soc. **114** (1993), no. 2, 203–214. MR1230127. ↑159

[Nic18a] Christopher Nicholls, *Descent methods and torsion on Jacobians of higher genus curves*, Ph.D. thesis, University of Oxford, 2018. ↑158

[Nic18b] ———, *Github repository*, `https://github.com/cgnicholls/phd-code.git`, 2018, Accessed November 2023. ↑158

[Pap99] Ioannis Papadopoulos, *Courbes elliptiques ayant même 6-torsion qu'une courbe elliptique donnée*, J. Number Theory **79** (1999), no. 1, 103–114. MR1724256. ↑5

[Pre73] Alexander Prestel, *Die Fixpunkte der symmetrischen Hilbertschen Modulgruppe zu einem reell-quadratischen Zahlkörper mit Primzahldiskriminante*, Math. Ann. **200** (1973), 123–139. MR330054. ↑55

[PSS07] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$*, Duke Math. J. **137** (2007), no. 1, 103–158. MR2309145. ↑1, ↑5, ↑24, ↑94, ↑116, ↑161

[Rob99] Joel Philip Roberts, *Explicit families of elliptic curves with prescribed mod 6 representations*, Ph.D. thesis, The Ohio State University, 1999. MR2699563. ↑5

[RS95] Karl Rubin and Alice Silverberg, *Families of elliptic curves with constant mod p representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 148–161. MR1363500. ↑4, ↑5, ↑94, ↑115, ↑121

[RS99] ———, *Mod 6 representations of elliptic curves*, Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), Proc. Sympos. Pure Math., vol. 66, Amer. Math. Soc., Providence, RI, 1999, pp. 213–220. MR1703752. ↑5

[RS01] ———, *Mod 2 representations of elliptic curves*, Proc. Amer. Math. Soc. **129** (2001), no. 1, 53–57. MR1694877. ↑4, ↑5, ↑115, ↑121

[RSZ21] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *Github repository*, `https://github.com/AndrewVSutherland/ell-adic-galois-images`, 2021, Accessed November 2023. ↑67, ↑85, ↑167

[RSZ22] ———, *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight)*, Forum Math. Sigma **10** (2022), Paper No. e62, 63, With an appendix with John Voight. MR4468989. ↑7, ↑8, ↑10, ↑14, ↑67, ↑85, ↑93, ↑103, ↑104, ↑109, ↑146

[RZ15a] Jeremy Rouse and David Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Res. Number Theory **1** (2015), Paper No. 12, 34. MR3500996. ↑7, ↑14, ↑17, ↑85, ↑87, ↑88, ↑93, ↑97, ↑100, ↑101, ↑105, ↑108

[RZ15b] Jeremy Rouse and David Zureick-Brown, *Images of the 2-adic galois representation attached to elliptic curves*, `https://users.wfu.edu/rouseja/2adic/index.html`, 2015, Accessed November 2023. ↑169

[Sage] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 9.2)*, 2023, `https://www.sagemath.org`. ↑11, ↑49, ↑159

[Ser79] Jean-Pierre Serre, *Local fields*, Springer-Verlag, New York-Berlin,,, 1979, Translated from the French by Marvin Jay Greenberg. MR554237. ↑157

[Ser97] ———, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. MR1757192. ↑89, ↑93, ↑102, ↑112

[Ser08] ———, *Topics in Galois theory*, second ed., Research Notes in Mathematics, vol. 1, A K Peters, Ltd., Wellesley, MA, 2008, With notes by Henri Darmon. MR2363329. ↑14, ↑146

[Sie68] Carl Ludwig Siegel, *Zum Beweise des Starkschen Satzes*, Invent. Math. **5** (1968), 180–191. MR228465. ↑113

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368. ↑37, ↑38, ↑91, ↑112

[Sil97] Alice Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 447–461. MR1638488. ↑4, ↑5, ↑91, ↑115, ↑121

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094. ↑8, ↑13, ↑89, ↑147

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR236190. ↑125

[Stacks] The Stacks project authors, *The stacks project*, `https://stacks.math.columbia.edu`, 2023. ↑124

[SW22] Ari Shnidman and Ariel Weiss, *Elements of prime order in Tate-Shafarevich groups of abelian varieties over* $\mathbb{Q}$, Forum Math. Sigma **10** (2022), Paper No. e98, 10. MR4504870. ↑8

[SZ17] Andrew V. Sutherland and David Zywina, *Modular curves of prime-power level with infinitely many rational points*, Algebra Number Theory **11** (2017), no. 5, 1199–1229. MR3671434. ↑7, ↑14, ↑93

[vB21] Raymond van Bommel, *Efficient computation of BSD invariants in genus 2*, Arithmetic geometry, number theory, and computation, Simons Symp., Springer, Cham, 2021, pp. 237–258. MR4427964. ↑160

[vdG88] Gerard van der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 16, Springer-Verlag, Berlin, 1988. MR930101. ↑2, ↑10, ↑24, ↑26, ↑27, ↑29, ↑31, ↑33, ↑37, ↑44, ↑46, ↑49, ↑55, ↑57, ↑58, ↑71

[Zyw15a] David Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over* $\mathbb{Q}$, arXiv e-prints (2015), arXiv:1508.07660. ↑89, ↑90, ↑91

[Zyw15b] ———, *Possible indices for the Galois image of elliptic curves over* $\mathbb{Q}$, arXiv e-prints (2015), arXiv:1508.07663. ↑17

[Zyw22] ———, *Explicit open images for elliptic curves over* $\mathbb{Q}$, arXiv e-prints (2022), arXiv:2206.14959. ↑147, ↑159, ↑167