WARWICK
THE UNIVERSITY OF WARWICK

A Thesis Submitted for the Degree of PhD at the University of Warwick

Permanent WRAP URL:

http://wrap.warwick.ac.uk/161941

Copyright and reuse:
This thesis is made available online and is protected by original copyright.
Please scroll down to view the document itself.
Please refer to the repository record for this item for information to help you to cite it.
Our policy information is available from the repository home page.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

warwick.ac.uk/lib-publications

Low degree points on modular curves

by

Josha Box

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Department of Mathematics

June 2021

Contents

List of Tables

List of Figures

Acknowledgements

I must start with an exceptionally big thank you to my supervisor, Professor Samir Siksek. I have encountered few people who possess the intelligence, patience and kindness that he has displayed to me on a weekly basis during the past years; for this I am truly grateful. It pleases me to say that Samir deserves much credit for the results displayed in this thesis, which could not have been obtained without his support and encouragement, not to mention his countless ideas and suggestions.

I have greatly enjoyed my time in Warwick, in no small part thanks to the people in the number theory group. The supportive and friendly atmosphere created by John Cremona, David Loeffler, Samir Siksek, Damiano Testa and the others have made my PhD a genuinely pleasant experience. In particular, I would like to warmly thank John Cremona for his generous time, help and ideas, which contributed greatly to my work on Chapter 3. I am also grateful to Damiano Testa and David Loeffler for their kind help both during and outside of the group meetings. Special thanks are due to my friend, co-author and former colleague Samuel Le Fourn for a fruitful and enjoyable collaboration, and, most importantly, for never failing to share his opinion on the latest developments in the Champions League. Finally, it is my pleasure to thank Alessandro, George, and Mattia for the many, often football-related, distractions they have provided me with.

To my collaborators Stevan Gajović and Pip Goodman I am grateful for making our project such a fun experience, particularly during our many online meetings.

I would also like to thank the examiners Tom Fisher and Damiano Testa for their careful reading of this thesis and for numerous valuable suggestions and corrections.

At long last, I must also extend my sincere gratitude to all who have put up with me during the previous years, in which number theory perhaps claimed more than its fair share of my time. In particular to my mum and to Francesca, I say thank you.

Declarations

During the course of my PhD, I have written five research articles: [Box21c], [Box21b], [Box21a], [BGG21] (joint with Stevan Gajović and Pip Goodman) and [BL20] (joint with Samuel Le Fourn). The first, [Box21c], has been published in *Mathematics of Computation*, while the remaining four have been submitted for publication. This thesis is made up of the first four mentioned articles, all of which are concerned with modular curves. The joint work [BL20] with Le Fourn about integral points on the Siegel modular variety $A_2(2)$ is not included in this thesis.

Chapter 1 starts with a short introduction to modular curves (Section 1.1.1), which is entirely based on the literature. The remainder of the thesis consists, unless stated otherwise, of my own original work, some of which (part of Chapter 3) was produced in collaboration with Stevan Gajović and Pip Goodman, and all of which was written under the guidance of Professor Siksek.

The remainder of Chapter 1 consists of the introductory sections of [Box21b] and [Box21a]. Chapter 2 is a combination of [Box21c] and [BGG21]. In [Box21c], we compute the set of quadratic points on modular curves using Siksek's symmetric Chabauty method [Sik09], while in [BGG21] we generalise Siksek's method and use the computational approach developed in [Box21c] to determine the cubic (and in one case quartic) points on the same modular curves. Chapter 3 thus contains the computational approach of [Box21c], the Chabauty method developed in [BGG21], and the combined results from both papers. Finally, Chapter 4 is a subset of the article [Box21a].

This thesis has not been submitted for a degree at another university.

Abstract

In this thesis we study modular curves and their points defined over number fields of degrees 2, 3 and 4. In Chapter 1, we introduce modular curves and describe the moduli interpretation of their morphisms. This is used in Chapter 2 to find an algorithm for computing models of quotients of general modular curves, by finding the equations satisfied by the corresponding cusp forms. We also provide in Chapter 1 an overview of the computational methods used in Chapters 3 and 4 for studying points of fixed degree on modular curves.

In Chapter 3 we examine the modular curves $X_0(N)$ for

$$N \in \{37, 43, 53, 57, 61, 65, 67, 73\}.$$

These are exactly the modular curves $X_0(N)$ of genus between 2 and 5 whose Jacobians have infinite Mordell–Weil group. We determine the (isolated) quadratic points on each of them, the cubic points on those with $N \geq 53$, and the isolated quartic points on $X_0(65)$. To analyse their quadratic points, we use Siksek's relative symmetric Chabauty method, while we develop a generalisation to study points of higher degrees. All these points are listed in the tables in Section 3.4.

Finally, in Chapter 4 we focus on the quartic points on various modular curves to prove that elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular. The algorithm developed in Chapter 2 and the generalised Chabauty method established in Chapter 3 are essential ingredients for the proof.

Chapter 1

Introduction

Modular curves are the main object of study in this thesis. They are examples of moduli spaces, nearly magical objects parametrising families of other objects. A modular curve is just one single curve, but each of its points represents another (elliptic) curve, with additional structure. By examining a single modular curve, we therefore learn about all elliptic curves at once, a fact that seems almost too good to be true. In this thesis, by studying "low degree points on modular curves", we implicitly learn about the properties of all elliptic curves defined over number fields of small degree.

In this chapter we begin by analysing modular curves in Section 1.1, after which we introduce the methods used to study points on modular curves of fixed degree in Section 1.2.

1.1 Modular curves and their morphisms

We start by defining modular curves and investigating the morphisms between them. This section, with the exception of its subsections 1.1.1 and 1.1.4, is part of the article [Box21b].

1.1.1 Complex modular curves

Let N be a positive integer, and consider a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. To G we associate the *congruence subgroup* Γ_G, defined to be the inverse image under $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ of $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Let $\mathcal{H}$ be the complex upper half plane. The group Γ_G acts on $\mathcal{H}$ by fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d} \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_G \text{ and } \tau \in \mathcal{H}.$$

The quotient $Y_{\Gamma_G} := \Gamma_G \backslash \mathcal{H}$ can be compactified to a projective curve X_{Γ_G} over the complex numbers, which we call the *complex modular curve* associated to Γ_G. Given $\tau \in \mathcal{H}$, we can also consider the lattice $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z} \subset \mathbb{C}$ and the associated torus $E_\tau = \mathbb{C}/\Lambda_\tau$. Using the identification between complex tori and complex elliptic curves (defined e.g. in [DS05]), we think of E_τ as an elliptic curve. Its N-torsion is $E_\tau[N] = (\frac{\tau}{N}\mathbb{Z} \oplus \frac{1}{N}\mathbb{Z})/\Lambda_\tau$, which has

an obvious choice of basis defining an isomorphism

$$\phi_\tau \colon (\mathbb{Z}/N\mathbb{Z})^2 \to E_\tau[N], \quad \phi_\tau(1,0) = \tau/N, \quad \phi_\tau(0,1) = 1/N.$$

On $E_\tau[N]$ we moreover have the Weil pairing $e_N \colon E_\tau[N] \times E_\tau[N] \to \mu_N$, where $\mu_N \subset \mathbb{C}^\times$ is the subgroup of Nth roots of unity. This satisfies $e_N(\phi_\tau(1,0), \phi_\tau(0,1)) = e^{2\pi i/N}$. Now the set of isomorphisms $\phi \colon (\mathbb{Z}/N\mathbb{Z})^2 \to E_\tau[N]$ has a left G-action given by

$$(g \cdot \phi)(a) = \phi(a \cdot g) \text{ for } g \in G \text{ and } a \in (\mathbb{Z}/N\mathbb{Z})^2,$$

where $a \cdot g$ is multiplication of the row vector a with the matrix g. This gives rise to equivalence classes $[\phi]_G$ of isomorphisms $(\mathbb{Z}/N\mathbb{Z})^2 \to E_\tau[N]$. The map

$$\Gamma_G \tau \mapsto (E_\tau, [\phi_\tau]_G) \tag{1.1}$$

defines a bijection between Y_{Γ_G} and the isomorphism classes of pairs $(E, [\phi]_G)$, where E is a complex torus and $\phi \colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$ is an isomorphism satisfying

$$e_N(\phi(1,0), \phi(0,1)) = e^{2\pi i a/N} \text{ for some } a \in \det(G).$$

This bijection thus endows Y_{Γ_G} with the structure of a moduli space parametrising elliptic curves with extra "G-structure".

1.1.2 Modular curves via their moduli interpretation

We use this moduli interpretation to define modular curves over more general rings, by generalising the bijection (1.1) to elliptic curves over arbitrary base schemes. While we shall not need the description of modular curves as schemes over $\mathbb{Z}[1/N]$ or $\mathbb{Z}[1/N, \zeta_N]$, this approach helps us decide the *field* of definition of modular curves and the Fourier coefficients of their cusp forms. We give an overview of standard results from Deligne and Rapoport [DR73] Katz and Mazur [KM85], which we attempt to describe as concretely as possible.

Let $N \in \mathbb{Z}_{\geq 1}$ be an integer, and choose a primitive Nth root of unity $\zeta_N := e^{2\pi i/N} \in \mathbb{C}$. Let S be a scheme over $\mathbb{Z}[1/N]$. An *elliptic curve over* S is a pair $(E \to S, O)$, where $E \to S$ is a proper smooth map, all of whose fibres are geometrically connected curves of genus 1, and O is a section of $E \to S$. Then E/S obtains the structure of a commutative group scheme. On E/S, there is the Weil pairing

$$e_N : \quad E[N] \times E[N] \to \mu_N, \quad (P, Q) \mapsto e_N(P, Q),$$

where $\mu_N = \mathrm{Spec}(\mathbb{Z}[X]/(X^n - 1))$ is the group scheme of Nth roots of unity. To such an elliptic curve E/S, we can associate its $\Gamma(N)$-*structures*, defined as the morphisms of group schemes over S

$$\phi : \ (\mathbb{Z}/N\mathbb{Z})^2_S \to E[N],$$

such that $E[N] = \sum_{(a,b) \in (\mathbb{Z}/N\mathbb{Z})^2} \phi(a,b)$ as effective Cartier divisors. (When $S = \mathrm{Spec}(K)$

for a field K of characteristic coprime to N, this means that $\phi(0,1)$ and $\phi(1,0)$ form a basis). Now suppose that $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then g acts on $(\mathbb{Z}/N\mathbb{Z})^2_S$ by right-multiplication of row vectors, and this is compatible with the Weil pairing in the sense that

$$e_N(\phi(a,b),\phi(c,d)) = e_N(\phi(1,0),\phi(0,1))^{\deg(g)} \text{ for each } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}). \quad (1.2)$$

We consider the functor

$$\mathcal{F}_N : \underline{\mathrm{Sch}}_{\mathbb{Z}[\zeta_N]} \to \underline{\mathrm{Set}}, \quad S \mapsto \{(E/S,\phi)\},$$

mapping a scheme S to the isomorphism classes of pairs $(E/S,\phi)$, where E is an elliptic curve over S and ϕ is a $\Gamma(N)$-structure on E/S. The Weil pairing defines a map of functors $e_N : \mathcal{F}_N \to \mu_N$, and we define the subfunctor $\mathcal{F}_N^{\mathrm{can}} : \underline{\mathrm{Sch}}_{\mathbb{Z}[\zeta_N]} \to \underline{\mathrm{Set}}$, mapping S to the set of pairs $(E/S,\phi) \in \mathcal{F}_N(S)$ such that $e_N(\phi(1,0),\phi(0,1)) = \zeta_N$. Now Katz and Mazur show in [KM85, Chapter 9] that $\mathcal{F}_N^{\mathrm{can}}$ admits a coarse moduli space $Y(N)/\mathbb{Z}[\zeta_N]$, whose compactification $X(N)$ is smooth over $\mathbb{Z}[\zeta_N, 1/N]$.

We now consider any subgroup $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Its group of determinants $\det(G)$ acts on $\mathbb{Z}[\zeta_N]$ by automorphisms via $\zeta_N \mapsto \zeta_N^a$ for $a \in \det(G)$. We obtain a fixed subring $\mathbb{Z}[\zeta_N]^{\det(G)} \subset \mathbb{Z}[\zeta_N]$. For schemes $S/\mathbb{Z}[\zeta_N]$, the right-action of G on $(\mathbb{Z}/N\mathbb{Z})^2_S$ by right-multiplication gives rise to a left-action action on $\Gamma(N)$-structures. For $g \in G$ and a $\Gamma(N)$-structure ϕ, we denote this action by $g \cdot \phi$. Denote the G-equivalence class of the $\Gamma(N)$-structure ϕ by $[\phi]_G$.

Given a $\mathbb{Z}[\zeta_N]^{\det(G)}$-scheme S and an elliptic curve E/S, we can consider schemes T/S and their base-change $T' := T \times_{\mathbb{Z}[\zeta_N]^{\det(G)}} \mathbb{Z}[\zeta_N]$.

Definition 1.1.1. We define the functor

$$\mathcal{F}_G : \underline{\mathrm{Sch}}_{\mathbb{Z}[\zeta_N]^{\det(G)}} \longrightarrow \underline{\mathrm{Set}}, \quad S \mapsto \{(E/S,[\phi]_G)\},$$

mapping a scheme S to the set of isomorphism classes of pairs $(E/S,[\phi]_G)$, where $[\phi]_G$ is a G-equivalence class of $\Gamma(N)$-structures on $E_{T'}/T'$ for some T/S, such that $[\phi]_G$ is "defined over S". We define $\mathcal{F}_G^{\mathrm{can}}$ as the subfunctor of those pairs $(E/S,[\phi]_G)$ where $e_N(\phi(1,0),\phi(0,1))$ and ζ_N have equal image in $(\mu_N/\det(G))(S)$, or, more concretely, where

$$e_N(\phi(1,0),\phi(0,1)) = \zeta_N^a \text{ for some } a \in \det(G).$$

Katz and Mazur show in [KM85, Chapter 9] that $\mathcal{F}_G^{\mathrm{can}}$ admits a coarse moduli scheme $Y_G/\mathbb{Z}[1/N,\zeta_N]^{\det(G)}$, whose compactification X_G is smooth. We call X_G the *modular curve associated to G*.

Finally, we mention what it means for $[\phi]_G$ to be "defined over S". Given an elliptic curve E/S, we consider the functor

$$(\mathcal{F}_N)_{E/S} : \underline{\mathrm{Sch}}_S \longrightarrow \underline{\mathrm{Set}}, \quad T \mapsto \{\Gamma(N)\text{-structures on } E_T/T\}.$$

This functor is represented by an S-scheme $\mathcal{M}_{E/S}$, meaning that we have bijections $\mathcal{M}_{E/S}(T) \longleftrightarrow (\mathcal{F}_N)_{E/S}(T)$, functorially in T. Now G acts on $\mathcal{M}_{E/S}$, and we say that $[\phi]_G$ is *defined over* S, when the image of ϕ in the T'-points $(\mathcal{M}_{E/S}/G)(T')$ of the quotient scheme is in fact in $(\mathcal{M}_{E/S}/G)(S)$.

Note that $(Y_G)_{\mathbb{C}}$ and $(X_G)_{\mathbb{C}}$ are via (1.1) identified with Y_{Γ_G} and X_{Γ_G} respectively.

1.1.3 Notation for modular curves

We define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$:

$$B_0(N) := \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \quad B_1(N) := \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}, \quad \widetilde{B}_1(N) := \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \quad G(N) := \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix},$$

and $\widetilde{G}(N) := \{I\}$. We denote their congruence subgroups by $\Gamma_0(N)$, $\Gamma_1(N)$, $\widetilde{\Gamma}_1(N)$, $\Gamma(N)$ and $\widetilde{\Gamma}(N)$ respectively. Note that $\widetilde{\Gamma}_1(N) = \Gamma_1(N)$ and $\widetilde{\Gamma}(N) = \Gamma(N)$. The corresponding modular curves are denoted by $X_0(N)$, $X_1(N)$, $\widetilde{X}_1(N)$, $X(N)$ and $\widetilde{X}(N)$.

Let p be a prime number. We denote by $C_{\mathrm{s}}^+(p) \subset \mathrm{GL}_2(\mathbb{F}_p)$ the normaliser of a split Cartan subgroup, and by $C_{\mathrm{ns}}^+(p) \subset \mathrm{GL}_2(\mathbb{F}_p)$ the normaliser of a non-split Cartan subgroup. Finally, we also consider

$$G(\mathrm{e}7) := \left\langle \begin{pmatrix} 0 & 5 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 3 & 2 \end{pmatrix} \right\rangle \subset \mathrm{GL}_2(\mathbb{F}_7),$$

which is an index 2 subgroup of $C_{\mathrm{ns}}^+(7)$.

We define $X(\mathrm{b}p)$, $X(\mathrm{s}p)$, $X(\mathrm{ns}p)$ and $X(\mathrm{e}7)$ to be the curves X_G, where G is $B_0(p)$, $C_{\mathrm{s}}^+(p)$, $C_{\mathrm{ns}}^+(p)$ and $G(\mathrm{e}7)$ respectively. We note that $X(\mathrm{b}p) = X_0(p)$. For distinct primes $p_1, \ldots, p_n$ and $\mathrm{u}_1, \ldots, \mathrm{u}_n \in \{\mathrm{b}, \mathrm{s}, \mathrm{ns}, \mathrm{e}\}$, we define

$$X(\mathrm{u}_1 p_1, \ldots, \mathrm{u}_n p_n)$$

to be the normalisation of $X(\mathrm{u}_1 p_1) \times_{X(1)} \cdots \times_{X(1)} X(\mathrm{u}_n p_n)$ (see Definition 1.1.3 for the definition of the map $X(\mathrm{u}_i p_i) \to X(1)$). This is the modular curve associated to the intersection of the inverse images of the corresponding subgroups of $\mathrm{GL}_2(\mathbb{Z}/p_1\mathbb{Z}), \ldots, \mathrm{GL}_2(\mathbb{Z}/p_n\mathbb{Z})$ in $\mathrm{GL}_2(\mathbb{Z}/p_1 \cdots p_n\mathbb{Z})$.

We also write $X(\Gamma_G)$ instead of X_G and $\widetilde{X}(\Gamma_G)$ instead of $X_{\widetilde{G}}$ when G is clear from context. For positive integers K, M, we define $X(\Gamma_0(M) \cap \Gamma_1(K))$, resp. $\widetilde{X}(\Gamma_0(M) \cap \Gamma_1(K))$, for the curve associated to the intersection of the inverse images of $B_0(M)$ and $B_1(K)$, resp. $B_0(M)$ and $\widetilde{B}_1(K)$, in $\mathrm{GL}_2(\mathbb{Z}/\mathrm{lcm}(K, M)\mathbb{Z})$. Similarly, define $X(\Gamma_0(M) \cap \Gamma(K))$ and $\widetilde{X}(\Gamma_0(M) \cap \Gamma(K))$.

For any ring R, we denote by $\mathrm{P}\Gamma$ the image of $\Gamma \subset \mathrm{GL}_2(R)$ in $\mathrm{PGL}_2(R)$. When $N = K \cdot M$, we denote by G_K the image of $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ in $\mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$. By $\mathcal{N}_{\Gamma_G}$ we denote the normaliser of $\mathrm{P}\Gamma_G$ in $\mathrm{PGL}_2^+(\mathbb{Q})$, where the superscript $+$ means "with positive determinant", and by $\mathcal{N}_G \subset \mathcal{N}_{\Gamma_G}$ the subgroup of those $\gamma \in \mathcal{N}_{\Gamma_G}$ satisfying condition (1.3), to be defined in Proposition 1.1.5.

Next, consider a positive integer k, a ring R and a congruence subgroup Γ. We

denote by $S_k(\Gamma, R)$ the space of weight k cusp forms with respect to Γ with Fourier coefficients contained in the ring R. When $R = \mathbb{C}$, we sometimes omit R and write $S_k(\Gamma)$.

1.1.4 More on the moduli interpretation of modular curves

We first mention two kinds of trivial morphisms between modular curves.

(M1) When $G \subset H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, denote by $\mathcal{F}_H^{\mathrm{can}}|_{\underline{\mathrm{Sch}}_{\mathbb{Z}[\zeta_N]^{\det(G)}}}$ the restriction of $\mathcal{F}_H^{\mathrm{can}}$ to $\underline{\mathrm{Sch}}_{\mathbb{Z}[\zeta_N]^{\det(G)}}$. We obtain a forgetful map of functors $\mathcal{F}_G^{\mathrm{can}} \to \mathcal{F}_H^{\mathrm{can}}|_{\underline{\mathrm{Sch}}_{\mathbb{Z}[\zeta_N]^{\det(G)}}}$ yielding a quotient morphism $X_G \to X_H \times_{\mathbb{Z}[\zeta_N]^{\det(H)}} \mathbb{Z}[\zeta_N]^{\det(G)}$.

(M2) Consider a group $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and an integer M. Define $\pi\colon \mathrm{GL}_2(\mathbb{Z}/MN\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The multiplication-by-$M$ map on NM-torsion of elliptic curves and the to-the-Mth-power map $\mu_{NM} \to \mu_N$ commute with respect to the Weil pairing by (1.2), and thus define an isomorphism of functors $\mathcal{F}_{\pi^{-1}(G)}^{\mathrm{can}} \to \mathcal{F}_G^{\mathrm{can}}$. We conclude that $X_{\pi^{-1}(G)} = X_G$.

By (M2), any morphism of modular curves can be viewed as a morphism between modular curves of the same level.

Example 1.1.2. When $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\Delta \subset \det(G)$ is a subgroup, we can consider the subgroup $H \subset G$ of elements $g \in G$ with $\det(g) \in \Delta$. Then G and H give rise to the same congruence subgroups, hence $(X_G)_{\mathbb{C}} = (X_H)_{\mathbb{C}}$. We obtain a morphism of curves $(X_H)_{\mathbb{Q}(\zeta_N)^{\det(H)}} \to (X_G)_{\mathbb{Q}(\zeta_N)^{\det(H)}}$ of the form (M1), which must be an isomorphism. For example, $\widetilde{X}(\Gamma_0(M) \cap \Gamma_1(K))_{\mathbb{Q}(\zeta_K)} = X(\Gamma_0(M) \cap \Gamma_1(K))_{\mathbb{Q}(\zeta_K)}$ and $\widetilde{X}(\Gamma_0(M) \cap \Gamma(K))_{\mathbb{Q}(\zeta_K)} = X(\Gamma_0(M) \cap \Gamma(K))_{\mathbb{Q}(\zeta_K)}$.

Definition 1.1.3. Recall that $X(1) = X_{G(1)}$. By (M2), this is isomorphic to $X_{\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})}$ for any N. For $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, we then obtain by (M1) a morphism

$$j\colon X_G \longrightarrow X(1) \times_{\mathbb{Z}} \mathbb{Z}[1/N, \zeta_N]^{\det(G)}$$

called the *j-map*. The j-invariant of an elliptic curve determines a morphism on the moduli space $Y(1)$, giving rise to an isomorphism $X(1)_{\mathbb{Q}} \simeq \mathbb{P}^1_{\mathbb{Q}}$. We thus view j as a map $X_G \to \mathbb{P}^1$. Define the *cusps* of X_G to be those $Q \in X_G(\overline{\mathbb{Q}})$ satisfying $j(Q) = \infty$. The cusps are exactly the set $X_G(\overline{\mathbb{Q}}) \setminus Y_G(\overline{\mathbb{Q}})$.

Suppose now that $-I \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. The latter implies that $\mathcal{F}_G = \mathcal{F}_G^{\mathrm{can}}$, and X_G is a $\mathbb{Z}[1/N]$-scheme. We consider it temporarily as a curve over $\mathbb{Q}$. For an elliptic curve E over a number field K, we denote by $\overline{\rho}_{E,N}$ its mod N representation $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[N](\overline{K}))$. Being a *coarse* moduli scheme, $Y_G(L)$ parametrises pairs $(E, [\phi]_G)$ whose isomorphism class is defined over L, a priori only for algebraically closed fields L. In this special case, however, we can say more. When $\alpha\colon G \to H$ is a group isomorphism, we denote the map $\mathrm{Aut}(H) \to \mathrm{Aut}(G)$, $\psi \mapsto \alpha^{-1} \circ \psi \circ \alpha$ by α^*.

Proposition 1.1.4. *Let K be a perfect field of characteristic not dividing N.*

(i) If E/K is an elliptic curve with j-invariant $j(E)$ and $\phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N](\overline{K})$ is an isomorphism satisfying $\phi^*\mathrm{Im}(\overline{\rho}_{E,N}) \subset G$, then there exists $Q \in Y_G(K)$ with $j(Q) = j(E)$.

(ii) Conversely, if $Q \in Y_G(K)$ with $j(Q) \notin \{0, 1728\}$, then there exist an elliptic curve E/K with j-invariant $j(Q)$ and an isomorphism $\phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N](\overline{K})$ such that $\phi^*\mathrm{Im}(\overline{\rho}_{E,N}) \subset G$.

Proof. This is well-known and should probably be attributed to Deligne and Rapoport [DR73]. We provide a proof similar to the one in [Zyw15, Proposition 3.2]. For (i), consider such E and ϕ and define $Q = (E, [\phi]_G) \in Y_G(\overline{K})$. Each $\sigma \in \mathrm{Gal}(\overline{K}/K)$ acts on both $Y_G(\overline{K})$ (by base change under $\sigma\colon \mathrm{Spec}(\overline{K}) \to \mathrm{Spec}(\overline{K})$) and on $\mathcal{F}_G(\overline{K})$ by mapping $(E, [\phi]_G)$ to $(E^\sigma, [\overline{\rho}_{E,N}(\sigma) \circ \phi]_G)$. These actions commute with respect to the bijection $Y_G(\overline{K}) \leftrightarrow \mathcal{F}_G(\overline{K})$. As K is perfect, it suffices to show that Q is fixed by $\mathrm{Gal}(\overline{K}/K)$, or, in other words, that the isomorphism class of $(E, [\phi]_G)$ is fixed by each $\sigma \in \mathrm{Gal}(\overline{K}/K)$. By assumption, $E = E^\sigma$, and, moreover, $\phi^*(\rho_{E,N}(\mathrm{Gal}(\overline{K}/K))) \subset G$ means that for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$ there exists $g \in G$ such that $\overline{\rho}_{E,N}(\sigma) \circ \phi = \phi \circ g$, so that $[\overline{\rho}_{E,N}(\sigma) \circ \phi]_G = [\phi]_G$. We conclude that $(E, [\phi]_G)$ is fixed by $\mathrm{Gal}(\overline{K}/K)$, so that $Q \in Y_G(K)$.

For part (ii), consider $E/\overline{K}$ and $\phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N](\overline{K})$ such that $Q = (E, [\phi]_G)$ as elements of $Y_G(\overline{K})$. Since $j\colon X_G \to X(1)$ is defined over K we find that $j(E) = j(Q) \in K$. We thus find an elliptic curve E'/K such that $j(E') = j(Q)$. Changing ϕ under the isomorphism $E' \simeq E$, we assume that $Q = (E, [\phi]_G)$ with E defined over K. Now consider $\sigma \in \mathrm{Gal}(\overline{K}/K)$. As $Q \in Y_G(K)$, there exists an automorphism $\alpha \in \mathrm{Aut}_{\overline{K}}(E)$ such that $[\overline{\rho}_{E,N}(\sigma) \circ \phi]_G = [\alpha \circ \phi]_G$. As $j(E) \notin \{0, 1728\}$ we have $\alpha \in \{\pm \mathrm{Id}\}$. Since $-I \in G$, we conclude that $[\overline{\rho}_{E,N}(\sigma) \circ \phi] = [\alpha \circ \phi]_G = [\phi]_G$, and indeed $\phi^*\overline{\rho}_{E,N}(\sigma) \in G$. □

This interpretation underlines the usefulness of modular curves, and why one should care about their K-rational points; see also Theorem 4.1.3 for an application.

When N, M are coprime, $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $H \subset \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$, we obtain a new group $F \subset \mathrm{GL}_2(\mathbb{Z}/NM\mathbb{Z})$ as the intersection of the inverse images of G and H under the reduction maps. As curves over $\mathbb{Q}$, X_F is then the normalisation of $X_H \times_{X(1)} X_G$, as noticed before. Since the j-map on modular curves is ramified only at points Q with $j(Q) \in \{\infty, 0, 1728\}$, we find away from those j-invariants that $Q \in (X_H \times_{X(1)} X_G)(K)$ if and only if $Q \in X_F(K)$. This provides a clear picture for the moduli interpretation of the curves $X(\mathrm{u}_1 p_1, \ldots, \mathrm{u}_n p_n)$ defined in Section 1.1.3. (Note that the Borel and Cartan subgroups, as well as $G(\mathrm{e}7)$, have surjective determinant and contain $-I$.)

1.1.5 Modular Curves not of the standard type

In the literature, modular curves tend to be described as being determined by a level $N \in \mathbb{Z}_{\geq 1}$ and a subgroup $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, as we have done in Definition 1.1.1. This is a convenient point of view, since such modular curves have (by definition) an interpretation as moduli spaces of elliptic curves with additional structure.

However, some "modular curves" do not fit in this framework. The curve $X_0(N)$ parametrises pairs (E, C) where E is an elliptic curves and $C \subset E$ is a cyclic subgroup of

order N. This curve admits a well-known involution, called the Atkin–Lehner involution w_N, mapping such a pair (E, C) to $(E/C, E[N]/C)$. The quotient curve $X_0(N)/w_N$ does not parametrise elliptic curves with additional structure, but rather certain pairs of elliptic curves with extra structure, and therefore the standard theory of "moduli problems" does not apply.

Nonetheless, $X_0(N)/w_N$ does have a moduli interpretation, it is defined over $\mathbb{Q}$, and it is a modular curve in the adelic sense: $(X_0(N)/w_N)_{\mathbb{C}} = \mathrm{GL}_2^+(\mathbb{Q})\backslash(\mathrm{GL}_2(\mathbb{A}_f)\times\mathcal{H})/U$, where $\mathbb{A}_f$ denotes the finite adèles, $\mathcal{H}$ is the complex upper half plane and U is the compact open subgroup of $\mathrm{GL}_2(\mathbb{A}_f)$ generated by w_N and the inverse image of G in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

While Atkin–Lehner involutions may be well understood, more modular curves can arise in this way. Firstly, when $h^2 \mid N$ for a non-trivial divisor h of 24, the normaliser of $\Gamma_0(N)$ in $\mathrm{PGL}_2(\mathbb{Q})$ is generated by more than just the Atkin–Lehner involutions (see Lemma 2.2.2), giving rise to extra automorphisms on $X_0(N)$ (not all defined over $\mathbb{Q}$, however). When $N \in \{40, 48\}$, two such automorphisms were explicitly determined by Bruin and Najman [BN15]. When $9 \mid N$, one normalising matrix is $\begin{pmatrix} 1 & 1/3 \\ 0 & 1 \end{pmatrix}$, giving rise to an automorphism α_3 of order 3, defined over $\mathbb{Q}(\zeta_3)$, such that the group $\langle\alpha_3\rangle$ generated by α_3 is $\mathbb{Q}$-rational. In particular, this yields a "new" morphism of curves over $\mathbb{Q}$, $X_0(N) \to X_0(N)/\langle\alpha_3\rangle$. None of these morphisms is of the trivial kinds (M1) and (M2) described in the previous section.

More types of examples occur on modular curves of mixed level by composing automorphisms. Up to conjugation, there is an inclusion $C_{\mathrm{s}}^+(3) \subset C_{\mathrm{ns}}^+(3)$ with index 2. Any matrix in $C_{\mathrm{ns}}^+(3) \setminus C_{\mathrm{s}}^+(3)$ determines an involution ϕ_3 on $X(\mathrm{s}3)$. On the level 15 modular curve $X(\mathrm{b}5, \mathrm{s}3)$, we then obtain an Atkin–Lehner involution w_5 as well as a lift ψ_3 of ϕ_3. These involutions commute and give rise to another involution $\psi_3 w_5$, and another modular curve $X(\mathrm{b}5, \mathrm{s}3)/\psi_3 w_5$. A similar situation occurs for the inclusion $G(\mathrm{e}7) \subset C_{\mathrm{ns}}^+(7)$, leading to an involution $\phi_7\colon X(\mathrm{b}5, \mathrm{e}7) \to X(\mathrm{b}5, \mathrm{e}7)$. In Section 2.4 we study the curves $X(\mathrm{b}5, \mathrm{e}7)/w_5$ and $X(\mathrm{b}5, \mathrm{e}7)/\phi_7 w_5$, which will play an essential role in Chapter 4. In order to understand such quotient curves, we first study the moduli interpretation of such (auto)morphisms.

1.1.6 Morphisms between modular curves and their moduli interpretation

Suppose that $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$ satisfies $\gamma\Gamma_G\gamma^{-1} \subset \Gamma_H$ for some $G, H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then γ defines a morphism $(X_G)_{\mathbb{C}} \to (X_H)_{\mathbb{C}}$ through its action as a fractional linear transformation on $\mathcal{H}$. This is a morphism defined a priori over $\mathbb{C}$. We investigate when this morphism is in fact defined over $\mathbb{Z}[\zeta_N]^{\det(G)}$. The following proposition generalises, and was inspired by, [BN15, Section 3].

Proposition 1.1.5. *Suppose that $G, H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and consider $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$. Assume (after scaling) that γ has integral coefficients, with $\delta := \det(\gamma)$. Denote by π :*

$\mathrm{GL}_2(\mathbb{Z}/N\delta\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ *the reduction map. If*

$$\gamma\pi^{-1}(G) \subset \pi^{-1}(H)\gamma \tag{1.3}$$

then $\det(G) \subset \det(H)$ *and* γ *determines a morphism* $\theta_\gamma : X_G \to X_H \times_{\mathbb{Z}[\zeta_N]^{\det(H)}} \mathbb{Z}[\zeta_N]^{\det(G)}$.

Moreover, $\gamma\Gamma_G\gamma^{-1} \subset \Gamma_H$ *and* $(\theta_\gamma)_{\mathbb{C}} : (X_G)_{\mathbb{C}} \to (X_H)_{\mathbb{C}}$ *corresponds to the action of* γ *on* $\Gamma_G\backslash\mathcal{H}$ *followed by projection onto* $\Gamma_H\backslash\mathcal{H}$ *.*

Proof. We shall replace G by $\pi^{-1}(G)$ and construct a morphism $\mathcal{F}^{\mathrm{can}}_{\pi^{-1}(G)} \to \mathcal{F}^{\mathrm{can}}_H|_{\mathbb{Z}[\zeta_N]^{\det(G)}}$. We first unravel formalities to make concrete what this means. The functor $\mathcal{F}^{\mathrm{can}}_G$ is the functor associated to the "moduli problem" $([\Gamma(N)]/G)^{\mathrm{can}}$, as defined in [KM85, 9.4]. There are two constructions at work here: the quotient by G (see [KM85, Chapter 7]), and the can-construction (see [KM85, Chapter 9]). It follows from (M2), [KM85, Corollary 9.1.9] and [KM85, Theorem 7.1.3] that it suffices to define a $(\pi^{-1}G, H)$-equivariant map $\alpha\colon \mathcal{F}_{N\delta} \to \mathcal{F}_N$ given by

$$\alpha : \ (E/S, \phi : (\mathbb{Z}/N\delta\mathbb{Z})_S \to E[N\delta]) \mapsto (E_\gamma/S, \phi_\gamma : (\mathbb{Z}/N\mathbb{Z})_S \to E_\gamma[N])$$

that gives rise to a commutative diagram

$$\begin{tikzcd} \mathcal{F}_{N\delta} \arrow[r, "\alpha"'] \arrow[d, "e_{N\delta}"'] & \mathcal{F}_N \arrow[d, "e_N"] \\ \mu_{N\delta} \arrow[r] & \mu_N \end{tikzcd}$$

where the bottom map is defined by $\zeta_{N\delta} \mapsto \zeta_N = \zeta_{N\delta}^{\delta}$. By $(\pi^{-1}G, H)$-equivariant we mean that E_γ/S depends only on $[\phi]_{\pi^{-1}(G)}$, and moreover for each $(E, \phi) \in \mathcal{F}_{N\delta}$ and each $g \in \pi^{-1}(G)$ there exists $h \in H$ such that $(g \cdot \phi)_\gamma = h \cdot \phi_\gamma$ and $e_N(\alpha(E/S, \phi))^{\det(h)} = e_{N\delta}(E/S, \phi)^{\delta\det(g)}$.

So we consider E/S and a $\Gamma(N\delta)$-structure $\phi : \ (\mathbb{Z}/N\delta\mathbb{Z})^2_S \to E[N\delta]$. For $M \in \mathbb{Z}_{\geq 1}$, denote by $\mathrm{Im}_M(\gamma)$ the image of the action of γ on $(\mathbb{Z}/M\mathbb{Z})^2_S$ by right-multiplication. We then define $C_\gamma := N\phi(\mathrm{Im}_{N\delta}(\gamma))$. Due to (1.3), the subgroup C_γ depends only on $[\phi]_{\pi^{-1}(G)}$. The size of $C_\gamma(S)$ is δ. We define $E_\gamma := E/C_\gamma$, and note that $E_\gamma[N] = [N]^{-1}C_\gamma/C_\gamma$, where $[N]$ denotes multiplication-by-N on E. Next, we define the map

$$\phi_\gamma : \ (\mathbb{Z}/N\mathbb{Z})^2_S \xrightarrow{\ \overline{\gamma}\ } \mathrm{Im}_{N\delta}(\gamma)/N\mathrm{Im}_{N\delta}(\gamma) \xrightarrow{\ \overline{\phi}\ } [N]^{-1}C_\gamma/C_\gamma = E_\gamma[N]. \tag{1.4}$$

Suppose $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The map denoted by $\overline{\gamma}$ is given by $(1,0) \mapsto (a,b)$ and $(0,1) \mapsto (c,d)$, while the map denoted by $\overline{\phi}$ is determined by ϕ.

Now consider $g \in \pi^{-1}(G)$. By (1.3), we find $h \in \pi^{-1}(H)$ such that $h\gamma = \gamma g$. For a matrix η, denote by m_η the right-multiplication map by η. Then

$$\overline{\phi} \circ m_g \circ m_{\overline{\gamma}} = \overline{\phi} \circ m_{\overline{\gamma}g} = \overline{\phi} \circ m_{\overline{\gamma}} \circ m_{\pi(h)}$$

so that indeed $(g \cdot \phi)_\gamma = \pi(h) \cdot \phi_\gamma$, as desired. The standard properties of the Weil pairing

under isogenies show that

$$e_N(\phi_\gamma(1,0),\phi_\gamma(0,1)) = e_{N\delta}(\phi(1,0),\phi(0,1))^\delta,$$

leaving us to show only that $\det(g) \equiv \det(h) \bmod N$. For this, we note that from the matrix γ of determinant δ, we have constructed an *invertible* linear map $\overline{\gamma}\colon (\mathbb{Z}/N\mathbb{Z})^2_S \to \mathrm{Im}_{N\delta}(\gamma)/N\mathrm{Im}_{N\delta}(\gamma)$, and $m_{\overline{\gamma}} \circ m_{\pi(h)} = m_g \circ m_{\overline{\gamma}}$ thus implies $\det(h) \equiv \det(g) \bmod N$. It follows that γ indeed determines a morphism of functors $\mathcal{F}^{\mathrm{can}}_{\pi^{-1}(G)} \to \mathcal{F}^{\mathrm{can}}_H|_{\mathbb{Z}[\zeta_N]^{\det(G)}}$, and thus of their compactified coarse moduli spaces.

Next, we consider $S = \mathrm{Spec}(\mathbb{C})$. We start by showing that $\gamma\Gamma_G\gamma^{-1} \subset \Gamma_H$. By (1.3), for each $s \in \Gamma_G$ there exists $s' \in \Gamma_H$ such that $s'\gamma \equiv \gamma s \bmod N\delta$. Then $s'\gamma - \gamma s$ has all entries divisible by $\det(\gamma)$, and consequently $\gamma s \gamma^{-1} \in \mathrm{SL}_2(\mathbb{Z})$. Hence $a = \gamma s \gamma^{-1}(s')^{-1}$ is in $\mathrm{SL}_2(\mathbb{Z})$ and reduces to the identity mod N, so $a \in \Gamma_H$. We conclude that $\gamma s \gamma^{-1} = as' \in \Gamma_H$, as desired.

Recall from (1.1) that we have a bijection $\Gamma_G\backslash\mathcal{H} \to \mathcal{F}_G(\mathrm{Spec}(\mathbb{C}))$ given by

$$\Gamma_G\tau \mapsto (E_\tau, [\phi_\tau]_G), \quad E_\tau = \frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}}, \quad \phi_\tau(1,0) = \frac{\tau}{N}, \ \phi_\tau(0,1) = \frac{1}{N},$$

and similarly for H. We check that the action of γ just defined corresponds under this bijection to the action of γ on $\mathcal{H}$ as a fractional linear transformation. So we consider $\tau \in \mathcal{H}$ and $(E_\tau, [\phi_\tau]_G) \in \mathcal{F}_G(\mathrm{Spec}(\mathbb{C}))$. First, we note that

$$C_\gamma = \left\langle \frac{a\tau}{\delta} + \frac{b}{\delta}, \frac{c\tau}{\delta} + \frac{d}{\delta} \right\rangle.$$

As $\det(\gamma) = \delta$, we have $\tau\mathbb{Z}\oplus\mathbb{Z} \subset \frac{1}{\delta}((a\tau+b)\mathbb{Z}\oplus(c\tau+d)\mathbb{Z})$, and we obtain an isomorphism

$$\beta\colon\ E_\tau/C_\gamma = \mathbb{C}/\left(\left(\frac{a\tau}{\delta} + \frac{b}{\delta}\right)\mathbb{Z} \oplus \left(\frac{c\tau}{\delta} + \frac{d}{\delta}\right)\mathbb{Z}\right) \longrightarrow E_{\gamma(\tau)}, \tag{1.5}$$

defined by $z \mapsto \delta \cdot z/(c\tau + d)$. Finally, $(1,0)$ transforms under $\beta \circ (\phi_\tau)_\gamma$ as follows:

$$\beta \circ (\phi_\tau)_\gamma\colon\ (1,0) \mapsto (a,b) \mapsto \frac{a\tau}{N\delta} + \frac{b}{N\delta} \mapsto \frac{\gamma(\tau)}{N}$$

and similarly it maps $(0,1)$ to $1/N$, so that indeed $(E_\tau, [\phi_\tau]_G)$ is mapped to $(E_{\gamma(\tau)}, [\phi_{\gamma(\tau)}]_H)$. □

Remark 1.1.6. Suppose that $\gamma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ normalises $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then the prescription $(E/S, [\phi]_G) \mapsto (E/S, [\gamma\cdot\phi]_G)$ determines a morphism of functors $\mathcal{F}_G \to \mathcal{F}_G$, and if moreover $\det(\gamma) \in \det(G)$, this specialises to a map $\mathcal{F}^{\mathrm{can}}_G \to \mathcal{F}^{\mathrm{can}}_G$. We obtain an automorphism of X_G. However, this does not correspond to the action of a lift of γ on $\mathcal{H}$ by fractional linear transformations.

Instead, we can choose $g \in G$ such that $\det(g) = \det(\gamma)$. Any lift of $g^{-1}\gamma$ to $\mathrm{SL}_2(\mathbb{Z})$ then normalises Γ_G and satisfies the conditions of Proposition 1.1.5. It determines the same morphism $X_G \to X_G$ as γ did.

Example 1.1.7. We consider the curve $X_0(N)/\mathbb{Z}[1/N]$. It is well-known that $W_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ normalises $\Gamma_0(N)$ and $\Gamma_1(N)$. Here we have $\delta = N$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. We verify that

$$W_N \pi^{-1}(B_0(N)) = \left\{ \begin{pmatrix} Na & b \\ Nc & Nd \end{pmatrix} \in M_2(\mathbb{Z}/N^2\mathbb{Z}) \mid b, c \in (\mathbb{Z}/N^2\mathbb{Z})^\times \right\} = \pi^{-1}(B_0(N)) W_N,$$

so that W_N indeed defines a morphism of $\mathbb{Z}[1/N]$-schemes $X_0(N) \to X_0(N)$. We similarly find that W_N defines a morphism of $\mathbb{Z}[1/N, \zeta_N]$-schemes $\widetilde{X}_1(N) \to \widetilde{X}_1(N)$.

Example 1.1.8. Remark 1.1.6 actually helps us find examples. This situation occurs when we have two groups $G_1 \subset G_2 \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that G_1 is normal in G_2 and $\det(G_1) = \det(G_2)$. Any lift $\gamma \in \Gamma_{G_2} \setminus \Gamma_{G_1}$ then determines an automorphism θ_γ on X_{G_1}.

A concrete example of this is $B_1(N) \subset B_0(N)$.

Other examples occur when $[\Gamma_{G_1} : \Gamma_{G_2}] = 2$ and $\det(G_1) = \det(G_2)$. Then also $[G_1 : G_2] = 2$, so that G_2 is normal in G_1. Then θ_γ (for any $\gamma \in \Gamma_{G_2} \setminus \Gamma_{G_1}$) is the involution on X_{G_1} such that $X_{G_1}/\theta_\gamma = X_{G_2}$.

Examples of this are $B_0(4) \subset \pi^{-1}(B_0(2))$, where $\pi : \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, $C_{\mathrm{s}}^+(3) \subset C_{\mathrm{ns}}^+(3)$, and the inclusion $G(\mathrm{e}7) \subset C_{\mathrm{ns}}^+(7)$.

Next, we lift automorphisms at level M to higher levels KM when K is coprime to M. This is important for understanding Atkin–Lehner operators at mixed level.

Lemma 1.1.9. *Suppose that $N = KM$ with $\gcd(K, M) = 1$, and we have $G_K \subset \mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$ and $G_M, H_M \subset \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. Consider $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$ with integral coefficients and determinant $\delta \in \mathbb{Z}$ coprime to K, satisfying (1.3) of Proposition 1.1.5 for G_M and H_M. Consider also $\eta \in \mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$ of determinant δ mod K normalising G_K.*

Define $G = \pi_K^{-1}(G_K) \cap \pi_M^{-1}(G_M)$ and $H = \pi_K^{-1}(G_K) \cap \pi_M^{-1}(H_M)$, where $\pi_K : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$ and $\pi_M : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$.

Then γ and η determine a morphism $X_G \to X_H$ such that the diagram

$$\begin{tikzcd} X_G \arrow[r] \arrow[d] & X_H \arrow[d] \\ X_{G_M} \arrow[r, "\theta_\gamma"] & X_{H_M} \end{tikzcd}$$

commutes. This morphism depends only on γ and on $\eta(G_K \cap \mathrm{SL}_2(\mathbb{Z}/K\mathbb{Z})) \subset \mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$.

Proof. Recall from the proof of Proposition 1.1.5 that $\theta_\gamma : X_{G_M} \to X_{H_M}$ is only determined by its image $\overline{\gamma}$ in $\mathrm{GL}_2(\mathbb{Z}/\delta M\mathbb{Z})$. As $\gcd(K, M\delta) = 1$, we can thus find $\alpha \in M_2(\mathbb{Z})$ of $\det(\alpha) = \delta$ lifting both η and $\overline{\gamma}$ (and the image of α in $M_2(\mathbb{Z}/\delta MK\mathbb{Z})$ is uniquely determined by $\overline{\gamma}$ and η). Denote by $\pi\colon \mathrm{GL}_2(\mathbb{Z}/\delta M\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ the natural map. Then α satisfies $\alpha\pi^{-1}(G_M) \subset \pi^{-1}(H_M)\alpha$ and $\alpha G_K = G_K \alpha$. As $\gcd(M\delta, K) = 1$, we conclude that also $\alpha G \subset H\alpha$, as desired. The commutativity of the diagram follows by construction. Finally, each $\widetilde{\beta} \in G_K \cap \mathrm{SL}_2(\mathbb{Z}/K\mathbb{Z})$ can be lifted to $\beta \in \Gamma_{G_K}$ that is the identity mod δM, and therefore acts trivially on X_G. The morphism determined by γ and $\eta\widetilde{\beta}$ is $\theta_\alpha \circ \theta_\beta = \theta_\alpha$. $\square$

Note that we do not assume in the lemma that $\eta \in G_K$. However, if there exists $\eta \in G_K$ of determinant δ mod K, then the map $X_G \to X_H$ determined by γ and η is independent of the choice of $\eta \in G_K$, and we call it *the* lift of $X_{G_M} \to X_{H_M}$ to $X_G \to X_H$. When such $\eta \in G_K$ does not exist, the obtained map really depends on the choice of η. This distinction becomes apparent when considering the Atkin–Lehner morphisms on $X_0(KM)$ and $\widetilde{X}_1(KM)$ determined by W_M.

Definition 1.1.10. Consider again $N = KM$ with $\gcd(M, K) = 1$, and a group $G_K \subset \mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$ which is normalised by $\eta \in \mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$ with $\det(\eta) = M$ mod K. Consider $G := \pi_K^{-1}(G_K) \cap \pi_M^{-1}(B_0(M)) \subset \mathrm{GL}_2(\mathbb{Z}/KM\mathbb{Z})$ or $G := \pi_K^{-1}(G_K) \cap \pi_M^{-1}(\widetilde{B}_1(M))$, where π_K and π_M are defined as in Lemma 1.1.9. By Lemma 1.1.9, W_M and η define an automorphism on X_G, which we call an *Atkin–Lehner morphism.* When $\eta \in G_K$, we call it *the* Atkin–Lehner *involution* and denote it by w_M.

Example 1.1.11. For coprime integers K, M, define $W_M(x, y, z, w) := \begin{pmatrix} Mx & y \\ MKz & Mw \end{pmatrix}$, where $x, y, z, w \in \mathbb{Z}$ satisfy $\det(W_M(x, y, z, w)) = M$. Its mod K reduction is in $B_0(K)$, and moreover

$$W_M(x, y, z, w) = \begin{pmatrix} -y & x \\ -Mw & zK \end{pmatrix} \begin{pmatrix} 0 & -1 \\ M & 0 \end{pmatrix},$$

so its reduction mod M^2 is γW_M, where $\gamma \in \mathrm{GL}_2(\mathbb{Z}/M^2\mathbb{Z})$ reduces into $B_0(M)$ mod M. So indeed $W_M(x, y, z, w)$ defines the Atkin–Lehner involution w_M on $X_0(KM)$ (which is independent of the choice of $x, y, z, w \in \mathbb{Z}$), and an Atkin–Lehner morphism $w_M(x, y, z, w)$ on $\widetilde{X}_1(KM)$ because $B_0(K)$ normalises $\widetilde{B}_1(K)$ (dependent on the choice of $x, y, z, w \in \mathbb{Z}$). These Atkin–Lehner morphisms will play an important role in Chapters 3 and 4.

For $K \in \mathbb{Z}$, we define

$$\gamma_K := \begin{pmatrix} K & 0 \\ 0 & 1 \end{pmatrix}.$$

The action of γ_K on $\mathcal{H}$ often leads to interesting morphisms between modular curves.

Example 1.1.12. Let p be a prime. The *split Cartan subgroup* of $\mathrm{GL}_2(\mathbb{F}_p)$ is the group $G(\mathrm{s}p)$ of diagonal matrices. We interpret this as a group of level p^2 by considering its inverse image in $\mathrm{GL}_2(\mathbb{Z}/p^2\mathbb{Z})$. We then apply Proposition 1.1.5 with γ_p to find a morphism

$$\phi : \ X_0(p^2) \longrightarrow X_{G(\mathrm{s}p)}$$

defined over $\mathbb{Q}$. By considering the congruence subgroups, we see that ϕ must be an isomorphism. Or, alternatively, the inverse is defined by $p \cdot \gamma_p^{-1}$.

On $X_0(p^2)$ we have the involution w_{p^2} defined by W_{p^2}, see Example 1.1.7. On $X(\mathrm{s}p)$ this corresponds under ϕ to the involution defined by the matrix $i := \frac{1}{p}\gamma_p W_{p^2} \gamma_p^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. This matrix is in fact invertible mod p. The normaliser $C_{\mathrm{s}}^+(p)$ of $G(\mathrm{s}p)$ is the group generated by i and $G(\mathrm{s}p)$. It defines a modular curve $X(\mathrm{s}p^+)$, a degree 2 quotient of $X(\mathrm{s}p)$. We conclude that ϕ descends to an isomorphism $X(\mathrm{s}p^+) \simeq X_0(p^2)/w_{p^2}$ over $\mathbb{Q}$, a fact also observed in [CDT99, p. 555].

Example 1.1.13. Consider again a prime p, and positive integers b, a. Define $c := \max(a, b)$. As in the previous example, γ_{p^a} defines an isomorphism

$$\widetilde{X}(\Gamma_0(p^b) \cap \Gamma(p^a)) \simeq \widetilde{X}(\Gamma_0(p^{c+a}) \cap \Gamma_1(p^a)).$$

For any $K, M \in \mathbb{Z}_{\geq 1}$ with $L := \gcd(K, M)$, we thus deduce from Lemma 1.1.9 that γ_K defines an isomorphism

$$\widetilde{X}(\Gamma_0(M) \cap \Gamma(K)) \simeq \widetilde{X}(\Gamma_0(MK^2/L) \cap \Gamma_1(K))$$

of curves over $\mathbb{Q}(\zeta_K)$.

1.2 Methods for determining the degree d points on a (modular) curve

To determine low degree points on modular curves in Chapters 3 and 4 we use a myriad of methods on a sizeable number of (quotients of) modular curves. In this section, we provide an overview.

We note that Sections 1.2.1-1.2.5 are part of the article [Box21a], while Section 1.2.6 is part of [BGG21].

1.2.1 The symmetric power

Computing the K-rational points on a curve $X/\mathbb{Q}$ for all number fields K of degree $d > 1$ simultaneously may seem like a daunting exercise. The trick is to study instead the rational points on the symmetric power

$$X^{(d)} := \mathrm{Sym}^d(X).$$

Those rational points $X^{(d)}(\mathbb{Q})$ correspond 1-1 with the effective $\mathbb{Q}$-rational divisors of degree d on $X_{\overline{\mathbb{Q}}}$, and we shall denote them as such. For each $Q \in X(\overline{\mathbb{Q}})$ defined over a number field of degree d, the sum of the Galois conjugates of Q is such a divisor, so it suffices to study $X^{(d)}(\mathbb{Q})$ instead. While $X^{(d)}$ is a d-dimensional variety, its Albanese variety is the Jacobian $J(X)$ of X. For each $\mathbb{Q}$-rational degree d divisor D_0 on X, we thus obtain an Abel–Jacobi map

$$\iota_{D_0} : X^{(d)}(\mathbb{Q}) \longrightarrow J(X)(\mathbb{Q}), \quad D \mapsto [D - D_0].$$

Many classical tools for studying the rational points on a curve X via its Jacobian's Mordell–Weil group can now also be used to study $X^{(d)}(\mathbb{Q})$, c.f. Sections 1.2.4 and 1.2.7.

1.2.2 Computing models for modular curves

The first important ingredient for carrying out computations on a curve is a set of defining equations. For modular curves, these can be obtained from the q-expansions of the

corresponding spaces of cusp forms, following Galbraith [Gal02].

For curves of the form $X_0(N)$, this has been implemented in the Modular Curves and Small Modular Curves packages in `Magma`, which we make use of. For other modular curves, however, such as $X(\mathrm{b5}, \mathrm{ns7})$ and $X(\mathrm{b3}, \mathrm{ns7})$, we develop in Chapter 2 a new algorithm to compute their models.

The Small Modular Curves package also contains an implementation for computing the maps $X_0(N) \to X_0(M)$ when $M \mid N$, for small values of N only. For larger values of N, we determine such maps using code written by Özman and Siksek in [OS19]. For other modular curves, we use the algorithm of Chapter 3 to find q-expansions for a basis of the corresponding space of cusp forms and use these to determine the morphisms, such as $X(\mathrm{b3}, \mathrm{ns7}) \to X(\mathrm{ns7})$, following the method outlined in [OS19, Section 3]. Let us give some more details.

Suppose that we would like to compute explicitly a morphism $\pi : X \to Y$ of modular curves, and we have models for $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$. Denote by $x_0, \ldots, x_n$ and $y_0, \ldots, y_m$ the coordinates in $\mathbb{P}^n$ and $\mathbb{P}^m$ respectively. Suppose that we know q-expansions for $y_0/y_m, \ldots, y_{m-1}/y_m \in \mathbb{Q}(Y)$ and $x_0/x_n, \ldots, x_{n-1}/x_n \in \mathbb{Q}(X)$. Given a degree $d \geq 1$, we can compute the q-expansions of all monomials of degree d in $x_0/x_n, \ldots, x_{n-1}/x_n$. Using linear algebra, we can thus attempt to find for each $i \in \{0, \ldots, m-1\}$ two polynomials p_i, r_i such that

$$p_i\left(\frac{x_0}{x_n}(q), \ldots, \frac{x_{n-1}}{x_n}(q)\right) = \frac{y_i}{y_m}(q) \cdot r_i\left(\frac{x_0}{x_n}(q), \ldots, \frac{x_{n-1}}{x_n}(q)\right),$$

at least up to some high order q^B. After multiplying p_i and r_i by the same polynomial, we may assume that $r_1 = \ldots = r_{m-1}$; we call this common value r. Having found such polynomials, we can check whether

$$\pi' : (x_0 : \ldots : x_n) \mapsto (P_1(x_0, \ldots, x_n) : \ldots : P_{m-1}(x_0, \ldots, x_n) : R(x_0, \ldots, x_n)),$$

defines a morphism $\pi' : X \to Y$, where $P_1, \ldots, P_{m-1}, R$ are the homogenisations of $p_1, \ldots, p_{m-1}, r$ respectively. If so, we can check that $\pi = \pi'$ when we know $\deg(\pi)$. We first verify that $\deg(\pi) = \deg(\pi')$. Then, we use the coordinate maps

$$\pi_i : Y \to \mathbb{P}^1, \ (y_0 : \ldots : y_m) \mapsto (y_i : y_m) \text{ for } i \in \{0, \ldots, m-1\}.$$

Now $\pi_i \circ \pi$ and $\pi_i \circ \pi'$ correspond to functions in $\mathbb{Q}(X)$ whose difference f_i has divisor with valuation at least B at the infinity cusp. Looking at the poles, we see that $\deg(\mathrm{div}_0(f_i)) \leq 2\deg(\pi)\deg(\pi_i)$. If $B > 2\deg(\pi) \cdot \deg(\pi_i)$ for each i, then we must have $f_i = 0$ for each i and thus $\pi = \pi'$.

1.2.3 Computing generators of Mordell–Weil groups

In general, computing Mordell–Weil groups of Jacobians of curves is an unsolved problem. For (modular) curves of small genus, however, a solution can often be found.

The rank

We first discuss the rank. For modular curves of the form $X(\mathrm{u}_1 p_1, \ldots, \mathrm{u}_n p_n)$ with $p_1, \ldots, p_n$ distinct primes and $\mathrm{u}_1, \ldots, \mathrm{u}_n \in \{\mathrm{b}, \mathrm{s}, \mathrm{ns}\}$, it can often be determined whether the rank is positive or not. We denote the Jacobian of such a curve by $J(\mathrm{u}_1 p_1, \ldots, \mathrm{u}_n p_n)$. Recall from Example 1.1.12 that $X(\mathrm{s}p)$ is isomorphic to $X_0(p^2)/w_{p^2}$. Also, $J(\mathrm{ns}p)$ is isogenous to the new part of $J(X_0(p^2)/w_{p^2})$ (see [Che96, Theorem 1]). We can therefore use an algorithm of Stein [Ste00] implemented in the Modular Curves package in `Magma` to identify Hecke eigenforms $f_1, \ldots, f_n \in S_2(\Gamma_0(N))$ for some N, such that

$$J(\mathrm{u}_1 p_1, \ldots, \mathrm{u}_n p_n) \sim A_{f_1} \times \cdots \times A_{f_n},$$

where A_f is the Abelian variety associated to f by Eichler and Shimura. By Kolyvagin and Logachëv [KL89], we then have $\mathrm{rk}(A_f(\mathbb{Q})) = 0$ when $L(f, 1) \neq 0$, where $L(f, 1)$ is the value of the L-function of f at 1. We apply this argument to all modular curves we consider in Chapters 3 and 4. If $L(f, 1)$ is zero up to `Magma`'s precision, this strongly suggests, but does not prove, that the rank is positive. Even when positive, the information which factors A_f do have rank zero can be invaluable. For example, $X(\mathrm{b}5, \mathrm{ns}7)$ and its "sisters" X_1 and X_2 defined in Section 4.5 have rank at least 2, but we successfully applied Chabauty's method using knowledge of such rank zero quotients.

When the modular curve X is not only built up of b, s and ns, one can still use the results of Chapter 2 to find a map $X_1(N) \to X$, defined in general over an abelian number field K. This yields a morphism with finite kernel $J(X) \to J_1(N)$ defined over K. Then the information on the ranks $\mathrm{rk}(A_f(K))$ for eigenforms $f \in S_2(\Gamma_1(N))$ can be used to find rank zero quotients of $J(X)$, as we do in Section 4.5.

When g is a Hecke eigenform, we saw that $\mathrm{rk}(A_g(\mathbb{Q})) = 0$ when $L(g, 1) \neq 0$. How does one verify that $\mathrm{rk}(A_g(K)) = 0$ when $K \neq \mathbb{Q}$? We solve this for abelian number fields K, based on the work of González-Giménez and Guitart [GJG10] and Guitart and Quer [GQ14]. Suppose that $g = \sum a_n q^n \in S_2(\Gamma_1(N))$ is a newform with Nebentypus character χ and without complex multiplication. We introduce three fields associated to g. Define $E_g := \mathbb{Q}(\{a_n\})$ to be the Hecke eigenvalue field of g, and $F_g := \mathbb{Q}(\{a_p^2 \chi(p)^{-1} \mid p \nmid N\})$. Then F_g is totally real and E_g/F_g is an abelian extension. When ψ is a Dirichlet character, we denote by $g \otimes \psi$ the unique newform with Fourier coefficients $a_n(g \otimes \psi) = a_n(g)\psi(n)$ for all n coprime to the level of g and the conductor of ψ. For each $s \in \mathrm{Gal}(E_g/F_g)$, there is a unique Dirichlet character $\chi_s \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$ such that $g^s = g \otimes \chi_s$ (see [Rib80, Section 3]). Here each χ_s factors via $\mathrm{Gal}(L_g/\mathbb{Q})$, where

$$L_g := \overline{\mathbb{Q}}^{\bigcap_{s \in \mathrm{Gal}(E_g/F_g)} \mathrm{Ker}(\chi_s)}.$$

Associated to g by Eichler and Shimura is the $\mathbb{Q}$-simple abelian variety $A_g/\mathbb{Q}$. Then, as noticed in [GJG10, below Proposition 1], A_g is L_g-isogenous to a power B^n of a $\overline{\mathbb{Q}}$-simple abelian variety B/L_g, which is L_g-isogenous to all of its Galois conjugates and has all its endomorphisms defined over L_g. We call B the *building block* of A_g.

We say that a newform $f \in S_2(\Gamma_0(N))$ has *inner twists* when there exists a non-trivial Dirichlet character χ such that f and $f \otimes \chi$ are Galois conjugates. This is the case when $[E_f : F_f] > 1$.

Proposition 1.2.1. *Suppose that $f \in S_2(\Gamma_0(N))$ is a newform without CM and without inner twists, K is an abelian number field, and for each Dirichlet character $\chi : \mathrm{Gal}(K/\mathbb{Q}) \to \overline{\mathbb{Q}}^\times$ we have $L(f \otimes \chi, 1) \neq 0$. Then for each such χ, we have*

$$\mathrm{rk}(A_{f\otimes\chi}(K)) = 0.$$

Proof. Define $G = \mathrm{Gal}(K/\mathbb{Q})$ and let $\widehat{G}$ be its character group. Consider $\chi \in \widehat{G}$ and define $g = f \otimes \chi$. By definition of the Weil restriction, we have

$$A_g(K) = (\mathrm{Res}_{K/\mathbb{Q}}((A_g)_K))(\mathbb{Q}),$$

so we study the latter. Now f having no inner twists means that $E_f = F_f$. Also note that $F_g = F_f$, because g has Nebentypus character χ^2. Recall that for each $s \in \mathrm{Gal}(E_g/F_g)$, we have a unique Dirichlet character χ_s such that $(f \otimes \chi)^s = f \otimes \chi\chi_s$. Indeed, in this case $\chi_s = \chi^s\chi^{-1}$, since s leaves f fixed. So $\chi_s \in \widehat{G}$, from which it follows that $L_g \subset K$. In [GJG10, Proposition 2], it is proved that $\mathrm{Res}_{L_g/\mathbb{Q}}((A_g)_{L_g})$ is $\mathbb{Q}$-isogenous to a product of modular abelian varieties A_{f_i}. We explain how their proof extends to abelian number fields K/L_g.

Guitart and Quer showed in [GQ14, Theorem 5.3] the following: if L is a Galois number field and A/L an abelian variety, then

$$\mathrm{Res}_{L/\mathbb{Q}}(A) \sim_{\mathbb{Q}} A_{f_1} \times \ldots \times A_{f_n}$$

for newforms $f_1, \ldots, f_n$ if and only if L is abelian, A is an *L-building block* (defined in [GQ14, Definition 4.1]) and the cocycle class $[c_{A/L}] \in H^2(\mathrm{Gal}(L/\mathbb{Q}), Z(\mathrm{End}_L(A) \otimes \mathbb{Q}))$ (defined on [GQ14, p. 181]) is symmetric. Now let B be the building block of A_g. Then B is indeed an L_g-building block in the definition of Guitart and Quer, and hence a K-building block. We shall not define $c_{A/L}$, but note that it is a map $\mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q}) \to Z(\mathrm{End}_L(A) \otimes \mathbb{Q})^\times$. In their proof of [GJG10, Proposition 2], Guitart and González-Giménez show that c_{B/L_g} is symmetric. Now note that $Z(\mathrm{End}_K(B)) = Z(\mathrm{End}_{L_g}(B))$ as all endomorphisms of B are defined over L_g. It follows that $c_{B/K}$ is simply the composition of $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(L_g/\mathbb{Q})$ and c_{B/L_g}. In particular, $c_{B/K}$ is also symmetric. We conclude that

$$\mathrm{Res}_{K/\mathbb{Q}}(B) \sim_{\mathbb{Q}} A_{f_1} \times \ldots \times A_{f_n}, \tag{1.6}$$

where $f_1, \ldots, f_n$ are newforms in some $S_2(\Gamma_1(M))$. Since B is K-isogenous to all its Galois conjugates, it follows that $\mathrm{Res}_{K/\mathbb{Q}}(B) \sim_K B^m$ for some $m > 0$. In particular, for each i we must have $A_{f_i} \sim_K B^{m_i}$ for some $m_i > 0$. Now, as noticed in [GJG10, Proposition 1], it follows from Ribet's work that if A_{f_i} and A_g are both K-isogenous to a power of B, then $g = f_i \otimes \psi$ for some Dirichlet character ψ on $\mathrm{Gal}(K/\mathbb{Q})$. We thus find that each $f_i = f \otimes \chi_i$

for some $\chi_i \in \widehat{G}$. From the isogeny $A_g \sim_K B^m$ for some $m > 0$, we find that $\mathrm{Res}_{K/\mathbb{Q}}(A_g)_K$ is $\mathbb{Q}$-isogenous to $\mathrm{Res}_{K/\mathbb{Q}}(B)^m$, which by (1.6) is $\mathbb{Q}$-isogenous to a product of abelian varieties $A_{f\otimes\chi_i}$. As $L(f \otimes \chi_i, 1) \neq 0$ by assumption, it follows from Kolyvagin–Logachëv that $\mathrm{rk}(A_{f\otimes\chi_i})(\mathbb{Q}) = 0$ for each i, so that $\mathrm{rk}(A_g(K)) = \mathrm{rk}(\mathrm{Res}_{K/\mathbb{Q}}(A_g)_K(\mathbb{Q})) = 0$, as desired. □

Generators of the free part

Let $X/\mathbb{Q}$ be a curve. Quotients of the Jacobian $J(X)$ of positive Mordell–Weil rank can sometimes be identified as Jacobians of quotients of X. When such a quotient curve C is elliptic, its rank can be determined by Cremona's algorithm [Cre97] available in `Magma`. When it is hyperelliptic of genus 2, Stoll's algorithm [Sto02] can be used to find generators. Note that these algorithms famously are not guaranteed to work in all cases. Those generators can be pulled back to $J(X)$ and in favourable circumstances generate the free part of its Mordell–Weil group up to known index.

Proposition 1.2.2. *Let $\rho\colon X \to C$ be a map of curves over $\mathbb{Q}$. If $\mathrm{rk}(J(X)(\mathbb{Q})) = \mathrm{rk}(J(C)(\mathbb{Q}))$, then*

$$\deg(\rho) \cdot J(X)(\mathbb{Q}) \subset \rho^* J(C)(\mathbb{Q})$$

up to torsion.

Proof. Denote by $\overline{J}(X)(\mathbb{Q})$ and $\overline{J}(C)(\mathbb{Q})$ the two quotients $J(X)(\mathbb{Q})/J(X)(\mathbb{Q})_{\mathrm{tors}}$ and $J(C)(\mathbb{Q})/J(C)(\mathbb{Q})_{\mathrm{tors}}$ respectively. Let $P_1, \ldots, P_r \in J(C)(\mathbb{Q})$ be linearly independent generators of $\overline{J}(C)(\mathbb{Q})$. Set $D_i = \rho^* P_i$ for each i. Then $\rho_* D_i = \deg(\rho) P_i$ and hence $D_1, \ldots, D_r$ are also linearly independent. In particular, they generate $\overline{J}(X)(\mathbb{Q})$ up to finite index, and the assumption on the ranks thus implies that $\rho_*\colon \overline{J}(X)(\mathbb{Q}) \to \overline{J}(C)(\mathbb{Q})$ is injective. Let $G = \langle D_1, \ldots, D_r \rangle \subset \overline{J}(X)(\mathbb{Q})$. From injectivity of ρ_* and the fact that $\deg(\rho) \cdot \rho_*(\overline{J}(X)(\mathbb{Q})) \subset \rho_*(G)$, we conclude that $\deg(\rho) \cdot \overline{J}(X)(\mathbb{Q}) \subset G$. □

We apply this proposition to find generators of subgroups of each of the modular curves $X_0(N)$ considered in Chapter 3 (see Section 3.3.5) as well as the rank 2 Mordell–Weil groups of $X(\mathrm{b5}, \mathrm{ns7})$ (see Section 4.4.3) and $X(\mathrm{b3}, \mathrm{ns7})$ (see Remark 4.5.2).

The torsion subgroup

For more details, we recommend the article of Özman and Siksek [OS19], where many torsion subgroups of modular curves are computed using a variety of techniques. We found those methods to also be effective for our curves; we summarise them here.

Let X be a modular curve, and denote by $C(\overline{\mathbb{Q}}) \subset J(X)(\overline{\mathbb{Q}})$ the subgroup generated by the differences of cusps. The *cuspidal subgroup* $C(\mathbb{Q})$ of $J(X)(\mathbb{Q})$ is the group of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariants of $C(\overline{\mathbb{Q}})$. By the Manin–Drinfeld theorem [Man72], [Dri73], $C(\mathbb{Q}) \subset J(X)(\mathbb{Q})_{\mathrm{tors}}$ when $X = X_0(N)$ for any N. Mazur [Maz77] proved that in fact $C(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ when N is prime, which was a conjecture of Ogg. The same statement for any N is often called Ogg's Conjecture [Ogg74]. See e.g. [Lin97] for partial results, and [OS19, Section 5.2] for more details.

Following this idea, the cuspidal subgroup provides a good starting point for attempting to compute $J(X)(\mathbb{Q})_{\text{tors}}$ even when X is not of the form $X_0(N)$. For example, on $X(\text{b5}, \text{ns7})$, there are 6 cusps defined over $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ splitting into two irreducible $\mathbb{Q}$-rational degree 3 divisors c_0, c_∞, and their difference $[c_0 - c_\infty]$ generates $J(\text{b5}, \text{ns7})(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/7\mathbb{Z}$, as was shown in [DNS20]. Moreover, we show in Propositions 4.2.3 and 4.2.9 that the rank 0 Mordell–Weil groups of $X_0(105)/w_5$ and $X_0(105)/w_{35}$ are generated by differences of images of cusps.

Remark 1.2.3. Ogg's conjecture cannot simply be extended to quotients of $X_0(N)$. For example, when p is prime, $X_0(p)$ has two cusps c_1 and c_2 satisfying $c_2 = w_p(c_1)$. On $X_0(p)/w_p$, the cuspidal subgroup is therefore trivial, whereas there can be torsion. For $X_0(105)/\langle w_7, w_{105}\rangle$ and $X_0(105)/\langle w_7, w_{21}\rangle$, we found in Proposition 4.2.9 the torsion subgroup to be larger than the cuspidal subgroup.

Given a subgroup $G \subset J(X)(\mathbb{Q})_{\text{tors}}$, it can often be verified that $G = J(X)(\mathbb{Q})_{\text{tors}}$ by using the fact [Kat81] that $J(X)(\mathbb{Q})_{\text{tors}}$ embeds into $J(X)(\mathbb{F}_p)$ for good primes $p > 2$. The Mordell–Weil group over $\mathbb{F}_p$ can be determined using an algorithm of Hess [Hes02] (implemented in `Magma`), and a combination of a few primes often leaves no other option but $G = J(X)(\mathbb{Q})_{\text{tors}}$. This is indeed the case for $X_0(N)$ with $N \in \{43, 53, 57, 61, 65, 67, 73\}$ (see Lemma 3.3.2) and for $X_0(35)$ and $X(\text{s3}, \text{b5})$ (see Proposition 4.3.3).

However, for some curves (such as $X_0(105)/w_5$, $X_0(105)/w_{35}$, $X_0(105)/\langle w_7, w_{105}\rangle$, $X_0(105)/\langle w_7, w_{21}\rangle$ and $X(\text{b3}, \text{ns7})$), this strategy fails to determine $J(X)(\mathbb{Q})_{\text{tors}}$, because there exists an abstract group H such that $G \subsetneq H$ and $H \subset J(X)(\mathbb{F}_p)$ (as abstract groups) for all primes p considered. In practice, often H has larger 2-torsion than G. This may be caused by the existence of fields $K_1, \ldots, K_n$ such that each prime p splits in one of them and each $J(X)(K_i)_{\text{tors}}$ has an extra 2-torsion element that is not $\mathbb{Q}$-rational.

This can often be remedied:

- When X is a hyperelliptic curve of genus 2 (e.g. $X = X_0(105)/\langle w_7, w_{105}\rangle$, $X_0(105)/\langle w_7, w_{21}\rangle$ or $X(\text{b3}, \text{ns7})/w_3$), algorithms for computing $J(X)(\mathbb{Q})[2]$ are implemented in `Magma`.

- When X is a plane quartic (e.g. $X = X_0(105)/w_{35}$), the Galois representation $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}_{\overline{\mathbb{Q}}} J(X)[2]$ can be determined by computing bitangents using an algorithm of Bruin, Poonen and Stoll [BPS16, Section 12]; see Proposition 4.2.9 for details.

- Sometimes (e.g. for $X = X_0(64)$ (see [OS19]) or $X = X_0(105)/w_5$) for an extension $K/\mathbb{Q}$ an extra 2-torsion element can be found, making it possible to determine $J(X)(K)[2]$ exactly. Then $J(X)(\mathbb{Q})[2]$ is its subset of Galois invariants.

- While H may as an abstract group be isomorphic to subgroups $H_p \subset J(X)(\mathbb{F}_p)$ for each p, there may not exist isomorphisms $\psi_{p,q} : H_p \simeq H_q$ for all such primes p and q such that $\psi_{p,q}$ restricted to the image of G is the map obtained from reducing G modulo p and q. This can be verified using an algorithm of Özman and Siksek [OS19]. We apply this to $X_0(105)/w_5$ in Proposition 4.2.3.

1.2.4 When the Mordell–Weil group is finite

Let X be a curve over a field K, and fix a divisor D_0 of degree d. When the Mordell–Weil group of $J(X)$ is finite and known, it can be used (when d is suitably small) to determine $X^{(d)}(K)$ using the Abel–Jacobi map ι_{D_0} defined in Section 1.2.1. When D is a divisor on X, we define

$$L(D) := \{f \in K(X)^\times \mid \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

This is a finite-dimensional vector space called the *Riemann–Roch space* of D, and an efficient implementation for finding bases of such spaces is available in `Magma`. We denote its dimension by $\ell(D)$. We obtain the following tautological lemma.

Lemma 1.2.4. *For each degree 0 divisor E on X, we have*

$$\{D \in X^{(d)}(K) \mid [D - D_0] = [E]\} = \{E + D_0 + \mathrm{div}(f) \mid f \in \mathbb{P}L(E + D_0)\}.$$

Ranging over representatives E of the elements in $J(X)(K)$, this yields an algorithm for determining $X^{(d)}(K)$ when it is finite. (This may even work when only a finite index subgroup of $J(X)(K)$ is known, in which case computations can be sped up with a Mordell–Weil sieve, as explained in [OS19].) Even when $X^{(d)}(K)$ is infinite, it can be useful to identify the Riemann–Roch spaces of dimension greater than 1.

Corollary 1.2.5. *Suppose that $\rho : X \to C$ is a degree d morphism of curves over K, and D_0 is a K-rational divisor of degree e on C. If $L(\rho^* D_0) = \rho^* L(D_0)$, we have*

$$\{D \in X^{(de)}(K) \mid [D - \rho^* D_0] = 0\} \subset \rho^* C^{(e)}(K).$$

Proof. This follows from Lemma 1.2.4 with $E = 0$, using that $\mathrm{div}(\rho^* f) = \rho^* \mathrm{div}(f)$. □

We use this argument repeatedly in Chapter 4.

1.2.5 The Mordell–Weil sieve

For both finite and infinite Mordell–Weil groups, the Mordell–Weil sieve can be an effective tool to determine the rational points on symmetric powers of curves. The Mordell–Weil sieve described here is similar to the one found in [Sik09], but we describe it in a slightly more general form, allowing us to use it in Chapter 3 as well as Section 4.5. For a more detailed discussion of the Mordell–Weil sieve, we refer to [BS10]. The idea of the sieve is to combine incomplete information about rational points in p-adic discs for various primes p, in order to determine the set of all rational points.

Consider a variety $V/\mathbb{Q}$, an integer N and a proper Noetherian model $\mathcal{V}/\mathbb{Z}[1/N]$ for V. Then we have reduction maps $V(\mathbb{Q}) \to \mathcal{V}(\mathbb{F}_p)$ for primes $p \nmid N$.

Remark 1.2.6. Typically, we consider a curve $X/\mathbb{Q}$ and $m \in \mathbb{Z}_{\geq 1}$, and define $V = X^{(m)}$. Then, given equations with integral coefficients for X in projective space, define N to be the product of the primes of bad reduction for this model of X, let $\mathcal{X}/\mathbb{Z}[1/N]$ be the curve defined by those equations, and set $\mathcal{V} = \mathcal{X}^{(m)}$.

We first choose primes $p_1, \ldots, p_r$ not dividing N, and we consider a subset $S \subset V(\mathbb{Q})$. Next, we need the following input:

(i) A (possibly infinite) list of *known points* $\mathcal{L} \subset S$.

(ii) A $\mathbb{Z}[1/N]$-morphism $\iota : \mathcal{V} \to \mathcal{A}$, where $\mathcal{A}/\mathbb{Z}[1/N]$ is an abelian scheme.

(iii) A finitely generated abelian group B, a homomorphism $\phi : B \to \mathcal{A}(\mathbb{Q})$ and a subset $W \subset B$ such that $\iota(S) \subset \phi(W)$.

(iv) For each $p \in \{p_1, \ldots, p_n\}$, a subset $\mathcal{M}_p \subset \mathcal{V}(\mathbb{F}_p)$ such that $S \setminus \mathcal{L}$ reduces into $\mathcal{M}_p$.

The aim of the sieve is to show that $\mathcal{L} = S$. Typically, $S = V(\mathbb{Q})$ and $W = B$, but the flexibility in this set-up will prove useful.

Remark 1.2.7. Note that $\mathcal{M}_p$ need not be optimal. Strict subsets $\mathcal{M}_p$ can be obtained from theorems such as Theorem 3.2.6 and Theorem 3.2.24, using points $\mathcal{Q}$ in an explicit finite subset $\mathcal{L}' \subset \mathcal{L}$.

Remark 1.2.8. When $V = X^{(e)}$ for a curve X, the abelian scheme $\mathcal{A}$ is usually derived from the Jacobian of X. For example, it could be the image of the multiplication-by-I map m_I on the Jacobian, and ι could be composition of the Abel–Jacobi map with m_I. The choice of $\mathcal{A}$ is then limited by knowledge of generators of $J(X)(\mathbb{Q})$.

Consider $p \in \{p_1, \ldots, p_n\}$. We obtain a commuting diagram

$$\begin{tikzcd}
\mathcal{L} \arrow[r] \arrow[dr] & V(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & \mathcal{A}(\mathbb{Q}) \arrow[d] & B \arrow[l, "\phi"'] \arrow[dl, "\phi_p"] \\
& \mathcal{V}(\mathbb{F}_p) \arrow[r, "\iota_p"] & \mathcal{A}(\mathbb{F}_p) &
\end{tikzcd},$$

from which the following proposition follows by definition of $\mathcal{M}_p$.

Proposition 1.2.9 (Mordell–Weil sieve)**.** *If*

$$W \cap \bigcap_{i=1}^{n} \phi_{p_i}^{-1}(\iota_{p_i}(\mathcal{M}_{p_i})) = \emptyset$$

then $S = \mathcal{L}$.

Remark 1.2.10. One may hope for this sieve to work in practice when $\dim(\mathcal{A}_{\overline{\mathbb{Q}}}) > \dim(V)$, as in each step, less than a proportion

$$\#\mathcal{V}(\mathbb{F}_p)/\#\mathcal{A}(\mathbb{F}_p) \sim p^{\dim(V) - \dim(\mathcal{A}_{\overline{\mathbb{Q}}})}$$

of elements of $\mathcal{A}(\mathbb{F}_p)$ is in $\iota(\mathcal{M}_p)$.

When X is a curve with good reduction $\widetilde{X}$ at p, we note that $J(\widetilde{X})(\mathbb{F}_p)$ can be computed using the class group algorithm of Hess [Hes02].

1.2.6 Searching for degree d points

Suppose that we have found a model for a curve X in $\mathbb{P}^k$, with coordinates $x_0, \ldots, x_k$. Following Özman and Siksek [OS19], we search for quadratic and cubic points on X by intersecting $X \subset \mathbb{P}^k$ with hyperplanes of the form

$$b_0 x_0 + \ldots + b_k x_k = 0,$$

where $b_0, \ldots, b_k \in \mathbb{Z}$ are chosen coprime and up to a certain bound. When the decomposition of the divisor (over $\mathbb{Q}$) corresponding to this intersection contains effective degree d divisors, we have found points of degree at most d. Unlike searching for rational points, this can be a time consuming exercise: for the genus 5 curve $X_0(67) \subset \mathbb{P}^4$, for example, it took multiple hours to find all points of degree 2. This is largely due to the time taken to decompose these hyperplane intersections into linear combinations of irreducible effective divisors.

In fact, we found this search to be too time-consuming to find all quartic points on curves of genus 5 or higher. To find a better search mechanism, let us do a thought experiment: what would happen when we run the Mordell–Weil sieve just described, with $S = V(\mathbb{Q})$, but our input set $\mathcal{L}$ of known points is too small, i.e. $\mathcal{L} \subsetneq V(\mathbb{Q})$? Certainly, after any number of primes $p_1, \ldots, p_n$, we find that $W \cap \cap_{i=1}^n \phi_{p_i}^{-1}(\iota(\mathcal{M}_{p_i})) \neq \emptyset$. This is because any $x \in V(\mathbb{Q}) \setminus \mathcal{L}$ gives rise to a point in that intersection. Let H_n be the intersection of the kernels $\mathrm{Ker}(\phi_{p_1}), \ldots, \mathrm{Ker}(\phi_{p_n})$. Then we find an explicit H_n-coset $Z \subset B$ such that $\phi(z) = \iota(x)$ for some $z \in Z$. Turning this around, we can use this coset Z to find x, as follows. After sufficiently many primes, the index $[B : H_n]$ is huge, so one expects Z to contain no elements with "small" coefficients for the generators of B. Conversely, actual rational points $x \in V(\mathbb{Q})$ do tend to correspond to such small elements of B. We can therefore use the LLL-algorithm [LLL82] to search for small vectors in Z. Given such a small vector $z \in Z$, we can compute Riemann–Roch spaces and use Lemma 1.2.4 to find $x \in V(\mathbb{Q})$ (if it exists) such that $\iota(x) = \phi(z)$. Running over the H_n-cosets making up the intersection $W \cap \cap_{i=1}^n \phi_{p_i}^{-1}(\iota(\mathcal{M}_{p_i}))$, we hope to find all of $V(\mathbb{Q})$ this way. We have found this to be an effective method for finding degree 4 points on $X_0(65)$ (see Chapter 3) and $X(\mathrm{b5}, \mathrm{ns7})$ (see Section 4.4).

1.2.7 When the Mordell–Weil group is infinite: Chabauty

The Mordell–Weil sieve described in Section 1.2.5 can only determine a non-empty set of rational points $V(\mathbb{Q})$ when combined with a method that can determine the set of rational points within a mod p residue class of a known point of $V(\mathbb{Q})$, for primes p. In terms of the notation of Section 1.2.5, we require a way to determine strict subsets $\mathcal{M}_p$. In some cases where the Mordell–Weil group is infinite, the Chabauty–Coleman method can provide this. We shall not discuss it further here, because it is the subject of Chapter 3.

We also use this method in Chapter 4 (Section 4.4) to determine the quartic points on the genus 6 curve $X(\mathrm{b5}, \mathrm{ns7})$, as well as the quadratic points on two curves of genus 5 and 8.

Chapter 2

Computing models for quotients of modular curves

In this chapter we describe an algorithm for computing a $\mathbb{Q}$-rational model for the quotient of a modular curve by an automorphism group, under mild assumptions on the curve and the automorphisms, by determining q-expansions for a basis of the corresponding space of cusp forms.

This chapter is a subset of the article [Box21b].

2.1 Introduction

Consider a positive integer N and a subgroup $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. More precisely, we present an algorithm (Algorithm 2.3.11) for finding a model for the modular curve $X_G/\mathbb{Q}$ in the case where $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, $-I \in G$ and G is normalised by $J := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. This algorithm determines q-expansions of a basis for the corresponding space of cusp forms, from which the equations can be deduced via Galbraith's techniques [Gal02] when the genus is at least 2.

Moreover, we can explicitly describe (auto)morphisms of modular curves. For finite groups $\mathcal{A}$ of such automorphisms, we can also determine $X_G/\mathcal{A}$ directly, without computing X_G first. These morphisms include, but, more importantly, are not limited to, Atkin–Lehner involutions. This opens the way for the explicit computation of trees of arbitrary modular curves and their quotients. We apply this in Section 2.4 to find models for three level 35 modular curves, as well as the j-map on one of them; this is an important ingredient in Chapter 4 for the proof that all elliptic curves over quartic fields not containing $\sqrt{5}$ are modular.

In Section 2.2, we develop the algorithm for computing q-expansions of a basis of cusp forms with respect to G, thus extending previous results dating back to Tingley [Tin75], who in 1975 computed cusp forms on $\Gamma_0(N)$ for N prime. Tingley's results were improved to all N and optimised by Cremona [Cre97], after which Stein [Ste00] generalised this approach further to the spaces $S_k(\Gamma_0(N), \epsilon)$, where ϵ is a mod N Dirichlet character.

The same approach, using modular symbols, does not simply carry over to general congruence subgroups. In Section 2.2.5, we describe the scaling issue that occurs, which we solve in subsequent sections using twist operators, an idea due originally to John Cremona, c.f. [BC].

Despite the lack of a general algorithm, models for several more complicated modular curves have been found previously. We mention some of these, as well as their strong implications. Baran [Bar10] found models for the curves $X(\mathrm{ns}20)$ and $X(\mathrm{ns}21)$, as well as for the isomorphic curves $X(\mathrm{ns}13)$ and $X(\mathrm{s}13)$ [Bar14]. The determination of the integral points of these curves gave new solutions to the class number one problem, while the rational points on the level 13 curves shed light onto Serre's uniformity problem over $\mathbb{Q}$ (see also [Ser72]).

Derickx, Najman and Siksek [DNS20] used a planar model for $X(\mathrm{b}5, \mathrm{ns}7)$ (defined in Section 2.4), to prove that all elliptic curves over cubic fields are modular. This planar model was derived from Le Hung's equations [LH14] for the curve as a fibred product $X_0(5) \times_{X(1)} X(\mathrm{ns}7)$. Furthermore, Banwait and Cremona [BC14] determined a model for the exceptional modular curve $X_{S_4}(13)$ by instead computing pseudo-eigenvalues of Atkin–Lehner operators. This allowed them to study the failure of the local-to-global principle for the existence of ℓ-isogenies of elliptic curves over number fields. Simultaneously, Cremona [BC] found a model for the same curve $X_{S_4}(13)$, as well as Baran's curves $X(\mathrm{ns}13)$ and $X(\mathrm{s}13)$ and equations describing the j-maps, using his method of modular symbols. This is not published, but available online as a `Sage` worksheet with annotations by Banwait and Cremona [BC].

Given the desire for a more general algorithm for computing models of modular curves, it may not come as a surprise that, during the author's work on this project, three independent results of similar nature were published – at least in preprint. Brunault and Neururer [BN20] used Eisenstein series to find an algorithm for computing the spaces of modular forms $M_k(\Gamma, \mathbb{C})$ of arbitrary weight and congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$. Zywina [Zyw20], on the other hand, generalised the work of Banwait and Cremona [BC14], using numerical approximation of pseudo–eigenvalues of Atkin–Lehner operators to determine q-expansions and models for modular curves. Finally, Assaf [Ass20] recently generalised the 'classical' strategy of Cremona by defining and successfully utilising modular symbols and Hecke operators on general congruence subgroups to compute Fourier coefficients, at least at primes not dividing the level. Currently, as far as the author is aware, Assaf's algorithm is unable to determine the Fourier coefficients at primes dividing the level for congruence subgroups such as those in Section 2.4, which may complicate provable determination of equations satisfied by those modular forms. Zywina can determine all Fourier coefficients, and his method can in fact be used to find a model for $X(\mathrm{b}5, \mathrm{e}7)$ (considered in Section 2.4), but not currently for its quotients.

Our approach instead generalises the work of Banwait and Cremona [BC] on $X_{S_4}(13)$. We can compute any Fourier coefficient for a basis of cusp forms for any congruence subgroup, without the need for numerical approximation. We have chosen this

approach because it is a natural extension of the current methods for determining q-expansions of cusp forms on $\Gamma_0(N)$. This enables us to use the current packages for cusp forms in `Sage`, making the algorithm relatively easy to implement. Another forte of our approach is that we can directly compute quotients of modular curves by automorphisms. As far as the author is aware, there is currently no other algorithm available that can directly compute models for the quotient modular curves defined in Section 2.4.

The `Sage` and `Magma` code used for the computations in Section 2.4 is publicly available at

`https://github.com/joshabox/modularcurvemodels` .

Given the existing comprehensive `Magma` implementations of Assaf [Ass20] and Zywina [Zyw20], we have not implemented a general version of our algorithm. We note that this should certainly be possible; in particular, the examples computed in Section 2.4 do not appear to be in any subcategory of "easier cases".

2.2 Operators on spaces of cusp forms

We use the definitions and notation introduced in Section 1.1. We shall only be concerned with curves over fields, and denote by X_G the modular curve associated to G (defined in Definition 1.1.1), base changed to $\mathbb{Q}(\zeta_N)^{\det(G)}$.

2.2.1 The regular 1-forms on modular curves

For $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we see that any lift of γ to $\mathrm{SL}_2(\mathbb{Z})$ acts on $X(N)$ as an automorphism θ_γ, by Proposition 1.1.5. Next, consider $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ and the matrix $\gamma_a := \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. As in Remark 1.1.6, the prescription $(E/S, \phi) \mapsto (E/S, \gamma_a \cdot \phi)$ determines a morphism of functors $\mathcal{F}_N \to \mathcal{F}_N$. However, unless $a = 1$, we have $\det(\gamma_a) \notin \det(\{1\})$ so that γ_a does not determine a morphism $\mathcal{F}_N^{\mathrm{can}} \to \mathcal{F}_N^{\mathrm{can}}$. Define the functor $\mathcal{F}_N^{\mathrm{can},a}$ by instead mapping a scheme S to those pairs $(E/S, \phi)$, where $e_N(\phi(1,0), \phi(0,1)) = \zeta_N^a$. This similarly has a coarse moduli space $\widetilde{X}(N)^a/\mathbb{Q}(\zeta_N)$, which is the base change of $\widetilde{X}(N)$ by Galois conjugation

$$\sigma_a : \mathbb{Q}(\zeta_N) \to \mathbb{Q}(\zeta_N),\ \zeta_N \mapsto \zeta_N^a.$$

Then γ_a does determine a morphism $\widetilde{X}(N) \to \widetilde{X}(N)^a$ *of curves over* $\mathbb{Q}(\zeta_N)$. Composing this map with base change by σ_a^{-1}, we obtain a map of *schemes* $\theta_a :\ X(N) \to X(N)$, whose corresponding map on function fields is merely a morphism of $\mathbb{Q}(\zeta_N)^{\langle \sigma_a \rangle}$-algebras.

Each function $f \in \mathbb{Q}(\zeta_N)(\widetilde{X}(N))$ has a Laurent series expansion around the infinity cusp (which is a $\mathbb{Q}(\zeta_N)$-rational point). Denote by $q_N(\tau) = e^{2\pi i \tau/N}$ a uniformiser at this cusp, and write the expansion of f in its completed local ring as $f = \sum_{n \geq -m} a_n(f) q_N^n$, where $m \in \mathbb{Z}_{\geq 1}$ and each $a_n(f) \in \mathbb{Q}(\zeta_N)$. As also shown by Shimura [Shi94, Proposition 6.9], we obtain a right action $\circ$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathbb{Q}(\zeta_N)(\widetilde{X}(N))$ such that for each $f =$

$\sum_{n\geq -m} a_n q_N^n \in \mathbb{Q}(\zeta_N)(X(N))$:

(i) for each $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ we have $f \circ \gamma = \theta^*_{\widetilde{\gamma}}(f)$, where $\widetilde{\gamma}$ is a lift of γ to $\mathrm{SL}_2(\mathbb{Z})$, and

(ii) $f \circ \gamma_a = \theta^*_a(f) = \sum_{n\geq -m} \sigma_a(a_n) q_N^n$.

From now on, we suppose that $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ satisfies

$$\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times \text{ and } -I \in G.$$

The first condition means we consider only curves defined over $\mathbb{Q}$. Then, again by Shimura's work [Shi94], the fixed field $\mathbb{Q}(\zeta_N)(\widetilde{X}(N))^G$ defines an irreducible projective curve over $\mathbb{Q}$, which is simply X_G.

The action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\widetilde{X}(N)$ gives rise to an action on its sheaf of regular 1-forms.

Proposition 2.2.1. *The map $f \mapsto f(q_N)(\mathrm{d}q_N)/q_N$ defines an isomorphism*

$$S_2(\Gamma(N), \mathbb{Q}(\zeta_N))^G \simeq H^0(X_G, \Omega).$$

Here Ω is the sheaf of regular 1-forms on X_G.

Proof. By definition of $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$, the map $S_2(\Gamma(N), \mathbb{Q}(\zeta_N)) \to H^0(\widetilde{X}9(N), \Omega_{\widetilde{X}(N)})$ is well-defined, an isomorphism and G-equivariant. We then take G-invariants, and note that $H^0(X_G, \Omega) = H^0(\widetilde{X}(N), \Omega)^G$ because $\mathbb{Q}(X_G) = \mathbb{Q}(\zeta_N)(\widetilde{X}(N))^G$. For more details, see [Zyw20, Lemma 6.5]. □

Our strategy will be to compute a basis for $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))^G$ and derive equations for X_G by finding equations between these cusp forms, following Galbraith [Gal02].

2.2.2 The conjugation trick

It will be useful to split the level N into two parts: $N = M \cdot K$, where $\gcd(M, K) = 1$, such that G is the intersection of the inverse images of $B_0(M) \subset \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ and $G_K \subset \mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$ in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then

$$S_2(\Gamma(N), \mathbb{Q}(\zeta_N))^G = S_2(\Gamma_0(M) \cap \Gamma(K), \mathbb{Q}(\zeta_K))^G, \tag{2.1}$$

by definition of $B_0(M)$.

From now on, we think of $\Gamma_G = \Gamma_0(M) \cap \Gamma_{G_K}$ as being a "level K congruence subgroup of $\Gamma_0(M)$", rather than a level N congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. When $M > 1$, the benefit of this is twofold: we will be able to consider more automorphisms on X_G, and computations are faster.

A problem with computing fixed spaces of modular forms as above, is that no algorithm for computing spaces of the form $S_2(\Gamma_0(M) \cap \Gamma(K), \mathbb{Q}(\zeta_K))$ is currently implemented in a computer algebra system. We fix this by conjugating with $\gamma_K = \begin{pmatrix} K & 0 \\ 0 & 1 \end{pmatrix}$. The trick

to studying modular forms on $\Gamma(K)$, as used by Banwait and Cremona [BC14] and later by Zywina [Zyw20], is to notice that $\gamma_K^{-1}\Gamma(K)\gamma_K = \Gamma_0(K^2) \cap \Gamma_1(K)$. In fact, we already saw in Example 1.1.13 that γ_K induces an isomorphism

$$\widetilde{X}(\Gamma_0(M) \cap \Gamma(K)) \simeq \widetilde{X}(\Gamma_0(MK^2) \cap \Gamma_1(K)). \tag{2.2}$$

Efficient algorithms for computing spaces of cusp forms for $\Gamma_0(MK^2) \cap \Gamma_1(K)$ using modular symbols *have* been implemented in `Magma` and `Sage` thanks to the work of Cremona [Cre97] and Stein [Ste00], amongst others.

2.2.3 Normalisers and statement of the main theorem

In this section, we explain for which elements of $A \in \mathcal{N}_{\Gamma_G}$ we can determine its action on X_G explicitly. We would like to be able to act with such A on $S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \overline{\mathbb{Q}})$, as is the case for G.

In their famous paper, Conway and Norton [CN79, Section 3] mention the "curious fact" that the divisors h of 24 are exactly those positive integers satisfying that $xy \equiv 1 \bmod h$ implies $x \equiv y \bmod h$. Equivalently, they are the integers h such that

$$\widetilde{T}_h := \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix}$$

normalises $\Gamma_0(h^2)$.

Lemma 2.2.2. *The normaliser of $\Gamma_0(M)$ in $\mathrm{PSL}_2(\mathbb{R})$ is generated by $\Gamma_0(M)$ itself, the Atkin–Lehner matrices $W_m(x, y, z, w)$ for $m \mid M$ with $\gcd(M/m, m) = 1$, and $\widetilde{T}_h$, where h is the largest divisor of 24 such that $h^2 \mid M$.*

This lemma is originally due to Atkin and Lehner [AL70]; see [CN79, Section 3] for an elegant proof. While the Atkin–Lehner matrices act on $X_0(M)$ over $\mathbb{Q}$, the matrix $\widetilde{T}_h$ determines an automorphism on $X_0(M)$ defined over $\mathbb{Q}(\zeta_h)$. When h divides M and $H \subset \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ is a subgroup, define

$$H^h := \{M \in H \mid \det(M) \equiv 1 \bmod h\}.$$

By Example 1.1.2, we find that $X_0(M)_{\mathbb{Q}(\zeta_h)} = X_{B_0(M)^h}$. Similarly, we have $(X_G)_{\mathbb{Q}(\zeta_h)} = X_{G^h}$. On X_{G^h}, the elements in $\mathcal{N}_{G^h}$ act by automorphisms. We restrict to those automorphisms which also act on $X(\Gamma_0(M) \cap \Gamma(K))$.

Corollary 2.2.3. *Let h be the largest divisor of 24 such that $h^2 \mid M$. The normaliser $\mathcal{N}_{\Gamma_0(M)}$ acts by automorphisms on $X(\Gamma_0(M) \cap \Gamma(K))_{\mathbb{Q}(\zeta_{Kh})}$.*

Proof. In view of Example 1.1.2, it suffices to show that $\mathcal{N}_{\Gamma_0(M)}$ acts by automorphisms on X_H, where $H \subset \mathrm{GL}_2(\mathbb{Z}/MK\mathbb{Z})$ is the intersection of the inverse images of $\widetilde{G}(K) = \{I\} \subset \mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$ and $B_0(M)^h \subset \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. Note that X_H is defined over $\mathbb{Q}(\zeta_{Kh})$. We can now verify explicitly that Atkin–Lehner matrices, $h\widetilde{T}_h$ and elements of $\Gamma_0(M)$ satisfy condition (1.3) to define a morphism $X_H \to X_H$. Here we note that any matrix in

$\mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$ normalises $\{I\} = \widetilde{G}(K)$. To see that $h\widetilde{T}_h$ satisfies (1.3), we crucially use that $xy \equiv 1 \bmod h$ implies $x \equiv y \bmod h$. $\square$

Consider a subgroup $\mathcal{A} \subset (\mathcal{N}_{\Gamma_0(M)} \cap \mathcal{N}_{G^h})/\mathrm{P}\Gamma_G$. By definition, this acts by automorphisms on $X_{G^h} = (X_G)_{\mathbb{Q}(\zeta_h)}$. Moreover, by intersecting with $\mathcal{N}_{\Gamma_0(M)}$, we have ensured that $\mathcal{A}$ acts on $X(\Gamma_0(M) \cap \Gamma(K))$ over $\mathbb{Q}(\zeta_{Kh})$, just like G does, and we can treat $\mathcal{A}$ and G in a similar way. Taking $\mathcal{A}$-invariants in Proposition 2.2.1 and applying (2.2) and (2.1), we obtain

$$H^0((X_G/\mathcal{A})_{\mathbb{Q}(\zeta_h)}, \Omega) = S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{Q}(\zeta_{Kh}))^{G,\mathcal{A}}, \tag{2.3}$$

where $\alpha \in \mathcal{A}$ and $\alpha \in \mathrm{SL}_2(\mathbb{Z}/MK\mathbb{Z})$ act on cusp forms f by $f \mapsto f[\gamma_K^{-1}\alpha\gamma_K]$, and matrices $\gamma_a = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/MK\mathbb{Z})$ act on cusp forms by Galois conjugating Fourier coefficients by σ_a (because γ_a and γ_K commute), c.f. Section 2.2.1.

Theorem 2.2.4. *Suppose that M and K are coprime integers, $G \subset \mathrm{GL}_2(\mathbb{Z}/MK\mathbb{Z})$ satisfies $-I \in G$, $\det(G) = (\mathbb{Z}/MK\mathbb{Z})^\times$, $JGJ = G$, and $G_M = B_0(M)$. Let h be the largest divisor of 24 such that $h^2 \mid M$. Consider a finite subgroup $\mathcal{A} \subset (\mathcal{N}_{\Gamma_0(M)} \cap \mathcal{N}_{G^h})/\mathrm{P}\Gamma_G$, normalised by J and determining a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant subgroup of $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X_G)$. Then Algorithm 2.3.13 is a terminating algorithm for computing a model for the curve $X_G/\mathcal{A}$ over $\mathbb{Q}$, provided it has genus $g \geq 2$.*

Remark 2.2.5. While we have restricted the allowed automorphisms by intersecting with $\mathcal{N}_{\Gamma_0(M)}$, we have not excluded the two natural subsets. Firstly, recall that any $\alpha \in \mathcal{N}_{\Gamma_0(M)}$ determines a morphism on $X_0(M)_{\mathbb{Q}(\zeta_h)}$. Because G_K has surjective determinant and α has determinant coprime to K, we can by Lemma 1.1.9 extend this to a morphism on X_G determined by a matrix in $\mathcal{N}_{\Gamma_0(M)} \cap \mathcal{N}_{G^h}$. The allowed automorphisms thus contain the Atkin–Lehner involutions and the morphisms determined by $\widetilde{T}_h$. We will see that J indeed normalises Atkin–Lehner operators. Secondly, any $\alpha \in \mathrm{SL}_2(\mathbb{Z}/K\mathbb{Z})$ normalising G_K determines an automorphism on X_{G_K}, after lifting α to $\mathrm{SL}_2(\mathbb{Z})$. By lifting α to $\Gamma_0(M)$, we obtain a morphism on X_G determined by a matrix in $\mathcal{N}_{\Gamma_0(M)} \cap \mathcal{N}_{G^h}$.

We shall first find a way (Algorithm 2.3.11) to determine the fixed space $S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{Q}(\zeta_{Kh}))^{\langle \Gamma_G, \mathcal{A} \rangle}$, after which we consider the action of matrices in G with determinant unequal to 1 in Section 2.3.3.

Remark 2.2.6. We have decided in the remainder of this chapter to work only with weight 2 cusp forms, but all computational arguments generalise to arbitrary even weight.

2.2.4 The homology group

We work in the homology group, following Cremona's strategy [Cre97]. More specifically, in this section, we follow unpublished work of Cremona (used in [BC]) to describe a $\mathbb{C}$-bilinear pairing between cusp forms and homology.

We consider any group $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ corresponding to a congruence subgroup $\Gamma := \Gamma_G$ of level N. We assume again that G is normalised by $J = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. For the

geometric curve $(X_G)_{\mathbb{C}}$, we then have the pairing between 1-forms and homology:

$$S_2(\Gamma, \mathbb{C}) \times H_1(X_G, \mathbb{Z}) \to \mathbb{C}, \ \ \langle f, \gamma \rangle := 2\pi i \int_\gamma f(z) \mathrm{d}z.$$

Extending this to $H_1(X_\Gamma, \mathbb{R})$, the pairing becomes $\mathbb{R}$-bilinear. As in Section 2.2.1, the action of $J = \gamma_{-1}$ on $\mathcal{H} \subset \mathbb{C}$ composed with complex conjugation determines an involution of $\mathbb{R}$-algebras $J^* : \mathbb{C}(X_G) \to \mathbb{C}(X_G)$, or equivalently an involution on the Weil restriction $\mathrm{Res}_{\mathbb{C}/\mathbb{R}}(X_G)_{\mathbb{C}}$. Here $z \in \mathcal{H}$ is mapped to $z^* := -\overline{z} = \overline{J(z)}$, and $f \in S_2(\Gamma, \mathbb{C})$ to $J^*(f) = \overline{f(z^*)}$. We note that $f \mapsto J^*(f)$ acts as complex conjugation on the Fourier coefficients of f, c.f. Section 2.2.1. We similarly obtain an involution on $H_1(X_\Gamma, \mathbb{R})$. Denote by $H_1(X_\Gamma, \mathbb{R})^+$ its $+1$-eigenspace. Then our pairing restricts to an exact duality of real vector spaces

$$S_2(\Gamma, \mathbb{R}) \times H_1(X_\Gamma, \mathbb{R})^+ \to \mathbb{R}.$$

Define

$$H_{\mathbb{C}}(\Gamma) := H_1(X_\Gamma, \mathbb{R})^+ \otimes \mathbb{C}.$$

Finally, we extend the pairing $\mathbb{C}$-linearly *on both sides* to obtain an exact $\mathbb{C}$-bilinear pairing

$$S_2(\Gamma, \mathbb{C}) \times H_{\mathbb{C}}(\Gamma) \to \mathbb{C}, \ (f, \mu) \mapsto \langle f, \mu \rangle. \tag{2.4}$$

The pairing (2.4) identifies $H_{\mathbb{C}}(\Gamma)$ with the dual of $S_2(\Gamma, \mathbb{C})$. Subsequently, the Petersson inner product identifies $S_2(\Gamma, \mathbb{C})$ with its own dual. We thus obtain an isomorphism

$$S_2(\Gamma, \mathbb{C}) \to H_{\mathbb{C}}(\Gamma), \ f \mapsto \gamma_f \tag{2.5}$$

(due to Cremona) defined by

$$\langle g, \gamma_f \rangle = \langle g, f \rangle \text{ for all } g \in S_2(\Gamma, \mathbb{C}),$$

where the latter pair of brackets denotes the Petersson inner product. Our strategy for studying $S_2(\Gamma, \mathbb{C})$ is to study $H_{\mathbb{C}}(\Gamma)$ instead, and transform the results under (2.5). We note that the Petersson inner product is sesqui-linear in its second argument, whereas (2.4) is $\mathbb{C}$-linear. This means that

$$\gamma_{\alpha f} = \overline{\alpha} \gamma_f \text{ for each } \alpha \in \mathbb{C}.$$

The great benefit of studying the homology group is that the action of $\mathcal{N}_\Gamma$ on $H_1(X(\Gamma), \mathbb{Z})$ can be computed explicitly when $\Gamma = \Gamma_0(K^2 M) \cap \Gamma_1(K)$, i.e. for each $\gamma \in \mathcal{N}_\Gamma$ one can find a matrix for this linear action on $H_1(X_\Gamma, \mathbb{C})$ in terms of an explicit basis. This uses a description of the homology group as *modular symbols*. For a detailed overview of these algorithms, we refer the reader to [Cre97] and [Ste00].

Thanks to these algorithms, when $\Gamma \supset \Gamma_0(MK^2) \cap \Gamma_1(K)$, one can compute $H_1(X_\Gamma, \mathbb{Q})$ as the subspace of $H_1(X_{\Gamma_0(MK^2) \cap \Gamma_1(K)}, \mathbb{Q})$ fixed by Γ with ease. The challenge is to relate this subspace $H_1(X_\Gamma, \mathbb{C})$ to q-expansions of modular forms under the

isomorphism (2.5), as explained in §2.2.5.

In the remainder of this section, we consider any congruence subgroup Γ normalised by J, but one may think of this as being $\Gamma_0(MK^2) \cap \Gamma_1(K)$.

Recall that every $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$ acts on the complex upper half-plane by fractional linear transformations, giving rise to an action on meromorphic functions on $\mathcal{H}$

$$[U]: \ f(\tau) \mapsto (f|U)(\tau) := (c\tau + d)^{-2} f \circ U(\tau)$$

and on paths $\gamma : [0,1] \to \mathcal{H}$:

$$[U]: \ \gamma \mapsto U(\gamma) := U \circ \gamma. \tag{2.6}$$

Definition 2.2.7. We define the *Hecke algebra* $\mathbb{T}_\Gamma$ to be the $\mathbb{C}$-algebra of $\mathbb{C}$-valued functions on $\mathrm{P}\Gamma\backslash\mathrm{PGL}_2^+(\mathbb{Q})/\mathrm{P}\Gamma$, where the P denotes the image in $\mathrm{PGL}_2(\mathbb{Q})$.

Each $T \in \mathbb{T}_\Gamma$ can be represented as a $\mathbb{C}$-linear combination of double cosets $\mathrm{P}\Gamma\alpha\mathrm{P}\Gamma$. Such a coset has a left-$\mathrm{P}\Gamma$ action, and splits as a finite disjoint union $\mathrm{P}\Gamma\alpha\mathrm{P}\Gamma = \sqcup \mathrm{P}\Gamma\alpha_i$. This way, we obtain a *Hecke operator* $T_\alpha = \sum_i [\alpha_i]$, acting on $(X_\Gamma)_\mathbb{C}$ as a correspondence, and consequently on $S_2(\Gamma, \mathbb{C})$ and $H_1(X_\Gamma, \mathbb{C})$.

The following lemma, due to Cremona and used in [BC], describes how these two actions interact with the pairing (2.4).

Lemma 2.2.8. *Consider $T \in \mathbb{T}_\Gamma$, and $\gamma \in H_\mathbb{C}(\Gamma)$ such that $JT(\gamma) = T(\gamma)$ (i.e. $T(\gamma)$ remains in the +1-eigenspace). This is always the case when $TJ = JT$. Then for all $f \in S_2(\Gamma, \mathbb{C})$ we have*

(a) $\langle f|T, \gamma\rangle = \langle f, T(\gamma)\rangle$

(b) $\gamma_{f|T^*} = T(\gamma_f)$,

where T^* is the adjoint of T with respect to the Petersson inner product.

Proof. By definition of the action, $(f|U)(\tau)\mathrm{d}\tau = f(U(\tau))\mathrm{d}U(\tau)$ for each matrix U. Integrating this relation for each U in T gives us part (a), as long as $T(\gamma) \in H_\mathbb{C}(\Gamma)$. Part (b) follows by definition of the Petersson inner product. □

We recall (see e.g. [DS05, Proposition 5.5.2]) that for each $U \in \mathrm{GL}_2^+(\mathbb{Q})$, we have $T_U^* = \det(U) T_{U^{-1}}$.

2.2.5 q-expansions

A downside of using the homology group is that the pairing (2.4) is not defined explicitly in terms of q-expansions. It is therefore a priori not obvious what the q-expansion is of the cusp form mapped to a given element of $H_\mathbb{C}(\Gamma)$ under (2.5).

When $\Gamma = \Gamma_0(MK^2) \cap \Gamma_1(K)$, the solution is to use Hecke operators and their common eigenvectors. Let $f_1, \ldots, f_n \in S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{C})$ be the Hecke eigenforms. Their q-expansions (up to scaling) are determined by Hecke eigenvalues, and these

Hecke eigenvalues can be computed for the corresponding Hecke eigenvectors $\mu_1, \ldots, \mu_n \in H_{\mathbb{C}}(\Gamma_0(MK^2) \cap \Gamma_1(K))$ instead, by Lemma 2.2.8. This yields the q-expansions for a basis of $S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{C})$.

This approach does not work for $S_2(\Gamma, \mathbb{C})$ when $\Gamma \supset \Gamma_0(MK^2) \cap \Gamma_1(K)$ and $S_2(\Gamma, \mathbb{C}) \subset S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{C})$ is not a direct sum of Hecke eigenspaces, the problem being that each μ_i only corresponds to f_i under (2.5) *up to scaling*. The scaling issue makes it hard to translate linear combinations of eigenforms under (2.5).

The aim for the remainder of this chapter is to present a solution to this problem. The crucial idea – due to Cremona (see [BC]) – is that we *can* find a q-expansion for the cusp form corresponding to a linear combination $\alpha_1\mu_1 + \alpha_2\mu_2$ when μ_2 is a twist of μ_1. While two Hecke eigenvectors need not always be twists, we define in Section 2.3.1 the *twist orbit space* of μ_1, and show that the action of Γ preserves this space.

2.2.6 Operators on modular forms and modular symbols

In this section, we study the congruence subgroup $\Gamma_0(MK^2) \cap \Gamma_1(K)$, where again $N, M \in \mathbb{Z}_{\geq 1}$ (but not necessarily coprime). We define $N := K^2M$. Let $\mathcal{D}_K$ be the group of Dirichlet characters on $(\mathbb{Z}/K\mathbb{Z})^\times$. Then

$$S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{C}) = \bigoplus_{\epsilon \in \mathcal{D}_K} S_2(N, \epsilon_N),$$

where ϵ_N denotes the composition of $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/K\mathbb{Z})^\times$ and ϵ, and $S_2(N, \epsilon)$ is the common eigenspace in $S_2(\Gamma_1(N), \mathbb{C})$ for the diamond operators $\langle d \rangle$ for $\gcd(d, N) = 1$ with eigenvalues $\epsilon(d)$ respectively. The diamond operators also act on modular symbols, and Stein [Ste00] defines their eigenspaces $H_1(N, \epsilon) \subset H_1(X_{\Gamma_1(N)}, \mathbb{C})$. We obtain a similar decomposition

$$H_1(X_{\Gamma_0(MK^2) \cap \Gamma_1(K)}, \mathbb{C}) = \bigoplus_{\epsilon \in \mathcal{D}_K} H_1(N, \epsilon).$$

The diamond operators commute with J, and $H_1(N, \epsilon)^+$ is identified with $S_2(N, \bar{\epsilon})$ under the isomorphism (2.5). Note here the complex conjugation of ϵ which occurs due to Lemma 2.2.8 (b) since $\langle d \rangle^* = \langle d \rangle^{-1}$ for d coprime to N. Similarly, for primes $p \nmid N$, we have (see e.g. [DS05])

$$T_p^* = \langle p \rangle^{-1} T_p.$$

Definition 2.2.9. Let V be a representation of the Hecke algebra. A *Hecke eigenspace* of V is a simultaneous eigenspace for the Hecke operators T_p and $\langle p \rangle$, for all but finitely many primes p.

Under the isomorphism (2.5), we conclude by Lemma 2.2.8 that Hecke eigenspaces in $S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{C})$ are identified with Hecke eigenspaces in $H_{\mathbb{C}}(\Gamma_0(MK^2) \cap \Gamma_1(K))$, but the eigenvalues get complex conjugated.

Definition 2.2.10. Let L be a positive integer, and define, as before, $\widetilde{T}_L := \begin{pmatrix} 1 & 1/L \\ 0 & 1 \end{pmatrix}$.

For $\chi \in \mathcal{D}_L$ we define the *twist operator*

$$R_\chi(L) := \sum_{u \in \mathbb{Z}/L\mathbb{Z}} \overline{\chi}(u)[\widetilde{T}_L^u].$$

When $L = \mathrm{cond}(\chi)$, we write $R_\chi(L) = R_\chi$.

It is important to note that, even if f is of level N and $L \mid N$, then χ is considered as a mod L character in the definition of $f|R_\chi(L)$, not as a mod N character.

We saw in Corollary 2.2.3 that $\widetilde{T}_1$ acts on $\widetilde{X}(\Gamma_0(M) \cap \Gamma(K))$ (and hence normalises $\Gamma_0(M) \cap \Gamma(K)$). By (2.2), conjugation by γ_K shows that $\widetilde{T}_K = \gamma_K^{-1}\widetilde{T}_1\gamma_K$ normalises $\Gamma_0(MK^2) \cap \Gamma_1(K)$ and acts on its spaces of cusp forms (with coefficients in $\mathbb{Q}(\zeta_K)$) and homology; hence so does $R_\chi(K)$ for $\chi \in \mathcal{D}_K$.

Definition 2.2.11. Consider $L \mid N$, $d \mid N/L$ and $\epsilon \in \mathcal{D}_N$ of conductor dividing L. Let $\epsilon' : (\mathbb{Z}/L\mathbb{Z})^\times \to \mathbb{C}^\times$ be the corresponding mod L character. Let $D_d := \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ and suppose that $\eta_1, \ldots, \eta_s$ are the defined so that $D_d\eta_1, \ldots, D_d\eta_s$ are a full set of coset representatives for the left-action of $\Gamma_0(N)$ on $D_d\Gamma_0(L)$. Then we have maps

$$B_d^{N/L} = B_d : S_2(L, \epsilon') \to S_2(N, \epsilon), \quad f \mapsto f|\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\mathrm{Tr}_d^{N/L} : S_2(N, \epsilon) \to S_2(L, \epsilon'), \quad f \mapsto \sum_{i=1}^{s} \epsilon'(\eta_i)^{-1} f|D_d\eta_i$$

satisfying that $\mathrm{Tr}_d^{N/L} \circ B_d^{N/L}$ is multiplication by $[\Gamma_0(N) : \Gamma_0(L)]$. These operators similarly act on homology as in (2.6).

Lemma 2.2.12. *We have $JR_\chi(L)J = \chi(-1)R_\chi(L)$, $JB_dJ = B_d$ and $J\mathrm{Tr}_d^{N/L}J = \mathrm{Tr}_d^{N/L}$ for all $\chi \in \mathcal{D}_L$ and all positive integers $d \mid N/L$.*

Proof. For B_d one simply multiplies matrices. For $\mathrm{Tr}_d^{N/L}$, it suffices to note that $\mathrm{Tr}_d^{N/L}$ is independent of the choice of coset representatives, and that J commutes with D_d and normalises $\Gamma_0(N)$ and $\Gamma_0(L)$. For $R_\chi(L)$, it suffices to note that $J\widetilde{T}_K^a J = \widetilde{T}_K^{-a}$. □

Lemma 2.2.13. *Consider $f \in S_2(N, \epsilon)$ and $g \in S_2(L, \epsilon')$, where $L \mid N$. Let $d \mid N/L$, and let $\chi \in \mathcal{D}_L$ with $\chi(-1) = 1$. Then*

$$\begin{aligned} \gamma_{f|R_\chi} &= R_{\overline{\chi}}(\gamma_f), \\ [\Gamma_0(N) : \Gamma_0(L)] \cdot \gamma_{g|B_d^{N/L}} &= \mathrm{Tr}_d^{N/L}(\gamma_g) \text{ and} \\ \gamma_{f|\mathrm{Tr}_d^{N/L}} &= [\Gamma_0(N) : \Gamma_0(L)] \cdot \mathrm{B}_d^{N/L}(\gamma_f). \end{aligned}$$

Proof. For the first equality, we use that $\widetilde{T}_L^* = \widetilde{T}_L^{-1}$ and recall that the pairing (2.4) is $\mathbb{C}$-linear in both arguments, to find that

$$\langle h, \gamma_{f|R_\chi} \rangle = \langle h, f|R_\chi \rangle = \langle h|R_{\overline{\chi}}, f \rangle = \langle h|R_{\overline{\chi}}, \gamma_f \rangle = \langle h, R_{\overline{\chi}}(\gamma_f) \rangle,$$

where we used Lemma 2.2.8 (a) in the last equality.

Next, recall that

$$\langle f|\mathrm{Tr}_d^{N/L}, g\rangle = [\Gamma_0(N):\Gamma_0(L)]\langle f, g|B_d\rangle.$$

Define $I := [\Gamma_0(N):\Gamma_0(L)]$. We thus find that

$$I\cdot\langle g, \gamma_{f|B_d}\rangle = I\cdot\langle g, f|B_d\rangle = \langle g|\mathrm{Tr}_d^{N/L}, f\rangle = \langle g|\mathrm{Tr}_d^{N/L}, \gamma_f\rangle = \langle g, \mathrm{Tr}_d^{N/L}(\gamma_f)\rangle,$$

as desired. Now repeat this with $I\cdot B_d$ and $\mathrm{Tr}_d^{N/L}$ reversed. □

We define one final operator.

Definition 2.2.14. Suppose that $L \mid N$ and $\epsilon \in \mathcal{D}_N$ of conductor dividing L. Then we denote by

$$\mathrm{pr}_{N/L}:\ S_2(N,\epsilon) \to B_1^{N/L}(S_2(L,\epsilon'))$$

the orthogonal projection map onto the subspace, where "orthogonal" refers to the Petersson inner product, and $\epsilon' : (\mathbb{Z}/L\mathbb{Z})^\times \to \mathbb{C}^\times$ is the character ϵ factors through.

Similarly, we denote by

$$\pi_{N/L}:\ H_1(N,\epsilon) \to \mathrm{Tr}_1^{N/L}(H_1(L,\epsilon'))$$

the orthogonal projection onto the image of $\mathrm{Tr}_1^{N/L}$.

By Lemma 2.2.13, we find that these operators are indeed dual to each other, i.e.

$$\pi_{N/L}(\gamma_f) = \gamma_{\mathrm{pr}_{N/L}(f)} \text{ for all } f \in S_2(N,\epsilon). \tag{2.7}$$

Next, we study the $R_\chi(L)$-operators in more detail. Define $U_q := \sum_{u=0}^{q-1}\left[\begin{pmatrix}1 & u\\ 0 & q\end{pmatrix}\right]$ and recall a list of properties of the $R_\chi(L)$ operators.

Lemma 2.2.15. *Consider a character χ of conductor dividing L, where $L \mid N$.*

(a) Suppose $f \in S_2(N,\epsilon)$ and $\mu \in H_1(N,\epsilon)$, where ϵ has conductor N', and set $\widetilde{N} := \mathrm{lcm}(N, N'L, L^2)$. Then $f|R_\chi(L) \in S_2(\widetilde{N}, \epsilon\chi^2)$ and $R_\chi(L)(\mu) \in H_1(\widetilde{N}, \epsilon\overline{\chi}^2)$.

(b) If $\gcd(L_1, L_2) = 1$, $\chi \in \mathcal{D}_{L_1}$, $\psi \in \mathcal{D}_{L_2}$, then $R_\chi(L_1)R_\psi(L_2) = \chi(L_2)\psi(L_1)R_{\chi\psi}(L_1L_2)$.

(c) We have $f|R_\chi = g(\overline{\chi})f\otimes\chi$, where $g(\overline{\chi})$ is the Gauss sum of $\overline{\chi}$.

(d) When $p \nmid LN$, we have $R_\chi(L)T_p = \chi(p)T_pR_\chi(L)$.

(e) For $a \in \mathbb{Z}$ with $\gcd(a, L) = 1$, we have $\phi(L)\widetilde{T}_L^a = \sum_{\epsilon\in\mathcal{D}_L}\epsilon(a)R_\epsilon(L)$.

(f) Suppose that q is prime and $N = q^sL$ for some $s > 0$. Suppose further that $f \in S_2(N,\epsilon)$ is a newform with $a_1(f) = 1$ and ψ is a character whose conductor is a power of q. Then $f\otimes\psi = g - g|U_Q|B_Q$, where Q is a power of q and $g \in S_2(QL, \epsilon\psi^2)$ is the newform with $a_1(g) = 1$.

Proof. These are standard properties first proved by Atkin and Li [AL78]. The proof of (a) for modular forms is a matrix computation (see [AL78, Proposition 3.1]) and thus similarly true for modular symbols, with a complex conjugation bar to account for the change from left-action to right-action. □

Parts (a) and (d) tell us exactly how $R_\chi(L)$ acts on the set of Hecke eigenspaces. We extend part (f) to non-prime power conductors.

Corollary 2.2.16. *Suppose that $f \in S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{C})$ is a newform at a level dividing N with $a_1(f) = 1$, and $\chi \in \mathcal{D}_K$. Then $f \mid R_\chi = g(\overline{\chi})(k - k')$, where k is the newform at a level L dividing N with $a_1(k) = 1$, and*

$$k' \in \bigoplus_{\substack{q \mid K \\ q>1 \text{ prime}}} \operatorname{Im}\left(B_q^{N/(N/q)}\right).$$

In particular, $\operatorname{pr}_{N/L}(f|R_\chi) = g(\overline{\chi})k$.

Proof. First, we note that

$$B_q R_\chi = \left(\sum_{u \in \mathbb{Z}/\operatorname{cond}(\epsilon)\mathbb{Z}} \chi(u) \widetilde{T}^{qu}_{\operatorname{cond}(\chi)} \right) B_q.$$

We now write $\chi = \prod_{p|K} \chi_p$ as a product of characters of prime-power conductor. Then $R_\chi = \lambda \prod_{p|K} R_{\chi_p}$ for some $\lambda \in \overline{\mathbb{Q}}$ by Lemma 2.2.15 (b). We now repeatedly apply Lemma 2.2.15 (f) to each R_{χ_p}, keeping in mind the displayed equation above. □

Given f and χ, we note that a q-expansion for k can be computed explicitly from its Hecke eigenvalues using Lemma 2.2.15 (d). For R_χ and B_d it is well-known how they act on q-expansions: $f|B_d(q) = f(q^d)$ and $f|R_\chi = g(\overline{\chi}) f \otimes \chi$, where $g(\overline{\chi})$ is the Gauss sum of $\overline{\chi}$. The above corollary allows us to determine how $\operatorname{pr}_{N/L}$ acts on the q-expansions of twists of newforms.

For $Q \mid N$ with $\gcd(Q, N/Q) = 1$, we defined Atkin–Lehner matrices $W_Q(x, y, z, w)$ in Example 1.1.11. Define the corresponding operators on cusp forms and homology by $w_Q(x, y, z, w)$. For simplicity of exposition, denote by w_Q the Atkin–Lehner operator $w_Q(x, y, z, w)$, where $x \equiv 1 \bmod N/Q$ and $y \equiv 1 \bmod Q$. We study how these interact with the Hecke operators, using classical properties due to Atkin and Li [AL78].

Lemma 2.2.17. *Consider an integer N, a divisor $Q \mid N$ such that $\gcd(Q, N/Q) = 1$, and $\epsilon \in \mathcal{D}_N$. Write $\epsilon = \epsilon_Q \epsilon_{N/Q}$, where $\epsilon_Q \in \mathcal{D}_Q$ and $\epsilon_{N/Q} \in \mathcal{D}_{N/Q}$. We consider $\mu \in H_1(N, \epsilon)$ and $f \in S_2(N, \epsilon)$. Then*

(a) Consider Q' such that $Q' \mid N$ and $\gcd(Q', NQ) = 1$, and write $\epsilon_{N/Q} = \epsilon_{Q'} \epsilon_{N/(QQ')}$. Then $w_Q w_{Q'}(\mu) = \epsilon_{Q'}(Q) w_{QQ'}(\mu)$.

(b) $w_Q(x, y, z, w)(\mu) = \epsilon_Q(y) \epsilon_{N/Q}(x) w_Q(\mu)$,

(c) $w_Q(x, y, z, w)$ maps $H_1(N, \epsilon_Q \epsilon_{N/Q})$ to $H_1(N, \overline{\epsilon_Q} \epsilon_{N/Q})$,

(d) $T_p w_Q(\mu) = \bar{\epsilon}_Q(p) w_Q T_p(\mu)$ *when* $\gcd(p, Q) = 1$,

Proof. These are analogues of standard results of Atkin and Li [AL78] for the corresponding action on modular forms. These are all based on matrix identities, and thus hold true on modular symbols for the same reason (and with appropriate complex conjugation bars to account for the change from left-action to right-action). □

Parts (b), (c) and (d) determine how the Atkin–Lehner operators act on the set of Hecke eigenspaces of $H_1(X_{\Gamma_0(MK^2)\cap\Gamma_1(K)}, \mathbb{C})$.

2.3 Algorithms

2.3.1 Twist orbit spaces

We consider again $N = KM$, $h \mid 24$ such that $h^2 \mid M$, and the congruence subgroup $\Gamma = \Gamma_G$, where G has level N and $G_M = B_0(M)$.

A crucial step in determining q-expansions for a basis of modular forms for $\Gamma_0(N)$ is to determine first the Hecke eigenforms. When N is prime, the Hecke algebra $\mathbb{T}_{\Gamma_0(N)}$ is generated by the Atkin-Lehner operator w_N and the Hecke operators T_p for primes p. The Hecke newforms thus generate 1-dimensional modules of the full Hecke algebra.

For $\Gamma_0(MK^2) \cap \Gamma_1(K)$, however, this is not the case. Recall that $\widetilde{T}_h$ normalises $\Gamma_0(M) \cap \Gamma(K)$. Hence $\widetilde{T}_{Kh} = \gamma_K^{-1}\widetilde{T}_h\gamma_K$ normalises $\Gamma_0(MK^2) \cap \Gamma_1(K)$, making the twist operators $R_\chi(Kh)$, for $\chi \in \mathcal{D}_{Kh}$, all elements of the Hecke algebra. These twist operators do not act on the 1-dimensional spaces generated by the Hecke eigenforms, however. In this section, we define the notion of *twist orbit spaces*, and we show that these are modules for the following subalgebra.

Definition 2.3.1. We define the *explicit Hecke algebra* $\mathbb{T}_{M,K}$ to be the sub-algebra of $\mathbb{T}_{\Gamma_0(MK^2)\cap\Gamma_1(K)}$ generated by the T_p-operators for $p \nmid MK$ prime, the diamond operators $\langle d\rangle$ for $d \in (\mathbb{Z}/K\mathbb{Z})^\times$, the Atkin–Lehner operators $w_m(x, y, z, w)$ for $m \mid MK^2$ such that $\gcd(MK^2/m, m) = 1$, and the twist operators $R_\chi(Kh)$ for $\chi \in \mathcal{D}_{Kh}$.

Remark 2.3.2. It is not unreasonable to expect that $\mathbb{T}_{M,K}$ is the full Hecke algebra, as we have added to the Hecke operators all matrices that visibly normalise $\Gamma_0(MK^2) \cap \Gamma_1(K)$, c.f. Lemma 2.2.2 and Corollary 2.3.5.

In the situation of our interest, some of the Atkin–Lehner operators coincide.

Lemma 2.3.3. *If* $Q = mK^2$ *for some* $m \mid M$ *with* $\gcd(m, M/m) = 1$, *then*

$$-W_Q(x, -y, -z, w) \cdot W_Q(x, y, z, w)^{-1} \in \Gamma_0(MK^2) \cap \Gamma_1(K).$$

In other words, $w_Q(x, y, z, w) \in \mathbb{T}_{M,K}$ *satisfies* $Jw_Q(x, y, z, w)J = w_Q(x, y, z, w)$.

Proof. Simply multiply the matrices. □

Define $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. In their studies of modular forms, Banwait and Cremona [BC14] and Zywina [Zyw20] made crucial use of the fact that

$\mathrm{SL}_2(\mathbb{Z})$ is generated by T and S, which satisfy $\gamma_K^{-1}T\gamma_K = \widetilde{T}_K$ and $\gamma_K^{-1}S\gamma_K = W_{K^2}$. A similar statement can be obtained for our "parent group" $\Gamma_0(M)$.

Lemma 2.3.4. *Suppose that $K > 1$ satisfies $\gcd(K, M) = 1$. Then $\Gamma_0(M)$ can be generated by T and a finite set of matrices of the form*

$$\begin{pmatrix} Ka & b \\ Mc & Kd \end{pmatrix} \text{ with } a, b, c, d \in \mathbb{Z}.$$

Proof. Let $T, \gamma_1, \ldots, \gamma_n$ be a set of generators for $\Gamma_0(M)$. We add $\gamma_0 := \begin{pmatrix} 1 & 0 \\ M & 1 \end{pmatrix}$ to this set. We note that

$$\gamma_0^k \begin{pmatrix} a & b \\ cM & d \end{pmatrix} = \begin{pmatrix} a & * \\ (ka+c)M & * \end{pmatrix}.$$

Consider $\gamma = \begin{pmatrix} a & b \\ cM & d \end{pmatrix} \in \Gamma_0(M)$. Then $\gcd(\det(\gamma), K) = 1$ implies that $\gcd(a, cM, K) = 1$. Therefore, given the finite set S of primes dividing K, we can choose $k \in \mathbb{Z}$ such that $(ka+c)M$ is not divisible by any prime in S. So after replacing each γ_i for $i > 0$ by $\gamma_0^{k_i}\gamma_i$ for some $k_i \in \mathbb{Z}$, we may assume that the bottom left entry of each γ_i ($i \in \{0, \ldots, n\}$) is coprime to K.

Next, let $\gamma = \begin{pmatrix} a & b \\ cM & d \end{pmatrix}$ be one of the γ_i. We note that

$$T^k\gamma T^{k'} = \begin{pmatrix} a + kcM & * \\ cM & d + k'cM \end{pmatrix}.$$

As cM is invertible mod K, we can find $k, k' \in \mathbb{Z}$ such that $kcM \equiv -a \bmod K$ and $k'cM \equiv -d \bmod K$. In particular, $T^k\gamma T^{k'}$ has its top left and bottom right coefficient divisible by K. We thus replace γ by $T^k\gamma T^{k'}$. Doing this for each γ_i, we obtain a suitable set of generators. □

Corollary 2.3.5. *The group $\Gamma_0(M)$ can be generated by T and elements $\gamma_1, \ldots, \gamma_n$ such that $K\gamma_K^{-1}\gamma_i\gamma_K$ is an Atkin–Lehner matrix $W_{K^2}(x, y, z, w)$. Moreover, if m is a prime power dividing M maximally, and $W_m(a, b, c, d)$ is a corresponding Atkin–Lehner matrix at level M, then there exist $\mu, \nu \in \Gamma_0(M)$ such that $K\gamma_K^{-1}\mu W_m(a, b, c, d)\nu\gamma_K = W_{mK^2}(x, y, z, w)$ for some choice of x, y, z, w.*

Proof. For the first statement, let $\gamma = \begin{pmatrix} Ka & b \\ Mc & Kd \end{pmatrix}$ be one of the generators γ_i from the previous lemma. Then $K\gamma_K^{-1}\gamma\gamma_K = W_{K^2}(a, b, c, d)$ at level K^2M. Next, we consider $W_m(a, b, c, d) = \begin{pmatrix} ma & b \\ Mc & md \end{pmatrix}$. As $\det(W_m(a, b, c, d))$ is coprime to K, the proof of the previous lemma allows us to find $\mu, \nu \in \Gamma_0(M)$ such that $\mu W_m(a, b, c, d)\nu$ is of the form $\begin{pmatrix} Kmx & y \\ Mz & Kmw \end{pmatrix}$. (When choosing the powers k, k' of T to multiply with, these need to be

chosen to be multiples of m, which is possible due to the Chinese Remainder Theorem.) Now conjugating with γ_K and multiplying with K gives $W_{mK^2}(x, y, z, w)$, as desired. $\square$

Corollary 2.3.6. *Suppose that $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$ normalises $\Gamma_0(M)$. Then $[\gamma_K^{-1}\gamma\gamma_K] \in \mathbb{T}_{M,K}$.*

Proof. By Lemma 2.2.2, we may suppose γ is a generator of $\Gamma_0(M)$, an Atkin–Lehner matrix, or $\widetilde{T}_h$ for some h. The result thus follows from the previous corollary and Lemma 2.2.15 (e). $\square$

Next, we describe a decomposition of $H_1(X_{\Gamma_0(MK^2)\cap\Gamma_1(K)}, \mathbb{C})$ into sub-$\mathbb{T}_{M,K}$-modules. Each Hecke eigenspace $H \subset H_1(X_{\Gamma_0(MK^2)\cap\Gamma_1(K)}, \mathbb{C})$ splits as a direct sum $H = H^+ \oplus H^-$, where H^+ is the $+1$-subspace for J, and H^- is the -1-subspace. We call H^+ and H^- *Hecke-J-eigenspaces.* Given a Hecke-J-eigenvector $\mu \in H_1(X_{\Gamma_0(MK^2)\cap\Gamma_1(K)}, \mathbb{C})$, denote by $H(\mu)$ its Hecke-J-eigenspace. This space has dimension 1 when μ is new, but not when μ is old.

Definition 2.3.7. Suppose that $\mu \in H_1(X_{\Gamma_0(MK^2)\cap\Gamma_1(K)}, \mathbb{C})$ is a Hecke-J-eigenvector. We define the *twist orbit space of μ* to be

$$O(\mu) := \mathop{+}_{\chi \in \mathcal{D}_{Kh}} H(R_\chi(\mu)).$$

Note that $R_\chi(\mu)$ is indeed a Hecke-J-eigenvector by Lemmas 2.2.15 (d) and 2.2.12. The subspace $O(\mu)^+$ on which J acts trivially is called the *real twist orbit space of μ.*

By Lemma 2.2.12, if $J\mu = \mu$, we have

$$O(\mu)^+ = \mathop{+}_{\chi \in \mathcal{D}_{Kh} \text{ even}} H(R_\chi(\mu)).$$

Proposition 2.3.8. *Suppose that $\mu \in H_1(X_{\Gamma_0(MK^2)\cap\Gamma_1(K)}, \mathbb{C})$ is a Hecke-J-eigenvector. Then $O(\mu)$ is a representation of $\mathbb{T}_{M,K}$.*

Proof. Since $O(\mu)$ is a direct sum of Hecke-J-eigenspaces, it suffices to determine how the twist and Atkin–Lehner operators act on the set of Hecke-J-eigenspaces. For the Atkin–Lehner operators $w_Q(x, y, z, w)$ we use Lemmas 2.2.17 (c), (d) and 2.2.15 (d) to see that the Hecke eigenspace of μ is mapped to the Hecke eigenspace of $R_\epsilon(\mu)$, where ϵ is the Nebentypus character of μ. Furthermore, Atkin–Lehner operators commute with J by Lemma 2.3.3, whereas $JR_\epsilon J = \epsilon(-1)R_\epsilon$. Note, however, that $\epsilon(-1) = 1$ unless $\mu = 0$, so indeed $H(\mu)$ is mapped to $H(R_\epsilon(\mu))$. Finally, for $\chi \in \mathcal{D}_{Kh}$, the operator $R_\chi(Kh)$ maps a Hecke-J-eigenspace to the same Hecke-J-eigenspace as R_χ does, and hence preserves $O(\mu)$ by definition. $\square$

Proposition 2.3.9. *Suppose that $f \in S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{C})$ is a newform at a level dividing N and $\mu = \gamma_f$. Then a basis for $O(\mu)^+$ is given by the elements*

$$\mathrm{Tr}_e^{N/L} \pi_{N/L} R_\chi(\mu),$$

where $\chi \in \mathcal{D}_{Kh}$ is even, $R_\chi(\mu)$ has new level $L \mid N$, and e divides N/L.

Proof. Translate this statement to modular forms using (2.7) and Lemma 2.2.13, then apply Corollary 2.2.16 and the standard theory of old and new subspaces. □

We note that each real twist orbit space contains an element $\mu = \gamma_f$, where f is a newform at a level dividing N, and thus has a basis of this form. In this case, denote by $O^+(f)$ the analogue of $O(\mu)^+$ under the isomorphism (2.5). We call this the *real twist orbit space* of f. Denote by

$$V(f)^+ \subset S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \overline{\mathbb{Q}})$$

the subspace spanned by the real twist orbit spaces $O^+(f^\sigma)$, where $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

2.3.2 Computing q-expansions

We consider again the set-up from the previous section. Now assume that $JGJ = G$, $-I \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Consider also a group $\mathcal{A} \subset (\mathcal{N}_{\Gamma_0(M)} \cap \mathcal{N}_{G^h})/\mathrm{P}\Gamma$ such that $J\mathcal{A}J = \mathcal{A}$. Here G^h is the subgroup of G with determinant 1 mod h, and h is the largest divisor of 24 such that $h^2 \mid M$. Then the group $F := \langle \mathrm{P}\Gamma, \mathcal{A}\rangle$ satisfies $JFJ = F$ and $F \subset \mathcal{N}_{\Gamma_0(M)}$. (Technically, we should replace $\mathcal{A}$ by a set of lifts to $\mathcal{N}_{\Gamma_0(M)}$, but note that F is independent of the choices of lifts.) Also define $V := H_1(X_{\Gamma_0(MK^2)\cap\Gamma_1(K)}, \mathbb{C})$ and decompose $V = \oplus_i O_i$ into distinct twist orbit spaces.

By Corollary 2.3.6 and Proposition 2.3.8, F acts on each O_i separately, and $V^F = \bigoplus_i O_i^F$. Now J acts on each O_i^F separately, and we obtain

$$V^{F,+} = \bigoplus_i O_i^{F,+}, \text{ where } O_i^{F,+} \subset O_i^+$$

and the superscript $+$ denotes the J-invariant subspace. This means that $V^{F,+}$ has a basis of elements of real twist orbit spaces. In order to determine q-expansions for a basis of $S_2(\Gamma, \mathbb{C})^{\mathcal{A}}$, it thus suffices to be able to compute q-expansions for cusp forms in a fixed real twist orbit space. To this end, recall that we have a sesqui-linear isomorphism

$$S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{C}) \to H_{\mathbb{C}}(\Gamma_0(MK^2) \cap \Gamma_1(K)), \quad f \mapsto \gamma_f,$$

under which the operators correspond as follows:

$$T_p \longleftrightarrow T_p^*, \quad R_\chi \longleftrightarrow R_{\overline{\chi}} \text{ if } \chi(-1) = 1, \quad \mathrm{pr}_{N/L} \longleftrightarrow \pi_{N/L},$$
$$[\Gamma_0(N) : \Gamma_0(L)]B_d^{N/L} \longleftrightarrow \mathrm{Tr}_d^{N/L}.$$

This means the following.

Proposition 2.3.10. *Suppose that $f \in S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{C})$ and $\mu = \gamma_f$ is in $H_{\mathbb{C}}(\Gamma_0(MK^2) \cap \Gamma_1(K))$. For each $i \in \{1, \ldots, n\}$, consider even $\chi_i \in \mathcal{D}_{Kh}$ and $a_i \in \mathbb{C}$. Let*

$L_i \mid N$ be the new level of $f|R_{\overline{\chi}_i}$, and consider $e_i \mid N/L_i$. Then

$$\sum_{i=1}^{n} a_i \mathrm{Tr}_{e_i}^{N/L_i} \pi_{N/L_i} R_{\chi_i}(\mu) = \gamma_g,$$

where

$$g = \sum_{i=1}^{n} [\Gamma_0(N) : \Gamma_0(L_i)] \cdot \overline{a_i} \cdot f|R_{\overline{\chi}_i} \mathrm{pr}_{N/L_i} B_{e_i}^{N/L_i}.$$

From the action of T_p on newforms we can determine q-expansions of newforms. Moreover, we know how B_e and R_χ act on q-expansions, and by Corollary 2.2.16, we can also determine what $\mathrm{pr}_{N/L}$ does to q-expansions. So, given a q-expansion for f in the above proposition, we can compute a q-expansion for g. This leads to the following algorithm.

Algorithm 2.3.11 (For computing q-expansions for a basis of $S_2(\Gamma, \mathbb{Q}(\zeta_{Kh})^+)^{\mathcal{A}}$)**.** Input*: Coprime integers K and M, a finite subset S of $\mathrm{GL}_2^+(\mathbb{Q})$ generating a subgroup $F \subset \mathcal{N}_{\Gamma_0(M)}$ normalised by J, and a positive integer* `prec`*. Let h be the largest divisor of 24 such that $h^2 \mid M$.*

Steps*:*

(1) Find a basis for $H_1(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{Q})$ and determine the fixed subspace $H_1(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{Q}(\zeta_{Kh}))^F$.

(2) Choose a divisor $L = L_1 L_2^2 \mid K^2 M$ with $L_1 \mid M$ and $L_2 \mid K$, and a newform $f \in S_2(\Gamma_0(L) \cap \Gamma_1(L_2), \overline{\mathbb{Q}})$. Compute the q-expansion for f up to $q^{\mathtt{prec}+1}$.

(3) Using Corollary 2.2.16, compute the q-expansions (up to $q^{\mathtt{prec}+1}$) for all $f|R_{\overline{\chi}} \mathrm{pr}_{N/L} B_e^{N/L}$, where $\chi \in \mathcal{D}_{Kh}$ is even, $L \mid N$ is the new level of $f|R_{\overline{\chi}}$ and $e \mid N/L$.

(4) Using (finitely many) T_p-operators and their eigenvalues, compute $\mu \in H_{\mathbb{C}}(\Gamma_0(MK^2) \cap \Gamma_1(K))$ such that $\mu = \alpha \gamma_f$ for some $\alpha \in \overline{\mathbb{Q}}^\times$.

(5) Compute the modular symbols $\mathrm{Tr}_e^{N/L} \pi_{N/L} R_\chi(\mu)$ corresponding to the modular forms computed in (3). The space $O(\mu)^+$ they generate is a real twist orbit space.

(6) Determine a basis for the intersection $O(\mu)^+ \cap H_1(\Gamma_0(MK^2) \cap \Gamma_1(K), \overline{\mathbb{Q}})^F$, as linear combinations of the modular symbols computed in Step (5).

(7) Using Proposition 2.3.10 and the result from Step (3), determine the q-expansions of the modular forms corresponding to the basis computed in Step (6).

(8) Return to Step (2), unless the spaces $O(\mu)^+$ considered so far span $H_{\mathbb{C}}(\Gamma_0(MK^2) \cap \Gamma_1(K))^F$.

(9) The q-expansions for the computed basis are defined over a number field containing $\mathbb{Q}(\zeta_{Kh})^+$. Take linear combinations to reduce to a basis over $\mathbb{Q}(\zeta_{Kh})^+$.

Output: *A finite set of q-expansions $a_1 q + a_2 q^2 + \ldots + a_{\mathtt{prec}+1} q^{\mathtt{prec}+1}$ with each $a_i \in \mathbb{Q}(\zeta_{Kh})^+$, corresponding to a basis for $S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \mathbb{Q}(\zeta_{Kh})^+)^F$. When $\mathcal{A}$, Γ and F are defined as at the start of this section, this space equals $S_2(\Gamma, \mathbb{Q}(\zeta_{Kh})^+)^{\mathcal{A}}$.*

Proof. The discussion at the start of this section shows that we indeed obtain a basis for the space $S_2(\Gamma_0(MK^2) \cap \Gamma_1(K), \overline{\mathbb{Q}})^F$. In (2.3) in Section 2.2.3, we saw that a basis of q-expansions with coefficients in $\mathbb{Q}(\zeta_{Kh})$ exists, and, as J normalises F, we can reduce further to $\mathbb{Q}(\zeta_{Kh})^+$. □

2.3.3 The $\mathbb{Q}$-rational structure

We continue the notation from the previous section. Assume also that $\mathcal{A}$ determines a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant automorphism *group*. Then we know that a model for $X_G/\mathcal{A}$ over $\mathbb{Q}$ must exist. Given the modular forms in $S_2(\Gamma, \mathbb{Q}(\zeta_{Kh})^+)^{\mathcal{A}}$ computed using Algorithm 2.3.11, we can compute *some* model for $(X_G/\mathcal{A})_{\mathbb{Q}(\zeta_{Kh})^+}$, but this model tends to be defined over $\mathbb{Q}(\zeta_{Kh})^+$ rather than over $\mathbb{Q}$.

We want to compute the fixed space for the action of the remaining matrices in $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of determinant unequal to 1, as defined in Section 2.2.1. This action on cusp forms is only $\mathbb{Q}$-linear, as opposed to $\mathbb{C}$-linear, which complicates matters: the pairing (2.4) between modular forms and modular symbols, being defined by integration, does not descend to a pairing between two $\mathbb{Q}$-vector spaces.

We first prove a Sturm bound. For a curve X and a divisor D on X, denote by Ω the sheaf of regular differential 1-forms, and by $\mathcal{O}_X(D)$ the sheaf such that for each open $U \subset X$, the set $\mathcal{O}_X(D)(U)$ consists of those functions f in the function field of X satisfying $\mathrm{div}(f|_U) \geq -D \cap U$.

Lemma 2.3.12. *Suppose that X is a curve, and $\omega \in H^0(X, \Omega^{\otimes k})$. We consider a point $x \in X$ and a uniformiser $q \in \widehat{\mathcal{O}}_x$ in the completed local ring. Write the image of ω in $(\Omega^{\otimes k})_x$ as $\omega_x = (a_1 + a_2 q + a_3 q^2 + \ldots)\,(\mathrm{d}q)^{\otimes k}$. If $a_i = 0$ for all $i \in \{1, \ldots, k(2g-2)+1\}$ then $\omega = 0$.*

Proof. This is a standard argument. Let $\mathcal{K}$ be the canonical divisor. By assumption, ω yields a global section of the sheaf $\mathcal{O}_X(k\mathcal{K} - (k(2g-2)+1)x)$. This sheaf has degree $k\deg(\mathcal{K}) - k(2g-2) - 1 < 0$, and therefore has no non-zero global sections. □

Algorithm 2.3.13 (For computing a model for $X_G/\mathcal{A}$ over $\mathbb{Q}$)**.** Input*: A finite set of matrices generating a subgroup $G \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, $-I \in G$ and $JGJ = G$. An integer M such that $N = MK$ with $\gcd(M, K) = 1$ and G surjects onto $B_0(M) \subset \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. Let h be the largest divisor of 24 such that $h^2 \mid M$. A finite subset of $\mathrm{GL}_2^+(\mathbb{Q})$ generating a subgroup $\mathcal{A} \subset (\mathcal{N}_{\Gamma_0(M)} \cap \mathcal{N}_{G^h})/\mathrm{P}\Gamma_G$ normalised by J, and defining a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant automorphism group on X_G such that $X_G/\mathcal{A}$ has genus $g \geq 2$. A positive integer* `prec`*.*

Steps*:*

(1) Define $F := \langle \Gamma_G, \mathcal{A} \rangle$ and run Algorithm 2.3.11 for $F, K, M, h,$ `prec` *to determine q-expansions for a basis of $S_2(\Gamma_G, \mathbb{Q}(\zeta_{Kh})^+)^{\mathcal{A}}$, and reduce to a basis of $S_2(\Gamma_G, \mathbb{Q}(\zeta_K^+))^{\mathcal{A}}$. The dimension of this space is the genus g of $X_G/\mathcal{A}$.*

(2) Find generators $A_1, \ldots, A_n, A_{n+1}, \ldots, A_{n'}$ for the image G_K of G in $\mathrm{GL}_2(\mathbb{Z}/K\mathbb{Z})$ such that $A_{n+1}, \ldots, A_{n'}$ generate $G_K \cap \mathrm{SL}_2(\mathbb{Z}/K\mathbb{Z})$ and $\det(A_i) \neq 1$ for all $i \in$

$\{1, \ldots, n\}$.

(3) *For each* $A \in \{A_1, \ldots, A_n\}$*, run Steps (4)-(6).*

(4) *Write* $A = B \cdot \gamma_d$*, where* $d = \det(A)$ *and* $\gamma_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$*. Determine a lift* $\widetilde{B}$ *of* B *to* $\Gamma_0(M) \subset \mathrm{SL}_2(\mathbb{Z})$*. For each real twist orbit space* $O(\mu)^+$ *computed in Algorithm 2.3.11,* $\widetilde{B}$ *maps* $O(\mu)^{\Gamma_G,+}$ *into* $O(\mu)^+$*. Run steps (5)-(6) for each such* $O(\mu)^+$*.*

(5) *As in Algorithm 2.3.11, compute the action of* $\widetilde{B}$ *on* $O(\mu)^{\Gamma_G,+}$*, and translate this to a* $\mathbb{Q}(\zeta_K)$*-linear map* $\widetilde{B} : V(f)^+ \cap S_2(\Gamma_G, \mathbb{Q}(\zeta_K)) \to V(f)^+$ *in terms of the basis computed in Step (1).*

(6) *Using a basis for* $\mathbb{Q}(\zeta_K)/\mathbb{Q}$*, consider the linear map computed in (5) as a* $\mathbb{Q}$*-linear map, and postcompose with the action of* $\gamma_d : V(f)^+ \to V(f)^+$*, which Galois conjugates coefficients in a q-expansion with* $\sigma_d : \zeta_K \to \zeta_K^d$*. This composition yields a map* $V(f)^+ \cap S_2(\Gamma_G, \mathbb{Q}(\zeta_K)) \to V(f)^+ \cap S_2(\Gamma_G, \mathbb{Q}(\zeta_K))$ *corresponding to the action of* A *on q-expansions.*

(7) *For each* $V(f)^+$*, determine q-expansions of a basis for* $(V(f)^+ \cap S_2(\Gamma_G, \mathbb{Q}(\zeta_K)))^{\mathcal{A}, A_1, \ldots, A_n}$*, up to the precision needed for the next step.*

(8) *Use the q-expansions to determine equations for* $X_G/\mathcal{A}$*, as done in [Gal02]. Unless* $X_G/\mathcal{A}$ *is hyperelliptic, this is done by computing homogeneous* $\mathbb{Q}$*-rational polynomial equations satsified by the q-expansions, up to* $q^{\mathtt{prec}}$*. To show an equation of degree* d *holds provably, we need* $\mathtt{prec} > d(2g-2) - (d-1)$*, where* $g = \dim(S_2(\Gamma_G, \mathbb{Q}(\zeta_K))^{\mathcal{A}})$*. For the details when* $X_G/\mathcal{A}$ *is hyperelliptic, we refer to [Gal02].*

Output: A finite number of homogeneous polynomials over $\mathbb{Q}$ *in* $g+1$ *variables in case* $X_G/\mathcal{A}$ *is non-hyperelliptic; a single polynomial in 2 variables if* $X_G/\mathcal{A}$ *is hyperelliptic.*

Remark 2.3.14. By Petri's theorem (see [SV88]), the canonical image of a non-hyperelliptic curve of genus $g \geq 4$ is an intersection of quadrics unless the curve is trigonal or (isomorphic to) a plane quintic. It thus often suffices to take $\mathtt{prec} > 4g - 5$. In the trigonal and plane quintic cases, the canonical image is defined by equations of degree 4, while for genus 3 curves the canonical image is cut out by equations of degrees up to 3 (see [Zyw20, Lemma 7.1]). In every case, therefore, $\mathtt{prec} > 8g - 11$ suffices.

Proof. This algorithm computes the right object since $S_2(\Gamma_G, \mathbb{Q}(\zeta_K))^{\mathcal{A}, A_1, \ldots, A_n}$ is equal to $H^0(X_G/\mathcal{A}, \Omega^1)$, as shown in Section 2.2.3.

In Step (1), a basis over $\mathbb{Q}(\zeta_K^+)$ exists because $\mathcal{A}$ is Galois invariant. The crucial claim in Step (4) that $\widetilde{B}$ maps $O(\mu)^{\Gamma_G,+}$ into $O(\mu)^+$ requires proof. Since $A \in G_K$ and $JAJ \in G_K$, we find that $JAJA^{-1} \in G_K \cap \mathrm{SL}_2(\mathbb{Z}/K\mathbb{Z})$. So JAJ and A, though different operators in general, have identical restriction to

$$(H_1(X(\Gamma_0(MK^2) \cap \Gamma_1(K)), \mathbb{R}) \otimes \mathbb{C})^{\Gamma_G}.$$

In particular, A acts maps the $+$-eigenspace $H_{\mathbb{C}}(\Gamma_0(MK^2) \cap \Gamma_1(K))^{\Gamma_G}$ into the space $H_{\mathbb{C}}(\Gamma_0(MK^2) \cap \Gamma_1(K))$. Since γ_d commutes with J (even as matrices), we conclude that $\widetilde{B}$ maps $H_{\mathbb{C}}(\Gamma_0(MK^2) \cap \Gamma_1(K))^{\Gamma_G}$ into $H_{\mathbb{C}}(\Gamma_0(MK^2) \cap \Gamma_1(K))$. Because $\widetilde{B} \in \Gamma_0(M)$ moreover acts on twist orbit spaces, this proves the claim. Furthermore, γ_d acts on $V(f)^+$, since for $\sigma : \zeta_K \to \zeta_K^d$, we have

$$(f|R_\chi \mathrm{pr}_L B_d)^\sigma = g(\overline{\chi})^\sigma (f^\sigma \otimes \chi^\sigma)|\mathrm{pr}_L B_d.$$

Step (5) again relies on Propositions 2.3.8 and 2.3.10. Steps (6) and (7) are linear algebra computations, and for the details of Step (8) we refer to [Gal02]. We recall that $S_{2k}(\Gamma_G, \mathbb{Q}(\zeta_K))^{\mathcal{A}} = H^0(X/\mathcal{A}, \Omega^{\otimes k})$. The lower bound on `prec` follows from Lemma 2.3.12 by noting that the coefficient for q^ℓ in the expansion of a product of d cusp forms is determined by the first $\ell - (d-1)$ coefficients of each cusp form. □

Remark 2.3.15. If $\alpha \in \mathcal{N}_G/\mathrm{P}\Gamma_G$ commutes with each element of $\mathcal{A}$, then α determines an automorphism of $X_G/\mathcal{A}$. If α also commutes with J, the action of α on each real twist orbit space can be determined explicitly, which can be translated into a matrix for the action of α on the basis of cusp forms found in Step (7). From this, we obtain the automorphism on $X_G/\mathcal{A}$ determined by α explicitly.

Moreover, having determined the q-expansions for generators of the function field of $X_G/\mathcal{A}$, we can determine maps to other modular curves, such as the j-map.

We note that the q-expansions computed in Step (7) still do not have $\mathbb{Q}$-rational coefficients in general, but do satisfy rational equations. Ultimately, this is because the image of the infinity cusp on (a rational model for) $X_G/\mathcal{A}$ is – in general – not a $\mathbb{Q}$-rational point, so the expansion of a regular differential form at this cusp also tends to have non-rational coefficients.

2.4 Examples

2.4.1 The three curves

Consider the subgroup $G(\mathrm{e}7) \subset \mathrm{GL}_2(\mathbb{F}_7)$ defined in Section 1.1.3. This group was first studied in [FLHS15, Proposition 9.1]. Recall that this is an index 2 subgroup of $C_{\mathrm{ns}}^+(7)$. We obtain a degree 2 map

$$X(\mathrm{b}5, \mathrm{e}7) \to X(\mathrm{b}5, \mathrm{ns}7).$$

Every degree 2 map of curves is the quotient by an involution. Let us call this involution $\phi_7 : X(\mathrm{b}5, \mathrm{e}7) \to X(\mathrm{b}5, \mathrm{e}7)$. This corresponds to the action of a matrix in $C_{\mathrm{ns}}^+(7) \setminus G(\mathrm{e}7)$ (c.f. Example 1.1.8) and commutes with the Atkin–Lehner involution w_5 (defined in Definition 1.1.10, using any $\eta \in G(\mathrm{e}7)$ of determinant 5 mod 7). We thus obtain the

following diagram of degree 2 maps between modular curves

$$\begin{tikzcd}
 & X(\mathrm{b5},\mathrm{e7}) \arrow[dl] \arrow[d] \arrow[dr] & \\
X(\mathrm{b5},\mathrm{ns7}) \arrow[dr] & X(\mathrm{b5},\mathrm{e7})/\phi_7 w_5 \arrow[d] & X(\mathrm{b5},\mathrm{e7})/w_5 \arrow[dl] \\
 & X(\mathrm{b5},\mathrm{ns7})/w_5 &
\end{tikzcd} \cdot$$

We note that ϕ_7 and w_5 represent the two subsets of allowed automorphisms described in Remark 2.2.5. We use Algorithm 2.3.13 to compute canonical models for the three modular curves in the middle row, as well as their maps to $X(\mathrm{b5},\mathrm{ns7})/w_5$, and a basis for their global differential forms by means of modular forms. We use this in Chapter 4 as part of the proof that all elliptic curves over quartic fields not containing $\sqrt{5}$ are modular.

We note that the genera of $X(\mathrm{b5},\mathrm{ns7})$, $X(\mathrm{b5},\mathrm{e7})/w_5$ and $X(\mathrm{b5},\mathrm{e7})/\phi_7 w_5$ are 6, 5 and 8 respectively, while $X(\mathrm{b5},\mathrm{e7})$ has genus 15 and $X(\mathrm{b5},\mathrm{ns7})/w_5$ is hyperelliptic of genus 2. A model for $X(\mathrm{b5},\mathrm{ns7})$ was first computed by Le Hung [LH14] using its description as a fibred product of $X(\mathrm{b5})$ and $X(\mathrm{ns7})$, and this was transformed into a planar model by Derickx, Najman and Siksek in [DNS20]. This known model serves as an extra verification for the correctness of our computations. We also compute the map $X(\mathrm{b5},\mathrm{ns7}) \to X(\mathrm{ns7})$. Composition with Chen's j-map [Che96, p. 69] on $X(\mathrm{ns7}) = \mathbb{P}^1$

$$j_{\mathrm{ns7}}(x) = \frac{\big((4x^2+5x+2)(x^2+3x+4)(x^2+10x+4)(3x+1)\big)^3}{(x^3+x^2-2x-1)^7} \tag{2.8}$$

thus yields the j-map on $X(\mathrm{b5},\mathrm{ns7})$.

Theorem 2.4.1. *A canonical model for $X(\mathrm{b5},\mathrm{ns7})$ in $\mathbb{P}^5_{X_0,\ldots,X_5}$ is given by:*

$$\begin{aligned}
X(\mathrm{b5},\mathrm{ns7}) : {} & 14X_0^2 + 12X_2X_3 - 16X_3^2 - 14X_2X_4 + 30X_3X_4 - 11X_4^2 \\
& \quad + 28X_2X_5 - 58X_3X_5 + 40X_4X_5 - 28X_5^2 = 0, \\
& 7X_0X_1 - 2X_2X_4 - 4X_3X_4 + 2X_4^2 + 12X_3X_5 - 7X_4X_5 + 10X_5^2 = 0, \\
& 14X_1^2 - 4X_2X_3 + 16X_3^2 + 10X_2X_4 + 14X_3X_4 - 21X_4^2 \\
& \quad + 4X_2X_5 - 58X_3X_5 + 64X_4X_5 - 66X_5^2 = 0, \\
& 2X_0X_2 - 2X_0X_3 + 2X_1X_3 - 5X_0X_4 - 6X_1X_4 + 8X_0X_5 + 4X_1X_5 = 0, \\
& 4X_1X_2 - 2X_0X_3 - 6X_1X_3 - X_0X_4 + 3X_1X_4 + 3X_0X_5 - 2X_1X_5 = 0, \\
& 8X_2^2 - 20X_2X_3 + 16X_3^2 - 14X_2X_4 + 14X_3X_4 - 21X_4^2 \\
& \quad + 28X_2X_5 - 42X_3X_5 + 56X_4X_5 - 28X_5^2 = 0.
\end{aligned}$$

and the Atkin–Lehner involution acts as

$$w_5 : \ (X_0 : X_1 : X_2 : X_3 : X_4 : X_5) \mapsto (-X_0 : -X_1 : X_2 : X_3 : X_4 : X_5).$$

The map $X(\mathrm{b5},\mathrm{ns7}) \to X(\mathrm{ns7}) = \mathbb{P}^1$ *is given by sending* $(X_0 : \ldots : X_5)$ *to*

$$(7X_0 - 2X_2 + 4X_3 - X_4 - 4X_5 : -14X_0 - 7X_1 + 6X_2 - 12X_4 + 10X_4 - 9X_5).$$

A canonical model for $X(\mathrm{b5},\mathrm{e7})/w_5$ *in* $\mathbb{P}^4_{X_0,\ldots,X_4}$ *is given by*

$$\begin{aligned}\frac{X(\mathrm{b5},\mathrm{e7})}{w_5} : 448X_0^2 - 9X_1^2 + 9X_2^2 + 54X_2X_3 + 9X_3^2 + 112X_0X_4 + 126X_1X_4 + 7X_4^2 = 0,\\ 16X_0X_1 - 3X_1^2 + 3X_2^2 + 6X_2X_3 + 3X_3^2 + 2X_1X_4 + 21X_4^2 = 0,\\ 3X_1X_2 + 28X_0X_3 + 12X_1X_3 + 21X_2X_4 + 14X_3X_4 = 0\end{aligned}$$

and ϕ_7 *acts by*

$$w_5 = \phi_7 : \ (X_0 : X_1 : X_2 : X_3 : X_4) \mapsto (X_0 : X_1 : -X_2 : -X_3 : X_4).$$

Finally, a canonical model for $X(\mathrm{b5},\mathrm{e7})/\phi_7 w_5$ *in* $\mathbb{P}^7_{X_0,\ldots,X_7}$ *is given by*

$$\begin{aligned}
&3528X_0^2 + 177X_4X_5 + 597X_5^2 - 2716X_0X_6 - 423X_1X_6 - 6365X_2X_6\\
&\quad - 1918X_3X_6 - 13454X_6^2 + 2842X_0X_7 + 626X_1X_7 + 9144X_2X_7\\
&\quad + 3010X_3X_7 + 35252X_6X_7 - 22960X_7^2 = 0,\\
&56X_0X_1 - 135X_4X_5 - 327X_5^2 - 140X_0X_6 - 37X_1X_6\\
&\quad + 2381X_2X_6 + 1890X_3X_6 + 2982X_6^2 + 910X_0X_7 + 16X_1X_7\\
&\quad - 3270X_2X_7 - 2758X_3X_7 - 7476X_6X_7 + 4816X_7^2 = 0,\\
&56X_1^2 + 1215X_4X_5 + 2835X_5^2 + 11340X_0X_6 - 715X_1X_6\\
&\quad - 22389X_2X_6 - 12726X_3X_6 - 38290X_6^2 - 19530X_0X_7 + 820X_1X_7\\
&\quad + 30894X_2X_7 + 21546X_3X_7 + 99764X_6X_7 - 64624X_7^2 = 0,\\
&168X_0X_2 - 15X_4X_5 - 3X_5^2 - 56X_0X_6 - 45X_1X_6 + 89X_2X_6 + 238X_3X_6\\
&\quad - 238X_6^2 + 182X_0X_7 + 52X_1X_7 - 138X_2X_7 - 406X_3X_7 + 532X_6X_7 - 224X_7^2 = 0,\\
&56X_1X_2 - 171X_4X_5 - 315X_5^2 + 168X_0X_6 - 253X_1X_6 + 2713X_2X_6\\
&\quad + 2562X_3X_6 + 2086X_6^2 + 1050X_0X_7 + 260X_1X_7 - 3910X_2X_7\\
&\quad - 3738X_3X_7 - 5292X_6X_7 + 3584X_7^2 = 0,\\
&56X_2^2 + 87X_4X_5 + 147X_5^2 - 364X_0X_6 + 141X_1X_6 - 1285X_2X_6 - 1582X_3X_6 - 714X_6^2\\
&\quad - 266X_0X_7 - 148X_1X_7 + 1894X_2X_7 + 2170X_3X_7 + 1764X_6X_7 - 1232X_7^2 = 0,\\
&1764X_0X_3 - 579X_4X_5 - 1050X_5^2 + 1505X_0X_6 - 774X_1X_6 + 7009X_2X_6\\
&\quad + 6083X_3X_6 + 7021X_6^2 + 1456X_0X_7 + 851X_1X_7 - 9837X_2X_7\\
&\quad - 8582X_3X_7 - 15778X_6X_7 + 9044X_7^2 = 0,\\
&28X_1X_3 + 9X_4X_5 + 6X_5^2 + 357X_0X_6 - X_1X_6 + 74X_2X_6 + 161X_3X_6\\
&\quad - 63X_6^2 - 364X_0X_7 - 20X_1X_7 - 144X_2X_7 - 168X_3X_7 + 210X_6X_7 - 140X_7^2 = 0,\\
&84X_2X_3 - 15X_4X_5 - 30X_5^2 - 35X_0X_6 - 27X_1X_6 + 80X_2X_6 + 133X_3X_6
\end{aligned}$$

$$
\begin{aligned}
&\quad + 329X_6^2 + 140X_0X_7 + 34X_1X_7 - 66X_2X_7 - 196X_3X_7 - 854X_6X_7 + 532X_7^2 = 0,\\
&252X_3^2 + 12X_4X_5 - 30X_5^2 + 70X_0X_6 + 45X_1X_6 + 443X_2X_6 + 28X_3X_6\\
&\quad + 350X_6^2 - 196X_0X_7 - 59X_1X_7 - 639X_2X_7 + 14X_3X_7 - 728X_6X_7 + 280X_7^2 = 0,\\
&18X_0X_4 - 19X_0X_5 - 12X_1X_5 - 27X_2X_5 + 17X_3X_5 - 120X_4X_6\\
&\quad - 66X_5X_6 + 114X_4X_7 + 54X_5X_7 = 0,\\
&2X_1X_4 - 21X_0X_5 + 8X_1X_5 + 7X_2X_5 - 21X_3X_5\\
&\quad + 28X_4X_6 + 56X_5X_6 - 28X_4X_7 - 84X_5X_7 = 0,\\
&6X_2X_4 + 7X_0X_5 + 3X_2X_5 + 7X_3X_5 = 0,\\
&9X_3X_4 - 28X_0X_5 - 3X_1X_5 - 9X_2X_5 + 8X_3X_5 - 39X_4X_6\\
&\quad - 30X_5X_6 + 33X_4X_7 + 27X_5X_7 = 0,\\
&63X_4^2 + 426X_4X_5 + 690X_5^2 + 1120X_0X_6 + 207X_1X_6 - 4405X_2X_6\\
&\quad - 2702X_3X_6 - 7000X_6^2 - 2464X_0X_7 - 263X_1X_7 + 6057X_2X_7\\
&\quad + 4298X_3X_7 + 18172X_6X_7 - 11984X_7^2 = 0
\end{aligned}
$$

and the remaining involution acts as

$$\phi_7 = w_5 : \ (X_0 : \ldots : X_7) \mapsto (X_0 : X_1 : X_2 : X_3 : -X_4 : -X_5 : X_6 : X_7).$$

The quotients of each of these three curves by their respective involutions give rise to the same genus 2 hyperelliptic curve

$$X(\mathrm{b5}, \mathrm{ns7})/w_5 : \ y^2 = x^6 + 2x^5 + 7x^4 - 4x^3 + 3x^2 - 10x + 5.$$

It is not surprising that we find only quadratic equations, c.f. Remark 2.3.14. Using `Magma`'s built-in `Genus6PlaneCurveModel` function, we can transform our model for $X(\mathrm{b5}, \mathrm{ns7})$ into a planar model. As in [DNS20], this planar model has four singular points, and we can make a translation such that the singular points have coordinates $(i : 0 : 1)$, $(-i : 0 : 1)$, $(0 : 1/\sqrt{5} : 1)$ and $(0 : -1/\sqrt{5} : 1)$. The planar equation thus obtained is identical to the one found by Derickx–Najman–Siksek, showing that our model is indeed isomorphic to theirs.

2.4.2 Finding generators

In [FLHS15] and in Section 1.1.3, the group $G(\mathrm{e7})$ was defined by explicit generators, and is contained in the normaliser of a non-split Cartan subgroup. Recall that these Cartan subgroups are only defined up to conjugacy. We work in the non-split Cartan subgroup

$$C_{\mathrm{ns}}(7) := \left\{ \begin{pmatrix} a & 5b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_7) \mid a, b \in \mathbb{F}_7 \right\}$$

and its normaliser $C_{\mathrm{ns}}^{+}(7)$ generated by $C_{\mathrm{ns}}(7)$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Note that 5 is a generator of $\mathbb{F}_7^{\times}$.

In order to determine which subgroup of $C_{\mathrm{ns}}^{+}(7)$ corresponds to $G(\mathrm{e}7)$, we first find a choice-independent definition.

Lemma 2.4.2. *Let G be the normaliser of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_7)$. The corresponding subgroup $G(\mathrm{e}7) \subset G$ is the unique index 2 subgroup $H \subset G$ such that*

(i) H is not cyclic and

(ii) $H \cap \mathrm{SL}_2(\mathbb{F}_7)$ is cyclic of order 8.

Proof. The group $\mathrm{GL}_2(\mathbb{F}_7)$ is a relatively small finite group, and we can do these computations in `Magma`. For uniqueness, we can use any normaliser of a non-split Cartan, and we use the one defined above. To verify that $G(\mathrm{e}7)$ indeed satisfies these properties, we can work with the group defined in Section 1.1.3. □

We also see from the definition of $C_{\mathrm{ns}}^{+}(7)$ and Lemma 2.4.2 that $C_{\mathrm{ns}}^{+}(7)$ and $G(\mathrm{e}7)$ are normalised by J. This means that also ϕ_7 is normalised by J. Since the only element of order 2 in $\mathrm{SL}_2(\mathbb{F}_7)$ is $-I$, we deduce from (ii) that $-I \in G(\mathrm{e}7)$. We also check that $\det(G(\mathrm{e}7)) = \mathbb{F}_7^{\times}$.

Next, we use Lemma 2.4.2 to find generators, and we lift them to $\Gamma_0(5)$ to obtain the following five matrices. Define

$$g_0 := \begin{pmatrix} 61 & -55 \\ 10 & -9 \end{pmatrix} \text{ and } \phi_7 := \begin{pmatrix} 3 & 1 \\ -10 & -3 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Then g_0 reduces to the identity mod 5 and to a generator of $G(\mathrm{e}7) \cap \mathrm{SL}_2(\mathbb{F}_7)$ mod 7, while ϕ_7 is in $\Gamma_0(5)$ and reduces mod 7 to an element in $C_{\mathrm{ns}}^{+}(7) \cap \mathrm{SL}_2(\mathbb{F}_7) \setminus G(\mathrm{e}7) \cap \mathrm{SL}_2(\mathbb{F}_7)$. Next, define

$$B := \begin{pmatrix} 6 & 5 \\ -5 & -4 \end{pmatrix}, \; C := B \cdot \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } w_5 := \begin{pmatrix} 2890 & 193 \\ -8685 & -580 \end{pmatrix} \in \mathrm{GL}_2^{+}(\mathbb{Q}).$$

We note that C reduces into $B_0(5)$ mod 5, $\det(w_5) = 5$ and w_5 reduces into $G(\mathrm{e}7)$ mod 7. So w_5 indeed corresponds to the Atkin–Lehner involution. Moreover,

$$G(\mathrm{e}7) = \langle \overline{g}_0, \overline{C}, \overline{J} \rangle \text{ and } C_{\mathrm{ns}}^{+}(7) = \langle \overline{g}_0, \overline{C}, \overline{J}, \overline{\phi}_7 \rangle,$$

where a bar denotes reduction mod 7.

Using the built-in commands in `Sage`, we compute $S := S_2(\Gamma_0(5 \cdot 7^2) \cap \Gamma_1(7), \mathbb{Q}(\zeta_7))$. This space has dimension 61. We need to determine the fixed spaces

$$S^{\langle g_0, \phi_7, C, J \rangle}, \; S^{\langle g_0, w_5, C, J \rangle} \text{ and } S^{\langle g_0, w_5 \cdot \phi_7, C, J \rangle}.$$

To this end, we first compute the fixed spaces $S^{\langle g_0, \phi_7 \rangle}, S^{\langle g_0, w_5 \rangle}$ and $S^{\langle g_0, w_5 \cdot \phi_7 \rangle}$, after which we determine the $\mathbb{Q}$-rational structure by considering C and J.

2.4.3 The twist orbit spaces

We execute Step (4) of Algorithm 2.3.11, by computing q-expansions for the eigenforms corresponding to the bases of the real twist orbit spaces as described in Proposition 2.3.9. There are two non-zero spaces of cusp forms of lower level: $S_2(\Gamma_0(49) \cap \Gamma_1(7), \mathbb{Q}(\zeta_7))$ (3-dimensional), and $S_2(\Gamma_0(5) \cap \Gamma_1(7), \mathbb{Q}(\zeta_7))$ (7-dimensional).

Define

$$\chi : (\mathbb{Z}/7\mathbb{Z})^\times \to \mathbb{C}^\times, \;\; \chi(3) = e^{\pi i/3}.$$

Then χ has order 6 and $\mathcal{D}_7 = \langle \chi \rangle$. Also, $\chi(-1) = -1$, so the even characters are generated by χ^2. We note all found equations have degree 2, so it suffices to take $\texttt{prec} = 2(2\cdot 8-2) = 28$. To save space, we here display modular forms only up to q^{10}.

We consider the following newforms, all of which have trivial Nebentypus character:

$$\begin{aligned}
f_{49} &:= q + q^2 - q^4 - 3q^8 - 3q^9 + O(q^{11}) \in S_2(\Gamma_0(49) \cap \Gamma_1(7), \overline{\mathbb{Q}}),\\
f_{35} &:= q + q^3 - 2q^4 - q^5 + q^6 - 2q^8 - 3q^{10} + O(q^{11}) \in S_2(\Gamma_0(5) \cap \Gamma_1(7), \overline{\mathbb{Q}}),\\
g_{35} &:= q + \alpha q^2 - (\alpha+1)q^3 + (2-\alpha)q^4 + q^5 - 4q^6, -q^7 + (\alpha-4)q^8 + (\alpha+2)q^9\\
&\qquad + \alpha q^{10} + O(q^{11}) \in S_2(\Gamma_0(5) \cap \Gamma_1(7), \overline{\mathbb{Q}}), \text{ where } \alpha = (-1+\sqrt{17})/2,\\
f_0 &:= q - 2q^2 - 3q^3 + 2q^4 + q^5 + 6q^6 + 6q^9 - 2q^{10} + O(q^{11}) \in S_2(\Gamma_0(5\cdot 7^2) \cap \Gamma_1(7), \overline{\mathbb{Q}}),\\
f_1 &:= q + \sqrt{2}q^2 - (\sqrt{2}+1)q^3 - q^5 - (\sqrt{2}+2)q^6 - 2\sqrt{2}q^8\\
&\quad + 2\sqrt{2}q^9 - \sqrt{2}q^{10} + O(q^{11}) \in S_2(\Gamma_0(5\cdot 7^2) \cap \Gamma_1(7), \overline{\mathbb{Q}}), \text{ and}\\
f_2 &:= q + (1+\sqrt{2})q^2 + (1-\sqrt{2})q^3 + (2\sqrt{2}+1)q^4 + q^5 - q^6 + (\sqrt{2}+3)q^8 - 2\sqrt{2}q^9\\
&\qquad + (1+\sqrt{2})q^{10} + O(q^{11}) \in S_2(\Gamma_0(5\cdot 7^2) \cap \Gamma_1(7), \overline{\mathbb{Q}}).
\end{aligned}$$

When f is a cusp form defined over a quadratic field, let f^c be its Galois conjugate cusp form. For brevity, we write $\mathrm{pr} := \mathrm{pr}_{245/35}$, and we omit any application of the B_1-operator, since it acts as the identity on q-expansions. This leads to the following real twist orbit spaces of modular forms:

$$\begin{aligned}
O_1^+ &:= \mathrm{Span}\{f_{49}, f_{49}\otimes\chi^2, f_{49}\otimes\chi^4, f_{49}|B_5, (f_{49}\otimes\chi^2)|B_5, (f_{49}\otimes\chi^4)|B_5\},\\
O_2^+ &:= \mathrm{Span}\{f_{35}, f_{35}\otimes\chi^2, f_{35}\otimes\chi^4, f_{35}|B_7\},\\
O_3^+ &:= \mathrm{Span}\{f_{35}\otimes\chi, f_{35}\otimes\chi^3, f_{35}\otimes\chi^5\},\\
O_4^+ &:= \mathrm{Span}\{g_{35}, g_{35}\otimes\chi^2, g_{35}\otimes\chi^4, g_{35}|B_7\}\\
&\quad \text{and } O_4^{c,+} := \mathrm{Span}\{g_{35}^c, g_{35}^c\otimes\chi^2, g_{35}^c\otimes\chi^4, g_{35}^c|B_7\},\\
O_5^+ &:= \mathrm{Span}\{g_{35}\otimes\chi, g_{35}\otimes\chi^3, g_{35}\otimes\chi^5\} \text{ and } O_5^{c,+} := \mathrm{Span}\{g_{35}^c\otimes\chi, g_{35}^c\otimes\chi^3, g_{35}^c\otimes\chi^5\},\\
O_6^+ &:= \mathrm{Span}\{f_0, f_0\otimes\chi^2, f_0\otimes\chi^4\},\\
O_7^+ &:= \mathrm{Span}\{f_0\otimes\chi, f_0\otimes\chi^3, f_0\otimes\chi^5\},\\
O_8^+ &:= \mathrm{Span}\{f_1, f_1\otimes\chi^2, f_1\otimes\chi^4\} \text{ and } O_8^{c,+} := \mathrm{Span}\{f_1^c, f_1^c\otimes\chi^2, f_1^c\otimes\chi^4\},\\
O_9^+ &:= \mathrm{Span}\{f_1\otimes\chi, f_1\otimes\chi^3, f_1\otimes\chi^5\} \text{ and } O_9^{c,+} := \mathrm{Span}\{f_1^c\otimes\chi, f_1^c\otimes\chi^3, f_1^c\otimes\chi^5\},\\
O_{10}^+ &:= \mathrm{Span}\{f_2, (f_2\otimes\chi^2)|\mathrm{pr}, (f_2\otimes\chi^4)|\mathrm{pr}, (f_2\otimes\chi^2)|\mathrm{pr}|B_7, (f_2\otimes\chi^4)|\mathrm{pr}|B_7\} \text{ and}\\
O_{10}^{c,+} &:= \mathrm{Span}\{f_2^c, (f_2^c\otimes\chi^2)|\mathrm{pr}, (f_2^c\otimes\chi^4)|\mathrm{pr}, (f_2^c\otimes\chi^2)|\mathrm{pr}|B_7, (f_2^c\otimes\chi^4)|\mathrm{pr}|B_7\},
\end{aligned}$$

$$O_{11}^{+} := \mathrm{Span}\{f_2 \otimes \chi, f_2 \otimes \chi^3, f_2 \otimes \chi^5\} \text{ and } O_{11}^{c,+} := \mathrm{Span}\{f_2^c \otimes \chi, f_2^c \otimes \chi^3, f_2^c \otimes \chi^5\}.$$

By counting dimensions, we see that these are all of the real twist orbit spaces. These computations were done in the "space of cusp forms" in `Sage`, but note that the underlying calculations do happen in the space of modular symbols.

For each $i \in \{1, \ldots, 11\}$, denote by V_i^+ the sum of O_i^+ and (if it exists) $O_i^{c,+}$.

2.4.4 Computations with modular symbols

We ask `Sage` to compute the 122-dimensional space $H_1(X_{\Gamma_0(5\cdot 7^2)\cap\Gamma_1(7)}, \mathbb{Q})$. Given a basis for this space, we ask for the matrix of the operator induced by J, and we determine the $+1$-eigenspace. Consider an eigenform $f \in S_2(\Gamma_0(5\cdot 7^2)\cap\Gamma_1(7), \overline{\mathbb{Q}})$. As T_p commutes with J, we can use Lemma 2.2.8 to determine the modular symbol $\gamma \in H_1(\Gamma_0(5\cdot 7^2)\cap\Gamma_1(7), \overline{\mathbb{Q}})^+$ such that $\gamma = \gamma_f$ up to a constant multiple. In practice, it sufficed for us to compute eigenvectors in $H_1(\Gamma_0(5\cdot 7^2)\cap\Gamma_1(7), \overline{\mathbb{Q}})^+$ for the T_2- and T_3-operators only: when the intersection of the kernels of $T_2 - \overline{a}_2(f)$ and $T_3 - \overline{a}_3(f)$ on $H_1(\Gamma_0(5\cdot 7^2)\cap\Gamma_1(7), \overline{\mathbb{Q}})^+$ is 1-dimensional, its elements must be multiples of γ_f. We thus obtain explicit eigensymbols

$$\mu_0 = \alpha_0\gamma_{f_0},\ \mu_1 = \alpha_1\gamma_{f_1},\ \mu_2 = \alpha_2\gamma_{f_2},\ \mu_{35} = \alpha_{35}\gamma_{f_{35}},\ \mu_{49} = \alpha_{49}\gamma_{f_{49}},\ \nu_{35} = \beta_{35}\gamma_{g_{35}},$$

where β_{35} and all α_i are non-zero but unknown. However, within twist orbit spaces these constants are also irrelevant.

Moreover, we recall that $R_{\chi^2}(\gamma_f) = g(\overline{\chi}^2)\gamma_{f\otimes\overline{\chi}^2}$ and $[\Gamma_0(N) : \Gamma_0(M)]\gamma_{f|B_d} = \mathrm{Tr}_d^{N/L}(\gamma_f)$, where the action of R_{χ^2}, Tr_7 and Tr_5, as well as that of $\pi_{245/35}$ and $\pi_{235/49}$, on $H_1(\Gamma_0(5\cdot 7^2)\cap\Gamma_1(7), \overline{\mathbb{Q}})$ can be determined explicitly. To compute the coset representatives needed for the $\mathrm{Tr}_d^{N/L}$ operators, we used an algorithm of Stein [Ste00, Algorithm 2.20]. We thus explicitly compute the real twist orbit spaces on the modular symbols side.

The next step is to conjugate g_0, ϕ_7 and w_5 by γ_7 and compute their action on $H_1(\Gamma_0(5\cdot 7^2)\cap\Gamma_1(7), \overline{\mathbb{Q}})$. This can be done in `Sage` via built-in functions. We intersect the different fixed-spaces with the real twist orbit spaces to obtain the desired basis of fixed modular symbols. For brevity reasons, we do not display all of these here, but we give two examples: we find that

$$4\left(\mu_{35} - \mathrm{Tr}_7(\mu_{35})\right) + \left(\frac{6\zeta_3}{7} + \frac{2}{7}\right) R_{\overline{\chi}^2}(\mu_{35}) + \left(\frac{36}{343}\zeta_3 - \frac{2}{343}\right) R_{\overline{\chi}^4}(\mu_{35})$$

is in $(H_{\mathbb{C}}(\Gamma_0(5\cdot 7^2)\cap\Gamma_1(7))^+)^{g_0, w_5\cdot\phi_7}$ and that

$$\begin{aligned}
\left(\frac{2}{21}\sqrt{2} + \frac{8}{21}\right)\mu_2 &+ \left(\left(\frac{10}{1029}\zeta_3 - \frac{2}{343}\right)\sqrt{2} + \frac{40}{1029}\cdot\zeta_3 - \frac{8}{343}\right) R_{\overline{\chi}^2}(\mu_2) \\
&+ \left(\left(\frac{16}{7203}\zeta_3 + \frac{10}{7203}\right)\sqrt{2} + \frac{64}{7203}\zeta_3 + \frac{40}{7203}\right) R_{\overline{\chi}^4}(\mu_2) \\
&+ \left(\left(-\frac{2}{147}\zeta_3 - \frac{4}{147}\right)\sqrt{2} - \frac{20}{1029}\zeta_3 - \frac{16}{1029}\right)\frac{B_7\mathrm{pr}R_{\overline{\chi}^4}(\mu_2)}{7} \\
&+ \left(\left(\frac{46}{1029}\zeta_3 + \frac{188}{1029}\right)\sqrt{2} - \frac{68}{1029}\zeta_3 + \frac{80}{1029}\right)\frac{B_7\mathrm{pr}R_{\overline{\chi}^2}(\mu_2)}{7}
\end{aligned}$$

is in $H_{\mathbb{C}}(\Gamma_0(5\cdot 7^2)\cap\Gamma_1(7))^{g_0,\phi_7}$. Finally, we determine the $\mathbb{C}$-linear action of B on these bases of fixed modular symbols, one real twist orbit at a time. We also find a matrix for the $\mathbb{Q}$-linear action of $\sigma_4:\ \zeta_7\mapsto\zeta_7^4$ and J on the corresponding cusp forms. We choose to translate the actions of σ_4 and J to a $\mathbb{Q}$-linear action on modular symbols (rather than translating the action of B to modular forms), and compose σ_4 and J with B. This yields two $\mathbb{Q}$-linear maps on each fixed subspace of a real twist orbit space, and we determine the $\mathbb{Q}$-linear subspace fixed by these two maps. Translating this back to modular forms, we obtain the desired cusp forms.

2.4.5 The cusp forms

Let $\beta_7=\zeta_7+\zeta_7^{-1}$. On each of the curves, denote by $q=e^{2\pi i\tau/7}$ a uniformiser at (the image of) ∞. The space $H^0(X(\mathrm{b5},\mathrm{ns7})/w_5,\Omega^1)$ has a basis of 1-forms with q-expansions $h_1(q)\frac{\mathrm{d}q}{q}$ and $h_2(q)\frac{\mathrm{d}q}{q}$, where

$$\begin{aligned}
h_1 :=& \left(10\beta_7^2+2\beta_7-16\right)q+\left(4\beta_7^2+12\beta_7-12\right)q^2+\left(-6\beta_7^2-4\beta_7+18\right)q^3\\
&+\left(8\beta_7^2+10\beta_7-10\right)q^5+\left(-8\beta_7^2+4\beta_7+24\right)q^6+O\left(q^8\right)\in V_8^+,\\
h_2 :=& \left(-6\beta_7^2-4\beta_7+4\right)q+\left(-8\beta_7^2-10\beta_7+10\right)q^2+\left(-2\beta_7^2-6\beta_7+6\right)q^3\\
&+\left(-2\beta_7^2-6\beta_7+6\right)q^5+\left(2\beta_7^2+6\beta_7+8\right)q^6+O\left(q^8\right)\in V_8^+.
\end{aligned}$$

The space $H^0(X(\mathrm{b5},\mathrm{ns7}),\Omega^1)$ has a basis of 1-forms $f(q)\frac{\mathrm{d}q}{q}$, where $f(q)$ is one of:

$$\begin{aligned}
&h_1,\ h_2,\in V_8^+,\\
&\left(-2\beta_7^2-6\beta_7+6\right)q+\left(-16\beta_7^2+8\beta_7+48\right)q^2+\left(-12\beta_7^2-8\beta_7+8\right)q^3\\
&\quad+\left(42\beta_7^2+28\beta_7-28\right)q^4+\left(-4\beta_7^2+2\beta_7+12\right)q^5+\left(2\beta_7^2+6\beta_7-6\right)q^6\\
&\quad+\left(-28\beta_7^2+28\beta_7+56\right)q^7+O\left(q^8\right)\in V_{10}^+,\\
&\left(-3\beta_7^2-9\beta_7+9\right)q+\left(-10\beta_7^2+5\beta_7+30\right)q^2+\left(3\beta_7^2+2\beta_7-2\right)q^3\\
&\quad+\left(21\beta_7^2+14\beta_7-14\right)q^4+\left(-6\beta_7^2+3\beta_7+18\right)q^5+\left(3\beta_7^2+9\beta_7-9\right)q^6\\
&\quad+\left(21\beta_7+7\right)q^7++O\left(q^8\right)\in V_{10}^+,\\
&\left(10\beta_7^2+2\beta_7-16\right)q+\left(-4\beta_7^2-12\beta_7+12\right)q^2+\left(-10\beta_7^2+12\beta_7+30\right)q^3+\\
&\quad\left(-8\beta_7^2-10\beta_7+10\right)q^5+\left(32\beta_7^2+12\beta_7-40\right)q^6+O\left(q^8\right)\in V_9^+,\\
&\left(6\beta_7^2+4\beta_7-4\right)q+\left(-8\beta_7^2-10\beta_7+10\right)q^2+\left(-6\beta_7^2+10\beta_7+18\right)q^3\\
&\quad+\left(-2\beta_7^2-6\beta_7+6\right)q^5+\left(22\beta_7^2+10\beta_7-24\right)q^6+O\left(q^8\right)\in V_9^+.
\end{aligned}$$

The space $H^0(X(\mathrm{b5},\mathrm{e7})/w_5\phi_7,\Omega^1)$ has a basis of 1-forms $f(q)\frac{\mathrm{d}q}{q}$, where $f(q)$ is one of:

$$\begin{aligned}
&\left(\beta_7^2-\beta_7-2\right)q+\left(-2\beta_7^2-\beta_7+3\right)q^2+\left(-\beta_7^2-2\beta_7+1\right)q^4\\
&\quad+\left(10\beta_7^2+5\beta_7-15\right)q^5+O\left(q^8\right)\in V_1^+,\\
&\left(-14\beta_7^2-14\beta_7+28\right)q+\left(-7\beta_7-7\right)q^2+\left(-7\beta_7^2+7\right)q^3+\left(35\beta_7^2-35\right)q^4\\
&\quad+\left(14\beta_7+14\right)q^5+\left(56\beta_7^2+56\beta_7-112\right)q^6+56q^7+O\left(q^8\right)\in V_4^+,\\
&\left(7\beta_7+7\right)q^2+\left(-7\beta_7^2+7\right)q^3+\left(-7\beta_7^2+7\right)q^4+O\left(q^8\right)\in V_4^+,
\end{aligned}$$

$$\left(-\beta_7^2+\beta_7+2\right)q+\left(-4\beta_7^2-2\beta_7+6\right)q^2+\left(3\beta_7^2+6\beta_7-3\right)q^3$$
$$+\left(-2\beta_7^2-4\beta_7+2\right)q^4+\left(2\beta_7^2+\beta_7-3\right)q^5+\left(-6\beta_7^2+6\beta_7+12\right)q^6+O\left(q^8\right)\in V_6^+,$$
$$h_1,\ h_2\in V_8^+,$$
$$\left(2\beta_7^2+2\beta_7+2\right)q+\left(-4\beta_7+8\right)q^2+\left(-6\beta_7^2+24\right)q^4+\left(-2\beta_7+4\right)q^5$$
$$+\left(-2\beta_7^2-2\beta_7-2\right)q^6+\left(12\beta_7^2-20\right)q^7+O\left(q^8\right)\in V_{10}^+,$$
$$\left(\beta_7^2+\beta_7+1\right)q+\left(-3\beta_7+6\right)q^2+\left(\beta_7^2-4\right)q^3+\left(-5\beta_7^2+20\right)q^4$$
$$+\left(-\beta_7+2\right)q^5+\left(-\beta_7^2-\beta_7-1\right)q^6+\left(12\beta_7^2+3\beta_7-19\right)q^7+O\left(q^8\right)\in V_{10}^+.$$

Finally, the space $H^0(X(\mathrm{b5},\mathrm{e7})/w_5,\Omega^1)$ has a basis of 1-forms $f(q)\frac{\mathrm{d}q}{q}$, where $f(q)$ is in the set

$$\left(-\beta_7^2+\beta_7+2\right)q+\left(2\beta_7^2+\beta_7-3\right)q^2+\left(\beta_7^2+2\beta_7-1\right)q^4$$
$$+\left(10\beta_7^2+5\beta_7-15\right)q^5+O\left(q^8\right)\in V_1^+,$$
$$\left(-7\beta_7^2-7\beta_7+14\right)q+\left(7\beta_7^2-7\right)q^3+\left(-14\beta_7^2+14\right)q^4$$
$$+\left(-7\beta_7-7\right)q^5-28q^7+O\left(q^8\right)\in V_2^+,$$
$$h_1,\ h_2\in V_8^+,$$
$$\left(-\beta_7^2+\beta_7+2\right)q+\left(-4\beta_7^2-2\beta_7+6\right)q^2+\left(-3\beta_7^2-6\beta_7+3\right)q^3+\left(-2\beta_7^2-4\beta_7+2\right)q^4$$
$$+\left(-2\beta_7^2-\beta_7+3\right)q^5+\left(6\beta_7^2-6\beta_7-12\right)q^6+O\left(q^8\right)\in V_7^+.$$

For each of the final three curves, these cusp forms satisfy the equations as displayed in Theorem 2.4.1, where the variable X_i corresponds to the $(i+1)$th displayed cusp form.

2.4.6 The map $X(\mathrm{b5},\mathrm{ns7})\to X(\mathrm{ns7})$

To determine $X(\mathrm{b5},\mathrm{ns7})\to X(\mathrm{ns7})$, we first use Chen's j-map (2.8) to find the q-expansion of a Hauptmodul n_7 on $X(\mathrm{ns7})$, by solving the equation

$$j(q^7)=j_{\mathrm{ns7}}(n_7(q)).$$

(Note the 7th power of q because we defined q as $e^{2\pi i\tau/7}$.) This yields

$$\eta_7(q)=-\beta_7^2-\beta_7+1+(-4\beta_7^2-\beta_7+11)q+(-18\beta_7^2-11\beta_7+38)q^2$$
$$+(-53\beta_7^2-26\beta_7+124)q^3+(-171\beta_7^2-102\beta_7+370)q^4+O(q^5).$$

Then we apply the method outlined in Section 1.2.2.

Chapter 3

Quadratic, cubic and quartic points on modular curves using Chabauty

The curves $X_0(N)$ for $N \in \{37, 43, 53, 57, 61, 65, 67, 73\}$ are exactly those $X_0(N)$ of genus $g \in \{2, \ldots, 5\}$ with infinite Mordell–Weil group $J_0(N)(\mathbb{Q})$. In this chapter we determine their quadratic points using (for $N \neq 37$) Siksek's (relative) symmetric Chabauty method. The quadratic points on the curves $X_0(N)$ of these genera with *finite* Mordell–Weil group were studied by Bruin and Najman [BN15] and Özman and Siksek [OS19], when $X_0(N)$ is hyperelliptic and non-hyperelliptic respectively. We thus complement their work. Furthermore, we prove a more general Chabauty method suitable for studying points of higher degrees. We then apply this, in combination with a Mordell–Weil sieve, to determine the cubic points on $X_0(N)$ for $N \in \{53, 57, 61, 65, 65, 73\}$ and the quartic points on $X_0(65)$. This set of quartic points is infinite, as are multiple sets of quadratic points; in these cases, we determine the finite set of isolated points. All points are listed in Section 3.4, together with their j-invariants; we also decide whether these j-invariants correspond to $\mathbb{Q}$-curves or elliptic curves with CM. An important part of our computations is the study of the Mordell–Weil groups of the Jacobians of these modular curves; we provide subgroups with quotient group of exponent at most 2 in Section 3.4.

N	37	43	53	61	57	65	67	73
g	2	3	4	4	5	5	5	5
r	1	1	1	1	1	1	2	2
d	2	2	2, 3	2, 3	2, 3	2, 3, 4	2, 3	2, 3

Table 3.1: The values of N and d for which we study the degree d points on $X_0(N)$, listed with the genus g of $X_0(N)$ and the rank r of the Mordell–Weil group $J_0(N)(\mathbb{Q})$.

This chapter is a combination of the articles [Box21c] and [BGG21].

3.1 Introduction

3.1.1 Interest in degree d points

Let N be a positive integer. In a celebrated paper [Maz77], Mazur determined exactly which modular curves $X_1(N)$ admit non-cuspidal rational points, thereby classifying the groups occurring as rational torsion subgroups of elliptic curves over $\mathbb{Q}$. For prime values of N, moreover, he repeated this for $X_0(N)$ [Maz78], a result later extended to composite levels by Kenku [Ken81]. Since this work of Mazur, there has been great interest in obtaining similar results for points of low degree d.

For $d = 2$, Kamienny [Kam92] and Kenku–Momose [KM88] indeed determined the integers N such that $X_1(N)$ admits a non-cuspidal point of degree d. More recently the same was established for $d = 3$ by Derickx, Etropolski, Van Hoeij, Morrow and Zureick-Brown [DEv$^+$20], after partial results of Parent [Par99] and others. Moreover, Derickx, Kamienny, Stein and Stoll achieved this for prime values of N for $d \in \{4, 5, 6\}$ [DKSS17], [Der16]. We also mention Merel's uniform boundedness theorem [Mer96], which proves the existence of an upper bound B_d such that $X_1(N)$ has no non-cuspidal degree d points for primes $N \geq B_d$. Many of the aforementioned authors studied the degree d points on several explicit curves $X_1(N)$. Of particular difficulty were the curves admitting a Mordell–Weil group $J_1(N)(\mathbb{Q})$ of positive rank, such as $X_1(65)$ in [DEv$^+$20].

Derickx et al. [DEv$^+$20] make use of the map $X_1(65) \to X_0(65)$ and study the cubic points on $X_0(65)$ in its image using the "formal immersion criterion" developed in [DKSS17]. Our joint work with Gajović and Goodman started with a question of David Zureick-Brown at the 2020 Arizona Winter School: can you determine the entire finite set of cubic points on $X_0(65)$? Indeed we can. On top of this, we provide a streamlined method for studying the degree d points on modular curves X of genus g admitting a Mordell–Weil group $J(X)(\mathbb{Q})$ of positive rank r, provided $r < g - (d - 1)$.

Similar results have also proved indispensible in the study of modularity of elliptic curves. Derickx, Najman and Siksek [DNS20] used the method of [DKSS17] to determine the cubic points on the modular curve $X(\mathrm{b5}, \mathrm{ns7})$ (of genus 6 and Mordell–Weil rank 2). They use this to show that all elliptic curves over totally real cubic fields are modular. In Chapter 4, we use the Chabauty method developed in this chapter to study the quartic points on $X(\mathrm{b5}, \mathrm{ns7})$, as part of our proof that all elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular.

3.1.2 Sources of (infinitely many) points

The low degree points on $X_0(N)$ are naturally more abundant than on $X_1(N)$, which complicates their study. Especially as the degree d increases, infinite families of degree d points appear.

For a curve X over a number field K, recall that we denote by $X^{(d)}$ its dth symmetric power. Also recall that the K-rational points on $X^{(d)}$ are exactly the K-rational effective degree d divisors on X, and that the $\mathrm{Gal}(\overline{K}/K)$-orbit of each point $P \in X$ defined over a degree d extension of K gives rise to such a divisor. By studying the K-rational

points on $X^{(d)}$ we can thus study the L-rational points on X for all degree d extensions L/K simultaneously.

An important tool to study $X^{(d)}$ is the Abel–Jacobi map introduced in Section 1.2.1, defined in terms of a degree d divisor D_0. Explicitly, this is given by

$$\iota\colon X^{(d)} \to J(X),\ D \mapsto [D - D_0].$$

So when does X/K have infinitely many points of degree d over K? Certainly when there is a degree d map $\rho : X \to \mathbb{P}^1$, as the inverse images of points in $\mathbb{P}^1(K)$ provide such an infinite set. This happens for example for $d = 2$ when X is a hyperelliptic (e.g. $X = X_0(37)$). More generally, suppose there is a map $\rho : X \to C$ of degree d_0 to a curve C/K such that

- $C^{(\ell)}(K)$ is infinite for some $\ell \in \mathbb{Z}_{\geq 1}$ satisfying $d_0 \cdot \ell \leq d$, and
- if $d_0 \cdot \ell < d$, there exists $P \in X^{(d-d_0\ell)}(K)$.

Then the infinite set

$$P + \rho^* C^{(\ell)}(K)$$

is a subset of $X^{(d)}(K)$. Note that ι maps this set into a translate of the abelian subvariety $\rho^*(J(C))$ of $J(X)$. This happens for $X = X_0(65)$ and $d = 3$. There is a degree 2 map $\rho\colon X_0(65) \to X_0^+(65)$ to an elliptic curve of rank 1, and each cusp $c \in X_0(65)(\mathbb{Q})$ thus yields an infinite subset $c + \rho^* X_0^+(65)(\mathbb{Q}) \subset X_0(65)^{(3)}(\mathbb{Q})$. Nonetheless, the set of cubic points on $X_0(65)$ is finite: to determine them, we need to be able to deal with such infinite sets.

Define $P \in X^{(d)}(K)$ to be an *isolated point* when it is neither in the inverse image of $\mathbb{P}^1(K)$ under a degree d map $X \to \mathbb{P}^1$, nor does $\iota(P)$ lie in a translate of a positive rank abelian subvariety of $J(X)$ contained in $\iota(X^{(d)})$. Recently, Bourdon, Ejder, Liu, Odumodu and Viray [BEL+19, Theorem 4.2] have shown that

(i) X has infinitely many points of degree d over K if and only if $X^{(d)}(K)$ contains a non-isolated point, and

(ii) there are finitely many isolated points in $X^{(d)}(K)$.

This result provides a road map for studying $X^{(d)}(K)$: first describe each infinite set, then determine the finite set of isolated points. This is what we do for the modular curves listed in Table 3.1 by developing a generalised symmetric Chabauty method.

3.1.3 Symmetric Chabauty

Chabauty's method is, classically, a method for effectively computing the rational points on a curve in the special case when the rank r of its Mordell–Weil group is strictly smaller than its genus g. The effectiveness is due to Coleman [Col85a], who realised that Chabauty's finiteness proof [Cha41] could be made effective using the machinery of locally analytic p-adic functions.

While nowadays many focus on weakening the $r < g$ condition in Chabauty's method via non-abelian generalisations (see e.g. [Kim05] and [BBB$^+$]), the reach of the method of Chabauty is still being increased. After partial results of Klassen [Kla93], Siksek [Sik09] extended Coleman's ideas to obtain an effective method for computing the K-rational points (when finite) on the dth symmetric powers of curves over any number field K, provided the stronger condition

$$r < g - (d - 1) \tag{3.1}$$

is satisfied. A similar result was obtained by Derickx, Kamienny, Stein and Stoll [DKSS17] using the theory of formal immersions, with strong consequences mentioned in Section 3.1.1.

Furthermore, Siksek [Sik09] developed a relative version of his symmetric Chabauty method, which can be used to determine the isolated points on $X^{(d)}$ if the infinite set consists entirely of pullbacks. To be precise, given a map $\rho : X \to C$ of curves over K of degree d, Siksek's relative Chabauty method can determine $X^{(d)}(K) \setminus \rho^* C(K)$ if that consists entirely of isolated points. We use this method to describe the quadratic points on $X_0(N)$ for $N \in \{43, 53, 57, 61, 65, 67, 73\}$. For $d > 2$, however, infinite subsets of the form $P + \rho^* C^{(\ell)}(\mathbb{Q})$ with $P \neq 0$ and $\ell > 1$ do appear, and we require a stronger Chabauty method to deal with such subsets.

We develop such a "partially relative symmetric Chabauty method" by generalising Siksek's ideas. Our method has the potential to determine the isolated degree d points on a curve X satisfying (3.1) if the infinite sets are of the form

$$P + \rho_1^* C_1^{(\ell_1)}(K) + \ldots + \rho_n^* C_n^{(\ell_n)}(K),$$

where $P \in X^{(\ell_0)}(K)$ and $\rho_i \ : X \to C_i$ are maps of degree d_i for $i \in \{1, \ldots, n\}$, such that $\ell_0 + \ell_1 d_1 + \ldots + \ell_n d_n = d$. The result that makes this possible is Theorem 3.2.6. However, there remain points on $X_0(57)^{(3)}$ and $X_0(73)^{(3)}$ which cause further difficulty (see Example 3.2.23). We treat these novelties by appealing to a "higher order" Chabauty theorem: Theorem 3.2.24.

3.1.4 An overview of the results

Each modular curve $X_0(N)$ admits an Atkin–Lehner involution w_N (c.f. Example 1.1.7), giving rise to a degree 2 map $\rho_N \colon X_0(N) \to X_0^+(N)$, where $X_0^+(N) = X_0(N)/w_N$.

- For $N = 43$, the quotient $X_0^+(43)$ is a rank 1 elliptic curve, and we determine the finite set $X_0(43)^{(2)}(\mathbb{Q}) \setminus \rho_{43}^* X_0^+(43)(\mathbb{Q})$ using Siksek's symmetric Chabauty method.

- For $N = 53$ and $N = 61$, the quotient $X_0^+(N)$ is also a rank 1 elliptic curve. The two cusps c_0, $c_\infty \in X_0(N)(\mathbb{Q})$ are its only two rational points. We show that $X_0(N)^{(2)}(\mathbb{Q}) = \rho_N^* X_0^+(N)(\mathbb{Q}) \cup \{2c_0, 2c_\infty\}$ using Siksek's relative symmetric

Chabauty method, and use Theorem 3.2.6 to determine the finite set

$$X_0(N)^{(3)}(\mathbb{Q}) \setminus \left((c_0 + \rho_N^* X_0^+(N)(\mathbb{Q})) \cup (c_\infty + \rho_N^* X_0(N)(\mathbb{Q}))\right).$$

- For $N = 57$, the quotient $X_0^+(57)$ is hyperelliptic curve of genus 2 whose Mordell–Weil group $J_0^+(57)(\mathbb{Q})$ has rank 1. We determine the finite set $X_0(57)^{(2)}(\mathbb{Q})$ using Siksek's symmetric Chabauty method, and the finite set $X_0(57)^{(3)}(\mathbb{Q})$ using Theorems 3.2.6 and 3.2.24. This is, together with $X_0(73)$, one of the two isolated cases where the higher order Chabauty theorem 3.2.24 is required. We note that $X_0(57)$ also satisfies (3.1) for $d = 4$. However, by the Existence Theorem in Brill–Noether Theory [ACGH85, Chapter V, p. 206], genus 5 curves have infinitely many degree four maps to $\mathbb{P}^1$, making it infeasible to study the quartic points on $X_0(57)$.

- For $N = 65$, the quotient $X_0^+(65)$ is again an elliptic curve of rank 1. Having genus 5, (3.1) is satisfied for $d \leq 4$. Here, unlike for $N = 57$, every degree 4 map to $\mathbb{P}^1$ factors via ρ_{65}, allowing us to study the quartic points relative to ρ_{65}. This curve has four rational cusps. We show that $X_0(65)^{(2)} \setminus \rho_{65}^* X_0^+(65)(\mathbb{Q})$ consists entirely of sums of two cusps, and use Theorem 3.2.6 to determine the finite sets

$$X_0(65)^{(3)}(\mathbb{Q}) \setminus \bigcup_{c \text{ cusp}} (c + \rho_{65}^* X_0^+(65)(\mathbb{Q}))$$

and

$$X_0(65)^{(4)}(\mathbb{Q}) \setminus \left(\rho_{65}^* X_0^+(65)^{(2)}(\mathbb{Q}) \cup \left(X_0(65)^{(2)}(\mathbb{Q}) + \rho_{65}^* X_0^+(65)(\mathbb{Q})\right)\right).$$

- For $N = 67$ and $N = 73$, the quotient $X_0^+(N)$ is a hyperelliptic curve of genus 2 whose Mordell–Weil group $J_0^+(N)(\mathbb{Q})$ has rank 2. The only rational points on $X_0(73)$ are the two cusps, whereas $X_0(67)$ has exactly one non-cuspidal rational point. We use Siksek's relative symmetric Chabauty method to determine $X_0(N)^{(2)}(\mathbb{Q}) \setminus \rho_N^* X_0^+(N)(\mathbb{Q})$. We note that $X_0^+(N)(\mathbb{Q})$ is finite, but cannot be determined using abelian Chabauty because the rank equals the genus. We do obtain a complete list of the quadratic points on $X_0(N)$ thanks to Balakrishnan et al. [BBB+], who determined $X_0^+(67)(\mathbb{Q})$ and $X_0^+(73)(\mathbb{Q})$ using quadratic Chabauty. We also determine $X_0(N)^{(3)}(\mathbb{Q}) \setminus \bigcup_{Q \in X_0(N)(\mathbb{Q})} \left(Q + \rho_N^* X_0^+(N)(\mathbb{Q})\right)$ using Theorem 3.2.6 for $N = 67$ (c.f. Example 3.2.12) and, for $N = 73$, Theorem 3.2.24 (c.f. Example 3.2.23).

- Finally, $X_0(37)$ is a special case because it is hyperelliptic, while w_{37} is not the hyperelliptic involution. In fact, $X_0^+(37)$ is a rank 1 elliptic curve. We describe the multitude of quadratic points on $X_0(37)$ separately in Section 3.5.

In Section 3.4, we display models for each of these curves, as well as generators for (finite index subgroups of) their Mordell–Weil groups and the finite point sets mentioned above. First, we develop our general symmetric Chabauty method in Section 3.2, after which we discuss its application to modular curves in Section 3.3.

The `Magma` [BCP97] code to verify all computations made in this chapter can be found at

`https://github.com/joshabox/quadraticpoints/`

and

`https://github.com/joshabox/cubicpoints/` .

3.2 A general symmetric Chabauty theorem

In this section we present a common generalisation of Theorems 3.2 and 4.3 in [Sik09], which are Chabauty-type theorems for computing K-rational points on symmetric powers of curves.

Before this, we give an overview of Siksek's Chabauty method.

3.2.1 Uniformisers and differentials

Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers R and residue field k. Consider a curve X/K together with a minimal proper regular model $\mathcal{X}/R$ for X. We write $\widetilde{X}$ for the special fibre of $\mathcal{X}$, and similarly denote reductions of objects associated to $\mathcal{X}$ with a tilde. Denote by $\mathcal{O}_S$ the sheaf of functions on a scheme S. For a sheaf $\mathcal{F}$ on S, we denote by $\mathcal{F}_s$ its stalk at s. When A is a discrete valuation ring (DVR), we denote by $\widehat{A}$ its completion. Finally, when $s \in S$ is such that $\mathcal{O}_{S,s}$ is a DVR, $U \subset S$ is an open subset containing s and $\mathcal{F}$ is an $\mathcal{O}_S$-module, we denote by loc_s the map $\mathcal{F}(U) \to \mathcal{F}_s$. For $x \in X^{(d)}(K)$ and $y \in \widetilde{X}^{(d)}(k)$, we denote by $D(x)$ and $D(y)$ the points in $X^{(d)}(K)$ reducing to $\widetilde{x}$ and y respectively.

When $x \in X$ is non-singular, a uniformiser $t \in \widehat{\mathcal{O}}_{X,x}$ is called a *local coordinate* at $x \in X$. When t also reduces to a uniformiser in the reduction $\widehat{\mathcal{O}}_{\widetilde{X},\widetilde{x}}$, we say that it is a *well-behaved local coordinate* or *well-behaved uniformiser*. This just means that the maximal ideal of $\widehat{\mathcal{O}}_{\mathcal{X},\widetilde{x}}$ is generated by t and p as an R-module. The following facts can be found for example in [LT02]. When t is a well-behaved local coordinate at x, we can evaluate t at points in the residue disc $D(x)$ of x, yielding a bijection between $D(x)$ and the maximal ideal of R.

Denote by $\Omega_{X/K}$ and $\Omega_{\mathcal{X}/R}$ (sometimes abbreviated to Ω_X, resp. $\Omega_{\mathcal{X}}$, or simply Ω) the sheafs of regular differentials on X and $\mathcal{X}$ respectively. A choice of uniformiser $t \in \widehat{\mathcal{O}}_{X,x}$ gives rise to the identifications $\widehat{\mathcal{O}}_{X,x} = K[\![t]\!]$ and $\widehat{\Omega}_{X,x} = K[\![t]\!]\mathrm{d}t$. If t is moreover well-behaved, we have $\widehat{\mathcal{O}}_{\mathcal{X},\widetilde{x}} = R[\![t]\!]$ and $\widehat{\Omega}_{\mathcal{X},\widetilde{x}} = R[\![t]\!]\mathrm{d}t$.

Now consider $\omega \in H^0(X, \Omega_{X/K})$. Then $H^0(\mathcal{X}, \Omega_{\mathcal{X}/R})$ is a lattice in $H^0(X, \Omega_{X/K})$, so after multiplication by a constant in R, we may assume that $\omega \in H^0(\mathcal{X}, \Omega_{\mathcal{X}/R})$. In sum, given a well-behaved uniformiser s at a point $Q \in X(K)$, we can write

$$\mathrm{loc}_Q(\omega) = \sum_{n=0}^{\infty} a_n s^n \mathrm{d}s \text{ with } a_n \in R \text{ for all } n. \tag{3.2}$$

Consider any point $P_0 \in X(\overline{K})$.

Lemma 3.2.1. *The map $\iota : X \to J(X),\ P \mapsto [P - P_0]$ induces an isomorphism*

$$\iota^* :\ H^0(J(X), \Omega_{J(X)/K}) \simeq H^0(X, \Omega_{X/K})$$

of global differential forms independent of the choice of P_0.

Proof. See e.g. [Sik09, Proposition 2.1]. □

We shall thus use ι^* to pass between these two spaces.

Now suppose that we have a map $\rho : X \to C$ between two curves over K. We obtain a pushforward map $\rho_* :\ J(X) \to J(C)$ and pullback map $\rho^* :\ J(C) \to J(X)$, leading to a decomposition up to isogeny

$$J(X) \sim J(C) \times A,$$

where $A \subset J(X)$ is an abelian subvariety. Denote by π_A the map $J(X) \to A$. We also obtain a pushforward, or "trace map",

$$\mathrm{Tr} :\ H^0(X, \Omega_{X/K}) \to H^0(C, \Omega_{C/K}).$$

Lemma 3.2.2. *We have*

(i) $H^0(X, \Omega_{X/K}) = \rho^* H^0(C, \Omega_{C/K}) \oplus \mathrm{Ker}(\mathrm{Tr})$, *and*

(ii) $\iota^* \pi_A^* H^0(A, \Omega_{A/K}) = \mathrm{Ker}(\mathrm{Tr})$.

Proof. Part (i) follows from surjectivity of the trace map. For part (ii) it suffices to compare dimensions and to check that $\iota^* \pi_A^* H^0(A, \Omega_{A/K}) \subset \mathrm{Ker}(\mathrm{Tr})$. □

3.2.2 Coleman integration

We consider the notation from the previous section. Again let K be a finite extension of $\mathbb{Q}_p$. Also let B/K be any abelian variety. In [Col85b, Section II], Coleman defines a pairing, now called *Coleman integration*:

$$H^0(B, \Omega_{B/K}) \times B(K) \to K,\ \ (\omega, P) \mapsto \int_P \omega. \tag{3.3}$$

We note that Coleman defines this integration in a much more general setting than this, but we shall only be concerned with the above case of abelian varieties and differentials of the first kind.

Proposition 3.2.3. *The integration pairing (3.3) is*

(i) locally analytic in $P \in B(K)$,

(ii) $\mathbb{Z}$-linear on the right,

(iii) K-linear on the left,

(iv) its left-hand kernel is zero,

(v) its right-hand kernel is $B(K)_{\mathrm{tors}}$, and

(vi) if $g : B \to B'$ is a morphism of abelian varieties over K, then

$$\int_P g^*\omega = \int_{g(P)} \omega$$

for all $\omega \in H^0(B', \Omega_{B'/K})$ and $P \in B(K)$.

Proof. Parts (i) and (ii) are [Col85b, Theorem 2.8]. Part (iii) follows from part (i) and [Col85b, Proposition 2.4 (i), (iii)]. Part (iv) follows from [Col85b, Theorem 2.8 (ii)], and Part (v) is [Col85b, Theorem 2.11]. Finally, part (vi) is [Col85b, Theorem 2.7]. □

Lemma 3.2.4. *Suppose that $G \subset B(K)$ is a subgroup of rank r. Then there is a vector space $\mathcal{V} \subset H^0(B, \Omega_{B/K})$ of dimension at least $\dim(B) - r$ such that for all $\omega \in \mathcal{V}$, we have*

$$\int_P \omega = 0 \text{ for all } P \in \overline{G},$$

where the closure is inside the p-adic topology on $B(K)$.

Proof. Suppose that $D_1, \ldots, D_r$ generate G up to torsion. Then $\overline{G} \otimes K = KD_1 + \ldots + KD_r$, of dimension $\leq r$. Now we find $\mathcal{V}$ because (3.3) extends to an exact pairing between $H^0(B, \Omega_{B/K})$ and $B(K) \otimes K$ by Proposition 3.2.3. □

When $B = J(X)/K$ and $G = J(X)(K)$, we call this space $\mathcal{V}$ the *space of vanishing differentials.* Moreover, when we have a map $\rho\colon X \to C$ as in the previous section, we call $\mathcal{V} \cap \mathrm{Ker}(\mathrm{Tr})$ the *space of vanishing differentials with trace zero.* This is the pullback along π_A of the space of vanishing differentials on A, where A is such that $J(X) \sim J(C) \times A$.

More notation: by pulling back along ι, we obtain integrals

$$H^0(X, \Omega_{X/K}) \times X(K)^2 \to K, \quad (\omega, Q, P) \mapsto \int_Q^P \omega := \int_{[P-Q]} (\iota^*)^{-1}(\omega).$$

Proposition 3.2.5. *(i) For $P, Q \in X(K)$ such that $P \in D(Q)$, and a well-behaved uniformiser s at Q, we have for each $\omega \in H^0(X, \Omega_{X/K})$*

$$\int_Q^P \omega = \sum_{n=0}^{\infty} \frac{a_n}{n+1} s(P)^{n+1},$$

where $\mathrm{loc}_Q(\omega) = \sum_n a_n s^n$ as in (3.2). We call such an integral between points in the same residue class a tiny integral.

(ii) If $\rho : X \to C$ is a non-constant morphism of curves over K with good reduction, then

$$\int_{\rho^* D} \omega = \int_D \mathrm{Tr}(\omega)$$

for all $\omega \in H^0(X, \Omega_{X/K})$ and every degree 0 divisor D on C defined over K.

Proof. Part (i) follows from Proposition 3.2.3 (i) together with the Fundamental Theorem of Calculus proved in [Col85b, Proposition 2.4 (ii)]. Part (ii) is [Sik09, Lemma 2.2]. □

3.2.3 An overview of the symmetric Chabauty–Coleman method

We refer the reader to [Wet97] and [MP12] for a clear overview of the Chabauty–Coleman method in the classical case. Here we give an overview of Chabauty and Coleman's original ideas in the symmetric power setting, after which we explain what needs to be changed in the relative case. For simplicity we work over $\mathbb{Q}$, but everything generalises to number fields.

We consider an integer d, a prime p and a curve $X/\mathbb{Q}$ of genus g_X and minimal proper regular model $\mathcal{X}/\mathbb{Z}_p$ for $X_{\mathbb{Q}_p}$. To determine $X^{(d)}(\mathbb{Q})$, it suffices to determine each of the mod p residue discs separately. So consider $\widetilde{\mathcal{Q}} \in X^{(d)}(\mathbb{F}_p)$ and its inverse image under the reduction map, the residue disc $D(\widetilde{\mathcal{Q}}) \subset X^{(d)}(\mathbb{Q}_p)$. We define the Abel–Jacobi map via $D_0 \in X^{(d)}(\mathbb{Q})$:

$$\iota : X^{(d)} \to J(X), \quad D \mapsto [D - D_0].$$

Chabauty's idea was to consider the diagram

$$\begin{tikzcd} D(\widetilde{\mathcal{Q}}) \cap X^{(d)}(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & J(X)(\mathbb{Q}) \arrow[d] \\ D(\widetilde{\mathcal{Q}}) \arrow[r, "\iota"] & J(X)(\mathbb{Q}_p) \end{tikzcd} \tag{3.4}$$

and instead determine

$$\iota(D(\widetilde{\mathcal{Q}})) \cap \overline{J(X)(\mathbb{Q})}, \tag{3.5}$$

where the closure is inside the p-adic topology on $J(X)(\mathbb{Q}_p)$. This set contains $\iota(D(\widetilde{\mathcal{Q}}) \cap X^{(d)}(\mathbb{Q}))$. Let r be the rank of $J(X)(\mathbb{Q})$. By Lemma 3.2.4, we obtain a space $\mathcal{V} \subset H^0(X, \Omega_{X/K})$ of dimension $\dim(\mathcal{V}) \geq g_X - r$ such that for all $\omega \in \mathcal{V}$, we have

$$\int_D \omega = 0 \text{ for all } D \in \overline{J(X)(\mathbb{Q})}.$$

In particular, when the *Chabauty condition*

$$r < g_X - (d-1) \tag{3.6}$$

is satisfied, there are d such linearly independent differentials, and dimensions suggest that

$$\mathcal{Z}_p(\widetilde{\mathcal{Q}}) := \left\{ \mathcal{P} \in D(\widetilde{\mathcal{Q}}) \mid \int_{\iota(\mathcal{P})} \omega = 0 \text{ for all } \omega \in \mathcal{V} \right\}$$

is finite. In the case $d = 1$, Chabauty [Cha41] proved that $\overline{J(\mathbb{Q})} \cap \iota(D(\widetilde{\mathcal{Q}}))$ is indeed finite when (3.6) is satisfied. For $d > 1$, $X^{(d)}(\mathbb{Q})$ can still be infinite even when (3.6) holds, e.g. due to the existence of a map $\rho : X \to C$ of degree $\leq d$. For now, however, let us

assume that X satisfies (3.6), and that we have no reason to believe that $X^{(d)}(\mathbb{Q}) \cap D(\widetilde{\mathcal{Q}})$ is infinite regardless.

It was Coleman's idea [Col85a] to introduce integration of differentials and compute $\mathcal{Z}_p(\widetilde{\mathcal{Q}})$ instead. Such zero sets can be computed for $d = 1$ by evaluating Coleman integrals between $\mathbb{Q}_p$-rational points. In `Sage` on hyperelliptic curves, the computation of Coleman integrals over $\mathbb{Q}_p$ has been implemented by Balakrishnan, Bradshaw, and Kedlaya [BBK10], [Bal15], while Balakrishnan and Tuitman [BT20] wrote a `Magma` implementation for all plane curves. For $d > 1$, however, one would need to evaluate Coleman integrals between points $P, Q \in X(K)$ for extensions $K/\mathbb{Q}_p$ of degree greater than 1, and this has not yet been done.

Instead, therefore, we shall restrict our attention to tiny (i.e. computable) integrals only: this suffices when combining the information from multiple primes p using the Mordell–Weil sieve. The drawback here is that information on $J(X)(\mathbb{Q})$ is needed. Thanks to the sieve, we need to consider only residue discs $D(\widetilde{\mathcal{Q}})$ containing a known point $\mathcal{Q} \in X^{(d)}(\mathbb{Q})$. For each such point $\mathcal{Q}$, (assuming that $X^{(d)}(\mathbb{Q})$ is finite) there is a prime p such that $X^{(d)}(\mathbb{Q}) \cap D(\widetilde{\mathcal{Q}}) = \{\mathcal{Q}\}$. To compute $X^{(d)}(\mathbb{Q})$, it then suffices to have a criterion to decide whether $\mathcal{Z}_p(\widetilde{\mathcal{Q}}) = \{\mathcal{Q}\}$.

Given the known point $\mathcal{Q}$, we can choose $D_0 = \mathcal{Q}$ to define ι. Then for $\mathcal{P} \in D(\widetilde{\mathcal{Q}})$, the integral $\int_{\iota(\mathcal{P})} \omega$ is a sum of d tiny integrals. By studying the power series obtained from these tiny integrals via Proposition 3.2.5 (i), Siksek [Sik09, Theorem 3.2] found a criterion for deciding whether $Z_p(\widetilde{\mathcal{Q}}) = \{\mathcal{Q}\}$.

3.2.4 An overview of our relative Chabauty–Coleman method

We continue the notation from the previous section. We now assume that we *do* have reason to believe that $X^{(d)}(\mathbb{Q}) \cap D(\widetilde{\mathcal{Q}})$ is infinite, due to the existence of a curve C with minimal proper regular model $\mathcal{C}/\mathbb{Z}_p$, a map $\rho : \mathcal{X} \to \mathcal{C}$ such that $\rho : X \to C$ has degree d_0, a positive integer ℓ such that $\ell \cdot d_0 \leq d$, and known points $P \in X^{(d-d_0\ell)}(\mathbb{Q})$ and $Q \in C^{(\ell)}(\mathbb{Q})$ such that $\mathcal{Q} := P + \rho^* Q \in D(\widetilde{\mathcal{Q}})$. Indeed, we then have a family

$$P + \rho^* C^{(\ell)}(\mathbb{Q}) \subset X^{(d)}(\mathbb{Q})$$

intersecting $D(\widetilde{\mathcal{Q}})$. Even when X satisfies the Chabauty condition (3.6), the approach from the previous section fails when either $C^{(\ell)}(\mathbb{Q})$ is infinite or when $C^{(\ell)}$ does not satisfy the Chabauty condition $r_C < g_C - (\ell - 1)$ itself, where $r_C = \mathrm{rk}(J(C)(\mathbb{Q}))$ and g_C is the genus of C.

As in Section 3.2.1, there is an abelian variety $A \subset J(X)$ such that $J(X) \sim J(C) \times A$, and we define $\pi_A : J(X) \to A$. As before, define the Abel–Jacobi map ι using $\mathcal{Q}$. We now replace $J(X)$ in Diagram (3.4) by A, and note that

$$\pi_A \circ \iota \left(P + \rho^* C^{(\ell)}(\mathbb{Q}) \right) = \{0\},$$

so the entire family has been collapsed to a single point on A. It may be easier to determine $\overline{A(\mathbb{Q})} \cap \pi_A(\iota(D(\widetilde{\mathcal{Q}})))$ than it is to determine $\overline{J(X)(\mathbb{Q})} \cap \iota(D(\widetilde{\mathcal{Q}}))$. Again by Lemma 3.2.2,

we find a space $\mathcal{V} \subset H^0(A, \Omega_{A/K})$ of dimension $\dim(\mathcal{V}) \geq \dim(A) - \operatorname{rank}(A(\mathbb{Q}))$ such that for all $\omega \in \mathcal{V}$

$$\int_D \omega = 0 \text{ for each } D \in \overline{A(\mathbb{Q})}.$$

Let r_X be the rank of $J(X)(\mathbb{Q})$, r_C the rank of $J(C)(\mathbb{Q})$, and g_X and g_C be the genera of X and C respectively. If the Chabauty condition

$$r_X - r_C < g_X - g_C - (d-1) \tag{3.7}$$

is satisfied, then $\dim(\mathcal{V}) \geq d$ and the dimensions suggest that the common zero set of $\int \omega$ for $\omega \in \mathcal{V}$ has finite intersection with $\pi_A \circ \iota(D(\widetilde{\mathcal{Q}}))$. Define

$$\mathcal{Z}_{p,A}(\widetilde{\mathcal{Q}}) := \left\{ \mathcal{P} \in D(\widetilde{\mathcal{Q}}) \mid \int_{\mathcal{Q}}^{\mathcal{P}} \omega = 0 \text{ for all } \omega \in \operatorname{Ker}(\operatorname{Tr}) \right\},$$

where $\operatorname{Tr}: \ H^0(X, \Omega_{X/K}) \to H^0(C, \Omega_{C/K})$ is the trace map. By Lemma 3.2.2 (ii) and Proposition 3.2.3 (vi), this is the inverse image to $D(\widetilde{\mathcal{Q}})$ of the common zero set of the integrals $\int \omega$ for $\omega \in \mathcal{V}$.

Analogous to the case of the previous section, we now desire a criterion to decide if $\mathcal{Z}_{p,A}(\widetilde{\mathcal{Q}}) = (P + \rho^* C^{(\ell)}(\mathbb{Q})) \cap D(\widetilde{\mathcal{Q}})$. This is the purpose of Theorem 3.2.6.

3.2.5 The main theorem

Consider a point Q on a curve X over a field K, and a regular 1-form $\omega \in H^0(X, \Omega_{X/K})$. We expand ω around Q in terms of a uniformiser t_Q at Q, giving $\operatorname{loc}_Q(\omega) = \sum_{j \geq 0} a_j t_Q^j$. We define

$$v(\omega, t_Q, k) := \left(-a_0, a_1, \ldots, (-1)^{k-2} a_{k-1} \right).$$

For an effective K-rational divisor $\mathcal{Q}$ on a curve X defined over a number field K, let $K(\mathcal{Q})$ be the (Galois) extension of K obtained by adjoining the coordinates of all points in the support of $\mathcal{Q}$.

Theorem 3.2.6. *Let $\rho_j : X \to C_j$ for $j \in \{1, \ldots, h\}$ be degree d_j maps of curves over a number field K, and consider given an effective divisor*

$$\mathcal{Q} = \mathcal{Q}_0 + \mathcal{Q}_1 + \ldots + \mathcal{Q}_h, \text{ where } \mathcal{Q}_0 \in X^{(\ell_0)}(K) \text{ and } \mathcal{Q}_j \in \rho_j^* C_j^{(\ell_j)}(K) \text{ for } j \geq 1.$$

Let $d = \ell_0 + d_1 \ell_1 + \ldots + d_h \ell_h$. Suppose that $\mathfrak{r}$ is a prime in $\mathcal{O}_K$ of good reduction for X and each C_j. Let p be the rational prime contained in $\mathfrak{r}$.

(1) Assume that the supports of $\mathcal{Q}_1, \ldots, \mathcal{Q}_h$ are pairwise disjoint, and no point in the support of any $\mathcal{Q}_i$ for $i \geq 1$ has ramification degree under ρ_i divisible by p.

(2) Let N be the ramification index of p in $K(\mathcal{Q})$. Assume that $p \geq N + 2$.

Write $\lambda = \ell_1 + \ldots + \ell_h$. Let $\mathcal{V}$ be the space of vanishing differentials on X with trace zero with respect to each ρ_j, and consider a basis $\widetilde{\omega}_1, \ldots, \widetilde{\omega}_q$ for the image of $\mathcal{V} \cap H^0(\mathcal{X}, \Omega)$

under the mod $\mathfrak{r}$ reduction map on differentials, where $\mathcal{X}/\mathcal{O}_{K_\mathfrak{r}}$ is the minimal proper regular model of X. Let $\mathfrak{p}$ be a prime in $K(\mathcal{Q})$ above $\mathfrak{r}$, and denote reductions of points with respect to $\mathfrak{p}$ with a tilde. Write $\mathcal{Q} = n_1Q_1 + \ldots + n_kQ_k$ with $Q_1, \ldots, Q_k \in X$ distinct points and each $n_i \geq 1$, and let $t_{\widetilde{Q}_i}$ be a uniformiser at $\widetilde{Q}_i$ for each i.

(3) Assume that the matrix

$$\widetilde{\mathcal{A}} := \begin{pmatrix} v(\widetilde{\omega}_1, t_{\widetilde{Q}_1}, n_1) & v(\widetilde{\omega}_1, t_{\widetilde{Q}_2}, n_2) & \cdots & v(\widetilde{\omega}_1, t_{\widetilde{Q}_k}, n_k) \\ v(\widetilde{\omega}_2, t_{\widetilde{Q}_1}, n_1) & v(\widetilde{\omega}_2, t_{\widetilde{Q}_2}, n_2) & \cdots & v(\widetilde{\omega}_2, t_{\widetilde{Q}_k}, n_k) \\ \vdots & \ddots & \ddots & \vdots \\ v(\widetilde{\omega}_q, t_{\widetilde{Q}_1}, n_1) & v(\widetilde{\omega}_q, t_{\widetilde{Q}_2}, n_2) & \cdots & v(\widetilde{\omega}_q, t_{\widetilde{Q}_k}, n_k) \end{pmatrix}$$

has rank $d - \lambda$.

Then every $\mathcal{P} \in X^{(d)}(K)$ in the mod $\mathfrak{r}$ residue disc of $\mathcal{Q}$ is in fact contained in

$$\mathcal{Q}_0 + \rho_1^* C_1^{(\ell_1)}(\overline{K}) + \ldots + \rho_h^* C_h^{(\ell_h)}(\overline{K}).$$

Remark 3.2.7. By Proposition 3.2.17 in the next section, $d - \lambda$ is in fact the maximal possible rank of this matrix. Moreover, note that condition (3) is not satisfied when two distinct points $Q_i \neq Q_j$ have the same reduction mod $\mathfrak{p}$. If they do, at least two columns in $\widetilde{\mathcal{A}}$ would agree, reducing its rank to less than $d - \lambda$ due to the nature of the linear equations between the columns obtained from Proposition 3.2.17.

Remark 3.2.8. In fact, from the proof we see that condition (2) can be replaced by $p \geq N' + 2$, where N' is the maximum of the ramification indices of p in $K(Q_i, Q_j)$ for $i, j \in \{1, \ldots, k\}$. This leads to a general lower bound $p \geq d(d-1) + 2$. In particular, for $d = 2$, $p \geq 5$ suffices; for $d = 3$, $p \geq 11$ suffices; and for $d = 4$, $p \geq 17$ suffices.

Remark 3.2.9. This theorem generalises [Sik09, Theorems 3.2 and 4.3]. More precisely, the case $\mathcal{Q} = \mathcal{Q}_0$ corresponds to [Sik09, Theorem 3.2] and the case $\mathcal{Q} = \mathcal{Q}_1$ corresponds to [Sik09, Theorem 4.3]. In both cases, we significantly improve the lower bound on the prime p compared to [Sik09]. Part of the improvement is due to the introduction in the proof of elementary symmetric polynomials replacing power sums. This removes denominators in the power series expansion and hence in the matrix $\widetilde{\mathcal{A}}$; this is an idea also used in [DKSS17]. Another improvement comes from a Galois theory argument, exploiting the fact that $\mathcal{P}$ is K-rational.

Remark 3.2.10. When p is small, it can happen that $X^{(d)}(\mathbb{Q})$ surjects onto $X^{(d)}(\mathbb{F}_p)$, in which case this theorem may be used to determine $X^{(d)}(\mathbb{Q})$ directly (i.e. without sieving). This has the advantage of requiring no information on the Mordell–Weil group of $J(X)$. When $\mathcal{Q} = \mathcal{Q}_0$ and the vanishing differentials come from a rank zero quotient of $J(X)$, it is best to use the formal immersion criterion of Derickx, Kamienny, Stein and Stoll [Der16, Chapter 3 Proposition 3.7] instead, which gives the same statement but works for all primes $p \geq 2$ of good reduction. See for example [DEv+20, §6.1] where this is done for $X_1(22)^{(3)}(\mathbb{Q})$ and $X_1(25)^{(3)}(\mathbb{Q})$ with $p = 3$. Our theorem covers all relative and positive rank cases, and can often be used with $p = 3$.

Remark 3.2.11. While we have stated the theorem for multiple maps $\rho_1, \ldots, \rho_h$, we only need the case $h = 1$ in our examples, in which case $\mathcal{P} \in \mathcal{Q}_0 + \rho_1^* C_1^{(\ell_1)}(K)$ (the pull-back part is K-rational since $\mathcal{P}$ and $\mathcal{Q}_0$ are). Also note that condition (1) is quite limiting when $h > 1$. If, for example, there are two degree 2 maps $\rho_1 : X \to C_1$ and $\rho_2 : X \to C_2$ and $Q \in X(\mathbb{Q})$ then $\rho_1^*\rho_1(Q) + \rho_2^*\rho_2(Q) \in X^{(4)}(\mathbb{Q})$ does not satisfy (1).

3.2.6 Trace maps and ramification

We note that all statements in this section are essentially well-known results in algebraic number theory. We nonetheless give proofs because we could not find the exact statements in the literature.

Any map $\rho : X \to C$ of curves as in the statement of Theorem 3.2.6 may be ramified at certain points of degree at most d.

Example 3.2.12. When ρ is the quotient map $\rho : X_0(67) \to X_0^+(67)$, there is a non-cuspidal rational point $Q \in X_0(67)(\mathbb{Q})$ that ramifies. Ramifying here means that $w_{67}(Q) = Q$. In order to deal with degree 3 effective divisors such as $3Q = Q + \rho^*\rho(Q) \in X_0(67)^{(3)}(\mathbb{Q})$, we study in more detail how differentials transform under (ramified) maps of curves.

First, we briefly recall some facts about maps between Krull domains. We consider a integral extension $A \to B$ of Krull domains. Krull domains can be viewed as higher-dimensional generalisations of Dedekind domains; see e.g. [Mat89] for their definition and theory. Consider a minimal prime ideal $\mathfrak{p} \subset A$. Then the localisation $A_\mathfrak{p}$ is a DVR. We denote by $k(\mathfrak{p})$ the residue field of $A_\mathfrak{p}$, and for $f \in A$ by $f(\mathfrak{p})$ the image of f in $k(\mathfrak{p})$. Now $\mathrm{Frac}(B)/\mathrm{Frac}(A)$ is a finite extension. This field extension comes with a trace map

$$\mathrm{Tr}_{B/A} : \mathrm{Frac}(B) \to \mathrm{Frac}(A).$$

Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be the minimal prime ideals of B above $\mathfrak{p}$, and denote by $e_i \geq 1$ the valuation of $\mathfrak{p}$ in the DVR $B_{\mathfrak{q}_i}$. We similarly obtain local trace maps $\mathrm{Tr}_{\widehat{B}_{\mathfrak{q}_i}/\widehat{A}_\mathfrak{p}}$ and $\mathrm{Tr}_{k(\mathfrak{q}_i)/k(\mathfrak{p})}$. Denote by $\mathrm{loc}_\mathfrak{r} : R \to \widehat{R}_\mathfrak{r}$ be the localisation map at the prime ideal $\mathfrak{r}$ in the ring R.

Lemma 3.2.13. *We have*

$$\mathrm{loc}_\mathfrak{p} \circ \mathrm{Tr}_{B/A} = \sum_i \mathrm{Tr}_{\widehat{B}_{\mathfrak{q}_i}/\widehat{A}_\mathfrak{p}} \circ \mathrm{loc}_{\mathfrak{q}_i}.$$

Moreover, for each $f \in B$ we have

$$\mathrm{Tr}_{B/A}(f)(\mathfrak{p}) = \sum_i e_i \mathrm{Tr}_{k(\mathfrak{q}_i)/k(\mathfrak{p})}(f(\mathfrak{q}_i)).$$

Proof. Upon localising A and B at the multiplicative subset $A \setminus \mathfrak{p}$, we may assume that A is a DVR with maximal ideal $\mathfrak{p}$, and B is a Dedekind domain with maximal ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$.

Now consider the completion of B with respect to $\mathfrak{p}B$ and apply the Chinese Remainder Theorem:

$$\widehat{B} := \varprojlim_n B/\mathfrak{p}^n B = \prod_i \widehat{B}_{\mathfrak{q}_i}. \tag{3.8}$$

Consider $b \in \widehat{B}$. We define the trace $\mathrm{Tr}_{\widehat{B}/\widehat{A}}(b)$ by taking the trace of the $\mathrm{Frac}(\widehat{A})$-linear map given by multiplication-by-b on $\widehat{B} \otimes_{\widehat{A}} \mathrm{Frac}(\widehat{A})$. Here B is finite and free as an A-module, and a basis for B/A also determines a basis for $\widehat{B}/\widehat{A}$. In particular, $\mathrm{Tr}_{B/A}(b) = \mathrm{Tr}_{\widehat{B}/\widehat{A}}(b)$, which is the trace of a block matrix on $\prod_i \widehat{B}_{\mathfrak{q}_i}$. This gives the first equality.

For the second equation, we begin by reducing the first modulo $\mathfrak{p}$. It then suffices to show the equality $e_i \mathrm{Tr}_{k(\mathfrak{q}_i)/k(\mathfrak{p})}(f(\mathfrak{q}_i)) = \mathrm{Tr}_{\widehat{B}_{\mathfrak{q}_i}/\widehat{A}_{\mathfrak{p}}}(f)(\mathfrak{p})$ for each i. To compute $\mathrm{Tr}_{\widehat{B}_{\mathfrak{q}_i}/\widehat{A}_{\mathfrak{p}}}(f)(\mathfrak{p})$, we may first determine the image of f in the $k(\mathfrak{p})$-vector space $\widehat{B}_{\mathfrak{q}_i}/\mathfrak{p}$, and then take the trace down to $k(\mathfrak{p})$.

We note that

$$\widehat{B}_{\mathfrak{q}_i}/\mathfrak{p} = \widehat{B}_{\mathfrak{q}_i}/\mathfrak{q}_i^{e_i} \simeq \widehat{B}_{\mathfrak{q}_i}/\mathfrak{q}_i \times \mathfrak{q}_i/\mathfrak{q}_i^2 \times \ldots \times \mathfrak{q}_i^{e_i-1}/\mathfrak{q}_i^{e_i}$$

as $k(\mathfrak{p})$-vector spaces. The right-hand side is a $k(\mathfrak{q}_i)$-vector space, and to compute the trace to $k(\mathfrak{p})$ we may first compute the trace to $k(\mathfrak{q}_i)$. Finally, we may consider a uniformiser $t \in \widehat{B}_{\mathfrak{q}_i}$. If $f = \sum_{n=0}^{\infty} a_n t^n \in \widehat{B}_{\mathfrak{q}_i}$ then the multiplication-by-f map on $\widehat{B}_{\mathfrak{q}_i}/\mathfrak{p}$ has, by the above, e_i diagonal entries equal to a_0, so the trace becomes $e_i a_0 = e_i f(\mathfrak{q}_i)$. □

When M is an R-module and $\mathfrak{r}$ is a prime ideal in R, denote by $M_{\mathfrak{r}}$ the localisation of M at $\mathfrak{r}$, and by $\widehat{M_{\mathfrak{r}}}$ its completion. Now suppose that A and B are Dedekind domains and that K is a field such that the A and B are K-algebras and $A \to B$ is an embedding of K-algebras.

We obtain an embedding $\Omega_{A/K} \to \Omega_{B/K}$ of the spaces of Kähler differentials. Now given $s \in A$ (but $s \notin K$), $\mathrm{d}s$ is a $\mathrm{Frac}(B)$-basis for $\Omega_{B/K}$, and we obtain a trace map

$$\mathrm{Tr}_{B/A} : \ \Omega_{B/K} \to \Omega_{A/K}, \ \ f\mathrm{d}s \mapsto \mathrm{Tr}_{B/A}(f)\mathrm{d}s$$

which is independent of the choice of s.

Corollary 3.2.14. *The equation*

$$\mathrm{loc}_{\mathfrak{p}} \circ \mathrm{Tr}_{B/A} = \sum_i \mathrm{Tr}_{\widehat{B}_{\mathfrak{q}_i}/\widehat{A}_{\mathfrak{p}}} \circ \mathrm{loc}_{\mathfrak{q}_i}$$

also holds true on $\Omega_{B/K}$.

We note that traces of n-th roots are easily computed.

Lemma 3.2.15. *Suppose that $F(\alpha)/F$ is a field extension of degree n defined by the minimal polynomial $\alpha^n = a$ for some $a \in F$. Then*

$$\mathrm{Tr}_{F(\alpha)/F}(\alpha^i) = 0 \text{ unless } n \mid i.$$

Proof. This follows directly from the shape of the minimal polynomial. □

We now consider a map $\rho : X \to C$ of curves over a field K and a K-rational point $R \in C(K)$. As divisors, we write $\rho^* R = \sum_{Q \mapsto R} e_{Q/R} Q$ as a sum of points Q on X. Assume that we have chosen K such that $Q \in X(K)$ for each Q mapping to R. Denote by v_Q the valuation of the discrete valuation ring $\widehat{\mathcal{O}}_{X,Q}$.

From now on, suppose that K is a finite extension of $\mathbb{Q}_p$ for a prime p of good reduction for X and C, with ring of integers $\mathcal{O}_K$ and prime ideal $\mathfrak{p}$. Then ρ extends to an $\mathcal{O}_K$-morphism $\mathcal{X} \to \mathcal{C}$ between the minimal proper regular models of X and C.

Suppose no two distinct points mapping to R have equal reduction mod $\mathfrak{p}$ and $p \nmid e_{Q/R}$ for all points $Q \mapsto R$.

Lemma 3.2.16. *Let $t \in \widehat{\mathcal{O}}_{C,R}$ be a well-behaved local coordinate, and consider $Q \in X$ mapping to R. Then, after base changing to an unramified extension of K of degree at most $e_{Q/R}$, there exists a well-behaved local coordinate $s_Q \in \widehat{\mathcal{O}}_{X,Q}$ such that $s_Q^{e_{Q/R}} = t$. Moreover, $\rho^* : \widehat{\mathcal{O}}_{C,R} \to \widehat{\mathcal{O}}_{X,Q}$ induces an embedding of fraction fields of degree $e_{Q/R}$ defined by the equation $x^{e_{Q/R}} - t = 0$.*

Proof. Consider $Q \in \rho^{-1}(\{R\})$. As Q is a K-rational point, its residue field is $k(Q) = K$. Let $\pi \in \widehat{\mathcal{O}}_{X,Q}$ and $t \in \widehat{\mathcal{O}}_{C,R}$ be two well-behaved uniformisers, and write $e = e_{Q/R}$. We can write $\rho^*(t) = b_0\pi^e + b_1\pi^{e+1} + \ldots$, with each $b_i \in \mathcal{O}_K$. Define $u = b_0 + b_1\pi + b_2\pi^2 + \ldots \in \widehat{\mathcal{O}}_{X,Q}^\times$, so that $\rho^*(t) = u\pi^e$. Then the mod $\mathfrak{p}$ reduction of u is $\widetilde{u} = \sum_{n=0}^\infty \widetilde{b}_n \widetilde{\pi}^n$ since π is well-behaved. Since also t is well-behaved and $\widetilde{\rho}$ still has ramification degree e at $\widetilde{Q}/\widetilde{R}$ by assumption, we must have $\widetilde{b}_0 \neq 0$ (c.f Section 3.2.1). Let k'/k be an extension of the residue field of K containing a root of $X^e - \widetilde{b}_0$. Then k' corresponds to an unramified extension K'/K and by Hensel's Lemma (applicable because $b_0 \in \mathcal{O}_K^\times$ and $p \nmid e$), K' contains a root of $X^e - b_0$. Then also $\widehat{\mathcal{O}}_{X_{K'},Q}$ contains an eth root of u by Hensel's lemma, and we simply define $s_Q = u^{1/e}\pi$. The map between fraction fields now has degree e because ρ^* is an isomorphism on residue fields. □

Using the lemma, we extend K and define t and s_Q (for each $Q \mapsto R$) to be well-behaved uniformisers satisfying $s_Q^{e_{Q/R}} = t$. We consider the Dedekind domain

$$\mathcal{O}_{X,\rho^* R} := \{f \in K(X) \mid v_Q(f) \geq 0 \text{ for all } Q \mapsto R\},$$

which is an integral extension of the DVR $\mathcal{O}_{C,R}$. This Dedekind domain has localisations $\mathcal{O}_{X,Q}$ at all places Q mapping to R. Denote by $\mathrm{Tr}_{Q/R}$ the trace map from $\mathrm{Frac}(\widehat{\mathcal{O}}_{X,Q})$ to $\mathrm{Frac}(\widehat{\mathcal{O}}_{C,R})$. Now suppose that ω is a global meromorphic differential on X/K. We can interpret ω as a Kähler differential in $\Omega_{\mathcal{O}_{X,\rho^* R}/K}$. From the integral extension $\rho^* : \mathcal{O}_{C,R} \to \mathcal{O}_{X,\rho^* R}$ of Dedekind domains, we thus obtain a trace map

$$\mathrm{Tr} : \ \Omega_{\mathcal{O}_{X,\rho^* R}/K} \to \Omega_{\mathcal{O}_{C,R}/K},$$

which for $\omega \in H^0(X, \Omega)$ equals the trace map defined in Section 3.2.1 (followed by localisation at R).

Proposition 3.2.17. *Write* $\mathrm{loc}_Q(\omega) = \sum_{i=0}^{\infty} a_i(Q) s_Q^i \mathrm{d}s_Q$ *for the expansion of* ω *in* $\Omega_{\widehat{\mathcal{O}}_{X,Q}/K}$. *Then* $\mathrm{loc}_R(\mathrm{Tr}(\omega)) = \sum_{Q \mapsto R} \sum_{j \geq 1} a_{je_{Q/R}-1}(Q) t^{j-1} \mathrm{d}t$.

In particular, if $\mathrm{Tr}(\omega) = 0$, *then for each* $j \geq 1$ *we have*

$$\sum_{Q \mapsto R} a_{j \cdot e_{Q/R}-1}(Q) = 0.$$

Remark 3.2.18. Note that this equality determines a linear relation between the columns of the matrix $\widetilde{\mathcal{A}}$ defined in the statement of Theorem 3.2.6. For example, when ρ has degree 2 and $Q \in X$ ramifies, the equation says $a_1(Q) = 0$, and $\widetilde{\mathcal{A}}$ has a vanishing column, c.f. Example 3.3.9.

Proof. We also obtain local trace maps $\mathrm{Tr}_{Q/R} : \Omega_{\mathcal{O}_{X,Q}/K} \to \Omega_{\mathcal{O}_{C,R}/K}$. By Corollary 3.2.14, we have

$$\mathrm{loc}_R(\mathrm{Tr}(\omega)) = \sum_{Q \mapsto R} \mathrm{Tr}_{Q/R}(\mathrm{loc}_Q(\omega)) = \sum_{Q \mapsto R} \mathrm{Tr}_{Q/R}\left(\sum_{i=1}^{\infty} a_{i-1}(Q) s_Q^{i-1} \mathrm{d}s_Q \right).$$

Next, we recall that by Lemma 3.2.15 we have $\mathrm{Tr}_{Q/R}(s_Q^i) = 0$, unless i is a multiple of $e_{Q/R}$, in which case $\mathrm{Tr}_{Q/R}(s_Q^{je_{Q/R}}) = e_{Q/R} t^j$. Now $i\mathrm{Tr}_{Q/R}(s_Q^{i-1}\mathrm{d}s_Q) = \mathrm{d}\mathrm{Tr}_{Q/R}(s_Q^i)$, from which we deduce that $\mathrm{loc}_R(\mathrm{Tr}(\omega)) = \sum_{Q \mapsto R} \sum_{j=1}^{\infty} a_{je_{Q/R}-1} t^{j-1} \mathrm{d}t$. Finally, we recall from Section 3.2.1 that $\Omega_{\widehat{\mathcal{O}}_{C,R}/K} = K[\![t]\!]\mathrm{d}t$, so the equality of power series yields a coefficient-wise equality. □

Finally, we show that traces of uniformisers can be computed as expected.

Lemma 3.2.19. *Consider given* $Q \in X(K)$ *with* $\rho(Q) = R$, *again such that no other point mapping to* R *has the same reduction as* Q. *Suppose* $P \in D(R)$ *and write, as divisors,* $\rho^* P \cap D(Q) = \sum_{i=1}^{e} P_i$ *(with possible repetition), where* e *is the common ramification index of* Q/R *and* $\widetilde{Q}/\widetilde{R}$. *We base change* X *and* C *from* K *to* $K(P_1, \ldots, P_e)$, *the extension of* K *containing all coordinates of* $P_1, \ldots, P_e$. *Then for a well-behaved uniformiser* s *at* Q *we have*

$$\mathrm{Tr}_{Q/R}(s)(P) = \sum_{i=1}^{e} s(P_i).$$

Consequently, if $f(X) = 1 - b_1 X + b_2 X^2 - \ldots + (-1)^e b_e X^e$ *is the reverse minimal polynomial of* $s \in \widehat{\mathcal{O}}_{X,Q}$ *over* $\widehat{\mathcal{O}}_{C,R}$, *then* $b_i(P)$ *is equal to the* i*th symmetric polynomial in* $s(P_1), \ldots, s(P_e)$.

Proof. We denote by $\widehat{\mathcal{O}}_{\mathcal{X},\widetilde{Q}}$ the completed local ring (and Krull domain) at the closed point $\widetilde{Q}$ and by $\widehat{\mathcal{O}}_{\mathcal{X},Q}$ the completed local ring (and DVR) at the non-closed point (or subscheme of codimension 1) Q. If $\mathfrak{m}_Q$ is the (minimal) prime ideal of $\widehat{\mathcal{O}}_{\mathcal{X},\widetilde{Q}}$ corresponding to Q, then $\widehat{\mathcal{O}}_{\mathcal{X},Q}$ is the localisation of $\widehat{\mathcal{O}}_{\mathcal{X},\widetilde{Q}}$ at $\mathfrak{m}_Q$. Well-behaved means that $s \in \widehat{\mathcal{O}}_{\mathcal{X},\widetilde{Q}}$. We note that the map $\rho^* \colon \widehat{\mathcal{O}}_{\mathcal{C},\widetilde{R}} \to \widehat{\mathcal{O}}_{\mathcal{X},\widetilde{Q}}$ determines an integral extension of Krull domains. We define $A = \widehat{\mathcal{O}}_{\mathcal{C},\widetilde{R}}$ and $B = \widehat{\mathcal{O}}_{\mathcal{X},\widetilde{Q}}$ and consider the minimal prime ideal $\mathfrak{m}_R \subset A$. To compute $\mathrm{Tr}_{B/A}(s)$, we apply the first part of Lemma 3.2.13 to $A \to B$ with $\mathfrak{p} = \mathfrak{m}_R$. By assumption, $\mathfrak{m}_Q$ is the only minimal prime of B above $\mathfrak{m}_R$, so we find $\mathrm{Tr}_{B/A}(s) = \mathrm{Tr}_{Q/R}(s)$.

Similarly, the minimal primes above $\mathfrak{m}_P$ are $\mathfrak{m}_{P_1}, \ldots, \mathfrak{m}_{P_e}$ (with possible repetition) and we apply the second part of Lemma 3.2.13 to $A \to B$ and the ideal $\mathfrak{p} = \mathfrak{m}_P$. This yields $\mathrm{Tr}_{B/A}(s)(P) = \sum_{i=1}^{e} s(P_i)$, as desired. □

3.2.7 Lemmas to control the prime bound

The following lemmas are needed to control the lower bound on the prime p in Theorems 3.2.6 and 3.2.24.

Lemma 3.2.20. *Let N, T and $\ell > T$ be positive integers, and $p > N+T$ a prime number. Then we have*

$$\ell - T \geq N\mathrm{ord}_p(\ell) + 1. \tag{3.9}$$

Proof. Write $\ell = p^a b$, where $a = \mathrm{ord}_p(\ell)$. When $a = 0$, this is true because $\ell > T$. Otherwise, we note that $\ell \geq p^a$, and

$$p^a - T \geq (N+T+1)^a - T \geq 1 + a(N+T) - T \geq 1 + aN,$$

as desired. □

Next, we consider the inclusions of polynomial rings $\mathbb{Q}[s_1, \ldots, s_n] = \mathbb{Q}[e_1, \ldots, e_n] \subset \mathbb{Q}[z_1, \ldots, z_n]$, where $s_k = \sum_{\ell=1}^{n} z_\ell^k$ for each $k \geq 1$ (we also make this definition for $k > n$), and e_k is the kth elementary symmetric polynomial in $z_1, \ldots, z_n$. We adopt the conventions $e_k = 0$ for $k > n$ and $e_0 = 1$. Let $\mathfrak{m} \subset \mathbb{Q}[e_1, \ldots, e_n]$ be the ideal generated by $e_1, \ldots, e_n$. Then in the ring of formal power series $\mathbb{Q}[z_1, \ldots, z_n][\![X]\!]$, Newton's identities can be given the following compact form:

$$\sum_{k=0}^{\infty} (-1)^k e_k X^k = \prod_{i=1}^{n} (1 - z_i X) = \exp\left(-\sum_{k=1}^{\infty} \frac{s_k}{k} X^k \right). \tag{3.10}$$

Lemma 3.2.21. *(1) For each $k \geq 1$, the difference $s_k/k - (-1)^{k-1} e_k$ is in $\mathfrak{m}^2$, and equals a sum of terms $b \cdot e_{i_1} \cdots e_{i_\ell}$ (for $\ell \geq 2$) with $i_1, \ldots, i_\ell \geq 1$ and with coefficient $b \in \mathbb{Q}$ of denominator dividing ℓ.*

(2) If $k > n$ we have

$$\frac{s_k}{k} - \left(\frac{(-1)^k}{2} \sum_{i=k-n}^{n} e_i e_{k-i} \right) \in \mathfrak{m}^3,$$

and it equals again a sum of terms $b \cdot e_{i_1} \cdots e_{i_\ell}$ (for $\ell \geq 3$) with $i_1, \ldots, i_\ell \geq 1$ and with coefficient b of denominator dividing ℓ. In particular, if $k > 2n$ then $s_k/k \in \mathfrak{m}^3$.

(3) Suppose that S is a ring with an ideal I, and we have $a_1, \ldots, a_{2n} \in I$ satisfying for each $i \leq n$ that $a_i \equiv a_{n+i}$ mod I^w, where $w \in \mathbb{Z}_{\geq 1}$. Then $a_1 \cdots a_n \equiv a_{n+1} \cdots a_{2n}$ mod I^{w+n-1}.

Proof. For part (3), it suffices to note the equality

$$a_1 \cdots a_n - a_{n+1} \cdots a_{2n} = \sum_{i=1}^{n} (a_i - a_{i+n}) a_{i+1} a_{i+2} \cdots a_{i+n-1}.$$

Parts (1) and (2) follow directly from (3.10) after applying Log to both sides of the equation and comparing coefficients for X^k. $\square$

3.2.8 Proof of Theorem 3.2.6

For simplicity of exposition (to avoid using triple indices), we assume that $h = 1$. Then there is one map $\rho : X \to C$, and we assume moreover that $\mathcal{Q}_1 = \rho^*(m \cdot R)$ for $R \in C(K)$ and $m \in \mathbb{Z}_{\geq 1}$. For the general case, one can simply sum all arguments that follow over the points in the curves C_j, because $\mathcal{Q}_1, \ldots, \mathcal{Q}_h$ are disjoint. We write $\rho^* R = \sum_{i=1}^k m_i Q_i$, where $m_i \geq 0$ for each i, and

$$\mathcal{Q} = \sum_{i=1}^{k} n_i Q_i,$$

where $n_i \geq m \cdot m_i$ for each i. We choose the ordering so that $m_i = 0$ for all $i > k'$, where $k' \leq k$. Note that $\mathcal{Q}_0 = \sum_{i=1}^k (n_i - mm_i) Q_i$ and $\mathcal{Q}_1 = \sum_{i=1}^{k'} mm_i Q_i$.

Let $L = K(\mathcal{Q})$ be the field obtained by adjoining the coordinates of $Q_1, \ldots, Q_k$ and consider all points, maps and curves as base-changed to L. Let t_R be a well-behaved uniformiser at R. Using Lemma 3.2.16, at each of the distinct points Q_i, consider a well-behaved uniformiser $t_{Q_i} \in \widehat{\mathcal{O}}_{X,Q_i}$ satisfying $t_{Q_i}^{m_i} = t_R$ if $i \leq k'$. For this we need to extend L by an unramified extension, which we still denote by L. Consider $F := L(\mathcal{P})$ and let $\mathfrak{q}$ be a prime in F above $\mathfrak{p}$. We write $\mathcal{P} = \sum_{i=1}^k (P_{i,1} + \ldots + P_{i,n_i})$, where $P_{i,j} \equiv Q_i \bmod \mathfrak{q}$ for each $j \in \{1, \ldots, n_i\}$.

We write $z_{i,j} := t_{Q_i}(P_{i,j})$ and $s_{i,\ell} = \sum_{j=1}^{n_i} z_{i,j}^\ell$, and let $e_{i,\ell}$ be the ℓth elementary symmetric polynomial in $z_{i,1} \ldots, z_{i,n_i}$. Note that each $z_{i,j} \in \mathfrak{q}\mathcal{O}_{F_\mathfrak{q}}$ because t_{Q_i} is well-behaved. Fix one vanishing differential ω of trace zero for all maps and write $\mathrm{loc}_{Q_i}(\omega) = \sum_{j \geq 0} a_j(Q_i, \omega) t_{Q_i}^j \mathrm{d}t_{Q_i}$. After multiplying ω with a scalar, we may assume $\omega \in H^0(\mathcal{X}, \Omega)$ and each $a_j(Q_i, \omega) \in \mathcal{O}_{L_\mathfrak{p}}$.

For $i > k'$, we know that $e_{i,1} = \ldots = e_{i,n_i} = 0$ implies that $z_{i,j} = 0$ for all $j \in \{1, \ldots, n_i\}$, and hence $P_{i,j} = Q_i$ for all $j \in \{1, \ldots, n_i\}$ by injectivity of t_{Q_i} on residue discs. For $i \leq k'$, we would like to be able to read off from the $e_{i,\ell}$ whether $\mathcal{P}$ is (partially) a pullback.

Lemma 3.2.22. *Consider the notation as defined so far, and define the effective divisor $\mathcal{P}' = \sum_{i=1}^{k'} (P_{i,1} + \ldots + P_{i,n_i})$ (sum only up to k').*

Then $\mathcal{P}' = \sum_{i=1}^{k'} (n_i - mm_i) Q_i + \rho^* \mathcal{S}$ for some $\mathcal{S} \in C^{(m)}(\overline{K})$ if (and only if) there exists a polynomial $f \in \overline{K}_\mathfrak{r}[X]$ of degree m with constant coefficient 1 such that for all $i \in \{1, \ldots, k'\}$ we have an equality of polynomials

$$1 - e_{i,1} X + \ldots + (-1)^{n_i} e_{i,n_i} X^{n_i} = f(X^{m_i}).$$

Proof. Denote by $\mathcal{R}$ the set of inverses of roots of f. Choose $i \in \{1, \ldots, k'\}$. By assumption, we find that

$$\prod_{j=1}^{n_i} (1 - z_{i,j} X) = f(X^{m_i}).$$

In particular, after reordering we find that

(a) $z_{i,mm_i+1} = 0, \ldots, z_{i,n_i} = 0$, and moreover

(b) $\{z_{i,j}^{m_i} \mid j \in \{1, \ldots, mm_i\}\} = \mathcal{R}$.

Because uniformisers are injective on residue classes, (a) implies that $Q_i = P_{i,mm_i+1} = \ldots = P_{i,n_i}$. Recall that $z_{i,j}^{m_i} = t_R(\rho(P_{i,j}))$ for $j \leq mm_i$. From (b) and because t_R is injective on $D(R)$, we find that $\{\rho(P_{ij}) \mid i \in \{1, \ldots, k'\}, j \in \{1, \ldots, mm_i\}\}$ has size m. Denote these points by $S_1, \ldots, S_m$. They satisfy $S_\ell \equiv R \bmod \mathfrak{q}$ for each ℓ, and $\{t_R(S_\ell) \mid \ell \in \{1, \ldots, m\}\} = \mathcal{R}$.

Write $\rho^*(S_\ell) = \sum_{i=1}^k \sum_{j=1}^{m_i} P'_{\ell ij}$, where again $P'_{\ell ij} \equiv Q_i$ modulo a fixed prime above $\mathfrak{q}$ in $F(\rho^* S_\ell)$ for each i. Write $z'_{\ell ij} = t_{Q_i}(P'_{\ell ij})$, and define $e'_{\ell ij}$ to be the jth elementary symmetric polynomial in $z'_{\ell,i,1}, \ldots, z'_{\ell,i,m_i}$. Recall that $t_{Q_i}^{m_i} = \rho^* t_R$. From Lemma 3.2.19, we see that $e'_{\ell,i,j} = 0$ for each $j \in \{1, \ldots, m_i - 1\}$ and $e'_{\ell,i,m_i} = (-1)^{m_i+1} t_R(S_\ell)$. We conclude that

$$\left(\prod_{\ell=1}^m \prod_{j=1}^{m_i} (1 - z'_{\ell,i,j} X)\right) = \prod_{\ell=1}^m (1 - t_R(S_\ell) X^{m_i}) = f(X^{m_i})$$

for each i, from which it follows by injectivity of t_{Q_i} that

$$P_{i,1} + \ldots + P_{i,mm_i} = \sum_{\ell=1}^m (P'_{\ell,i,1} + \ldots + P'_{\ell,i,m_i}),$$

and thus $\mathcal{P} = \sum_{i=1}^k (n_i - mm_i) Q_i + \rho^*(S_1 + \ldots + S_m)$. □

We continue the proof of Theorem 3.2.6. As $[\mathcal{P} - \mathcal{Q}] \in J(K)$ and ω is a vanishing differential, we find that $\int_{\mathcal{Q}}^{\mathcal{P}} \omega = 0$. This is a sum of tiny integrals equal by Proposition 3.2.5 (i) to

$$\sum_{i=1}^k \sum_{\ell=1}^\infty a_{\ell-1}(Q_i, \omega) \frac{s_{i,\ell}}{\ell} = 0. \tag{3.11}$$

For $i \in \{1, \ldots, k'\}$, write $p_{i,\ell} := \frac{1}{m_{k'}} \sum_{j=1}^{n_{k'}} \mathrm{Tr}_{Q_i/R}(t_{Q_i}^\ell)(\rho(P_{k',j}))$. Then $p_{i,\ell} = 0$ when $m_i \nmid \ell$ and $\frac{p_{i,jm_i}}{jm_i} = \frac{s_{k',jm_{k'}}}{jm_{k'}}$ for $j \geq 1$. Now we consider $i = k'$, and subtract

$$0 = \frac{1}{m_{k'}} \int_{n_{k'} Q_{k'}}^{P_{k',1} + \ldots + P_{k',n_{k'}}} \rho^* \mathrm{Tr}(\omega) = \sum_{i=1}^{k'} \sum_{\ell=1}^\infty \frac{a_{\ell-1}(Q_i, \omega)}{\ell} p_{i,\ell}$$

from (3.11). Here we used Proposition 3.2.17 to evaluate the integral. We thus obtain

$$\sum_{i=1}^{k'} \sum_{\ell=1}^\infty a_{\ell-1}(Q_i, \omega) \left(\frac{s_{i,\ell} - p_{i,\ell}}{\ell}\right) + \sum_{i=k'+1}^k \sum_{\ell \geq 1} a_{\ell-1}(Q_i, \omega) \frac{s_{i,\ell}}{\ell} = 0. \tag{3.12}$$

For $i \leq k'$, define $r_{i,\ell}$ for $\ell \in \mathbb{Z}_{\geq 1}$ by $r_{i,\ell} = 0$ when $m_i \nmid \ell$ and $r_{i,jm_i} = (-1)^{jm_i - jm_{k'}} e_{k',jm_{k'}}$. For $i > k'$, define $r_{i,\ell} = 0$ for all ℓ. We now use Lemma 3.2.21 (1) to rewrite traces/power sums in terms of elementary symmetric polynomials:
$p_{i,jm_i}/jm_i = s_{k',jm_{k'}}/jm_{k'} = (-1)^{jm_i - 1} r_{i,jm_i} + \text{h.o.t}$ and $s_{i,\ell}/\ell = (-1)^{\ell-1} e_{i,\ell} + \text{h.o.t.}$ This

yields

$$0 = \sum_{i=1}^{k} \sum_{\ell=1}^{n_i} (-1)^{\ell-1} a_{\ell-1}(Q_i, \omega)(e_{i,\ell} - r_{i,\ell}) + \text{h.o.t.}, \tag{3.13}$$

where the higher order terms are of the form

$$\frac{\alpha}{s} \left(e_{i,i_1} \cdots e_{i,i_s} - r_{i,i_1} \cdots r_{i,i_s} \right) \text{ with } s \geq 2 \text{ and } \alpha \in \mathcal{O}_{L_\mathfrak{p}}. \tag{3.14}$$

Now define $f(X) = 1 + (-1)^{m_{k'}} e_{k',m_{k'}} X + \ldots + (-1)^{mm_{k'}} e_{k',mm_{k'}} X^m$. Then for each $i \leq k'$, we find that $f(X^{m_i}) = 1 - r_{i,1}X + \ldots + (-1)^{n_i} r_{i,n_i} X^{n_i}$. In view of Lemma 3.2.22, it is our aim to show that for each $i \in \{1, \ldots, k'\}$, we have

$$f(X^{m_i}) = 1 - e_{i,1}X + \ldots + (-1)^{n_i} e_{i,n_i} X^{n_i},$$

and for $i > k'$ we have $e_{i,\ell} = 0$ for all $\ell \in \{1, \ldots, n_i\}$. In other words, we aim to show $e_{i,\ell} = r_{i,\ell}$ for all $i \in \{1, \ldots, k\}$ and $\ell \leq n_i$.

We first show that $e_{i,\ell}, r_{i,\ell} \in L_\mathfrak{p}$. Note that F/L is Galois. Suppose that $\sigma \in \mathrm{Gal}(F_\mathfrak{q}/L_\mathfrak{p})$. For each $P_{i,j} \in \mathcal{P}$ (that is, in the support of $\mathcal{P}$) reducing mod $\mathfrak{q}$ to $\widetilde{P_{i,j}} = \widetilde{Q_i}$, also $P_{i,j}^\sigma$ must reduce to $\widetilde{Q_i} = \widetilde{Q_i^\sigma}$. Also $P_{i,j}^\sigma \in \mathcal{P}$ as $\mathcal{P}$ is K-rational, so $P_{i,j}^\sigma = P_{i,j'}$ for some $j' \in \{1, \ldots, n_i\}$. As moreover $t_{Q_i}^\sigma = t_{Q_i}$, we find that $e_{i,\ell}^\sigma = e_{i,\ell}$. By definition, then also $r_{i,\ell}^\sigma = r_{i,\ell}$, and all $e_{i,\ell}$ and $r_{i,\ell}$ are in $L_\mathfrak{p}$. We define

$$\nu := \min_{\substack{i \geq 1 \\ \ell \leq n_i}} v_\mathfrak{p}(e_{i,\ell} - r_{i,\ell}),$$

where $v_\mathfrak{p}$ is the $\mathfrak{p}$-adic valuation. We argue by contradiction and assume that $\nu < \infty$. Recall that $\nu \geq 1$ because $\mathcal{P}$ and $\mathcal{Q}$ are in the same residue disc.

Recall that N is the ramification index of $\mathfrak{p}/p$. We apply Lemma 3.2.21 (3) with $I = \mathfrak{p}$, which yields $e_{i,i_1} \cdots e_{i,i_s} \equiv r_{i,i_1} \cdots r_{i,i_s} \bmod \mathfrak{p}^{\nu+s-1}$. By Lemma 3.2.20 with $T = 1$, and because $p \geq N + 2$, we find that $s - 1 \geq N \mathrm{ord}_p(s) + 1$. We conclude that each of the higher order terms (3.14) vanishes mod $\mathfrak{p}^{\nu+1}$.

Let $\omega_1, \ldots, \omega_q \in H^0(\mathcal{X}, \Omega)$ be linearly independent generators for the space of vanishing differentials with trace zero with respect to each ρ_i. We obtain equation (3.13) for each $\omega \in \{\omega_1, \ldots, \omega_q\}$. Let $\mathcal{A}$ be the matrix made up of the $v(\omega_j, t_{Q_i}, n_i)$, so that its reduction mod $\mathfrak{p}$ is the matrix $\widetilde{\mathcal{A}}$ from the statement of the theorem. Denote by $\mathcal{B}$ the matrix obtained from $\mathcal{A}$ by removing for each $j \in \{1, \ldots, m\}$ the column with entries

$$((-1)^{jm_{k'}} a_{jm_{k'}-1}(Q_{k'}, \omega_1), \ldots, (-1)^{jm_{k'}} a_{jm_{k'}-1}(Q_{k'}, \omega_q)).$$

By Proposition 3.2.17, the columns of $\mathcal{A}$ satisfy m linear equations, each of which has coefficient 1 for exactly one of the removed columns. Since $\widetilde{\mathcal{A}}$ has rank $n - m$, we conclude that the reduction $\widetilde{\mathcal{B}}$ of $\mathcal{B}$ has full rank $n - m$. Denote by $\mathbf{v}$ the vector of length $n - m$ with as entries the list $e_{1,1} - r_{1,1}, \ldots, e_{1,n_1} - r_{1,n_1}, \ldots, e_{k,n_k} - r_{k,n_k}$, from which we remove the elements $e_{k',jm_{k'}} - r_{k',jm_{k'}}$ for $j \in \{1, \ldots, m\}$ (each of which is zero by definition of

$r_{i,\ell}$). Then $\mathbf{v} = 0 \bmod \mathfrak{p}^\nu$ by definition of ν, and from (3.13) and the analysis of the higher order terms, we conclude that

$$\mathcal{B} \cdot \mathbf{v} = 0 \bmod \mathfrak{p}^{\nu+1}.$$

Since $\widetilde{\mathcal{B}}$ has full rank, we find that $\mathbf{v} = 0 \bmod \mathfrak{p}^{\nu+1}$, contradicting the definition of ν, unless indeed $\nu = \infty$ and $\mathbf{v} = 0$. We find that $e_{i,\ell} = r_{i,\ell}$ for all values of i and ℓ, as desired.

For $i > k'$, this means $z_{i,j} = 0$ for all $j \in \{1, \ldots, n_i\}$, so that $\mathcal{P}_{i,j} = Q_i$ for each such i and j. We then apply Lemma 3.2.22 with $\mathcal{P}' = \sum_{i=1}^{k'}(P_{i,1} + \ldots + P_{i,n_i})$ and polynomial f. We conclude that $\mathcal{P}$ is of the desired form. □

3.2.9 Chabauty using the higher order terms

In some situations, there is an obstruction that prevents the matrix in Theorem 3.2.6 to have sufficiently high rank at any prime, but we do expect the outcome of the theorem to hold true.

Example 3.2.23. We consider the degree 2 map $\rho : X_0(73) \to X_0^+(73)$. Let $c_0, c_\infty \in X_0(73)(\mathbb{Q})$ be the two cusps, and consider $\mathcal{Q} = 3c_0$. Note that w_{73} interchanges these cusps, i.e. $\rho(c_0) = \rho(c_\infty)$. Let t be the pullback under ρ of a well-behaved uniformiser at $\rho(c_0)$. Then t is a well-behaved uniformiser at c_0 and at c_∞. The curve $X_0(73)$ has genus 5, and its quotient $X_0^+(73)$ has genus 2. We find a 3-dimensional space of vanishing differentials with trace zero on $X_0^+(73)$ (see Section 3.3.6). Denote by $\omega_1, \omega_2, \omega_3$ a basis. By Proposition 3.2.17, if we write $\mathrm{loc}_{c_0}(\omega_i) = \sum_{j\geq 0} a_{i,j} t^j \mathrm{d}t$ then $\mathrm{loc}_{c_\infty}(\omega_i) = \sum_{j\geq 0}(-a_{i,j}) t^j \mathrm{d}t$. Consider the matrices

$$\mathcal{A}_0 = (a_{i,j})_{\substack{1\leq i\leq 3\\ 0\leq j\leq 2}} \text{ and } \mathcal{A}_\infty = -\mathcal{A}_0.$$

Then $\mathcal{A} := (\mathcal{A}_0 \mid \mathcal{A}_\infty)$ satisfies $\mathrm{rk}(\mathcal{A}) = \mathrm{rk}(\mathcal{A}_0)$. Also, $\mathcal{A}$ is the matrix whose mod p reduction corresponds to the matrix in condition (3) of Theorem 3.2.6 for the point $\mathcal{Q} = 3c_0 + 3c_\infty$. If its reduction $\widetilde{\mathcal{A}}$ modulo any large prime p had rank 3, the entire mod p residue class of $3c_0 + 3c_\infty$ would be contained in $\rho^*\left((X_0^+(73))^{(3)}(\mathbb{Q})\right)$

This is not the case, however. We compute that the Riemann–Roch space $L(3c_0 + 3c_\infty)$ is 3-dimensional, which is unusually large. In fact, we find a degree 6 function $f \in L(3c_0 + 3c_\infty)$ such that $w_{73}^* f \neq f$, i.e. the corresponding map $f : X \to \mathbb{P}^1$ does not factor via ρ. Now note that $3c_0 + 3c_\infty = f^*(1:0)$. So for each prime p of good reduction, the points $R \in \mathbb{P}^1(\mathbb{Q})$ such that $R \equiv (1:0) \bmod p$ satisfy also that $f^*R \equiv 3c_0 + 3c_\infty$. But, as f does not factor via $X_0^+(73)$, f^*R is in general not the pullback of a degree 3 divisor on $X_0^+(73)$. By Theorem 3.2.24, $\widetilde{\mathcal{A}}$ therefore cannot have rank 3, and neither can $\widetilde{\mathcal{A}}_0$. Indeed, we find that ω_3 satisfies $a_{3,0} = a_{3,1} = a_{3,2} = 0$, so that the entire bottom row of $\mathcal{A}_0$ is zero. Therefore, condition (3) in Theorem 3.2.6 is never satisfied for $\mathcal{Q} = 3c_0$.

A similar situation occurs on $X_0(57)$.

In such cases, it can help to look further into the expansion of the 1-forms. We begin with some notation. Consider a point Q on a curve X and a regular 1-form $\omega \in H^0(X, \Omega)$. We expand ω around Q in terms of a uniformiser t_Q at Q, giving $\mathrm{loc}_Q(\omega) = \sum_{j\geq 0} a_j t_Q^j$,

and define

$$v(\omega, t_Q, \ell, k) := \left((-1)^{\ell-1}a_\ell, (-1)^{\ell}a_{\ell+1}, \ldots, (-1)^{k-2}a_{k-1}\right).$$

With this notation, we have $v(\omega, t_Q, k) = v(\omega, t_Q, 0, k)$. For integers j and i such that $j+1 \leq i \leq 2j$ and any $x_1, \ldots, x_j$ in some field, we define

$$\psi_i(x_1, \ldots, x_j) = \sum_{\ell=i-j}^{j} x_\ell x_{i-\ell}.$$

Theorem 3.2.24. *Consider a number field K, a curve X/K and $\mathcal{Q} = \sum_{i=1}^{k} n_i Q_i \in X^{(d)}(K)$, where $d = \sum_{i=1}^{k} n_i$ and $Q_1, \ldots, Q_k \in X$ are distinct points. Let $\mathfrak{r}$ be a prime of K, of good reduction for X, containing the rational prime $p \in \mathfrak{r}$. Denote by $\mathcal{X}/\mathcal{O}_{K_\mathfrak{r}}$ a minimal proper regular model of X/K. Let N be the ramification index of p in $K(\mathcal{Q})$.*

(1) Suppose that $p \geq N+3$.

(2) Suppose that the space $\mathcal{V}$ of vanishing differentials has dimension at least d, and consider linearly independent $\omega_1, \ldots, \omega_d \in \mathcal{V}$ on X. For each Q_i, choose a uniformiser t_{Q_i}, and suppose that the $d \times d$-matrix

$$\mathcal{A} := \begin{pmatrix} v(\omega_1, t_{Q_1}, n_1) & \cdots & v(\omega_1, t_{Q_k}, n_k) \\ \vdots & \ddots & \vdots \\ v(\omega_n, t_{Q_1}, n_1) & \cdots & v(\omega_n, t_{Q_k}, n_k) \end{pmatrix}$$

has rank $r < d$.

We thus choose uniformisers $t_{\widetilde{Q}_i}$ at $\widetilde{Q}_i$, and a basis $\widetilde{\omega}_1, \ldots, \widetilde{\omega}_d$ for the image of $\mathcal{V} \cap H^0(\mathcal{X}, \Omega)$ under reduction mod $\mathfrak{r}$, such that the vectors $v(\widetilde{\omega}_j, t_{\widetilde{Q}_i}, n_i)$ for all $1 \leq i \leq k$ and $r < j \leq d$ are zero vectors.

(3) Assume that the $r \times d$ matrix $\widetilde{\mathcal{A}}_1$ defined below has rank r.

(4) Let $\mathbb{F}$ be the residue field of a prime in $K(\mathcal{Q})$ above $\mathfrak{r}$. Suppose moreover that there are no non-zero vectors $(\widetilde{\mathbf{x}}_1, \ldots, \widetilde{\mathbf{x}}_k) \in \mathbb{F}^d$ solving the system of equations $\widetilde{\mathcal{L}} \cdot \widetilde{\mathbf{w}} = \boldsymbol{0}$, where

$$\widetilde{\mathbf{x}}_i = (\widetilde{x}_{i,1}, \ldots, \widetilde{x}_{i,n_i}),\ \widetilde{\mathcal{L}} = \begin{pmatrix} \widetilde{\mathcal{A}}_1 & 0 \\ 0 & \widetilde{\mathcal{A}}_2 \end{pmatrix},\ \widetilde{\mathcal{A}}_1 = \begin{pmatrix} v(\widetilde{\omega}_1, t_{\widetilde{Q}_1}, n_1) & \cdots & v(\widetilde{\omega}_1, t_{\widetilde{Q}_k}, n_k) \\ \vdots & \ddots & \vdots \\ v(\widetilde{\omega}_r, t_{\widetilde{Q}_1}, n_1) & \cdots & v(\widetilde{\omega}_r, t_{\widetilde{Q}_k}, n_k) \end{pmatrix},$$

$$\widetilde{\mathcal{A}}_2 = \begin{pmatrix} -v(\widetilde{\omega}_{r+1}, t_{\widetilde{Q}_1}, n_1, 2n_1) & \cdots & -v(\widetilde{\omega}_{r+1}, t_{\widetilde{Q}_k}, n_k, 2n_k) \\ \vdots & \ddots & \vdots \\ -v(\widetilde{\omega}_d, t_{\widetilde{Q}_1}, n_1, 2n_1) & \cdots & -v(\widetilde{\omega}_d, t_{\widetilde{Q}_k}, n_k, 2n_k) \end{pmatrix},$$

and

$$\widetilde{\mathbf{w}} = (\widetilde{\mathbf{x}}_1, \ldots, \widetilde{\mathbf{x}}_k, \psi_{n_1+1}(\widetilde{\mathbf{x}}_1), \ldots, \psi_{2n_1}(\widetilde{\mathbf{x}}_1), \psi_{n_2+1}(\widetilde{\mathbf{x}}_2), \ldots, \ldots, \psi_{2n_k}(\widetilde{\mathbf{x}}_k))^T.$$

Then $\mathcal{Q} \in X^{(d)}(K)$ is alone in its mod $\mathfrak{r}$ residue class.

Remark 3.2.25. We emphasize that $\mathrm{rk}(\mathcal{A}) < d$ means that modulo any prime $\mathfrak{p}$ of $K(\mathcal{Q})$ the reduction of $\mathcal{A}$ mod $\mathfrak{p}$ has rank smaller than d, and Theorem 3.2.6 therefore cannot be applied.

Proof. Let $\mathfrak{p}$ be a prime above $\mathfrak{r}$ in $L := K(\mathcal{Q})$ with uniformiser $\pi \in \mathfrak{p}$. Let $\mathcal{P} = \sum_{i=1}^{k}\sum_{j=1}^{n_i} P_{i,j} \in X^{(d)}(K)$ belong to the residue disc of $\mathcal{Q}$, where the sum is arranged such that points $P_{i,j}$ reduce to the same point as Q_i modulo a prime $\mathfrak{q}$ of $F := L(\mathcal{P})$ above $\mathfrak{p}$. For each i, choose t_{Q_i} to be a well-behaved uniformiser at Q_i, and for each i and j, define $z_{i,j} = t_{Q_i}(P_{i,j}) \in \mathcal{O}_{F_\mathfrak{q}}$. Define $s_{i,\ell} = \sum_{j=1}^{n_i} z_{i,j}^{\ell}$, and let $e_{i,\ell}$ be the ℓth elementary symmetric polynomial in $z_{i,1}\ldots, z_{i,n_i}$.

In the theorem's statement, condition (3) implies that $\mathrm{Span}\{\widetilde{\omega}_{r+1},\ldots,\widetilde{\omega}_n\}$ is exactly the space of differentials $\widetilde{\omega}$ on $\widetilde{X}$ satisfying $v(\widetilde{\omega}, t_{\widetilde{Q}_i}, n_i) = 0$ for all i. Note that condition (4) is independent of the choice of bases for $\mathrm{Span}\{\widetilde{\omega}_1,\ldots,\widetilde{\omega}_r\}$ and $\mathrm{Span}\{\widetilde{\omega}_{r+1},\ldots,\widetilde{\omega}_d\}$. Now let $\omega_1,\ldots,\omega_d \in \mathcal{V}\cap H^0(\mathcal{X},\Omega)$ be linearly independent such that $v(\omega_j, t_{Q_i}, n_i) = 0$ for all i and for each $j \in \{r+1,\ldots,d\}$. Having chosen well-behaved uniformisers and integral differential forms we conclude that condition (4) holds for the reductions $\widetilde{\omega}_1,\ldots,\widetilde{\omega}_d$ of $\omega_1,\ldots,\omega_d$ modulo $\mathfrak{r}$. Moreover, the matrices $\widetilde{\mathcal{L}}, \widetilde{\mathcal{A}}_1$ and $\widetilde{\mathcal{A}}_2$ are the mod $\mathfrak{p}$ reductions of corresponding matrices over $\mathcal{O}_{L_\mathfrak{p}}$, defined in terms of $\omega_1,\ldots,\omega_d$.

As in the proof of Theorem 3.2.6, we find that each $e_{i,j} \in \mathcal{O}_{L_\mathfrak{p}}$ by Galois theory. Define

$$\nu := \min_{\substack{i\in\{1,\ldots,k\}\\ j\in\{1,\ldots,n_i\}}} v_\mathfrak{p}(e_{i,j})$$

and assume that $\nu < \infty$. We aim to find a contradiction, giving $\nu = \infty$. Recall that $\nu \geq 1$ because $\mathcal{P}$ and $\mathcal{Q}$ are in the same residue disc. Now define $x_{i,\ell}$ by $e_{i,\ell} = \pi^\nu x_{i,\ell}$. Their mod $\mathfrak{p}$ reductions $\widetilde{x}_{i,\ell}$ will correspond to a non-zero solution of $\widetilde{\mathcal{L}}\cdot\widetilde{\mathbf{w}} = \mathbf{0}$, which we shall show in two parts.

For $\omega \in \{\omega_1,\ldots,\omega_d\}$, we have at each Q_i the expansion $\mathrm{loc}_{Q_i}(\omega) = \sum_{\ell\geq 0} a_\ell(Q_i,\omega)t_{Q_i}^{\ell}\mathrm{d}t_{Q_i}$. As before, we obtain from $\int_{\mathcal{Q}}^{\mathcal{P}}\omega = 0$ the equation

$$0 = \sum_{i=1}^{k}\sum_{\ell=1}^{\infty} a_{\ell-1}(Q_i,\omega)\frac{s_{i,\ell}}{\ell} = 0. \tag{3.15}$$

We again use Lemma 3.2.21 (1) to rewrite this in terms of $e_{i,\ell}$s, and apply Lemma 3.2.21 (3) and Lemma 3.2.20 (with $T = 1$) to the higher order terms to obtain

$$\sum_{i=1}^{k}\sum_{\ell=1}^{n_i}(-1)^{\ell-1}a_{\ell-1}(Q_i,\omega)e_{i,\ell} \equiv 0 \pmod{\mathfrak{p}^{\nu+1}}. \tag{3.16}$$

Dividing by π^ν and ranging over $\omega \in \{\omega_1,\ldots,\omega_r\}$, we obtain $\widetilde{\mathcal{A}}_1\cdot(\widetilde{\mathbf{x}}_1,\ldots,\widetilde{\mathbf{x}}_k)^T = \mathbf{0}$, the "upper half" of $\widetilde{\mathcal{L}}\cdot\widetilde{\mathbf{w}} = \mathbf{0}$.

Consider now any of the remaining vanishing differential forms $\omega \in \{\omega_{r+1},\ldots,\omega_d\}$. Recall that all $a_{\ell-1}(Q_i,\omega) = 0$ for $1 \leq i \leq k$, $1 \leq \ell \leq n_i$. Hence, using Lemma 3.2.21 (2), equation (3.15) in this case becomes

$$\sum_{i=1}^{k} \sum_{\ell=n_i+1}^{2n_i} a_\ell(Q_i,\omega) \cdot \frac{(-1)^\ell}{2} \sum_{m=\ell-n_i}^{n_i} e_{i,m} e_{i,\ell-m} + \text{h.o.t} = 0, \tag{3.17}$$

where each of the higher order terms is of the form $\frac{b}{s} \cdot e_{i,i_1} \cdots e_{i,i_s}$ with $s \geq 3$ and $b \in \mathcal{O}_{L_\mathfrak{p}}$. Now $s \geq 3$ implies by Lemma 3.2.20 (with $T = 2$) that $v_\mathfrak{p}(e_{i,i_1} \cdots e_{i,i_s}) \geq 2\nu + (s-2) \geq 2\nu + 1 + N\mathrm{ord}_p(s)$. We conclude that all higher order terms vanish mod $\mathfrak{p}^{2\nu+1}$. Multiplication by 2 (note that $2 \notin \mathfrak{p}$) and division by $\pi^{2\nu}$ of (3.17) now yields

$$\widetilde{\mathcal{A}}_2 \cdot (\psi_{n_1+1}(\widetilde{\mathbf{x}}_1), \ldots, \psi_{2n_1}(\widetilde{\mathbf{x}}_1), \psi_{n_2+1}(\widetilde{\mathbf{x}}_2), \ldots, \psi_{2n_k}(\widetilde{\mathbf{x}}_k))^T = 0,$$

as desired. Note that $(\mathbf{x}_1, \ldots, \mathbf{x}_k) \neq \mathbf{0} \bmod \mathfrak{p}$ by maximality of ν. This solution of $\widetilde{\mathcal{L}} \cdot \widetilde{\mathbf{w}} = \mathbf{0}$ contradicts our assumption, so we must have $\nu = \infty$ and $e_{i,\ell} = 0$ for all i and ℓ, so that also $z_{i,j} = 0$ for all i and j and $\mathcal{P} = \mathcal{Q}$ by injectivity of well-behaved uniformisers on residue classes. □

3.3 Applying Chabauty to modular curves

To compute quadratic, cubic and quartic points on our modular curves, we use Theorems 3.2.6 and 3.2.24 in combination with the Mordell–Weil sieve described in Section 1.2.5.

3.3.1 The input of the sieve

For each $N \in \mathbb{Z}_{>1}$, we have a degree 2 map $\rho_N \colon X_0(N) \to X_0^+(N)$, where $X_0^+(N)$ is the quotient of $X_0(N)$ by the Atkin–Lehner involution w_N. In this section, we describe how we computed the necessary input to successfully sieve for the rational points on $X_0(N)^{(d)}$. This consists of the following four parts:

(i) explicit defining equations for $X_0(N)$ as well as the corresponding Atkin–Lehner involutions,

(ii) a (finite) list $\mathcal{L}'$ of known rational points on $X_0(N)^{(d)}$,

(iii) a list of generators of a subgroup $G \subset J(\mathbb{Q})$ and an integer I such that $I \cdot J(\mathbb{Q}) \subset G$,

(iv) for each prime p used in the sieve, at least d linearly independent "reductions of vanishing differentials", with trace zero unless $N = 57$, i.e. elements of the image $\widetilde{\mathcal{V}}$ of $\mathcal{V} \cap H^0(\mathcal{X}_0(N), \Omega)$ under reduction mod p, where $\mathcal{V} \subset H^0(X_0(N), \Omega)$ is the space of vanishing differentials, with trace zero to $X_0^+(N)$ unless $N = 57$, and $\mathcal{X}_0(N)/\mathbb{Z}_p$ is a minimal proper regular model for $X_0(N)_{\mathbb{Q}_p}$.

When $N = 57$, we define $\mathcal{L} = \mathcal{L}'$. For the other values of N, we define $\mathcal{L}$ to be the union of $\mathcal{L}'$ and

- $\rho_N^* X_0^+(N)(\mathbb{Q})$ (when $d = 2$),
- each set $P + \rho_N^* X_0^+(N)(\mathbb{Q})$ for known points $P \in X_0(N)(\mathbb{Q})$ (when $d = 3$), and

- $\rho_N^* X_0^+(N)^{(2)}(\mathbb{Q})$ and $\mathcal{P} + \rho_N^* X_0^+(N)(\mathbb{Q})$ for known points $\mathcal{P} \in X_0(N)^{(2)}(\mathbb{Q})$ (when $d = 4$).

With this set $\mathcal{L}$ of "known points", we then apply the Mordell–Weil sieve as described in Section 1.2.5, where $V = X_0(N)^{(d)}$, $S = V$, $\mathcal{A} = J_0(N)$,

$$\iota\colon X_0(N)^{(d)}(\mathbb{Q}) \to J_0(N)(\mathbb{Q}),\ D \mapsto I \cdot [D - D_0]$$

for given $D_0 \in X_0(N)^{(d)}(\mathbb{Q})$, $B = W = G$ and $\phi : G \hookrightarrow J_0(N)(\mathbb{Q})$. Finally, we define

$$\mathcal{M}_p = \iota_p^{-1}(\phi_p(B)) \setminus \mathcal{N}_p,$$

where $\mathcal{N}_p \subset \widetilde{X}_0(N)^{(d)}$ are the reductions of those points in $\mathcal{L}'$ satisfying the conditions of Theorem 3.2.6 or Theorem 3.2.24. To apply these theorems, we need the input (iv).

We note that knowing more than d vanishing differentials tends to increase the size of $\mathcal{N}_p$, therefore improving the speed and the chance of success of the sieve. After giving some details regarding our implementation of the sieve, we describe how to obtain the input (i)-(iv) for our modular curves in the sections to come.

Remark 3.3.1. Suppose that we can find one rational point P on $X = X_0(N)$. Then each other rational point $Q \in X(\mathbb{Q})$ will occur in $X^{(2)}(\mathbb{Q})$ at least twice: as $2Q$ and as $P + Q$. At most one of these degree 2 points is the pullback of $\rho_N(Q)$, so at least one pair will occur as an isolated point of $X^{(2)}(\mathbb{Q})$. This means that, as a byproduct, we also determine the rational points when we find these isolated points. Indeed each of the modular curves we consider contains a rational point. Similarly, $X^{(3)}(\mathbb{Q}) \setminus \cup_{Q \in X(\mathbb{Q})}(Q + \rho_N^* X_0^+(N)(\mathbb{Q}))$ determines $X^{(2)}(\mathbb{Q}) \setminus \rho_N^* X_0^+(N)(\mathbb{Q})$, and $X^{(4)}(\mathbb{Q}) \setminus (\rho_N^* X_0^+(N)^{(2)}(\mathbb{Q}) \cup (\rho_N^* X_0^+(N)(\mathbb{Q}) + X^{(2)}(\mathbb{Q})))$ determines $X^{(3)}(\mathbb{Q}) \setminus \cup_{Q \in X(\mathbb{Q})}(Q + \rho_N^* X_0^+(N)(\mathbb{Q}))$.

3.3.2 Implementing the sieve efficiently

We use the notation introduced in Section 1.2.5. Let X be a curve, and suppose that we are sieving for $V = X^{(d)}$. Assume for simplicity that $S = V(\mathbb{Q})$ and $W = B$ in the sieve described in Section 1.2.5. We also assume that $\mathcal{A} = J(X)$ and $\iota\colon X^{(d)} \to J(X)$ is given by $\iota(D) = I \cdot [D - D_0]$ for given $D_0 \in X^{(d)}(\mathbb{Q})$ and $I \in \mathbb{Z}_{\geq 1}$. This is the situation in which we find ourselves for $X = X_0(N)$. The groups $J(\widetilde{X})(\mathbb{F}_p)$ can be computed using the class group algorithm of Hess [Hes02]. When d and p are large (especially when $d \geq 4$), it is important to implement the sieve in an efficient way. Rather than first computing $\mathcal{M}_{p_i}$ for each i and intersecting afterwards, we compute intersections recursively. It also turns out that computing $\widetilde{X}^{(d)}(\mathbb{F}_p)$ and ι_p for large values of d and p is suboptimal, so instead we compute Riemann–Roch spaces (defined in Section 1.2.4) as follows.

Consider the setting of Section 1.2.5, and define $H_{i-1} := \ker(\phi_{p_1}) \cap \ldots \cap \ker(\phi_{p_{i-1}})$. Suppose that we have computed the finite set W_{i-1} of H_{i-1}-coset representatives for $\cap_{j=1}^{i-1} \phi_{p_j}^{-1}(\iota_{p_j}(\mathcal{M}_{p_j}))$, and we want to compute W_i. First, we split up $W_{i-1} + H_{i-1}$ into H_i-cosets, yielding a set W_i' of H_i-coset representatives for the same intersection up to

$i-1$. For each $w \in W_i'$, we check whether $w \in W_i$ by computing the $\mathbb{F}_p$-vector spaces

$$L(z + \widetilde{D}_0) \text{ for each } z \text{ such that } I \cdot z = \phi_{p_i}(w).$$

Often these spaces will simply all be 0-dimensional and $w \notin W_i$. For each non-zero $f \in L(z + \widetilde{D}_0)$, we obtain $\operatorname{div}(f) + z + \widetilde{D}_0 \in \widetilde{X}^{(d)}(\mathbb{F}_p)$, and we verify whether it is in the image of $\mathcal{L}'$ and satisfies the conditions of Theorem 3.2.6 or Theorem 3.2.24. This way, we determine $W_i \subset W_i'$ without the need to compute $\widetilde{X}^{(d)}(\mathbb{F}_p)$. When W_{i-1} is small, these computations tend to be fast.

We mention another improvement. When p_1 and p_2 are distinct primes such that $\#J(\widetilde{X})(\mathbb{F}_{p_1})$ and $\#J(\widetilde{X})(\mathbb{F}_{p_2})$ are coprime, we have $\phi_{p_2}(\operatorname{Ker}(\phi_{p_1})) = \phi_{p_2}(B)$ by the Chinese Remainder theorem, so the two primes provide "disjoint" information. One thus tends to choose primes p such that the numbers $\#J(\widetilde{X})(\mathbb{F}_p)$ have prime factors in common. Often these common factors are powers of small primes, whereas $\#J(\widetilde{X})(\mathbb{F}_p)$ tends to also be divisible by a large prime factor, let us call it r. It is unlikely that r will also divide $\#J(\widetilde{X})(\mathbb{F}_q)$ for any other prime q we consider, hence the "mod r" information is of little use. It does, however, slow the sieve down considerably, because information is stored in H_i-cosets and the factor r increases the index of H_i. We remedy this by composing ι_p and ϕ_p with the multiplication-by-r map m_r, thereby "forgetting" the mod r information. For more information about choosing primes in the sieve, we refer to [BS10].

3.3.3 A model for $X_0(N)$

We compute the models as described in Section 1.2.2.

For primes p where the chosen model has good reduction, we define $\mathcal{X}_0(N)$ to be the $\mathbb{Z}_p$-scheme defined by these equations. In these cases, $\mathcal{X}_0(N)$ is our minimal proper regular model.

3.3.4 Searching for points

We search for points as described in Section 1.2.6. For rational, quadratic and cubic points, the hyperplane decomposition method of Özman and Siksek suffices, whereas for the quartic points on $X_0(65)$, we used the sieve method.

3.3.5 Determining subgroups of the Mordell–Weil groups

To determine subgroups of the Mordell–Weil groups, we remind the reader that we outlined possible methods in Section 1.2.3; particularly useful will be Proposition 1.2.2.

Let us first compute the torsion subgroups. For each N, let $C_0(N)(\mathbb{Q})$ be rational cuspidal subgroup of $J_0(N)(\mathbb{Q})$, defined in Section 1.2.3.

Lemma 3.3.2. *For $N \in \{43, 53, 61, 67, 73\}$ the torsion subgroup of $J_0(N)(\mathbb{Q})$ is generated by the difference of the two cusps, the orders of which are, respectively, 7, 13, 5, 11 and 6. The torsion subgroups of $J_0(57)(\mathbb{Q})$ and $J_0(65)(\mathbb{Q})$ also equal their rational cuspidal subgroups, which are $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$ respectively as abstract groups.*

Proof. For the prime values of N, this is the theorem of Mazur mentioned in Section 1.2.3. For $N = 57$, we use `Magma` code of Özman and Siksek [OS19] to compute $C_0(57)(\mathbb{Q})$ as a group, which gives $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$. As 5 is a prime of good reduction for $X_0(57)$, we find that $J_0(57)(\mathbb{Q})_{\text{tors}}$ injects into $J_0(57)(\mathbb{F}_5)$. We compute that

$$J_0(57)(\mathbb{F}_5) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$

so that the index $[J_0(57)(\mathbb{Q})_{\text{tors}} : C_0(57)(\mathbb{Q})]$ divides 18. Looking at $J_0(57)(\mathbb{F}_{23})$, we find that the index is coprime to 3, and from $J_0(57)(\mathbb{F}_{11})$ we learn that the index is odd, leaving index 1 as only option. A similar computation at the primes 3 and 11 allows us to determine $J_0(65)(\mathbb{Q})_{\text{tors}}$. □

We verify that the hypothesis for Proposition 1.2.2 holds true for the maps $\rho_N \colon X_0(N) \to X_0^+(N)$.

Lemma 3.3.3. *For each $N \in \{43, 53, 61, 57, 65, 67, 73\}$, we have*

$$\operatorname{rk}(J_0(N)(\mathbb{Q})) = \operatorname{rk}(J_0^+(N)(\mathbb{Q})).$$

Proof. For each N, there is an abelian variety A satisfying $J_0(N) \sim J_0^+(N) \times A$. As described in Section 1.2.3, we use the algorithm of Stein [Ste00] as implemented in the Modular Arithmetic Geometry package in `Magma`, together with Kolyvagin–Logachëv [KL89], to decide that $\operatorname{rk}(A(\mathbb{Q})) = 0$. □

We note that $\operatorname{rk}(J_0(N)(\mathbb{Q})) = 2$ for $N \in \{67, 73\}$ and $\operatorname{rk}(J_0(N)(\mathbb{Q})) = 1$ for the other values of N. Also $X_0^+(N)$ has genus 2 for $N \in \{57, 67, 73\}$ and genus 1 otherwise, making $X_0^+(N)$ either an elliptic curve or a hyperelliptic curve. When $X_0^+(N)$ is an elliptic curve, we can compute a basis for its Mordell–Weil group using Cremona's algorithm [Cre97] implemented in `Magma`. When it is hyperelliptic of genus 2, we manage to do the same using height bounds and an algorithm of Stoll [Sto02]. We pull these generators back to $X_0(N)$. Together with the torsion subgroup, this gives us by Proposition 1.2.2 an explicit finite index subgroup $G \subset J_0(N)(\mathbb{Q})$ satisfying $2 \cdot J_0(N)(\mathbb{Q}) \subset G$, for each of the values of N we consider. We have written down the explicit generators in Section 3.4.

Example 3.3.4. Let us give a few more details in the case $X = X_0(57)$. The quotient $X_0^+(57)$ has a model defined by $y^2 = x^6 - 2x^5 + 3x^4 + 3x^2 - 2x + 1$. Stoll's algorithm [Sto17] may be used to show the free part of $J_0^+(N)(\mathbb{Q})$ is generated by $Q = \infty^+ - \infty^-$. Pulling Q back to $J_0(57)$ gives $\rho^*(Q) = (1 : 1 : 0 : 1 : 0) + (6 : 9 : -1 : 7 : 2) - P - \overline{P}$, where

$$P = \left(-\sqrt{-2} + 4 : -4\sqrt{-2} + 7 : \sqrt{-2} - 1 : -2\sqrt{-2} + 2\right).$$

The Mordell-Weil group of $J_0(65)$

Let $\rho : X_0(65) \to X_0^+(65)$ be the quotient map. The latter is the elliptic curve

$$X_0^+(65) \colon y^2 + xy = x^3 - x,$$

and we find that $(1,0)$ generates the free part of its rank 1 Mordell–Weil group. The group $G \subset J_0(65)(\mathbb{Q})$ generated by the two subgroups

$$\rho^*(J_0^+(65)(\mathbb{Q})) \text{ and } J_0(65)(\mathbb{Q})_{\text{tors}}$$

is isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$. Denote by $D = \rho^*((1,0) - O)$ a generator of the free part of G, where $O \in X_0^+(65)(\mathbb{Q})$ is the zero element. To determine the quartic points on $X_0(65)$, we use the Abel–Jacobi map $\iota : X_0(65)(\mathbb{Q})^{(4)} \to J_0(\mathbb{Q})$ given by $P \mapsto [P - 2\rho^* O]$.

A priori $G \subset J_0(65)(\mathbb{Q})$ has at most index two. Whilst the Mordell–Weil sieve normally allows one to get away with a subgroup of known finite index, this appears not to be the case here for quartic points. We thus make an effort to show that $G = J_0(65)(\mathbb{Q})$ by studying $J_0(65)(K)$ for a quadratic extension $K/\mathbb{Q}$. Then we obtain the set of rational points as $J_0(65)(\mathbb{Q}) = J_0(65)(K)^{\text{Gal}(K/\mathbb{Q})}$.

Theorem 3.3.5. *The Mordell-Weil group $J_0(65)(\mathbb{Q})$ of $X_0(65)$ is the group generated by the two subgroups*

$$\rho^*(J_0^+(65)(\mathbb{Q})) \textit{ and } J_0(65)(\mathbb{Q})_{\text{tors}}.$$

Proof. Let us abbreviate $J_0(65)$ to J. We still define $G = \langle \rho^*(J_0^+(65)(\mathbb{Q})), J(\mathbb{Q})_{\text{tors}} \rangle$. We have explicit generators for $G \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$; let us denote them by D, T_2 and T_{84} respectively, where D is as above. By Lemmas 3.3.3 and 3.3.2 and Proposition 1.2.2, it suffices to show that no element in $D + \langle T_2, T_{84} \rangle$ is the double of a point in $J(\mathbb{Q})$, or, equivalently, that none of D, $D + T_2$, $D + T_{84}$ and $D + T_2 + T_{84}$ are doubles. The mod 7 reductions of the latter three are *not* doubles in $J(\mathbb{F}_7)$, so they cannot be doubles in $J(\mathbb{Q})$ either. We thus focus our attention on D.

There are four points which double to $(1,0)$ on $X_0^+(65)$, one of which is $d_0 := ((\sqrt{5}+1)/2, -(\sqrt{5}+3)/2)$. The pullback $D_0 := \rho^*(d_0 - O)$ then satisfies $2D_0 = D$.

We claim $J(K)_{\text{tors}} = J(\mathbb{Q})_{\text{tors}}$ for $K = \mathbb{Q}(\sqrt{5})$. To verify this, we compute $J(\mathbb{F}_p)$ as an abstract group for $p = 11$ and $p = 19$, primes that split in $\mathbb{Q}(\sqrt{5})$. For these primes we have embeddings $J(K)_{\text{tors}} \hookrightarrow J(\mathbb{F}_p)$. We obtain

$$J(\mathbb{F}_{11}) = \mathbb{Z}/2\mathbb{Z} \times \frac{\mathbb{Z}}{2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 37\mathbb{Z}} \text{ and } J(\mathbb{F}_{19}) = \frac{\mathbb{Z}}{2 \cdot 3 \cdot 23\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2 \cdot 3 \cdot 7 \cdot 13 \cdot 23},$$

from which it is quickly deduced that $J(K)_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z}$. We thus have an equality of sets

$$S := \{x \in J(K) \mid 2x = D\} = \{D_0 + T \mid T \in J(\mathbb{Q})[2]\}.$$

We show that $D_0 \notin J(\mathbb{Q})$. Denote by d_0^c the Galois conjugate of d_0. Then both $d_0 + d_0^c$ and $2d_0$ are in $X_0^+(65)(\mathbb{Q})$, so also $Q := d_0 - d_0^c \in X_0^+(65)(\mathbb{Q})$. Now $Q = Q^c = -Q$, so Q is the unique non-trivial point in $X_0^+(65)(\mathbb{Q})[2]$. We find that $D_0 - D_0^c = \rho^* Q$, and it suffices to show that $\rho^* Q \neq 0 \in J(\mathbb{Q})$. We can check this modulo 7. Hence none of the elements in S is in $J(\mathbb{Q})$, and so we must have that $J(\mathbb{Q}) = G$, as desired. $\square$

3.3.6 The vanishing differentials

Let $\rho\colon X \to C$ be a non-constant morphism of curves over $\mathbb{Q}$ such that $\mathrm{rk}(J(X)(\mathbb{Q})) = \mathrm{rk}(J(C)(\mathbb{Q}))$. This is exactly the case in which we find ourselves, where for us $X = X_0(N)$ and $C = X_0^+(N)$. We obtain a trace, or pushforward, map

$$\rho_* = \mathrm{Tr}\colon H^0(X, \Omega) \to H^0(C, \Omega).$$

Define $\mathcal{V} := \mathrm{Ker}(\mathrm{Tr})$. Now suppose that p a prime of good reduction for X and C and that $\mathcal{X}/\mathbb{Z}_p$ and $\mathcal{C}/\mathbb{Z}_p$ are minimal proper regular models for $X_{\mathbb{Q}_p}$ and $C_{\mathbb{Q}_p}$ respectively.

Lemma 3.3.6. *All differentials $\omega \in \mathcal{V}$ annihilate $J(X)(\mathbb{Q})$ via the integration pairing, i.e.*

$$\int_0^D \omega = 0 \textit{ for all } D \in J(X)(\mathbb{Q}).$$

Proof. We again find that $J(X) \sim J(C) \times A$ for some abelian variety A such that $A(\mathbb{Q})$ is torsion. If we identify $\mathcal{V}$ with a subspace of $H^0(J(X), \Omega_{J(X)/\mathbb{Q}})$, then $\mathcal{V} = \pi^* H^0(A, \Omega_{A/\mathbb{Q}})$ by Lemma 3.2.2 (ii), where π is the map $J(X) \to A$. Let $\omega \in \mathcal{V}$ and consider $\eta \in H^0(A, \Omega_{A/\mathbb{Q}})$ such that $\omega = \pi^*\eta$. Consider $D \in J(X)(\mathbb{Q})$ and let n be the order of $\pi(D)$ in $A(\mathbb{Q})$. By Proposition 3.2.3 (ii) and (vi), we find

$$\int_D \omega = \int_{\pi(D)} \eta = \frac{1}{n} \int_{n\pi(D)} \eta = 0,$$

as desired. □

Having computed X, C and ρ explicitly, one can also compute $\mathcal{V}$ explicitly. Note that $\dim(\mathcal{V}) = \mathrm{genus}(X) - \mathrm{genus}(C)$. In order to apply Theorems 3.2.6 and 3.2.24, we need to compute the image $\widetilde{\mathcal{V}}$ of $\mathcal{V} \cap H^0(\mathcal{X}, \Omega)$ under the reduction map. Rather than deciding which 1-forms are integral and reducing them, we compute this space directly in terms of the reduction $\widetilde{X}$ of X. Note that ρ extends to a map $\rho\colon \mathcal{X} \to \mathcal{C}$ of minimal proper regular models over $\mathbb{Z}_p$. Denote its restriction to special fibres by $\widetilde{\rho}\colon \widetilde{X} \to \widetilde{C}$. The following proposition allows us to easily compute $\widetilde{\mathcal{V}}$ in practice.

Proposition 3.3.7. *Suppose that p is coprime to $\deg(\rho)$. Then the space $\widetilde{\mathcal{V}}$ is the kernel of $\widetilde{\rho}_*\colon H^0(\widetilde{X}, \Omega) \to H^0(\widetilde{C}, \Omega)$.*

Proof. It is clear that $\widetilde{\mathcal{V}} \subset \mathrm{Ker}(\widetilde{\rho}_*)$. Conversely, consider $\eta \in \mathrm{Ker}(\widetilde{\rho}_*)$. We shall show in Lemma 3.3.8 that there exists $\omega \in H^0(\mathcal{X}, \Omega)$ lifting η. Since $\eta \in \mathrm{Ker}(\widetilde{\rho}_*)$, we find that $\rho_*\omega$ reduces to zero mod p. In particular, by our assumption on p we find that $\omega_0 := \omega - \frac{1}{d}\rho^*\rho_*\omega \in H^0(\mathcal{X}, \Omega)$ is still a lift of η, where $d = \deg(\rho)$. Also, by construction, $\omega_0 \in \mathrm{Ker}(\rho_*)$, so indeed $\eta \in \widetilde{\mathcal{V}}$. □

By Lemma 3.3.3, we are indeed in the situation of a map $\rho\colon X \to C$ such that $\mathrm{rk}(J(X)(\mathbb{Q})) = \mathrm{rk}(J(C)(\mathbb{Q}))$ for $X = X_0(N)$ with $N \in \{43, 53, 61, 65, 67, 73\}$ and $C = X_0^+(N)$. Then for $p > 2$, we have $\widetilde{\mathcal{V}} = \mathrm{Ker}(\widetilde{\rho}_{N,*}) = \mathrm{Ker}(1 + \widetilde{w}_N^*) = \mathrm{Im}(1 - \widetilde{w}_N^*)$,

where $\widetilde{w}_N^*\colon H^0(\widetilde{X}_0(N),\Omega) \to H^0(\widetilde{X}_0(N),\Omega)$ is the reduction of the Atkin–Lehner operator. While we are also in this situation for $X = X_0(57)$, we can do better. Here, in fact $X_0(57)/\langle w_3, w_{19}\rangle$ is a rank 1 elliptic curve, so that we can apply the above to the degree 4 map $\pi_{57}\colon X_0(57) \to X_0(57)/\langle w_3, w_{19}\rangle$ and obtain a 4-dimensional space of vanishing differentials. Now $\widetilde{\mathcal{V}} = \mathrm{Ker}(\widetilde{\pi}_{57,*}) = \mathrm{Im}(1-\widetilde{w}_3^*) + \mathrm{Im}(1-\widetilde{w}_{19}^*)$.

It remains to prove the following lemma. While this fact is commonly known, we could not find a satisfying reference.

Lemma 3.3.8. *Let $X/\mathbb{Q}$ be a (smooth projective) curve with minimal proper regular model $\mathcal{X}/\mathbb{Z}_p$. Then the reduction map $H^0(\mathcal{X},\Omega_{\mathcal{X}/\mathbb{Z}_p}) \to H^0(\widetilde{X},\Omega_{\widetilde{X}/\mathbb{F}_p})$ is surjective.*

Proof. On the level of sheaves, the Cartesian diagram defining the fibre $\widetilde{X}$ yields the isomorphism

$$\Omega_{\widetilde{X}/\mathbb{F}_p} \simeq \Omega_{\mathcal{X}/\mathbb{Z}_p}|_{\widetilde{X}} \otimes_{\mathbb{Z}_p} \mathbb{F}_p,$$

where $\Omega_{\mathcal{X}/\mathbb{Z}_p}|_{\widetilde{X}}$ is the sheaf associated to

$$U \mapsto \varinjlim_{V\supset U} H^0(V,\Omega_{\mathcal{X}/\mathbb{Z}_p})$$

(see Proposition 8.10 in [Har77]). Moreover, this isomorphism defines the reduction map $H^0(\mathcal{X},\Omega_{\mathcal{X}/\mathbb{Z}_p}) \to H^0(\widetilde{X},\Omega_{\widetilde{X}/\mathbb{F}_p})$ on global sections.

We first note that every Zariski-open subset of $\mathcal{X}$ containing $\widetilde{X}$ equals $\mathcal{X}$: if $V \subset \mathcal{X}$ is a Zariski-open set containing $\widetilde{X}$, then its complement is a closed subset (in $\mathcal{X}$) of the generic fibre X. However, the closure (in $\mathcal{X}$) of any point $P \in X$ contains its reduction $\widetilde{P} \in \mathcal{X}$, so $\mathcal{X} \setminus V = \emptyset$.

Now for simplicity, we write $A = H^0(\mathcal{X},\Omega_{\mathcal{X}/\mathbb{Z}_p})$ and $B = H^0(\widetilde{X},\Omega_{\widetilde{X}/\mathbb{F}_p})$. We will show that $A/pA \simeq B$. Note that pA is in the kernel of $A \to B$. Next, by flatness of $\mathcal{X} \to \mathrm{Spec}\mathbb{Z}_p$, we have that $\mathrm{rank}_{\mathbb{Z}_p} A = g = \dim_{\mathbb{F}_p} B$. Therefore, the induced map $A/pA \to B$ is a linear map of $\mathbb{F}_p$-vector spaces of equal dimension. It thus suffices to show that each $\omega \in \ker(A \to B)$ is a p-fold. We first show this to be true locally. Consider $\omega \in \ker(A \to B)$. By the above isomorphism of sheaves, there exists an open cover $\{U\}$ of $\widetilde{X}$ such that

$$H^0(U,\Omega_{\widetilde{X}/\mathbb{F}_p}) \simeq \varinjlim_{V\supset U} H^0(V,\Omega_{\mathcal{X}/\mathbb{Z}_p}) \otimes_{\mathbb{Z}_p} \mathbb{F}_p \quad \text{for each } U.$$

Note that it does not matter whether we tensor with $\mathbb{F}_p$ inside or outside the limit. By this isomorphism, there must be open $V_U \supset U$ and $\eta_U \in H^0(V_U,\Omega_{\mathcal{X}/\mathbb{Z}_p})$ such that $\omega|_{V_U} = p\eta_U$. Since $\bigcup_U V_U$ is an open subset of $\mathcal{X}$ containing $\widetilde{X}$, the V_U must cover $\mathcal{X}$ entirely. As $(\omega|_{V_U})_{V_U}$ lifts to the global section ω and we are working in characteristic zero, also the η_U must agree on overlaps and lift to $\eta \in A$ such that $\omega = p\eta$. □

3.3.7 Two examples

We now give explicit examples of Theorems 3.2.6 and 3.2.24 in use.

Example 3.3.9. Let us consider the non-cuspidal rational point Q ramified under the map $\rho : X_0(67) \to X_0^+(67)$. This gives rise to the point $3Q$ in $X_0(67)(\mathbb{Q})^{(3)}$. We will apply Theorem 3.2.6 with $\mathfrak{r} = 19$ to show any other element in its residue disc also belongs to the set $Q + \rho^* X_0^+(67)(\mathbb{Q})$. Writing $3Q = Q + \rho^*\rho(Q)$, we see it is enough to show the matrix $\widetilde{\mathcal{A}}$ defined in Theorem 3.2.6 has rank two. We find three linearly independent vanishing differentials with trace zero, generating the subspace $\mathrm{Im}(1 - \widetilde{w}_{67}^*) \subset H^0(\widetilde{X}_0(67), \Omega)$. We compute $\widetilde{\mathcal{A}}$ with respect to the reduction $\widetilde{s}$ of a well-behaved uniformiser s at Q such that $s^2 = \rho^* t$, where t is a well-behaved uniformiser at $\rho(Q)$. We find

$$\widetilde{\mathcal{A}} = \begin{pmatrix} 15 & 0 & 0 \\ 2 & 0 & 2 \\ 6 & 0 & 11 \end{pmatrix},$$

indeed of rank 2. The second column is identically zero, as predicted by Proposition 3.2.17.

Example 3.3.10. As explained in Example 3.2.23, Theorem 3.2.6 will always fail for the points $3c_0, 3c_\infty \in X_0(73)(\mathbb{Q})^{(3)}$, where $c_0, c_\infty \in X_0(73)(\mathbb{Q})$ are the cusps. To fix this, we need to look further into the expansion of the differentials. We find three linearly independent vanishing differentials with trace zero generating $\mathrm{Im}(1 - w_{73}^*) \subset H^0(X_0(73), \Omega)$. We verify the conditions of Theorem 3.2.24. Given a choice of uniformiser, the corresponding matrix $\mathcal{A}$ for $3c_\infty$ defined in Theorem 3.2.24 is

$$\mathcal{A} = \begin{pmatrix} 2 & -13 & 47 \\ 0 & -1 & 11 \\ 0 & 0 & 0 \end{pmatrix},$$

which clearly has rank 2. We consider the prime $\mathfrak{r} = 19$. Choosing three generators of $\mathrm{Im}(1 - \widetilde{w}_{73}^*) \subset H^0(\widetilde{X}_0(73), \Omega)$ we obtain the $\mathbb{F}_{19}$-matrices (defined in Theorem 3.2.24)

$$\widetilde{\mathcal{A}}_1 = \begin{pmatrix} 9 & 1 & 1 \\ 0 & 16 & 9 \end{pmatrix} \text{ and } \widetilde{\mathcal{A}}_2 = \begin{pmatrix} 2 & 6 & 3 \end{pmatrix}.$$

One then checks $\widetilde{\mathcal{L}} \cdot (x, y, z, y^2 + 2xz, 2yz, z^2)^T = \mathbf{0}$ has no non-zero solutions $(x, y, z) \in \mathbb{F}_{19}^3$.

3.4 Results

In this section we list the found points on our curves. We provably determined that these are *all* the claimed points, by implementing the Mordell–Weil sieve for each of the curves as described in Section 3.3. By an *isolated quadratic (resp. quartic) point* on $X_0(N)$ we mean a quadratic (resp. quartic) point on $X_0(N)$ also mapping to a quadratic (resp. quartic) point on $X_0^+(N)$. We determined the isolated quadratic points on $X_0(N)$ for $N \in \{43, 53, 61, 65, 67, 73\}$ and all quadratic points on $X_0(57)$. For $X_0(67)$ and $X_0(73)$, we nonetheless obtain a list of *all* quadratic points thanks to the work of [BBB+], who determined $X_0^+(67)(\mathbb{Q})$ and $X_0^+(73)(\mathbb{Q})$. For $N \in \{53, 57, 61, 65, 67, 73\}$ we determine the set of cubic points on $X_0(N)$, and for $X_0(65)$ we moreover list the 44 Galois orbits of

isolated quartic points. We also list any non-cuspidal rational points, c.f. Remark 3.3.1.

Models for $X_0(N)$ are always given in projective space. For elliptic curves, O always denotes the zero element, which equals $(0:1:0)$ in every case. For even degree hyperelliptic curves $y^2 = f(x)$, we denote by $\infty^+ = (1:1:0)$ and $\infty^- = (1:-1:0)$ the points at infinity. The column denoted by CM lists the discriminant of the order by which the elliptic curve has complex multiplication if it does, and NO if it does not have CM.

An elliptic curve E defined over a number field K is said to be a $\mathbb{Q}$-curve if it is $\overline{\mathbb{Q}}$-isogenous to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates. For example, all elliptic curves with rational j-invariant are $\mathbb{Q}$-curves, as are CM elliptic curves. The column "$\mathbb{Q}$-c" denotes the Atkin–Lehner operators defining an isogeny between the elliptic curve and one of its Galois conjugates if there is one, and moreover NO or YES according to whether the curve is a $\mathbb{Q}$-curve. For quadratic points, YES is omitted when an isogeny is already given.

We note that each non-isolated quadratic point on $X_0(N)$ corresponds to a $\mathbb{Q}$-curve, because the isogeny w_N maps the elliptic curve to its Galois conjugate. Similarly, each non-isolated quartic point on $X_0(N)$ is a K-curve for some quadratic field K.

Let us explain how we determined which j-invariants of isolated points correspond to $\mathbb{Q}$-curves. We know that the non-CM cubic points on $X_0(N)$ for $N \in \{53, 57, 61, 67, 73\}$ do not give rise to $\mathbb{Q}$-curves: this follows from Theorem 1.1 in [CN20]. For $N = 65$, the same may be deduced from combining [CN20, Theorem 2.7] and [CN20, Corollary 3.4]. Cremona and Najman describe an algorithm to determine whether an elliptic curve is a $\mathbb{Q}$-curve or not in §5.5 of [CN20]. We use this algorithm to show the isolated quartic points on $X_0(65)$ which give rise to $\mathbb{Q}$-curves are exactly the CM points. This algorithm has been implemented in `Sage` [Cre]. However, as part of this implementation the conductor is computed, and this appears to be too costly for our elliptic curves. Instead, we partially implemented the algorithm in `Magma` and avoid computing the conductor.

3.4.1 $X_0(43)$

Model for $X_0(43)$:

$$x_0^3x_2 - 2x_0^2x_1^2 + 2x_0^2x_1x_2 - 2x_0^2x_2^2 + x_0x_1^3 + 3x_0x_1^2x_2 - 5x_0x_1x_2^2 + 3x_0x_2^3 - 9x_1^4 + 24x_1^3x_2 - 28x_1^2x_2^2 + 16x_1x_2^3 - 4x_2^4 = 0.$$

Genus $X_0(43)$: 3.
Cusps: $(1:0:0)$, $(1:1:1)$.
$X_0(43)^+$: elliptic curve $y^2 + y = x^3 + x^2$ of conductor 43.
Mordell–Weil group of quotient: $J_0^+(43)(\mathbb{Q}) = \mathbb{Z} \cdot [Q - O]$, where $Q := (0, -1)$.
A subgroup $G \subset J_0(43)(\mathbb{Q})$ satisfying $2 \cdot J_0(43)(\mathbb{Q}) \subset G$ is $G = \mathbb{Z} \cdot D_1 \oplus \mathbb{Z}/7\mathbb{Z} \cdot D_{\mathrm{tor}}$, where $D_{\mathrm{tor}} = [(1:1:1) - (1:0:0)]$ and $D_1 = [P + \overline{P} - (1:1:1) - (1:0:0)] = \rho^*[Q - O]$ for

$$P := \left(\sqrt{-7} + 3 : -\sqrt{-7} + 5 : 8\right) \in X_0(43)(\mathbb{Q}(\sqrt{-7}))$$

satisfying $\rho_{43}(P) = Q$.
Primes used in sieve for quadratic points: 5, 7, 11.

Name	minpol(α)	Coordinates	j-invariant	CM	$\mathbb{Q}$-c
P_0	-	$(0:4:2:5)$	-884736000	-43	-
P_1	$x^2 + 131$	$(\alpha + 65 : 3(\alpha + 17) : 72)$	$(2646379314349235349704820159442238\alpha + 707132167227358231308116050702291 81)/3410605131648480892181396484375$	NO	NO
$w_{43}(P_1)$	$x^2 + 131$	$(-2\alpha + 9 : 10 : 25)$	$(24550846739648768658311 8\alpha - 5588464515419225929913951)/16412848369726853881 35$	NO	NO
P_2	$x^2 + 71$	$(\alpha + 1 : 4 : 0)$	$-(49\alpha + 977)/4$	NO	NO
$w_{43}(P_2)$	$x^2 + 71$	$(2(-\alpha + 8) : -\alpha + 23 : 30)$	$(5111948195521623101849\alpha - 2251985393661771956312 3)/17592186044416$	NO	NO

Table 3.2: All non-cuspidal rational points and all isolated quadratic points on $X_0(43)$, up to Galois conjugacy.

3.4.2 $X_0(53)$

Model for $X_0(53)$:

$$9x_0^2x_3 - 5x_0x_3^2 - 27x_1^3 - 18x_1^2x_2 + 78x_1^2x_3 - 18x_1x_2^2 + 30x_1x_2x_3 - 64x_1x_3^2 - 57x_2^3 + 136x_2^2x_3 - 104x_2x_3^2 + 49x_3^3 = 0,$$
$$x_0x_2 - 2x_0x_3 - 3x_1^2 + 5x_1x_3 - 2x_2^2 + x_2x_3 - 2x_3^2 = 0.$$

Genus $X_0(53)$: 4.
Cusps: $(1:0:0:0)$, $(1:1:1:1)$.
$X_0^+(53)$: elliptic curve $y^2 + xy + y = x^3 - x^2$ of conductor 53.
Mordell–Weil group of quotient: $J_0^+(53)(\mathbb{Q}) = \mathbb{Z} \cdot [Q - O]$, where $Q := (0, -1)$.
A subgroup $G \subset J_0(53)(\mathbb{Q})$ satisfying $2 \cdot J_0(53)(\mathbb{Q}) \subset G$ is $G = \mathbb{Z} \cdot D_1 \oplus \mathbb{Z}/13\mathbb{Z} \cdot D_{\mathrm{tor}}$, where $D_{\mathrm{tor}} = [(1:1:1:1) - (1:0:0:0)]$ and $D_1 = [P + \overline{P} - (1:1:1:1) - (1:0:0:0)] = \rho^*[Q - O]$ for

$$P := \left(0 : \sqrt{-11} + 5 : 6 : 6\right) \in X_0(53)(\mathbb{Q}(\sqrt{-11}))$$

satisfying $\rho_{53}(P) = Q$.
Primes used in sieve for quadratic points: 11, 7.
Primes used in sieve for cubic points: 31, 17.
There are **no** isolated quadratic points on $X_0(53)$. In particular, all quadratic points are supported on $\mathbb{Q}$-curves.

Name	minpol(α)	Coordinates	j-invariant	CM	$\mathbb{Q}$-c
P_1	$x^3 - x^2 + 5x + 52$	$(12\alpha^2 - 59\alpha + 254 : -9\alpha^2 + 22\alpha + 32 : 7\alpha^2 - 27\alpha + 252 : 178)$	$(-3837914263070281678212621808478529 05\alpha^2 + 1545152415129700179443672757063109789\alpha - 659496644272221374693115066287906363 3)/ 19383245667680019896796723$	NO	NO
$w_{53}(P_1)$	$x^3 - x^2 + 5x + 52$	$(\alpha^2 - 2\alpha + 7 : 3\alpha - 3 : 9 : 0)$	$(-15648377\alpha^2 + 63003373\alpha - 268896737)/3$	NO	NO
P_2	$x^3 + 11x - 8$	$(143\alpha^2 + 63\alpha + 1740 : 53\alpha^2 + 49\alpha + 1004 : 25\alpha^2 + 33\alpha + 612 : 524)$	$(42965953489184285395017927595764270 1\alpha^2 + 2992792298752272848302011617592469 04\alpha + 4934717748383394121661044694765075727)/ 9007199254740992$	NO	NO
$w_{53}(P_2)$	$x^3 + 11x - 8$	$(107\alpha^2 + 72\alpha + 1345 : 42\alpha^2 + 16\alpha + 718 : 20\alpha^2 - 8\alpha + 420 : 328)$	$(1594853540089340101\alpha^2 + 1110894791062576754\alpha + 18317182399622734527)/2$	NO	NO
P_3	$x^3 - x^2 + 53x + 147$	$(3(47\alpha^2 - 38\alpha + 3271) : 31\alpha^2 - 250\alpha + 7331 : 3(13\alpha^2 - 48\alpha + 1767) : 5286)$	$(576019597560169489453888165775270 8\alpha^2 - 1960123279945502107360380689616669 1\alpha + 3523897191114334331996141667853418 99)/134217728$	NO	NO
$w_{53}(P_3)$	$x^3 - x^2 + 53x + 147$	$(39\alpha^2 - 129\alpha + 2550 : 11\alpha^2 - 42\alpha + 927 : 4\alpha^2 - 2\alpha + 430 : 292)$	$(5908628533072\alpha^2 - 20106331622569\alpha + 361470319752701)/2$	NO	NO
P_4	$x^3 - 2x - 3$	$(-15\alpha^2 - 27\alpha - 21 : 3\alpha^2 + 7\alpha + 9 : -\alpha^2 - \alpha + 1 : 4)$	$-26\alpha^2 - 123\alpha - 74$	NO	NO
$w_{53}(P_4)$	$x^3 - 2x - 3$	$(-6\alpha^2 + 81\alpha + 120 : -11\alpha^2 + 15\alpha + 220 : 18\alpha^2 + 24\alpha + 174 : 267)$	$-1355386571852169691346960613096 29\alpha^2 - 2566138753303902800028206173000 50\alpha - 2147669634144232669641580365179 00$	NO	NO
P_5	$x^3 - 3x - 4$	$(11\alpha^2 + 23\alpha + 20 : 3\alpha^2 + 5\alpha + 8 : \alpha^2 + \alpha + 4 : 6)$	$117843669992\alpha^2 + 258763889291\alpha + 214668790692$	NO	NO
$w_{53}(P_5)$	$x^3 - 3x - 4$	$(131\alpha^2 + 98\alpha + 80 : 38\alpha^2 + 80\alpha + 410 : \alpha^2 + 91\alpha + 396 : 563)$	$2973440748198580894041028382550 4\alpha^2 + 6529150611193816026557987308677 1\alpha + 5416539093394354248923138255334 8$	NO	NO

Table 3.3: All non-cuspidal rational points, all isolated quadratic points, and all cubic points on $X_0(53)$, up to Galois conjugacy.

3.4.3 $X_0(57)$

Model for $X_0(57)$:

$$x_0x_2 - x_1^2 + 2x_1x_3 + 2x_1x_4 - 2x_2^2 - 2x_2x_3 + 3x_2x_4 - x_3^2 - 2x_3x_4 - x_4^2 = 0,$$
$$x_0x_3 - x_1x_2 - 2x_1x_4 + 4x_2x_3 - 6x_2x_4 - x_3^2 + 5x_3x_4 - 5x_4^2 = 0, \quad x_0x_4 - x_2^2 + x_2x_3 - 2x_2x_4 - 2x_4^2 = 0.$$

Genus of $X_0(57)$: 5.
Cusps: $c_1 = (1:0:0:0:0)$, $c_2 = (1:1:0:1:0)$, $c_3 = (3:3:1:2:1)$, $c_4 = (3:9/2:-1/2:7/2:1)$.
$X_0^+(57)$: hyperelliptic curve $y^2 = x^6 - 2x^5 + 3x^4 + 3x^2 - 2x + 1$
Mordell–Weil group of quotient: $J_0^+(57)(\mathbb{Q})$: $\mathbb{Z} \cdot [\infty^+ - \infty^-] \oplus \mathbb{Z}/3\mathbb{Z} \cdot [(0,-1) - \infty^-]$.
A subgroup $G \subset J_0(57)(\mathbb{Q})$ satisfying $2 \cdot J_0(57)(\mathbb{Q}) \subset G$ is $G = \mathbb{Z} \cdot D_1 \oplus \mathbb{Z}/6\mathbb{Z} \cdot D_{\mathrm{tor},1} \oplus \mathbb{Z}/30\mathbb{Z} \cdot D_{\mathrm{tor},2}$, where $D_{\mathrm{tor},1} = [c_2 - c_1]$, $D_{\mathrm{tor},2} = [c_3 - c_1]$ and $D_1 = [c_2 + c_4 + -P_5 - \overline{P_5}]$ where P_5 is defined in Table 3.4 and satisfies $\rho_{57}(P_5) = \infty^-$.
Primes used in sieve for quadratic points: 11, 13. Primes used in sieve for cubic points: 17, 43.

Name	minpol(α)	Coordinates	j-invariant	CM	$\mathbb{Q}$-c
P_1	x^2+23	$(-11\alpha+47 : 2(-7\alpha+43) : 4(\alpha-5) : 8(-\alpha+9) : 32)$	$(343\alpha+4021)/4$	NO	NO
$w_3(P_1)$	x^2+23	$(\alpha-3 : \alpha+3 : 2 : 2 : 0)$	$(402878\alpha+2212325)/32$	NO	NO
$w_{57}(P_1)$	x^2+23	$(-\alpha+3 : 2(-\alpha+2) : -2 : -\alpha+1 : 2)$	$(152503825515346075337\alpha - 1518681643605456439979)/288230376151711744$	NO	NO
$w_{19}(P_1)$	x^2+23	$(\alpha-1 : \alpha+11 : -22(\alpha+1) : \alpha+15 : 8)$	$(-56278625425021601\alpha - 102516814328210867)/1048576$	NO	NO
P_2	x^2+3	$(4 : -\alpha+7 : 0 : -\alpha+5 : 2)$	-12288000	-27	w_{19}
$w_{57}(P_2)$	x^2+3	$(-2\alpha : 2(-\alpha+3) : \alpha-1 : 2(-\alpha+2) : 2)$	0	-3	w_{19}
P_3	x^2+3	$(-\alpha+3 : -\alpha+3 : \alpha-1 : 4 : 2)$	54000	-12	w_{19}, w_{57}
P_4	x^2+3	$(-5\alpha+1 : -5\alpha+1 : \alpha-3 : 2(-\alpha+1) : 2)$	0	-3	w_{19}, w_{57}
P_5	x^2+2	$(\alpha+4 : 4\alpha+7 : -\alpha-1 : 2\alpha+5 : 3)$	8000	-8	w_{57}

$w_3(P_5)$	x^2+2	$(-\alpha+2:3:\alpha:-\alpha+6:2)$	8000	-8	w_{57}
P_6	x^2-13	$(4(\alpha+7):4(\alpha+7):-\alpha-1:5\alpha+29:6)$	$(3387888351672962316333\alpha-1221520516750408764332 3)/2$	NO	w_3
$w_{57}(P_6)$	x^2-13	$(5\alpha+23:-3\alpha-3:\alpha+3:-\alpha+3:2)$	$-(-17787\alpha-61763)/2$	NO	w_3
P_7	x^3-x^2+x+2	$(\alpha^2-3\alpha+7:2(-\alpha^2+\alpha+1):\alpha^2-\alpha+1:$ $-\alpha^2+\alpha+3:2)$	$-9209701\alpha^2+16880722\alpha-21658080$	NO	NO
$w_3(P_7)$	x^3-x^2+x+2	$(2\alpha^2-3\alpha+8:2\alpha^2-3\alpha+11:-\alpha^2-1:$ $2\alpha^2-3\alpha+11:3)$	$-1580665385097\alpha^2-921044021830\alpha+291907686304$	NO	NO
$w_{57}(P_7)$	x^3-x^2+x+2	$(-2\alpha^2+4:\alpha^2-3\alpha+1:\alpha^2-1:\alpha^2+3:1)$	$114\alpha^2-163\alpha-218$	NO	NO
$w_{19}(P_7)$	x^3-x^2+x+2	$(\alpha^2-3\alpha+7:4(\alpha^2+1):\alpha^2-3\alpha-1:\alpha^2-3\alpha+3:4)$	$-18553245055702\alpha^2+33591312773593\alpha-45780203714514$	NO	NO
P_8	x^3-x^2-2	$(3\alpha+9:-3\alpha^2+9\alpha+12:-2:2(3\alpha+4):4)$	$(-7449\alpha^2-1673\alpha-948)/2$	NO	NO
$w_{57}(P_8)$	x^3-x^2-2	$(2\alpha+2:-\alpha^2+\alpha+4:\alpha^2-\alpha:-\alpha^2+\alpha+4:2)$	$(-1810169986337\alpha^2-1259199868019\alpha-2135110941902)/4$	NO	NO
$w_{19}(P_8)$	x^3-x^2-2	$(3\alpha^2-2\alpha+6:4(\alpha^2-\alpha+3):-\alpha^2+2\alpha-2:$ $3\alpha^2-2\alpha+10:4)$	$(-17777315457\alpha^2+14416014175\alpha-$ $86766426948)/536870912$	NO	NO
$w_3(P_8)$	x^3-x^2-2	$(3\alpha+3:-3\alpha^2+9:2:-3\alpha+7:2)$	$(-73465339921\alpha^2-51104061891\alpha-86652910958)/1024$	NO	NO
P_9	$x^3-16x-27$	$(55\alpha^2-27\alpha+983:24(2\alpha^2+76):$ $9(-5\alpha^2+9\alpha+35):27(\alpha^2+3\alpha+65):648)$	$(353435648\alpha^2-1133445120\alpha-2409267200)/3$	NO	NO
$w_{57}(P_9)$	$x^3-16x-27$	$(25\alpha^2-53\alpha-243:4\alpha^2-2\alpha:-\alpha^2+5\alpha-9:$ $17\alpha^2-31\alpha-153:18)$	$(-3860067463716106958367531119411 2\alpha^2+$ $1246971309345980136990819373547 52\alpha+$ $2568268265634928784036325378949 12)/$ $157004289908208161164053456 3$	NO	NO
$w_3(P_9)$	$x^3-16x-27$	$(5\alpha^2+45\alpha+604:-7\alpha^2-63\alpha+661:$ $9(3\alpha^2-4\alpha-22):-4\alpha^2-36\alpha+577:279)$	$(-1754586552521644333563904\alpha^2+$ $3777138616478919143030784\alpha+$ $2059379801112199616846233 6)/1162261467$	NO	NO
$w_{19}(P_9)$	$x^3-16x-27$	$(-8\alpha^2+20\alpha+90:\alpha^2-4\alpha:\alpha^2-\alpha-15:-2\alpha^2+5\alpha+24:3)$	$-(29985636352\alpha^2+139955503104\alpha+173460488192)/27$	NO	NO

Table 3.4: All non-cuspidal rational points, all quadratic points and all cubic points on $X_0(57)$, up to Galois conjugacy.

3.4.4 $X_0(61)$

Model for $X_0(61)$:

$$x_0^2x_3 + x_0x_1x_3 - 2x_0x_3^2 - 2x_1^3 - 6x_1^2x_2 + 5x_1^2x_3 - 5x_1x_2^2 + 4x_1x_2x_3 - 6x_2^3 + 14x_2^2x_3 - 11x_2x_3^2 + 4x_3^3 = 0,$$
$$x_0x_2 - x_1^2 - x_1x_2 - 2x_2^2 + 2x_2x_3 - x_3^2 = 0$$

Genus of $X_0(61)$: 4.
Cusps: $c_1 = (1:0:0:0)$, $c_2 = (1:0:1:1)$.
$X_0^+(61)$: elliptic curve $y^2 + xy = x^3 + 6x^2 + 11x + 6$ of conductor 61.
Mordell–Weil group of quotient: $J_0^+(61)(\mathbb{Q}) = \mathbb{Z} \cdot [Q - O]$, where $Q = (-1, 1)$.
A subgroup $G \subset X_0(61)$ satisfying $2 \cdot J_0(61) \subset G$ is $G = \mathbb{Z} \cdot D_1 \oplus \mathbb{Z}/5\mathbb{Z} \cdot D_{\text{tor}}$, where $D_{\text{tor}} = [c_2 - c_1]$ and $D_1 = [P + \overline{P} - c_1 - c_2] = \rho^*[Q - O]$ for

$$P := \left(0 : \sqrt{-3} - 1 : 2 : 2\right) \in X_0(61)(\mathbb{Q}(\sqrt{-3}))$$

satisfying $\rho_{65}(P) = Q$.
Primes used in sieve for quadratic points: 7. Primes used in sieve for cubic points: 31, 19, 53, 23.
There are **no** isolated quadratic points on $X_0(61)$. In particular, all quadratic points are supported on $\mathbb{Q}$-curves.

Name	minpol(α)	Coordinates	j-invariant	CM	$\mathbb{Q}$-c
P_1	$x^3 - 2x - 20$	$(4\alpha^2+16\alpha-16 : -6\alpha^2+12\alpha-12 : 5\alpha^2+2\alpha+34 : 72)$	$-(1996874400742389760403631439516303\alpha^2 + 5909569160562647305266609005744561\alpha + 13495086575687455058014736453622810)/2147483648$	NO	NO
$w_{61}(P_1)$	$x^3 - 2x - 20$	$(\alpha^2 + 2\alpha + 8 : -2\alpha - 4 : 4 : 0)$	$(148823\alpha^2 - 301199\alpha - 470790)/2$	NO	NO

Table 3.5: All non-cuspidal rational points, all isolated quadratic points and all cubic points on $X_0(61)$, up to Galois conjugacy.

3.4.5 $X_0(65)$

Model for $X_0(65)$:

$$\begin{aligned}
&x_0x_2 - x_1^2 + x_1x_4 - 2x_2^2 - x_2x_3 + 3x_2x_4 - x_3^2 + 2x_3x_4 - 2x_4^2 = 0,\\
&x_0x_3 - x_1x_2 - 2x_2^2 - x_2x_3 + 4x_2x_4 - x_3^2 + 2x_3x_4 - 2x_4^2 = 0,\\
&x_0x_4 - x_1x_3 - 2x_2^2 - 3x_2x_3 + 5x_2x_4 + 3x_3x_4 - 3x_4^2 = 0.
\end{aligned}$$

Genus of $X_0(65)$: 5.
Cusps: $c_1 = (1:0:0:0:0)$, $c_2 = (1:1:1:1:1)$, $c_3 = (1:2:2:2:3)$, $c_4 = (1:1:1:1:2)$.
$X_0^+(65)$: elliptic curve $y^2 + xy = x^3 - x$ of conductor 65.
Mordell–Weil group of quotient: $J_0^+(65)(\mathbb{Q}) = \mathbb{Z}\cdot[Q-O] \oplus \mathbb{Z}/2\mathbb{Z}\cdot[(0,0)-O]$, where $Q = (1,0)$.
Full Mordell–Weil group: $J_0(65)(\mathbb{Q}) = \mathbb{Z}\cdot D_1 \oplus \mathbb{Z}/2\mathbb{Z}\cdot(-9D_{\mathrm{tor},1} + 2D_{\mathrm{tor},2}) \oplus \mathbb{Z}/84\mathbb{Z}\cdot(17D_{\mathrm{tor},1} + 13D_{\mathrm{tor},2})$, where $D_{\mathrm{tor},1} = [c_2 - c_1]$, $D_{\mathrm{tor},2} = [c_3 - c_1]$ and $D_1 = [P + \overline{P} - c_1 - c_2] = \rho^*([Q-O])$ for

$$P = (0:2:1+i:2:2) \in X_0(65)(\mathbb{Q}(i))$$

satisfying $\rho(P) = Q$. Primes used in sieve for quadratic and cubic points: 17, 23. Primes used in sieve for quartic points: 17, 19, 23.
There are **no** isolated quadratic points on $X_0(65)$. In particular, all quadratic points are supported on $\mathbb{Q}$-curves.

Name	minpol(α)	Coordinates	j-invariant	CM	$\mathbb{Q}$-c
P_1	x^3-x^2+x-2	$(-3\alpha^2+15\alpha+23 : 9\alpha^2-2\alpha+17 : 10\alpha^2-7\alpha+38 : 7\alpha^2+8\alpha+18 : 43)$	$-309978521360308365337524647976 32\alpha^2 - 109487502432234040671924733656 96\alpha - 458138100606905237912589172332 16$	NO	NO
$w_{65}(P_1)$	x^3-x^2+x-2	$(28\alpha^2+10\alpha+42 : -9\alpha^2-3\alpha-12 : 3\alpha^2+\alpha+6 : -\alpha^2 : 2)$	$16448\alpha^2 + 49984\alpha - 102976$	NO	NO
$w_{13}(P_1)$	x^3-x^2+x-2	$(16(\alpha^2-3\alpha+3) : 16(\alpha^2-\alpha+1) : 3\alpha^2+7\alpha+5 : 2(-\alpha^2+3\alpha+9) : 32)$	$1629248\alpha^2 - 2904256\alpha + 946624$	NO	NO
$w_5(P_1)$	x^3-x^2+x-2	$(4(3\alpha^2-5\alpha+14) : 2(2\alpha^2-11\alpha+40) : -5\alpha^2-7\alpha+61 : 2(-4\alpha^2-\alpha+35) : 92)$	$136553952252949568\alpha^2 + 102819038189152064\alpha - 389190231909361216$	NO	NO

P_2	x^4+3x^2+1	$(-2\alpha^3+\alpha^2-\alpha+1:\alpha^3+\alpha^2+1:-\alpha^2:\alpha^2+1:1)$	1728	-4	YES w_{13}
$w_{65}(P_2)$	x^4+3x^2+1	$(2\alpha^3+2\alpha^2+4\alpha+12:4\alpha^3-\alpha^2+9\alpha+11:$ $-2\alpha^3+3\alpha^2-5\alpha+19:3\alpha^3+2\alpha^2+8\alpha+19:18)$	$19691491018752\alpha^2+51552986141376$	-100	YES w_{13}
P_3	x^4-x^3+ $2x^2+x+1$	$(8\alpha^3+18\alpha^2-46\alpha+220:93\alpha^3-92\alpha^2+128\alpha+509:-35\alpha^3+$ $102\alpha^2-100\alpha+363:-77\alpha^3+128\alpha^2-220\alpha+413:482)$	$-146329141248\alpha^3-619860197376$	-75	YES w_{13}
$w_{65}(P_3)$	x^4-x^3+ $2x^2+x+1$	$(2\alpha^3-4\alpha^2+6\alpha:\alpha^3+\alpha+6:-\alpha^3+2\alpha^2-3\alpha+2:$ $-\alpha^3+\alpha^2-\alpha+1:4)$	0	-3	YES w_{13}
P_4	x^4-2x^3- $4x^2+4x+10$	$(3(9\alpha^3+3\alpha^2-29\alpha+65):5(4\alpha^3+11\alpha^2-29\alpha+74):$ $23\alpha^3-89\alpha^2-58\alpha+730:-7\alpha^3+46\alpha^2-58\alpha+610:870)$	$(-11331665\alpha^3+42997532\alpha^2-23611406\alpha-39687952)/6$	NO	NO
$w_{65}(P_4)$	x^4-2x^3- $4x^2+4x+10$	$(7\alpha^3-15\alpha^2-21\alpha+65:-6\alpha^3+25\alpha^2+\alpha-29:$ $\alpha^3-7\alpha^2+14\alpha+19:-5\alpha^3+18\alpha^2-2\alpha+7:51)$	$(565729615\alpha^3+1124273732\alpha^2+11474554\alpha-508128592)/393216$	NO	NO
$w_{13}(P_4)$	x^4-2x^3- $4x^2+4x+10$	$(3(-3\alpha^3-2\alpha^2+8\alpha+12):3(3\alpha^3-12\alpha-12):$ $3(-\alpha^3+4\alpha+6):-5\alpha^3-4\alpha^2+10\alpha+20:6)$	$(-8144181273275\alpha^3+25312371833066\alpha^2+8043694506022\alpha-$ $57216807377536)/48$	NO	NO
$w_5(P_4)$	x^4-2x^3- $4x^2+4x+10$	$(-2\alpha^3+5\alpha^2+\alpha+5:3\alpha^2-6:\alpha^3-\alpha^2-5\alpha+8:$ $-\alpha^3+4\alpha^2-4\alpha+4:9)$	$(103767807\alpha^3-312011900\alpha^2-149464130\alpha+782896654)/4$	NO	NO
P_5	x^4-5x^2+36	$(8\alpha^3-8\alpha^2+32\alpha+160:\alpha^3+3\alpha^2+4\alpha+84:$ $6(\alpha^3-5\alpha+54):6(\alpha^3-3\alpha^2+4\alpha+60):144)$	$(188921499633\alpha^3+905537632545\alpha^2+1655605513116\alpha+$ $766437509340)/16384$	NO	NO w_{13}
$w_{65}(P_5)$	x^4-5x^2+36	$(-10\alpha^3+12\alpha^2-286\alpha-300:12(2\alpha^3+11\alpha^2+17\alpha+60):$ $5\alpha^3-6\alpha^2+143\alpha+954:4(16\alpha^3+21\alpha^2-65\alpha+78):1608)$	$(4276343715810283541951 37\alpha^3-43883609874795920055937 5\alpha^2-$ $3302486685333702076993956\alpha+$ $986944609470296495134 7100)/73786976294838206464$	NO	NO w_{13}
P_6	x^4-x^2+64	$(-23\alpha^3+56\alpha^2-41\alpha-184:2(3\alpha^3-24\alpha^2+61\alpha+24):$ $4(\alpha^3-9\alpha+72):8(-\alpha^3+9\alpha-8):256)$	$(-352692275\alpha^3-703166360\alpha^2+274492275\alpha+6008246680)/512$	NO	NO w_5
$w_{65}(P_6)$	x^4-x^2+64	$(16(-\alpha^3-7\alpha+72):16(-\alpha^3-7\alpha+72):-15\alpha^3+8\alpha^2+$ $207\alpha+1400:2(-11\alpha^3-24\alpha^2+11\alpha+856):2048)$	$(185618461058956310814189183475\alpha^3+$ $451625115647050834040533476755\alpha^2+$ $191531841188243058702903432000\alpha-$ $250959527137353871878284971 7440)/73786976294838206464$	NO	NO w_5

P_7	$x^4+10x^2-13x+6$	$(4(3\alpha^3+11\alpha^2-57\alpha+134):4(6\alpha^3+22\alpha^2+77\alpha+77):-31\alpha^3-50\alpha^2-366\alpha+971:2(25\alpha^3+28\alpha^2+98\alpha+289):764)$	$(-939963245658151156020994081326897076830779 69\alpha^3-2727258314136873995360630222734080876847821 3\alpha^2-9226025046493772475686437033632095927877784 19\alpha+9856864379222872249508554187549589110832741 26)/32963364674808119852715351257097 6$	NO	NO
$w_{13}(P_7)$	$x^4+10x^2-13x+6$	$(-116\alpha^3-61\alpha^2-1021\alpha+2589:3(-43\alpha^3-14\alpha^2-341\alpha+1479):9(4\alpha^3+8\alpha^2+47\alpha+294):4617/171(2\alpha^3+\alpha^2+22\alpha+114):4617)$	$(-4448701283860241826508312883 3\alpha^3-3735563291779903495449876491 7\alpha^2-4669663552623763860844671799 07\alpha+1976441336867805260628664031 18)/8965117619822842085376$	NO	NO
$w_5(P_7)$	$x^4+10x^2-13x+6$	$(-\alpha^3+3\alpha^2+\alpha+102:2(-4\alpha^3-2\alpha^2-37\alpha+78):2(-\alpha^3-\alpha^2-12\alpha+36):2(-\alpha^2-\alpha+42):144)$	$(3947219255855060389392315160508 63\alpha^3-2768103066312680500698037612142213\alpha^2+3322177705362944338498999061316877\alpha-9515853456940546114698189074489 46)/2060210292175507490794709453568 6$	NO	NO
$w_{65}(P_7)$	$x^4+10x^2-13x+6$	$(2(-13\alpha^3-15\alpha^2-139\alpha+46):6(2\alpha^3+3\alpha^2+20\alpha+4):9(\alpha^3+10\alpha-13):54:0)$	$(-74128331233\alpha^3-1035513003989\alpha^2+1305535708381\alpha-583073890962)/1990656$	NO	NO
P_8	$x^4-2x^3+33x^2+124x+324$	$(\alpha^3+79\alpha^2-696\alpha+1420:3(-\alpha^3+29\alpha^2-60\alpha+1388):9(\alpha^3+7\alpha^2+24\alpha+844):27(-\alpha^3+5\alpha^2-36\alpha+188):7776)$	$(-43105827974237\alpha^3-309174638866315\alpha^2-858567581971168\alpha-1476381721011948)/7962624$	NO	NO
$w_5(P_8)$	$x^4-2x^3+33x^2+124x+324$	$(21384/1458(7\alpha^3-22\alpha^2+233\alpha+972):29\alpha^3-176\alpha^2+1837\alpha+11934:6(-8\alpha^3+11\alpha^2-121\alpha+1098):9(-\alpha^3+22\alpha^2-11\alpha+1614):21384)$	$(1261803104493572110234408 3\alpha^3-6415701372160651100368383 5\alpha^2+5551061516746492106882598 72\alpha+1539188227090727464592290 12)/3586047047929136834150 4$	NO	NO
$w_{13}(P_8)$	$x^4-2x^3+33x^2+124x+324$	$(1053\alpha^3-997\alpha^2+36528\alpha+219596:10(127\alpha^3-643\alpha^2+2948\alpha+41036):4(33\alpha^3-677\alpha^2+868\alpha+81236):8(114\alpha^3-131\alpha^2-681\alpha+49558):518080)$	$(-9093710816344298141898748671938973046 37\alpha^3+1258695415831541799600085990600503403 6565\alpha^2-8353438170645264640408368107584694722 9408\alpha+3445188381872662833659917461589517842 44372)/8240841168702029963178837814274 4$	NO	NO

$w_{65}(P_8)$	$x^4-2x^3+33x^2+124x+324$	$(8(-25\alpha^3+85\alpha^2-944\alpha-2168):4(39\alpha^3-230\alpha^2+1609\alpha+2486):45\alpha^3-153\alpha^2+920\alpha+15980:2(-17\alpha^3-137\alpha^2+410\alpha-3656):15584)$	$(-1143480552635346193461521689947909016607863 7\alpha^3+5228953638910671575533618290081115693190725\alpha^2+8333882441449890246911214503405720001532291 2\alpha+3256800399279108103325929716286936922242018 12)/1318534586992324794108614050283904$	NO	NO
P_9	$x^4-2x^3+2x^2+2x-4$	$(-384\alpha^3+1189\alpha^2-2064\alpha+1526:150\alpha^3-445\alpha^2+744\alpha-386:-55\alpha^3+177\alpha^2-306\alpha+302:16\alpha^3-53\alpha^2+86\alpha+54:166)$	$(8981190973311252557442 1\alpha^3-2474034431202397592367 72\alpha^2+4707854583145267944810 74\alpha-3422408322697797324918 66)/73786976294838206464$	NO	NO
$w_5(P_9)$	$x^4-2x^3+2x^2+2x-4$	$(11(3\alpha^3-4\alpha^2+6\alpha+18):-39\alpha^3+52\alpha^2-14\alpha-58:27\alpha^3-36\alpha^2+30\alpha+162:-19\alpha^3-4\alpha^2+18\alpha+62:88)$	$(12716759153730866\alpha^3-27727513674538234\alpha^2-16708346390401773\alpha+29993540624153550)/4194304$	NO	NO
$w_{65}(P_9)$	$x^4-2x^3+2x^2+2x-4$	$(241\alpha^3+876\alpha^2-3030\alpha+10510:2(317\alpha^3-436\alpha^2+2\alpha+6390):4(-215\alpha^3+604\alpha^2-862\alpha+2654):8(-75\alpha^3+116\alpha^2-206\alpha+1494):16288)$	$(875447901069538838047255095 1\alpha^3-2693152503640096408318722476 4\alpha^2+4649573143896228033194830153 7\alpha-3253504172551570643224279926 0)/4$	NO	NO
$w_{13}(P_9)$	$x^4-2x^3+2x^2+2x-4$	$(\alpha^3+3\alpha^2:\alpha^3-2\alpha^2-2\alpha+4:2\alpha+4:2\alpha^2:4)$	$(-121794908716379\alpha^3+95010271213628\alpha^2-127685261383726\alpha-399355122270266)/64$	NO	NO
P_{10}	$x^4-2x^3-6x^2+3x+8$	$(27\alpha^3-78\alpha^2-66\alpha+193:10(-\alpha^3+2\alpha^2+6\alpha-3):4(-3\alpha^3+12\alpha^2+4\alpha-7):8(\alpha^3-4\alpha^2+2\alpha+9):80)$	$(-73415413682485\alpha^3-96687558634718\alpha^2+119780562840206\alpha+177065002925201)/2$	NO	NO
$w_{65}(P_{10})$	$x^4-2x^3-6x^2+3x+8$	$(2(33\alpha^3+21\alpha^2-31\alpha+101):2(-5\alpha^3-59\alpha^2+14\alpha+301):27\alpha^3+73\alpha^2-137\alpha+278:2(20\alpha^3-71\alpha^2-56\alpha+331):614)$	$(2977937553037019865543114 35\alpha^3-1401720256809888215691668318\alpha^2-2793829614711904798744788 34\alpha+2112213001641271144506379601)/36893488147419103232$	NO	NO
$w_5(P_{10})$	$x^4-2x^3-6x^2+3x+8$	$(-452\alpha^3+348\alpha^2+3048\alpha+2713:164\alpha^3-70\alpha^2-1221\alpha-946:-84\alpha^3+57\alpha^2+569\alpha+696:29\alpha^3-30\alpha^2-193\alpha+90:289)$	$(-10248101735925\alpha^3+25536131264162\alpha^2+56923104477966\alpha-95768669529519)/32$	NO	NO
$w_{13}(P_{10})$	$x^4-2x^3-6x^2+3x+8$	$(-167\alpha^3+518\alpha^2+178\alpha+383:-171\alpha^3+590\alpha^2+294\alpha-241:-73\alpha^3+70\alpha^2+562\alpha+741:5\alpha^3-90\alpha^2+166\alpha+1091:1244)$	$(8699697034245003878315770635\alpha^3-5951864245642353783162260318\alpha^2-6002996567854179168258160715 4\alpha-5289157025760808537919607671 9)/8192$	NO	NO

P_{11}	$x^4-x^3-5x^2-12x+4$	$(\alpha^3+5\alpha^2-7\alpha+10:\alpha^3-3\alpha^2+9\alpha+10:-\alpha^3+3\alpha^2+7\alpha+6:\alpha^3-3\alpha^2+\alpha+10:16)$	$(1699588421018410771117575\alpha^3+4085001869259831852583379\alpha^2+5405460540196338811614783\alpha-1997445389150221782346154)/32768$	NO	NO
$w_{65}(P_{11})$	$x^4-x^3-5x^2-12x+4$	$(2(63\alpha^3+197\alpha^2+285\alpha+548):67\alpha^3+103\alpha^2+367\alpha+2010:4(13\alpha^3+30\alpha^2-69\alpha+390):4(15\alpha^3-17\alpha^2-28\alpha+450):2684)$	$(4240749998674792523504 7\alpha^3+1019274517136892933213 95\alpha^2+1348750467771268735059 51\alpha-4983951659493782331953 0)/128$	NO	NO
$w_{13}(P_{11})$	$x^4-x^3-5x^2-12x+4$	$(-9\alpha^3+3\alpha^2+47\alpha+182:2(3\alpha^3-\alpha^2-21\alpha-18):8(-\alpha^3+\alpha^2+5\alpha+16):32:64)$	$(1212893975\alpha^3-854535645\alpha^2-6316920369\alpha-16421016074)/8$	NO	NO
$w_5(P_{11})$	$x^4-x^3-5x^2-12x+4$	$(8(-89\alpha^3+75\alpha^2+407\alpha+1630):32(12\alpha^3-7\alpha^2-86\alpha+51):-535\alpha^3+289\alpha^2+2957\alpha+13446:2(13\alpha^3-123\alpha^2-47\alpha+3310):8864)$	$(8253087476343440710498852889755 9\alpha^3-5838932241895994341015715588937 3\alpha^2-4287931718375570689855082339740 65\alpha-1118102278756799246262107049140746)/147573952589676412928$	NO	NO
P_{12}	$x^4-x^3+x^2+15x+8$	$(4(\alpha^3-2\alpha^2-5\alpha+6):8(\alpha^2+\alpha+1):\alpha^3-4\alpha^2+5\alpha+40:2(\alpha^3-3\alpha+8):24)$	$(-5290961501564850626442394 34\alpha^3+8335472160996535336268226 33\alpha^2-1008733619395736267637671387\alpha-7355999499831154760170196264)/18786186952704$	NO	NO
$w_5(P_{12})$	$x^4-x^3+x^2+15x+8$	$(-282\alpha^3+891\alpha^2-1847\alpha+496:202\alpha^3-487\alpha^2+1197\alpha+3602:-259\alpha^3+686\alpha^2-1438\alpha+695:-17\alpha^3-3\alpha^2+84\alpha+2248:3554)$	$(1455331341030054027299383378\alpha^3-4035164875167567001867400433\alpha^2+8609137673795812100808665275\alpha+6567184709951911955583590440)/711559752519106944$	NO	NO
$w_{13}(P_{12})$	$x^4-x^3+x^2+15x+8$	$(2(-2\alpha^3+6\alpha^2-11\alpha+4):3(\alpha^3-2\alpha^2+5\alpha+18):3(-\alpha^3+3\alpha^2-7\alpha+5):36:54)$	$(295009796578\alpha^3-818007129969\alpha^2+1745183842219\alpha+1331261559976)/24$	NO	NO
$w_{65}(P_{12})$	$x^4-x^3+x^2+15x+8$	$(2(7\alpha^3-12\alpha^2+13\alpha+112):4(-2\alpha^3+3\alpha^2-5\alpha-20):7\alpha^3-12\alpha^2+19\alpha+136:-2\alpha^3-2\alpha+16:48)$	$(456884149846\alpha^3-292804658823\alpha^2-2750405339723\alpha-1410079750568)/54$	NO	NO
P_{13}	$x^4+22x^2-36x-1587$	$(-7423\alpha^3+56049\alpha^2-380713\alpha+4990147:10(31\alpha^3-3409\alpha^2+9017\alpha+473485):4(-823\alpha^3+9049\alpha^2-123993\alpha+1840387):8(-499\alpha^3-2823\alpha^2-19569\alpha+788591):8416960)$	$(5515002242812156648291672807694 59\alpha^3-2916026023363419895375635644340249\alpha^2+2755132644412428518403544645336222 3\alpha-1655300773651924685361191142776054 49)/10317616411527050688$	NO	NO

$w_5(P_{13})$	$x^4+22x^2-36x-1587$	$(2(1540\alpha^3+24771\alpha^2+279122\alpha+2323657):5413\alpha^3+747\alpha^2+217423\alpha+5494649:6063\alpha^3+18979\alpha^2+101933\alpha+3263633:3317\alpha^3+23025\alpha^2+73939\alpha+3159503:4790452)$	$(9532686206605602132494213100460737798241 7\alpha^3+5455286490474350907455907533321035253347 68\alpha^2+5219097010417755802150885707010029194059739\alpha+2643564787504995740059499134041501774586822 8)/532030685184$	NO	NO
$w_{65}(P_{13})$	$x^4+22x^2-36x-1587$	$(2/3(-350\alpha^3+2133\alpha^2-20414\alpha+131049):99\alpha^3-821\alpha^2+7209\alpha-10283:-121\alpha^3+765\alpha^2-4519\alpha+49527:3(\alpha^3-95\alpha^2+463\alpha+7483):38628)$	$(2728218420678120434591504 63\alpha^3-1441756036037485113891638193\alpha^2+1362899099307814601720050996 1\alpha-818840122180075837847909371 23)/1283893387530184792473 6$	NO	NO
$w_{13}(P_{13})$	$x^4+22x^2-36x-1587$	$(2255\alpha^3+12903\alpha^2+122561\alpha+667341:727\alpha^3+3783\alpha^2+38017\alpha+283941:205\alpha^3+1173\alpha^2+13483\alpha+128559:31\alpha^3+303\alpha^2+5305\alpha+93933:103008)$	$(27395558102194290407\alpha^3+15677734881598349010 3\alpha^2+1499898372357530447969\alpha+7597242259694917251093)/25657344$	NO	NO
P_{14}	$x^4-x^3-26x^2-612x-376$	$(2(-7\alpha^3+819\alpha^2+338\alpha+3140):2(\alpha^3-117\alpha^2+4030\alpha+7708):41\alpha^3-39\alpha^2-1300\alpha+11516:-43\alpha^3+273\alpha^2+2756\alpha+11132:19032)$	$(9696652518865066949806479791\alpha^3+8762953089695930971311877117 2\alpha^2+6274326075953841792057605366 27\alpha+3632468171067635722052100321 74)/6030134083584$	NO	NO
$w_5(P_{14})$	$x^4-x^3-26x^2-612x-376$	$(1/233064(-1727\alpha^3+2535\alpha^2+45058\alpha+1115008):1/38844(-129\alpha^3+130\alpha^2+3445\alpha+104558):1/621504(-953\alpha^3+1755\alpha^2+24388\alpha+953788):1/103584(-71\alpha^3+13\alpha^2+884\alpha+116148):1)$	$(-4618241016324392977893 43\alpha^3+7530527413939114373716 20\alpha^2+1153254773341812930542510 9\alpha+2753638666333062791123057 30)/9984$	NO	NO
$w_{65}(P_{14})$	$x^4-x^3-26x^2-612x-376$	$(1/755872(1097\alpha^3+7553\alpha^2+26728\alpha+269940):1/14536(9\alpha^3+110\alpha^2+211\alpha+7982):1/377936(283\alpha^3-377\alpha^2+780\alpha+246548):1/188968(171\alpha^3+273\alpha^2-8710\alpha+89880):1)$	$(4256408352336373807957394927\alpha^3+3846554947652887786228847922 0\alpha^2+2754156020648987736650897888 99\alpha+1594495402701198111482345324 30)/113724$	NO	NO
$w_{13}(P_{14})$	$x^4-x^3-26x^2-612x-376$	$(4(-22207\alpha^3+29081\alpha^2+576784\alpha+14718564):4(-10641\alpha^3+10907\alpha^2+310180\alpha+7975676):-21479\alpha^3+48581\alpha^2+609596\alpha+17635140:2(-4957\alpha^3+4823\alpha^2+91364\alpha+6258412):10977824)$	$(-7533292230825378659055246790818024319\alpha^3+1228382482874303999440235142161656189 2\alpha^2+1881193552581778018132179952290967213 97\alpha+4491745817999145473916690222308277724 034)/1156284597843548784$	NO	NO

Table 3.6: All non-cuspidal rational points, all isolated quadratic points, all cubic points and all isolated quartic points on $X_0(65)$, up to Galois conjugacy.

3.4.6 $X_0(67)$

Model for $X_0(67)$:

$$\begin{aligned}
&x_0x_2 - x_1^2 + 2x_1x_3 + 2x_1x_4 - 2x_2^2 - 2x_2x_3 + 3x_2x_4 - x_3^2 - 2x_3x_4 - x_4^2 = 0,\\
&x_0x_3 - x_1x_2 - 2x_1x_4 + 4x_2x_3 - 6x_2x_4 - x_3^2 + 5x_3x_4 - 5x_4^2 = 0,\\
&x_0x_4 - x_2^2 + x_2x_3 - 2x_2x_4 - 2x_4^2 = 0.
\end{aligned}$$

Genus of $X_0(67)$: 5.
Cusps: $c_1 = (1:0:0:0:0)$, $c_2 = (1:2:1:1:2)$.
$X_0^+(67)$: genus 2 hyperelliptic curve $y^2 = x^6 - 2x^5 + x^4 + 2x^3 + 2x^2 + 4x + 1$.
Mordell–Weil group of quotient: $J_0^+(67)(\mathbb{Q})$: $\mathbb{Z} \cdot [Q_1 - \infty^-] \oplus \mathbb{Z}[Q_2 - \infty^-]$, where $Q_1 = \infty^+$ and $Q_2 = (0,1)$.
A subgroup $G \subset J_0(67)(\mathbb{Q})$ satisfying $2 \cdot J_0(67)(\mathbb{Q}) \subset G$ is $G = \mathbb{Z} \cdot D_1 \oplus \mathbb{Z}D_2 \oplus \mathbb{Z}/11\mathbb{Z} \cdot D_{\text{tor}}$, where $D_{\text{tor}} := [c_2 - c_1]$, $D_1 := [P_7 + \overline{P}_7 - c_1 - c_2]$ and $D_2 := [P_1 + \overline{P}_1 - c_1 - c_2]$ for P_1 and P_7 as defined in Table 3.4.6 satisfying $\rho(P_1) = Q_1$ and $\rho(P_7) = Q_2$.
Primes used in sieve for for isolated quadratic points: 73, 59, 53, 31, 19, 5.
Primes used in sieve for cubic points: 73, 59, 53, 37, 17, 131, 167, 359.
There are **no** non-isolated quadratic points on $X_0(67)$. In particular, all quadratic points are supported on $\mathbb{Q}$-curves.

Name	minpol(α)	Coordinates	j-invariant	CM	$\mathbb{Q}$-c
P_0	-	$(9:7:7:4:12)$	-147197952000	-67	-
P_1	x^2+2	$(-\alpha+4:\alpha+14:-\alpha+4:2(-\alpha+4):18)$	8000	-8	w_{67}
P_2	x^2+3	$(0:\alpha+3:\alpha+3:\alpha+3:6)$	54000	-12	w_{67}
P_3	x^2+3	$(3\alpha+5:1:-\alpha+7:2(\alpha+6):26)$	-12288000	-27	w_{67}
P_4	x^2+3	$(4(9\alpha+11):-27\alpha+149:15\alpha+79:-3\alpha+57:182)$	0	-3	w_{67}
P_5	x^2+7	$(\alpha+5:-\alpha+11:\alpha+5:\alpha+5:16)$	-3375	-7	w_{67}
P_6	x^2+7	$(-\alpha+1:-\alpha+21:\alpha+7:-\alpha+9:20)$	16581375	-28	w_{67}
P_7	x^2+11	$(0:2(\alpha+11):-\alpha+11:\alpha+11:22)$	-32768	-11	w_{67}
P_8	x^2+43	$(-\alpha-13:2(-2\alpha+27):-5\alpha+41:$ $2(-2\alpha+27):106)$	-884736000	-43	w_{67}
P_9	x^3-x^2+ $x-3$	$(7\alpha^2-4\alpha+13:-\alpha^2-2\alpha+11:\alpha^2+2\alpha+7:$ $-\alpha^2-2\alpha+11:18)$	$-8522452\alpha^2-4897575\alpha-16236160$	NO	NO
$w_{67}(P_9)$	x^3-x^2+ $x-3$	$(19\alpha^2-13\alpha+79:-2\alpha^2-20\alpha+184:$ $19\alpha^2-13\alpha+79:-\alpha^2-10\alpha+92:203)$	$-3728415892268407\alpha^2-2142881183120745\alpha-$ 7102903223125105	NO	NO
P_{10}	x^3-x^2- $3x+5$	$(11(3\alpha^2-18\alpha+29):7\alpha^2-94\alpha+371:$ $13(\alpha^2-4\alpha+9):2(-\alpha^2-7\alpha+90):286)$	$182164461337778119200 0\alpha^2-$ $5318545688116020360000\alpha+$ 4744756895498802918000	-268	YES

Table 3.7: All non-cuspidal rational points, all quadratic points, and all cubic points on $X_0(67)$, up to Galois conjugacy.

3.4.7 $X_0(73)$

Model for $X_0(73)$:

$$x_0x_2-2x_1^2+2x_1x_2-2x_1x_4-x_2^2+3x_2x_3+3x_3^2-x_4^2=0,$$
$$2x_0x_3-x_1x_2-2x_1x_3+x_2^2-x_2x_3+2x_2x_4-8x_3^2+9x_3x_4-x_4^2=0,$$
$$x_0x_4-x_1x_3+x_1x_4-x_2x_3-5x_3^2+4x_3x_4=0.$$

Genus of $X_0(73)$: 5.

Cusps: $c_1 = (1:0:0:0:0)$, $c_2 = (1:1:1:0:0)$.

$X_0^+(73)$: genus 2 hyperelliptic curve $y^2 = x^6 + 2x^5 + x^4 + 6x^3 + 2x^2 - 4x + 1$.

Mordell–Weil group of quotient: $J_0^+(73)(\mathbb{Q})$: $\mathbb{Z} \cdot [Q_1 - \infty^+] \oplus \mathbb{Z} \cdot [Q_2 - \infty^-]$, where $Q_1 := (0, -1)$ and $Q_2 := (0, 1)$.

A subgroup $G \subset J_0(73)(\mathbb{Q})$ satisfying $2 \cdot J_0(73)(\mathbb{Q}) \subset G$ is $G = \mathbb{Z} \cdot D_1 \oplus \mathbb{Z} \cdot D_2 \oplus \mathbb{Z}/6\mathbb{Z} \cdot D_{\text{tor}}$, where $D_{\text{tor}} = [c_1 - c_2]$, $D_1 = [P_2 + \overline{P}_2 - c_1 - c_2]$, $D_2 = [P_5 + \overline{P}_5 - c_1 - c_2]$ for P_2, P_5 as defined in Table 3.4.7 and satisfying $\rho(P_2) = Q_1$ and $\rho(P_5) = Q_2$.

Primes used in sieve for quadratic points: 43, 67, 41, 17, 37, 13. Primes used in sieve for cubic points: 19, 41, 59, 43, 13, 103.

Name	minpol(α)	Coordinates	j-invariant	CM	$\mathbb{Q}$-c
P_1	$x^2 + 31$	$(-\alpha - 33 : -2(\alpha + 9) : -3\alpha - 35 : \alpha + 17 : 32)$	$(-2186237291314790238425374 41\alpha - 752765304839881478853034 71)/1888946593147858085478 4$	NO	NO
$w_{73}(P_1)$	$x^2 + 31$	$(-\alpha - 31 : 2(\alpha - 17) : -24 : 8 : 16)$	$(-6561\alpha + 1809)/4$	NO	NO
P_2	$x^2 + 19$	$(2(\alpha - 10) : \alpha - 17 : \alpha - 17 : \alpha + 11 : 14)$	-884736	-19	w_{73}
P_3	$x^2 + 1$	$(\alpha - 7 : 2\alpha - 4 : 3\alpha - 6 : \alpha + 3 : 1)$	287496	-16	w_{73}
P_4	$x^2 + 1$	$(2\alpha - 16 : -8\alpha - 14 : -2\alpha - 23 : 2\alpha + 10 : 13)$	1728	-4	w_{73}
P_5	$x^2 + 2$	$(-\alpha - 8) : -1 : -\alpha - 8 : -\alpha + 4 : 6)$	8000	-8	w_{73}
P_6	$x^2 + 127$	$(8(-\alpha-47) : -5\alpha-163 : 8(-\alpha-26) : 4(-\alpha+29) : 176)$	$(1475869227014015515734916 5\alpha + 814500172065991097081405 25)/1888946593147858085478 4$	NO	w_{73}
P_7	$x^2 + 3$	$(-22(9\alpha + 41) : -15\alpha - 51 : -22(9\alpha + 28) : -9\alpha + 37 : 52)$	0	-3	w_{73}
P_8	$x^2 + 3$	$(-4 : \alpha - 3 : \alpha - 5 : 2 : 4)$	54000	-12	w_{73}
P_9	$x^2 + 1$	$(-2 : \alpha - 3 : -4 : 2 : 2)$	-12288000	-27	w_{73}
P_{10}	$x^2 + 67$	$(2(-4\alpha-43) : -7\alpha-35 : -2(3\alpha+15) : 2(-\alpha+18) : 46)$	-147197952000	-67	w_{73}
P_{11}	$x^3 - x^2 + 7x + 8$	$(-\alpha^2 + 3\alpha - 1 : -\alpha - 2 : \alpha - 3 : 1 : 0)$	$-494084542528\alpha^2 + 945810849040\alpha - 4323317577856$	NO	NO
$w_{73}(P_{11})$	$x^3 - x^2 + 7x + 8$	$(5\alpha^2 - 9\alpha + 39 : \alpha^2 - \alpha + 4 : 4\alpha^2 - 7\alpha + 29 : -\alpha^2 + 2\alpha - 7 : 2)$	$1180375709887537307176 32\alpha^2 - 4385598835461226620641176 0\alpha - 4019484801318806967796953 6$	NO	NO

Table 3.8: All non-cuspidal rational points, all quadratic points, and all cubic points on $X_0(73)$, up to Galois conjugacy.

3.5 The hyperelliptic curve $X_0(37)$ and its quadratic points

This curve deserves a special section due to its peculiar nature. A model for $X_0(37)$, computed using the Small Modular Curves package in `Magma`, is given by

$$X_0(37): \ y^2 = x^6 + 8x^5 - 20x^4 + 28x^3 - 24x^2 + 12x - 4.$$

It is hyperelliptic of genus 2. We note that Mazur and Swinnerton–Dyer [MSD74, Section 5] already computed a model for this curve, as well as for $X_0^+(37)$, in 1974 without the aid of computers. They noticed that 37 is the smallest value of N such that $X_0^+(N)$ has positive genus.

Being hyperelliptic, $X_0(37)$ admits a hyperelliptic involution, mapping $(x, y) \mapsto (x, -y)$. Naturally, one is led to wonder: what is its moduli interpretation? Is it perhaps the Atkin–Lehner involution? There are exactly nineteen values of N such that $X_0(N)$ is hyperelliptic, as was discovered by Ogg [Ogg74]. Only in three of those nineteen cases, the hyperelliptic involution is not an Atkin–Lehner involution. For two of these, $N = 40$ and $N = 48$, there are different matrices in $\mathrm{SL}_2(\mathbb{R})$ inducing the hyperelliptic involution (see [BN15]). Not for $N = 37$, however.

Lehner and Newman computed in 1964 in a page of corrections to their paper [LN64] that the hyperelliptic involution of $X_0(37)$ is not induced by any automorphism of the complex upper half plane. Instead, the two cusps $(1 : 1 : 0)$ and $(1 : 1 : 1)$ (in the closure in $\mathbb{P}(1, 3, 1)$ of the above model) are mapped to the non-cuspidal rational points $(1 : -1 : 0)$ and $(1 : -1 : 1)$ respectively. We now know by [Maz78] that in fact these are the only non-cuspidal rational points. This observation of Lehner and Newman means that any moduli interpretation of the hyperelliptic involution must include an interpretation of the cusps. Such an interpretation in terms of "generalized elliptic curves" was given by Deligne and Rapoport [DR73], but we do not attempt to describe the hyperelliptic involution in those terms here.

Define $\infty_+ := (1 : 1 : 0)$ and $\infty_- := (1 : -1 : 0)$ and let i be the hyperelliptic involution on $X_0(37)$. We then have three non-trivial involutions i, w_{37} and $i \circ w_{37} = w_{37} \circ i$. In fact, we compute in `Magma` that $\mathrm{Aut}_{\mathbb{Q}}(X_0(37)) = \langle i, w_{37} \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We compute w_{37} to be

$$w := w_{37} : X_0(37) \to X_0(37), \ (x : y : z) \mapsto (x : y : x - z).$$

We refer to the four mentioned rational points as ∞_+, ∞_-, $w(\infty_+)$ and $w(\infty_-)$. The fact that $i \neq w_{37}$ has dramatic consequences for the abundance of quadratic points on $X_0(37)$. The hyperelliptic covering map $x : X_0(37) \to \mathbb{P}^1$ is one source of infinitely many quadratic points. Unlike in the cases $N = 40$ and $N = 48$ (see [BN15]), here the quotient $\rho : X_0(37) \to X_0^+(37) := X_0(37)/\langle w_{37} \rangle$ is an elliptic curve of rank 1. A model is given by

$$X_0^+(37): \ y^2 + y = x^3 - x$$

and its Mordell-Weil group is the free abelian group generated by the point $Q_1 := (0, -1)$ (choosing $O = \rho(\infty_+) = (0 : 1 : 0)$). Hence this bielliptic quotient $X_0^+(37)$ is a second

source of infinitely many quadratic points. Moreover, we also have the quotient map $\pi : X_0(37) \to E := X_0(37)/\langle i \circ w_{37} \rangle$. A model for E is

$$E: \ y^2 + y = x^3 + x^2 - 23x - 50.$$

This elliptic curve has Mordell-Weil group $\mathbb{Z}/3\mathbb{Z}$, generated by the point $Q_E := (8 : 18 : 1)$ (choosing $O = \pi(\infty_+) = (0 : 1 : 0)$). Another source of points, albeit just three. In this section we describe how these different sources fit together to make up all points on $X_0(37)^{(2)}(\mathbb{Q})$.

Consider the Abel–Jacobi map

$$\kappa : X_0(37)^{(2)}(\mathbb{Q}) \to J_0(37)(\mathbb{Q}), \ P + Q \mapsto [P + Q - \infty_+ - \infty_-].$$

Lemma 3.5.1. *Let X be any hyperelliptic curve of genus 2 with involution i. Then an effective degree 2 divisor D is linearly equivalent to the canonical divisor K if and only if D is of the form $P + i(P)$ for some point P on X.*

Proof. This is well-known. Riemann–Roch implies that $\ell(K - P - i(P)) = \ell(P + i(P)) - 1$, and $\deg(K - P - i(P)) = 0$. Post-composed with an automorphism of $\mathbb{P}^1$, the hyperelliptic covering map $X \to \mathbb{P}^1$ defines a non-constant function in the Riemann–Roch space $L(P + i(P))$, so that $K = [P + i(P)]$. Conversely, suppose that $P + Q \sim R + i(R)$ for points P, Q, R on X. Note that $\ell(R + i(R)) = 2$ by Riemann–Roch, hence $L(R + i(R)) = \{\alpha + \beta f : \alpha, \beta \in \overline{\mathbb{Q}}\}$, where f is the hyperelliptic covering map with poles in $R, i(R)$. This shows that $R + i(R)$ is only linearly equivalent to degree 2 divisors of the form $P + i(P)$. □

Lemma 3.5.2. *Let X be a hyperelliptic genus 2 curve with Jacobian J, hyperelliptic involution i and $\kappa : X^{(2)} \to J$, $P \mapsto [P - \infty - i(\infty)]$ for some point ∞ on X. The fibre $\kappa^{-1}(\{0\})$ consists of the effective divisors linearly equivalent to the canonical divisor K. Moreover, κ is a bijection away from this fibre.*

Proof. This is again a well-known consequence of Riemann–Roch. □

Proposition 3.5.3. *Let $P_1 = (1/2(\sqrt{-3}+1), -1) \in X_0(37)(\overline{\mathbb{Q}})$. The Jacobian $J_0(37)(\mathbb{Q}) = \mathbb{Z} \cdot D \oplus \mathbb{Z}/3\mathbb{Z} D_{\text{tor}}$, where $D = [P_1 + \overline{P_1} - \infty_+ - \infty_-] = \rho^*([Q_1 - O])$ and $D_{\text{tor}} = [\infty_+ + w(\infty_-) - \infty - \infty_-] = [\infty_+ - w(\infty_+)] = \pi^*[Q_E - O]$.*

Proof. As $X_0(37)$ is hyperelliptic of genus 2, its Mordell–Weil group can be determined using height bounds and an algorithm of Stoll [Sto02]. As 37 is prime, we know by Mazur's [Maz77] proof of Ogg's conjecture that the torsion subgroup equals the rational cuspidal subgroup, and we check that the difference of the cusps has order 3, equals $\pi^*([Q_E - O])$ and is of the form $\kappa(\{\infty_+, i(w(\infty_+)\})$. □

Note that $\rho(P_1) \neq Q_1$ because the basedivisor of κ is not w_{37}-invariant. This gives us a description of all points in $X_0(37)^{(2)}(\mathbb{Q})$. First, there is the set $\mathcal{Q}_i$ of quadratic points Q_x with rational x-coordinate x. Though easy to describe coordinatewise, we lack a moduli interpretation of elliptic curves corresponding to these points. Then we have the

points $\mathcal{P}_{1,0} := P_1 + \overline{P_1}$ and $\mathcal{P}_{0,1} := \infty_+ + w(\infty_-)$. For any $(a,b) \in \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \setminus \{(0,0)\}$, there is another point $\mathcal{P}_{a,b} \in X_0(37)^{(2)}(\mathbb{Q})$ defined as the unique effective degree 2 divisor $\mathcal{P}$ such that $\mathcal{P} - \infty_+ - \infty_- \sim a\mathcal{P}_{1,0} + b\mathcal{P}_{0,1} - (a+b)(\infty_+ + \infty_-)$ for any lift of b to $\mathbb{Z}$. To compute $\mathcal{P}_{a,b}$, one simply computes the 1-dimensional Riemann–Roch space $L(a\mathcal{P}_{1,0} + b\mathcal{P}_{0,1} - (a+b-1)(\infty_+ + \infty_-))$. We conclude the following.

Proposition 3.5.4. *The map*

$$\mathbb{P}^1(\mathbb{Q}) \sqcup (\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \setminus \{(0,0)\}) \to X^{(2)}(\mathbb{Q}),\ x \mapsto Q_x,\ (a,b) \mapsto \mathcal{P}_{a,b}$$

is a bijection. Moreover, w_{37} interchanges the two points in $\mathcal{P} \in X_0(37)^{(2)}(\mathbb{Q})$ if and only if $\mathcal{P} = \mathcal{P}_{a,0}$ for some $a \in \mathbb{Z}$, and in that case $\mathcal{P}$ corresponds to a $\mathbb{Q}$-curve.

Remark 3.5.5. If P is a quadratic point such that $\rho(P) \in X_0^+(37)(\mathbb{Q})$, then $[P + \overline{P} - \infty_+ - \infty_-]$ is not equal to $\rho^*[\rho(P) - O] = [P + \overline{P} - \infty_+ - w(\infty_+)]$. As $[w(\infty_+) - \infty_-] = -3[P_1 - \infty_+ - \infty_-]$, this amounts to a shift: if $\rho(P) = n[Q_1 - O]$ then $P + \overline{P} = P_{n-3,0}$. This justifies the claim that $P_{a,b}$ is fixed by w_{37} if and only if $b = 0$, despite the incompatiblity of the basedivisors.

The three points $P + Q$ in $X_0(37)^{(2)}(\mathbb{Q})$ such that $Q = i \circ w_{37}(P)$ are $\infty_+ + w(\infty_-)$, $w(\infty_+) + \infty_-$ and $R + \overline{R}$, where $R = (2, 2\sqrt{37})$, so $E(\mathbb{Q})$ only contributes one pair of genuinely quadratic points. Yet, this is an interesting pair. We see that i also interchanges the two points R and $\overline{R}$, so $R + \overline{R} = Q_2$. Again, this is no problem, because $[R + \overline{R} - \infty_+ - \infty_-] \neq \pi^*([\pi(R) - O])$ due to ∞_- not mapping to O under π. As both i and $i \circ w$ interchange R and $\overline{R}$, we find that w_{37} fixes R and $\overline{R}$. The corresponding elliptic curve thus has a degree 37 endomorphism and must have CM by the maximal order in $\mathbb{Q}(\sqrt{-37})$. It is no coincidence that the point is defined over $\mathbb{Q}(\sqrt{37})$: this follows from Theorem 4.1 in [Sil94] as the Hilbert class field of $\mathbb{Q}(\sqrt{-37})$ is $\mathbb{Q}(\sqrt{-37}, \sqrt{37})$. The j-invariant of the elliptic curve corresponding to R is $3260047059360000\sqrt{37} + 19830091900536000$.

Chapter 4

Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular

In this chapter we prove that every elliptic curve defined over a totally real number field of degree 4 not containing $\sqrt{5}$ is modular. To this end, we study the quartic points on four modular curves.

This chapter is a subset of the article [Box21a].

4.1 Introduction

After the major breakthrough of Wiles [Wil95] and Taylor–Wiles [TW95] on semi-stable elliptic curves, Breuil, Conrad, Diamond and Taylor [BCDT01] proved in 2000 that all elliptic curves over $\mathbb{Q}$ are modular. Since then, the natural follow-up question was: can we extend these results to elliptic curves over other number fields? In this chapter we do so for all totally real quartic fields not containing a root of 5, by combining a variety of computational methods to study the quartic points on multiple modular curves. Crucial is the use of the "partially relative" symmetric Chabauty method developed in Chapter 3.

Let K be a totally real number field. We say that an elliptic curve E over K of conductor $\mathcal{N}$ is *modular* when there is a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}$, parallel weight 2 and with rational Hecke eigenvalues, such that their corresponding systems of compatible ℓ-adic Galois representations are isomorphic. Here the ℓ-adic Galois representation attached to E arises from the action of $\mathrm{Gal}(\overline{K}/K)$ on the Tate module $T_\ell(E)$, and the Galois representation associated to $\mathfrak{f}$ was defined by Taylor [Tay89], extending the construction of Eichler and Shimura for $K = \mathbb{Q}$ (see e.g. [DS05]).

The first modularity results beyond $\mathbb{Q}$ were proved by Jarvis and Manoharmayum [JM08], who showed that all semi-stable elliptic curves over $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{17})$ are modular. A real leap forward was then made in 2014 by Freitas, Le Hung and Siksek [FLHS15] when they proved modularity of elliptic curves over all real quadratic fields simultaneously.

More recently, Derickx, Najman and Siksek [DNS20] extended this to elliptic curves over all totally real cubic fields. We go one step further to totally real quartic fields, albeit only those not containing a root of 5. In Section 4.6, we discuss some of the difficulties one encounters for quartic fields containing $\sqrt{5}$ and for quintic fields.

Theorem 4.1.1. *Let E be an elliptic curve over a totally real quartic number field not containing a square root of 5. Then E is modular.*

Our strategy for proving modularity is similar to that of Wiles [Wil95], Freitas–Le Hung–Siksek [FLHS15] and Derickx–Najman–Siksek [DNS20]. We make use of strong modularity lifting theorems due to Breuil–Diamond [BD14], Thorne [Tho16] and Kalyanswami [Kal18] (building on the work of many others), which *almost* prove modularity over all totally real number fields, in the following sense: the mod p Galois representation of a non-modular elliptic curve over a totally real number field must have "small" image for $p \in \{3, 5, 7\}$. This particular meaning of "small" can be parametrised precisely by modular curves, leading to the following corollary of the aforementioned modularity lifting results.

Theorem 4.1.2. *Suppose that E is an elliptic curve over a totally real number field K satisfying $K \cap \mathbb{Q}(\sqrt{5}) = \mathbb{Q}$ and $K \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$, where ζ_7 is a primitive 7th root of unity. If E is not modular, then E gives rise to a K-point on one of the following modular curves:*

$$X(\mathrm{b3}, \mathrm{b5}, \mathrm{b7}), \quad X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7}), \quad X(\mathrm{b3}, \mathrm{b5}, \mathrm{e7}), \quad X(\mathrm{s3}, \mathrm{b5}, \mathrm{e7}).$$

In Section 4.1.1 we define these curves and show how this theorem follows from modularity lifting results. Theorem 4.1.2 reduces the modularity question to studying K-rational points on these four curves. In the classical case $K = \mathbb{Q}$, it sufficed to forget about the prime 7 and consider only the curves $X(\mathrm{b3}, \mathrm{b5})$ and $X(\mathrm{s3}, \mathrm{b5})$. Both of these are ellipic curves with finite Mordell–Weil group, and the rational points were swiftly found to correspond to cusps or modular elliptic curves. When considering elliptic curves over totally real fields of degree $d > 1$, this final piece of the puzzle, i.e. finding all degree d points on these four curves (or their quotients), ceases to be a trivial exercise. In the quadratic case, Freitas, Le Hung and Siksek in fact had to study seven modular curves, as they did not yet have the results of Thorne [Tho16] and Kalyanswamy [Kal18] at their disposal. In Remark 4.4.4, we describe a shorter proof of modularity of elliptic curves over real quadratic fields now made possible by these stronger modularity lifting theorems.

We prove Theorem 4.1.1 by studying the quartic points on these four curves. Determining all quartic points on either of those curves directly is not computationally feasible: the curves have genera 13, 21, 73 and 153 respectively. The saving grace here is the fact that all four curves give rise to a rich tree of quotient curves of smaller genus, on which explicit computations can be performed. For none of the four curves, however, did it suffice to study the quartic points on a single such quotient curve; instead, we combine information from multiple quotient curves using their maps to common quotients further down the tree. For $X(\mathrm{b3}, \mathrm{b5}, \mathrm{b7})$, we work on 10 different quotients by Atkin–Lehner involutions of genus up to 5, whereas for $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$ we consider two genus 3 quotients.

To study the final two curves, we need two important new ingredients: the relative symmetric Chabauty method developed in Chapter 3, and the algorithm for determining models for quotients of modular curves developed in Chapter 2.

4.1.1 Consequences of modularity lifting theorems

We mention three consequences of modularity lifting theorems, and how they lead to Theorem 4.1.2. Recall that we defined various subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, for p prime, in Section 1.1.3. For an elliptic curve E over a field K and $N \in \mathbb{Z}_{\geq 1}$, denote by $\overline{\rho}_{E,N} \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (defined up to conjugation by an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$) the map determined by the action of the Galois group on $E[N](\overline{K})$.

Theorem 4.1.3. *Suppose that E is a non-modular elliptic curve over a totally real field K. Then*

(i) $\mathrm{Im}(\overline{\rho}_{E,3})$ *is conjugate to a subgroup of* $C_s^+(3)$ *or* $B(3)$*,*

(ii) if $\sqrt{5} \notin K$*, then* $\mathrm{Im}(\overline{\rho}_{E,5})$ *is conjugate to a subgroup of* $B(5)$*, and*

(iii) if $K \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$*, then* $\mathrm{Im}(\overline{\rho}_{E,7})$ *is conjugate to a subgroup of* $B(7)$ *or* $G(\mathrm{e}7)$*.*

Proof. Part (i) is a consequence of modularity lifting theorems due amongst others to Breuil and Diamond [BD14], which show that the restriction of $\overline{\rho}_{E,3}$ to $\mathrm{Gal}(\overline{K}/K(\zeta_3))$ is absolutely reducible. See [FLHS15, Theorem 3] for more details. It then follows from [Rub97, Proposition 6] that $\overline{\rho}_{E,3}$ is conjugate to a subgroup of $C_s^+(3)$ or $B(3)$.

Part (ii) was shown by Thorne [Tho16]. In [Kal18, Proposition 4.3 and Theorem 4.4], Kalyanswami shows that if $K \cap \mathbb{Q}(\zeta_7) = \mathbb{Q}$, then $\mathrm{Im}(\overline{\rho}_{E,7})$ is conjugate to a subgroup of either $B(7)$ or $C_{\mathrm{ns}}^+(7)$. In the latter case, Freitas, Le Hung and Siksek study the subgroups of $C_{\mathrm{ns}}^+(7)$ and show in [FLHS15, Proposition 4.1 (c)] that in fact the image must be contained in the index 2 subgroup $G(\mathrm{e}7)$. □

Recall that an elliptic curve E over a number field K is a $\mathbb{Q}$-curve when E is $\overline{K}$-isogenous to each of its Galois conjugates. Another important modularity result we shall need is the following.

Theorem 4.1.4 (Ribet [Rib04])**.** *Every $\mathbb{Q}$-curve is modular.*

Finally, let E/K be a non-modular elliptic curve over a totally real field. Theorem 4.1.3 and Proposition 1.1.4 imply that E gives rise to a K-point on $X(\mathrm{b}3, \mathrm{b}5, \mathrm{b}7)$, $X(\mathrm{s}3, \mathrm{b}5, \mathrm{b}7)$, $X(\mathrm{b}3, \mathrm{b}5, \mathrm{e}7)$ or $X(\mathrm{s}3, \mathrm{b}5, \mathrm{e}7)$, which proves Theorem 4.1.2.

It thus suffices to find the quartic points on those curves. In fact, it suffices to find the quartic points P whose j-invariant $j(P)$ also has degree 4: if smaller, then P is supported on an elliptic curve E that either has j-invariant 0 or 1728 and hence is a $\mathbb{Q}$-curve, or is a quadratic twist $E = E' \otimes \chi$, where χ is a quadratic character and E' is an elliptic curve defined over a real number field of degree 1 or 2. In the latter case, E' is known to be modular by [FLHS15]. If E' corresponds to the Hilbert modular form $\mathfrak{f}$, then E is also modular and corresponds to $\mathfrak{f} \otimes \chi$.

Theorem 4.1.5. *On $X(\mathrm{b3}, \mathrm{b5}, \mathrm{b7}) = X_0(105)$ and $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$, all quartic points with quartic j-invariant are supported on a $\mathbb{Q}$-curve. On $X(\mathrm{b3}, \mathrm{b5}, \mathrm{e7})$ and $X(\mathrm{s3}, \mathrm{b5}, \mathrm{e7})$, all quartic points with quartic j-invariant are either supported on a $\mathbb{Q}$-curve, or have a non-totally real j-invariant displayed in Table 4.1.*

The preceding discussion shows that this theorem implies Theorem 4.1.1. The remainder of this chapter is thus devoted to the proof of Theorem 4.1.5

4.1.2 Overview

We study the quartic points on $X(\mathrm{b3}, \mathrm{b5}, \mathrm{b7})$ in Section 4.2 by making use of ten of its quotients, after which we study the quartic points on $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$ in Section 4.3 using the two genus 3 hyperelliptic quotients $X(\mathrm{b5}, \mathrm{b7})$ and $X(\mathrm{s3}, \mathrm{b7})$. We then use the Chabauty–Coleman method developed in Chapter 3 to study the quartic points on $X(\mathrm{b5}, \mathrm{ns7})$ in Section 4.4. Finally, we use the knowledge of the (infinitely many) quartic points on $X(\mathrm{b5}, \mathrm{ns7})$ to study the quartic points on $X(\mathrm{b3}, \mathrm{b5}, \mathrm{e7})$ and $X(\mathrm{s3}, \mathrm{b5}, \mathrm{e7})$ in Section 4.5, using a combination of Chabauty's method on two quotient curves with a Mordell–Weil sieve.

The explicit computations on these curves were done in `Magma`, and are publicly available at

`https://github.com/joshabox/quarticpoints/` .

4.2 $X_0(105)$

In this section we prove the following theorem.

Theorem 4.2.1. *Let E be an elliptic curve with quartic j-invariant that occurs as a quartic point on $X_0(105)$. Then E is a $\mathbb{Q}$-curve, and in particular E is modular.*

4.2.1 A convenient model

As described in Section 1.2.3, we compute that $L(f, 1) \neq 0$ for each eigenform $f \in S_2(\Gamma_0(N))$, from which we conclude by [KL89] that the Mordell–Weil group $J_0(105)(\mathbb{Q})$ is finite. The genus of $X_0(105)$ is 13, however, making it computationally infeasible to do the Riemann–Roch space computations described in Section 1.2.4. Instead, we begin by studying the quotient $X_0(105)/w_5$, where w_5 is the Atkin–Lehner involution corresponding to 5. This quotient has genus 5.

We compute the map $X_0(105) \to X_0(105)/w_5$ explicitly. To this end, we first find a basis of 13 linearly independent cusp forms in $S_2(\Gamma_0(105))$, consisting of 5 cusp forms that are fixed by w_5 and 8 cusp forms f such that $f|w_5 = -f$. Equations between the first five cusp forms yield the following model for $X_0(105)/w_5$ in $\mathbb{P}^4_{x_1,\ldots,x_5}$:

$$\begin{aligned} X_0(105)/w_5 : \quad & x_1x_3 - x_2^2 - x_3x_5 - x_4^2 = 0, \\ & x_1x_4 - x_2x_3 + x_2x_4 - x_3^2 - x_4x_5 = 0, \\ & 2x_1x_5 + x_2x_4 - 2x_2x_5 - 3x_3^2 + 3x_3x_4 + 2x_3x_5 - 2x_4^2 - 2x_4x_5 + 2x_5^2 = 0, \end{aligned}$$

and the (quadratic) equations between all 13 cusp forms result in an explicit canonical model for $X_0(105) \subset \mathbb{P}^{12}$. We do not display this model here (it consists of 55 quadratic equations in 13 variables), but we invite the curious reader to run the `Magma` code. The quotient map $X_0(105) \to X_0(105)/w_5$ is then simply projection onto the first 5 coordinates.

Since the map $X_0(105) \to X_0(105)/w_5$ is of degree 2, there must be a $g \in \mathbb{Q}(X_0(105)/w_5)$, not a square, whose pullback to $\mathbb{Q}(X_0(105))$ is a square. In fact, we find such a g in the coordinate ring of our model for $X_0(105)/w_5$. This reveals to us the extra equation $z^2 = g$, where z is a new coordinate, which determines $X_0(105)$ as a degree 2 cover of $X_0(105)/w_5$. Using the equations defining $X_0(105)$, we search for a polynomial $f \in \mathbb{Q}[x_1, \ldots, x_{13}] \setminus \mathbb{Q}[x_1, \ldots, x_5]$ such that f^2 is, modulo the equations defining $X_0(105)$, a polynomial in $x_1, \ldots, x_5$. We square f to obtain

$$g = 9x_1^2 - 6x_1x_2 + x_2^2 + 6x_2x_3 + 21x_2x_4 - 12x_2x_5 - 17x_3^2 + 19x_3x_4 + 18x_3x_5 + 7x_4^2 - 18x_4x_5 + 27x_5^2.$$

It can be easily verified that g is indeed a square in the coordinate ring of $X_0(105)$, but that g/x_1^2 is not a square in $\mathbb{Q}(X_0(105)/w_5)$. We conclude that $X_0(105) \to X_0(105)/w_5$ is the degree 2 cover given by $z^2 = g$. We denote the coordinates of $X_0(105) \subset \mathbb{P}^5$ in this model by $(x_1 : \ldots : x_5 : z)$. We obtain the following lemma, which proves the convenience of this model.

Lemma 4.2.2. *Suppose that K is a field and $P \in (X_0(105)/w_5)(K)$. Let $Q \in X_0(105)$ be a point mapping to P. Then $Q \in X_0(105)(K)$ if and only if $g(P)$ is a square in K.*

4.2.2 Quartic points on $X_0(105)/w_5$

Next, we study the quartic points on $X_0(105)/w_5$. Its cover $X_0(105)$ has eight cusps, mapping to the four rational points

$$P_1 = (3 : 0 : 2 : 2 : 1), \quad P_2 = (0 : 0 : -1 : -1 : 1),$$
$$P_3 = (1 : 0 : 0 : 0 : 0), \quad P_4 = (-1 : 0 : 0 : 0 : 1)$$

on $X_0(105)/w_5$. Our curve $X_0(105)/w_5$ has three quotients by Atkin–Lehner involutions:

$$\pi_3 : X_0(105)/w_5 \to C := X_0(105)/\langle w_5, w_3 \rangle,$$

$$\pi_7 : X_0(105)/w_5 \to E_7 := X_0(105)/\langle w_5, w_7 \rangle$$

and

$$\pi_{21} : X_0(105) \to E_{21} := X_0(105)/\langle w_5, w_{21} \rangle.$$

Here C is hyperelliptic of genus 3. The curves E_7 and E_{21} are elliptic curves of conductors 21 and 35 respectively. On all three of these, the remaining Atkin–Lehner operator acts as a non-trivial involution. Here are their models:

$$C: \ y^2 = x^8 + 6x^7 + 7x^6 - 2x^5 + 17x^4 + 8x^3 - 28x^2 + 36x - 24,$$
$$E_7: \ y^2 + xy = x^3 + x \text{ and}$$

$$E_{21}:\ y^2+y=x^3+x^2-x.$$

Proposition 4.2.3. *The Mordell–Weil group of $X_0(105)/w_5$ equals*

$$\mathbb{Z}/6\mathbb{Z}\cdot(7[P_2-P_1]-6[P_3-P_1])\oplus\mathbb{Z}/24\mathbb{Z}\cdot[P_4-P_1].$$

Proof. We denote our curve by $X:=X_0(105)/w_5$ and its Jacobian by J. We know that $J(\mathbb{Q})$ has rank 0, as it maps to $J_0(105)(\mathbb{Q})$ with finite kernel. In particular, at each prime $p>2$ of good reduction for the displayed model, $J(\mathbb{Q})$ embeds into $J(\mathbb{F}_p)$. The primes $p=11$ and $p=13$ are of good reduction. Using the embedding for $p=11$, we check that the cuspidal subgroup of $J(\mathbb{Q})$ generated by $[P_4-P_1],[P_3-P_1],[P_2-P_1]$ equals the claimed group. We use the class group algorithm of Hess [Hes02], implemented in `Magma`, to find that $J(\mathbb{F}_{11})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/60\mathbb{Z}\times\mathbb{Z}/600\mathbb{Z}$ and $J(\mathbb{F}_{13})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/3168\mathbb{Z}$. As $\gcd(600,3168)=24$, we find that $J(\mathbb{Q})$ is isomorphic to one of

$$\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z},\quad \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z},\quad \mathbb{Z}/2\mathbb{Z}^2\times\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/24\mathbb{Z}.$$

It thus suffices to determine the 2-torsion of $J(\mathbb{Q})$. Considering more primes does not narrow it down any further. Instead, we will show that

$$J(\mathbb{Q}(\sqrt{21}))[2]\simeq(\mathbb{Z}/2\mathbb{Z})^3$$

and determine $J(\mathbb{Q})[2]$ by taking Galois invariants. In order to find the extra 2-torsion element, we look at the quotient $C=X/w_3$. The quadratic point $(2,4\sqrt{105})\in C$ generates a rational effective degree 2 divisor pulling back to a degree 4 divisor D on X, irreducible over $\mathbb{Q}$, whose points are defined over $\mathbb{Q}(\sqrt{5},\sqrt{21})$. Over $\mathbb{Q}(\sqrt{21})$, however, D splits into a sum of two effective degree 2 divisors: $D=D_1+D_2$, where D_1 is the sum of

$$\begin{gathered}((-254\sqrt{21}+1326)\sqrt{5}+5(-111\sqrt{21}+594):(84\sqrt{21}-516)\sqrt{5}+5(38\sqrt{21}-210):\\ 5(-4\sqrt{21}+48)\sqrt{5}+5(-11\sqrt{21}+91):(22\sqrt{21}-18)\sqrt{5}+5(8\sqrt{21}-14):205)\end{gathered}$$

and its $\mathrm{Gal}(\mathbb{Q}(\sqrt{5},\sqrt{21})/\mathbb{Q}(\sqrt{21}))$-conjugate. We then verify that

$$D_{\mathrm{tors}}:=[D_1-2P_1]-[P_2-P_1]-2[P_3-P_1]-[P_4-P_1]$$

is a non-trivial two-torsion element in $J(\mathbb{Q}(\sqrt{21}))$, and moreover that the difference of D_1 and its $\mathrm{Gal}(\mathbb{Q}(\sqrt{21})/\mathbb{Q})$-conjugate is not principal. This means that D_{tors} is not defined over $\mathbb{Q}$. In particular, $J(\mathbb{Q}(\sqrt{21}))[2]$ must have dimension at least 3 over $\mathbb{F}_2$.

Next, note that 17 and 47 split in $\mathbb{Q}(\sqrt{21})$, so that $J(\mathbb{Q}(\sqrt{21}))_{\mathrm{tors}}$ embeds into $J(\mathbb{F}_{17})$ and $J(\mathbb{F}_{47})$. Both of these groups have 2-torsion isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. Let $H:=\langle[P_2-P_1],[P_3-P_1],[P_4-P_1]\rangle\subset J(\mathbb{Q})$. We use the algorithm developed by Özman and Siksek [OS19] to show the following: there does not exist a group isomorphism $\phi:H_{17}\to H_{47}$, such that H_{17} and H_{47} are subgroups of $J(\mathbb{F}_{17})$ and $J(\mathbb{F}_{47})$ respectively, both containing the image of H and the subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$, where the restriction of ϕ to

the image of H is the isomorphism obtained by reducing H modulo 17 and 47. It follows that $J(\mathbb{Q}(\sqrt{21}))[2] \simeq (\mathbb{Z}/2\mathbb{Z})^3$ and $J(\mathbb{Q})[2] = J(\mathbb{Q}(\sqrt{21}))[2]^{\mathrm{Gal}(\mathbb{Q}(\sqrt{21})/\mathbb{Q})} \simeq (\mathbb{Z}/2\mathbb{Z})^2$, as desired. □

The hyperelliptic curve C admits the involution w_7, giving rise to a degree 2 map $C \to \mathbb{P}^1 = X_0(105)/\langle w_3, w_5, w_7\rangle$. The curve C thus has an infinite set of quadratic points coming from $\mathbb{P}^1(\mathbb{Q})$ under this map. The two elliptic curves, however, have more sources of infinitely many quadratic points: by the Riemann–Roch theorem, there is an infinite set of effective degree 2 divisors mapping to each point in the Mordell–Weil groups $E_7(\mathbb{Q})$ and $E_{21}(\mathbb{Q})$ under the Abel–Jacobi map (c.f. Section 1.2.4). All of these give rise to quartic points on $X_0(105)/w_5$. We compute that $E_7(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ and $E_{21}(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$.

Denote the generators of $J(X_0(105)/w_5)(\mathbb{Q})$ by

$$D_1 := 7(P_2 - P_1) - 6(P_3 - P_1) \text{ and } D_2 := P_4 - P_1,$$

and write

$$D_0 := P_1 + P_2 + P_3 + P_4.$$

The two elliptic curves E_7 and E_{21} supply us with a total of 6 classes $[D]$ in $J(X_0(105)/w_5)(\mathbb{Q})$ such that $\ell(D + D_0) \geq 2$, by pulling back the elements in the Mordell–Weil groups $E_7(\mathbb{Q})$ and $E_{21}(\mathbb{Q})$ (there is one overlapping class). As we know the Mordell–Weil group of $X_0(105)/w_5$, we can verify that pullbacks of quadratic points from E_7 and E_{21} are the only sources of infinitely many quartic points on $X_0(105)/w_5$ by computing Riemann–Roch spaces, c.f. Section 1.2.4.

Proposition 4.2.4. *Consider $(a, b) \in \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$. The dimension of the Riemann–Roch space $L(aD_1 + bD_2 + D_0)$ is at least 2 precisely when $(a, b) \in \{(0, 0), (0, 6), (0, 8), (0, 12), (0, 16), (0, 18)\}$, in which case the dimension equals 2. As the above set has size 6, each of these Riemann–Roch spaces is the pullback of a corresponding Riemann–Roch space on E_7 or E_{21} (or both, when $(a, b) = (0, 0)$). In particular, the set*

$$(X_0(105)/w_5^{(4)})(\mathbb{Q}) \setminus \left(\pi_7^* E_7^{(2)}(\mathbb{Q}) \cup \pi_{21}^* E_{21}^{(2)}(\mathbb{Q})\right)$$

is finite and explicitly computable.

Proof. We apply Lemma 1.2.4 to the Riemann–Roch spaces $L(D)$ of dimension 1 to compute the points. By Corollary 1.2.5, the elements $D \in (X_0(105)/w_5)^{(4)}(\mathbb{Q})$ such that $\ell(D) = 2$ correspond precisely to pullbacks because the Riemann–Roch spaces are pullbacks. The Riemann–Roch computations were done explicitly in `Magma`, which took multiple hours. □

Proposition 4.2.5. *Each quartic point on $X_0(105)$ maps to a rational or quadratic point on E_7 or E_{21}.*

Proof. Each quartic point on $X_0(105)$ maps to a quartic or quadratic point on $X_0(105)/w_5$. Using Proposition 4.2.4, we find the quartic points on $X_0(105)/w_5$ not mapping to a quadratic point on E_7 or E_{21}, and we find that none of those are the image of a quartic point

on $X_0(105)$ by Lemma 4.2.2. There are three pairs of quadratic points on $X_0(105)/w_5$. We can find these either by decomposing the degree 4 divisors found in Proposition 4.2.4 into irreducible divisors, or by doing the equivalent Riemann–Roch space computation for degree 2 points. We verify that each of these three quadratic points maps to a rational point on E_7 or E_{21}. □

4.2.3 Exploiting the tree

Next, we focus our attention on the quadratic points on E_7 and E_{21}. There are infinitely many of those, but few are in the image of a quartic point on $X_0(105)$. The following lemma allows us to exploit this.

Lemma 4.2.6. *Suppose that X is a curve over a field K admitting two distinct commuting involutions $v, w : X \to X$. Suppose that $Q \in X$ is defined over a quartic extension of K, but its image in $X/\langle v, w\rangle$ is defined over a quadratic extension of K. Then the image of Q is quadratic over K in one of the three curves X/v, X/w and X/vw.*

$$\begin{tikzcd}
 & X \arrow[dl] \arrow[d] \arrow[dr] & \\
X/v \arrow[dr] & X/vw \arrow[d] & X/w \arrow[dl] \\
 & X/\langle v, w\rangle &
\end{tikzcd}$$

Proof. Consider the effective degree 2 divisor $D \in (X/\langle v, w\rangle)^{(2)}(K)$ that is the sum of the image of Q and its conjugate over K. Let us assume towards a contradiction that D pulls back to an irreducible effective degree 4 divisor over K on X/w, X/vw and X/v. Write the pullback to X as $D_1 + D_2$, where D_1 and D_2 are degree 4 divisors over K. Then for each $u \in \{v, w, vw\}$, we must have $u^*D_1 = D_2$ and $u^*D_2 = D_1$. In particular, $(vw)^*D_1 = w^*v^*D_1 = w^*D_2 = D_1$, so that $D_1 = D_2$ and $u^*D_1 = D_1$ for each $u \in \{v, w, vw\}$. Now the pullback of D to X/u is the double of a degree 2 divisor over K, unless u fixes D_1 pointwise. We conclude that v, w and vw fix D_1 pointwise. But then D is irreducible of degree 4, a contradiction. □

We note that the analogue of this lemma holds true for every point of even degree $2n$ ($n \in \mathbb{Z}_{\geq 1}$) on the top curve X mapping to a point of degree n on the bottom curve.

Proposition 4.2.7. *Suppose that $P \in E_7$ or $P \in E_{21}$ is a quadratic point that is the image of a quartic point of $X_0(105)$. Then P is the image of a quadratic point on one of the curves*

$$X_0(105)/w_5,\ \ X_0(105)/w_7,\ \ X_0(105)/w_{35},\ \ X_0(105)/w_{21},\ \ X_0(105)/w_{105}.$$

Proof. We apply Lemma 4.2.6 to $X_0(105)$, first with involutions w_5 and w_7, then with involutions w_5 and w_{21}; see also Figure 4.1. □

$$
\begin{tikzcd}
 & & & X_0(105) \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
 & \frac{X_0(105)}{w_5} \arrow[dl, "\pi_3"'] \arrow[d, "\pi_{21}"] \arrow[dr, "\pi_7"] & \frac{X_0(105)}{w_{21}} \arrow[dr] & \frac{X_0(105)}{w_7} \arrow[d] \arrow[dr] & \frac{X_0(105)}{w_{105}} \arrow[d] & \frac{X_0(105)}{w_{35}} \\
\frac{X_0(105)}{\langle w_5,w_3\rangle} \arrow[drrr] & \frac{X_0(105)}{\langle w_5,w_{21}\rangle} \arrow[drr] & \frac{X_0(105)}{\langle w_5,w_7\rangle} \arrow[dr] & \frac{X_0(105)}{\langle w_7,w_{21}\rangle} \arrow[d] & \frac{X_0(105)}{\langle w_7,w_{105}\rangle} \arrow[dl] & \\
 & & & X_0(105)^* = \mathbb{P}^1 & &
\end{tikzcd}
$$

Figure 4.1: Part of the Atkin–Lehner tree of $X_0(105)$.

For coprime prime powers $p_1, \ldots, p_n$, we write

$$X_0(p_1 \cdots p_n)^* = X_0(p_1 \cdots p_n)/\langle w_{p_1}, \ldots, w_{p_n}\rangle.$$

Lemma 4.2.8. *Suppose that p_1, p_2, p_3 are pairwise coprime prime powers, and consider a non-cuspidal quartic point $P \in X_0(p_1p_2p_3)$ mapping to a rational point on $X_0(p_1p_2p_3)^*$. Then P is supported on a $\mathbb{Q}$-curve.*

Proof. Define $W := \langle w_{p_1}, w_{p_2}, w_{p_3}\rangle$. The image of P in $X_0(p_1p_2p_3)^*$ pulls back to the degree 8 divisor $\sum_{w\in W} w(P)$ on $X_0(p_1p_2p_3)$. A subset of these 8 (not necessarily distinct) points is the set of Galois conjugates of P, so each conjugate equals $w(P)$ for some $w \in W$. This means the elliptic curve with j-invariant $j(P)$ is isogenous to all of its conjugates. $\square$

By Proposition 4.2.5 and 4.2.7 and Lemma 4.2.8, we have now reduced our search for quartic points on $X_0(105)$ not corresponding to $\mathbb{Q}$-curves, to a search on five different curves, for the quadratic points not mapping to a rational point on $X_0(105)^*$.

For $X_0(105)/w_5$ we have already verified (see the proof of Proposition 4.2.5) that each of the three quadratic points maps to a rational point on E_7 or E_{21}. The curves $X_0(105)/w_{35}$, $X_0(105)/w_{21}$, $X_0(105)/w_{105}$ and $X_0(105)/w_7$, have genera 3, 5, 5 and 7 respectively and none of them is hyperelliptic. As also their Mordell–Weil groups are finite, their sets of quadratic points must be finite.

Following Section 1.2.4, we would like to determine their Mordell–Weil groups. For the latter three of those curves, however, this is challenging due to their high genus. Instead, we make it easier for ourselves by considering the quotients

$$X_0(105)/\langle w_7, w_{105}\rangle \text{ and } X_0(105)/\langle w_7, w_{21}\rangle.$$

Each quadratic point on $X_0(105)/w_{21}, X_0(105)/w_{105}$ or $X_0(105)/w_7$ maps to a quadratic or rational point on one of these two curves. Both $X_0(105)/\langle w_7, w_{105}\rangle$ and $X_0(105)/\langle w_7, w_{21}\rangle$ are hyperelliptic of genus 3, so they have finitely many quadratic points, except for one

infinite set coming from the double cover of $\mathbb{P}^1$. Both hyperelliptic curves have an automorphism group of order 2, meaning the hyperelliptic involution equals the remaining Atkin–Lehner involution, and the map to $\mathbb{P}^1$ is the map to $X_0(105)^*$.

By Lemma 4.2.8, the quadratic points coming from $\mathbb{P}^1$ correspond to $\mathbb{Q}$-curves, so it suffices to determine the quadratic points on the hyperelliptic curves $X_0(105)/\langle w_7, w_{105}\rangle$ and $X_0(105)/\langle w_7, w_{21}\rangle$ that do not come from $\mathbb{P}^1(\mathbb{Q})$. First, we compute their models:

$$\begin{aligned}
X_0(105)/w_{35} :\ & -x_1^4 + 2x_1^3x_2 - 2x_1^2x_2^2 + x_1x_2^3 + 2x_1^3x_3 - 5x_1^2x_2x_3 \\
& + 4x_1x_2^2x_3 - x_2^3x_3 - 2x_1^2x_3^2 + 4x_1x_2x_3^2 - 3x_2^2x_3^2 + x_1x_3^3 - x_2x_3^3 = 0, \\
X_0(105)/\langle w_7, w_{105}\rangle :\ & y^2 = -28x^7 - 36x^6 + 64x^5 + 21x^4 - 66x^3 + 39x^2 - 10x + 1 \text{ and} \\
X_0(105)/\langle w_7, w_{21}\rangle :\ & y^2 = 20x^7 + 44x^6 - 16x^5 - 47x^4 + 22x^3 + 7x^2 - 6x + 1.
\end{aligned}$$

Proposition 4.2.9. *The Mordell–Weil groups of the above curves are the following:*

$$\begin{aligned}
&J(X_0(105)/w_{35})(\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z} \cdot [(1:0:1) - (0:1:0)] \oplus \mathbb{Z}/8\mathbb{Z} \cdot [(0:0:1) - (0:1:0)], \\
&J(X_0(105)/\langle w_7, w_{105}\rangle)(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \cdot [D_1 - 2\cdot\infty] \oplus \mathbb{Z}/16\mathbb{Z} \cdot [(0,-1) - \infty] \text{ and} \\
&J(X_0(105)/\langle w_7, w_{21}\rangle)(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \cdot [D_2 - 2\cdot\infty] \oplus \mathbb{Z}/32\mathbb{Z} \cdot [(0,-1) - \infty],
\end{aligned}$$

where D_1 and D_2 are the effective degree 2 divisors given by the equations $x^2 - 5/7x + 1/7 = 0$ and $x^2 + x - 1 = 0$ respectively.

Proof. Note that all Mordell–Weil groups have rank 0 because $J_0(105)(\mathbb{Q})$ has rank 0. First we compute the subgroups generated by the differences of rational points. Using the fact [Kat81] that $J(X)(\mathbb{Q})$ embeds in $J(X)(\mathbb{F}_p)$ for each of the curves X and each prime $p > 2$ of good reduction for X, we then reduce the possibilities. The primes 11, 17 and 79 (for $X_0(105)/\langle w_7, w_{105}\rangle$) and 13, 31 and 43 (for $X_0(105)/\langle w_7, w_{21}\rangle$) tell us that the only possible Mordell–Weil groups are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/16\mathbb{Z}$ for $X_0(105)/\langle w_7, w_{105}\rangle$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$ and $\mathbb{Z}/32\mathbb{Z}$ for $X_0(105)/\langle w_7, w_{21}\rangle$. In both cases it thus suffices to compute the 2-torsion subgroup, which is easy for hyperelliptic curves. For odd-degree hyperelliptic curves, this is available in `Magma`.

Next, for $X_0(105)/w_{35}$, we find that the subgroup of its Mordell–Weil group generated by the four rational points (the images of the cusps of $X_0(105)$) is isomorphic to $H := \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Computing Mordell–Weil groups over $\mathbb{F}_p$ for $p \in \{11, 29, 107\}$, we limit the possiblities for $J(X_0(105)/w_{35})(\mathbb{Q})$ to

$$H,\ \ \mathbb{Z}/2\mathbb{Z} \times H \text{ and } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times H.$$

So here, too, it suffices to compute the 2-torsion. This curve is not hyperelliptic, but it is a plane quartic. For plane quartics, Bruin, Poonen and Stoll [BPS16, Section 12] found an algorithm for computing the Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\overline{\mathbb{Q}}} J[2]$ by first computing the bitangents. This was used by Özman and Siksek [OS19, Section 5.5] to compute $J_0(45)[2](\mathbb{Q})$. The implementation used by Özman and Siksek for computing these bitangents (using the `EliminationIdeal` function in `Magma`) was too time-expensive

for our curve. Instead, we will use the Euclidean algorithm. We work on the affine chart $x_2 = 1$. We substitute a generic line $x_3 = -\beta x_1 - \gamma$ into the quartic equation, giving us a degree 4 polynomial $p_{\beta,\gamma}(x_1) \in \mathbb{Q}[\beta,\gamma][x_1]$. The values (β,γ) for which $p_{\beta,\gamma}(x_1)$ is a square, correspond to bitangents. When $p_{\beta,\gamma}(x_1)$ is a square, we have $\deg(\gcd(p_{\beta,\gamma}, p'_{\beta,\gamma})) \geq 2$, so we can use the Euclidean algorithm to find a degree 1 polynomial $f \in \mathbb{Q}[\beta,\gamma][x_1]$ that must vanish identically in order to have $\deg(\gcd(p_{\beta,\gamma}, p'_{\beta,\gamma})) \geq 2$. The equations in β and γ obtained by setting the coefficients of f equal to zero, yield a 0-dimensional scheme of which the finitely many $\overline{\mathbb{Q}}$-points are swiftly found. We then check which of those pairs (β,γ) indeed correspond to bitangents. This yields 27 of the 28 bitangents; the final bitangent line $x_1 = x_2$ does not have non-zero coefficient for x_3. The field of definition of the bitangents is $K = \mathbb{Q}(\sqrt{5}, \sqrt{-3}, \sqrt{-7})$, so in particular $K = \mathbb{Q}(J[2])$.

We then use the implementation of Özman and Siksek [OS19] to compute the Galois representation. We conclude that the 2-torsion is $J(X_0(105)/w_{35})(\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

We call a quadratic point on a hyperelliptic curve *isolated* when it does not map to a rational point on $\mathbb{P}^1$.

Proposition 4.2.10. *(i) The curve $X_0(105)/w_5$ has three pairs of quadratic points, each of which maps to a rational point on $X_0(105)^*$.*

(ii) The curve $X_0(105)/w_{35}$ has two pairs of quadratic points, each of which maps to a rational point on $X_0(105)^*$.

(iii) Each quadratic point on $X_0(105)/w_7$ maps to a rational point on $X_0(105)^*$.

(iv) Each quadratic point on $X_0(105)/w_{105}$ maps to a rational point on $X_0(105)^*$.

(v) The curve $X_0(105)/w_{21}$ has exactly two pairs of quadratic points that do not map to a rational point on $X_0(105)^*$. They are defined over $\mathbb{Q}(\sqrt{5})$ and their inverse images in $X_0(105)$ are quartic points with quadratic j-invariants $632000 \pm 282880\sqrt{5}$.

Remark 4.2.11. These two quartic points on $X_0(105)$ and their conjugates yield 8 ramification points for $X_0(105) \to X_0(105)/w_{21}$, in agreement with the Riemann–Hurwitz formula.

Proof. For part (i) we refer to the proof of Proposition 4.2.5. Given the Mordell–Weil groups, we now compute the isolated quadratic points on $X_0(105)/w_{35}$, $X_0(105)/\langle w_7, w_{21}\rangle$ and $X_0(105)/\langle w_7, w_{105}\rangle$ using Lemma 1.2.4, again by computing the 1-dimensional Riemann–Roch spaces. For the two hyperelliptic curves, we exclude the zero class in the Mordell–Weil group, which corresponds to the infinitely many quadratic points coming from $\mathbb{P}^1 = X_0(105)^*$ by Corollary 1.2.5. We then pull back those quadratic points on the hyperelliptic curves to $X_0(105)/w_7$, $X_0(105)/w_{105}$ and $X_0(105)/w_{21}$, and check which have quadratic inverse images.

Only on $X_0(105)/w_{21}$, this results in two pairs of quadratic points. Since $X_0(105)$ has genus 13, it is not feasible to pull back these degree 2 divisors to $X_0(105)$, and challenging to compute directly the j-invariant morphism on $X_0(105)$. Instead, we compute

the Atkin–Lehner involution w_5 on $X_0(105)/w_{21}$, and check that both quadratic points P satisfy $w_5(P) = P$. Let Q be a quartic point on $X_0(105)$ mapping to one of these quadratic points. Then either $w_5(Q) = Q$ or $w_{105}(Q) = w_5 w_{21}(Q) = Q$.

We first suppose that $w_{105}(Q) = Q$. We compute the matrix W defining the action of w_{105} on the cusp forms defining our canonical model in $\mathbb{P}^{12}_{x_1,\ldots,x_{13}}$ for $X_0(105)$. We find that $\mathrm{Ker}(W - \mathrm{I})$ is 5-dimensional. From its basis, we find the equation $x_1 - 2x_3 - 2x_4 - x_5 = 0$ satisfied by the w_{105}-fixed points of $X_0(105)$, along with 4 other equations. This particular equation is defined in terms of the first 5 coordinates, which are the coordinates corresponding to the cusp forms fixed by w_5. So the image of Q on $X_0(105)/w_5$ must satisfy $x_1 - 2x_3 - 2x_4 - x_5 = 0$. This equation defines a divisor on $X_0(105)/w_5$ that decomposes as a sum of two irreducible degree 4 divisors. Using Lemma 4.2.2, we find that these come from degree 8 points on $X_0(105)$.

We conclude that we must have $w_5(Q) = Q$. Then also the image R of Q on $X_0(5)$ must satisfy $w_5(R) = R$. We compute $X_0(5)$ as well as the action of w_5 on $X_0(5)$. The points on $X_0(5)$ fixed by w_5 are quadratic and have the claimed j-invariant. □

Finally, Propositions 4.2.5, 4.2.7 and 4.2.10 together with Lemma 4.2.8 prove Theorem 4.2.1. Recall that the quartic points on $X_0(105)$ with quadratic j-invariants correspond to modular elliptic curves and can therefore safely be ignored.

4.3 $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$

The second modular curve we need to look at is $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$.

Theorem 4.3.1. *Let E be an elliptic curve with quartic j-invariant that occurs as a quartic point on $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$. Then E is a $\mathbb{Q}$-curve, and in particular E is modular.*

In order to do computations with this curve, we make use of the isomorphism

$$X(\mathrm{b}p^2, *)/w_{p^2} \longrightarrow X(\mathrm{s}p, *),$$

where p is prime and $*$ denotes any prime-to-p level structure, as observed in Example 1.1.12. Pulled back to the upper half plane, this isomorphism is just $\tau \mapsto p\tau$. This yields $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7}) \simeq X_0(315)/w_9$, allowing us to study this curve using modular forms on $\Gamma_0(315)$. We find that $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$ has genus 21. Moreover, evaluating $L(f, 1)$ for the eigenforms in the $+1$-eigenspace for w_9 of $S_2(\Gamma_0(315))$ suggests (but does not prove) that the Mordell–Weil groups of several components of $J(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$ have positive rank, c.f. Section 1.2.3. The genus of $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$ is too large to do explicit computations, so one hopes to find a quotient (such as $X_0(105)/w_5$ in the previous section) that is more amenable to computations. We found each quotient to be either too complicated to study computationally (high genus with positive rank Mordell–Weil group) or too simple to distinguish between quartic points (genus less than 4).

We resolve this issue by combining information from two small quotients: $X_0(35)$ and $X(\mathrm{s3}, \mathrm{b7}) \simeq X_0(63)/w_9$. Both quotients are hyperelliptic of genus 3 and, conveniently,

the Mordell–Weil groups of their Jacobians are finite. The small genus means that both curves have infinitely many quartic points.

$$\begin{tikzcd}
& X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7}) \arrow[dl] \arrow[dr] & \\
X(\mathrm{s3}, \mathrm{b7}) \arrow[dr] & & X_0(35) \arrow[dl] \\
& X_0(7) &
\end{tikzcd}$$

Note that $X_0(7)$ has genus 0. We compute models for the curves and maps in the lower half of the diagram via modular forms. The models for $X_0(35)$ and $X_0(7)$, as well as the map between them, can be computed in `Magma` using the Small Modular Curves package. The map from $X_0(63)/w_9$ to $X_0(7)$ is not implemented, but we computed it using the method described in Section 1.2.2. We display here only the curves.

$$\begin{aligned}
X_0(35) &: y^2 = x^8 - 4x^7 - 6x^6 - 4x^5 - 9x^4 + 4x^3 - 6x^2 + 4x + 1, \\
X(\mathrm{s3}, \mathrm{b7}) &: y^2 = x^8 + 6x^7 + 23x^6 + 36x^5 + 57x^4 + 36x^3 + 23x^2 + 6x + 1, \\
X_0(7) &= \mathbb{P}^1.
\end{aligned}$$

On these hyperelliptic curves, we write $\infty^+ = (1 : 1 : 0)$ and $\infty^- = (1 : -1 : 0)$ (in weighted projective space). The cusps of $X_0(35)$ are ∞^+, ∞^-, $(0, 1)$ and $(0, -1)$, and the cusps of $X(\mathrm{s3}, \mathrm{b7})$ are (also) ∞^+, ∞^-, $(0, 1)$ and $(0, -1)$.

As observed e.g. in [FLHS15, Remark in Section 5.3] (see also Section 1.1.5), there is an exceptional inclusion (up to conjugation) $C_{\mathrm{ns}}^+(3) \subset C_{\mathrm{s}}^+(3)$, and this inclusion of subgroups has index 2 after intersecting with $\mathrm{SL}_2(\mathbb{F}_3)$. This means that there is a morphism of degree 2

$$X(\mathrm{s3}, \mathrm{b7}) \to X(\mathrm{ns3}, \mathrm{b7}).$$

Each degree 2 morphism of curves is the quotient by an involution. We call this involution $\phi_3 : X(\mathrm{s3}, \mathrm{b7}) \to X(\mathrm{s3}, \mathrm{b7})$.

Lemma 4.3.2. *(i) The hyperelliptic involution on $X_0(35)$ is w_{35}.*

(ii) The hyperelliptic involution on $X(\mathrm{s3}, \mathrm{b7})$ is $\phi_3 w_7$.

Proof. Part (i) is due to Ogg [Ogg74]. For part (ii), we can check in `Magma` that $X(\mathrm{s3}, \mathrm{b7})$ has an automorphism group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We then note that Le Hung [LH14, Remark 5.2] showed that $X(\mathrm{ns3}, \mathrm{b7})$ has genus 2. We can also check that the subspace of $S_2(\Gamma_0(63))$ fixed by w_7 and w_9 is 1-dimensional, or alternatively use the `ModularCurveQuotient` function in `Magma` to check that $X_0(63)/\langle w_9, w_7\rangle$ (which is isomorphic to $X(\mathrm{s3}, \mathrm{b7})/w_7$) has genus 1. This shows that $w_7 \neq \phi_3$, and thus $\mathrm{Aut}(X(\mathrm{s3}, \mathrm{b7})) = \langle \phi_3, w_7\rangle$. It also shows that neither w_7 nor ϕ_3 is the hyperelliptic involution, leaving $\phi_3 w_7$ as the only remaining candidate. □

It is possible to compute w_7 and ϕ_3 on $X(\mathrm{s3}, \mathrm{b7})$ explicitly using the methods of

Chapter 2 and verify by computation that $w_3\phi_7$ is the hyperelliptic involution, but we have not done this.

Next, we need to compute Mordell–Weil groups.

Proposition 4.3.3. *The Mordell–Weil groups of $J_0(35)$ and $J(\mathrm{s3}, \mathrm{b7})$ are*

$$J_0(35)(\mathbb{Q}) = \mathbb{Z}/24\mathbb{Z} \cdot [\infty^- - \infty^+] \oplus \mathbb{Z}/2\mathbb{Z} \cdot [3 \cdot (0, -1) - 3 \cdot \infty^+]$$

and

$$\begin{aligned} J(\mathrm{s3}, \mathrm{b7})(\mathbb{Q}) = \mathbb{Z}/24\mathbb{Z} &\cdot [2 \cdot \infty^+ + (0, 1) - 3 \cdot \infty^-] \\ \oplus \mathbb{Z}/2\mathbb{Z} &\cdot [-9\infty^+ + (0, 1) + 8 \cdot \infty^-] \end{aligned}$$

Proof. For $X_0(35)$, we use the prime 3 to embed $J_0(35)(\mathbb{Q})$ in $J_0(35)(\mathbb{F}_3) \simeq \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We find that the images of the claimed generators indeed have the right order and generate $J_0(35)(\mathbb{F}_3)$. This agrees with the Mordell–Weil group $J_0(35)(\mathbb{Q})$ found in [FLHS15, Lemma 12.1].

For $X(\mathrm{s3}, \mathrm{b7})$ we embed its Mordell–Weil group in $J(\mathrm{s3}, \mathrm{b7})(\mathbb{F}_5) \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/24\mathbb{Z}$ and $J(\mathrm{s3}, \mathrm{b7})(\mathbb{F}_{11}) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/264\mathbb{Z}$. The group generated by the images of the claimed generators is isomorphic to $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with these generators having orders 24 and 2 respectively, as desired. □

For each of the two hyperelliptic curves, let $\infty = \infty^+ + \infty^-$ denote the (degree 2) divisor at infinity. Also, for each $Y \in \{X(\mathrm{s3}, \mathrm{b7}), X_0(35)\}$, we define the Abel–Jacobi map by

$$\iota_Y : Y^{(4)} \to J(Y), \quad D \mapsto [D - 2 \cdot \infty].$$

Proposition 4.3.4. *For each $Y \in \{X_0(35), X_0(63)/w_9\}$, the Riemann–Roch spaces*

$$L(D + 2 \cdot \infty) \text{ for } D \in J(Y)(\mathbb{Q})$$

are 2-dimensional, except for when $D = 0$, in which case $L(D + 2 \cdot \infty) = L(2 \cdot \infty)$ is 3-dimensional and generated by $1, x, x^2$.

Proof. This is true for any genus 3 hyperelliptic curve. It is clear that $1, x, x^2 \in L(2 \cdot \infty)$ and $\ell(2 \cdot \infty) \leq 3$ by Clifford's theorem, from which we deduce the final statement. The first statement follows from the Riemann–Roch theorem. □

For $Y \in \{X(\mathrm{s3}, \mathrm{b7}), X_0(35)\}$, we define $\pi_Y : X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7}) \to Y$ to be the projection map.

Proposition 4.3.5. *Consider $D \in X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})^{(4)}(\mathbb{Q})$ supported on an elliptic curve E with quartic j-invariant. Suppose the push-forwards $\pi_{Y,*}D$ for $Y \in \{X(\mathrm{s3}, \mathrm{b7}), X_0(35)\}$ both satisfy $[\pi_{Y,*}D - 2 \cdot \infty] = 0 \in J(Y)(\mathbb{Q})$. Then E is a $\mathbb{Q}$-curve.*

Proof. For each $Y \in \{X(\mathrm{s3}, \mathrm{b7}), X_0(35)\}$, our assumption on the push-forward and the previous proposition imply that there is a function f on Y, which is a quadratic function

of x and hence factors via $x : Y \to \mathbb{P}^1$, such that $\pi_{Y,*}D = \mathrm{div}(f) + 2 \cdot \infty$. Writing $f = g \circ x$, we find $\pi_{Y,*}D = x^*(\mathrm{div}(g) + 2 \cdot \infty_{\mathbb{P}^1})$. Now assume that D is generated by a quartic point P, defined over the degree 4 number field K. We assume that P is supported on an elliptic curve E/K. By the above and by Lemma 4.3.2, the images of P in both $X(\mathrm{s3}, \mathrm{b7})/\phi_3 w_7$ and $X_0(35)/w_{35}$ are quadratic, because $\mathrm{div}(g) + 2 \cdot \infty_{\mathbb{P}^1}$ is a divisor of degree 2. Note that ϕ_3 acts only on the 3-level structure and leaves underlying elliptic curves fixed, whereas each Atkin–Lehner involution changes an underlying elliptic curve defined over a field F by an F-isogeny. In particular, the hyperelliptic involution on each Y maps $\pi_Y(P)$ to a conjugate of $\pi_Y(P)$, supported on a conjugate E^Y of E which is K-isogenous to E. Suppose first that $j(E^{X_0(35)}) \neq j(E^{X(\mathrm{s3},\mathrm{b7})})$. Then E is isogenous by a K-isogeny to two distinct Galois conjugates. In particular, these two conjugates of E are also defined over K (hence so must the final conjugate), and K is Galois with Galois group $(\mathbb{Z}/2\mathbb{Z})^2$. Suppose that we have $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\phi_3 w_7$ maps $\pi_{X(\mathrm{s3},\mathrm{b7})}(P)$ to $\pi_{X(\mathrm{s3},\mathrm{b7})}(P)^\sigma$ and w_{35} maps $\pi_{X_0(35)}(P)$ to $\pi_{X_0(35)}(P)^\tau$. Since w_{35} is defined over $\mathbb{Q}$, it maps $\pi_{X_0(35)}(P^\sigma)$ to $w_{35}(\pi_{X_0(35)}(P))^\sigma = P^{\tau\sigma}$, supported on $E^{\tau\sigma}$. This, finally, defines an isogeny between E^σ and $E^{\tau\sigma}$, proving that E is isogenous to all of its conjugates and is therefore a $\mathbb{Q}$-curve.

If $j(E^{X_0(35)}) = j(E^{X(\mathrm{s3},\mathrm{b7})})$ then $\phi_3 w_7(\pi_{X(\mathrm{s3},\mathrm{b7})}(P))$ and $w_{35}(\pi_{X_0(35)}(P))$ are supported on the same elliptic curve, so $Q = w_7(P)$ satisfies $j(Q) = j(w_5(Q))$. Thus Q gives rise to a quartic point R on $X_0(5)$ such that R and $w_5(R)$ have the same j-invariant. We can explicitly compute the j-invariant j and Atkin–Lehner involution w_5 on $X_0(5) \simeq \mathbb{P}^1$ and find the zeros of $j - j \circ w_5$. All of them are defined over quadratic fields. $\square$

Again consider $Y \in \{X(\mathrm{s3}, \mathrm{b7}), X_0(35)\}$. Note that an r-dimensional Riemann–Roch space yields an $(r-1)$-dimensional linear system because the divisors depend only on the functions up to scaling.

Now consider a pair $(D_1, D_2) \in J_0(35)(\mathbb{Q}) \times J(\mathrm{s3}, \mathrm{b7})(\mathbb{Q})$. We compute explicit bases for the Riemann–Roch spaces of $D_1 + 2 \cdot \infty$ and $D_2 + 2 \cdot \infty$; let us call these $f_0, \ldots, f_n$ and $g_0, \ldots, g_m$ respectively. The effective degree 4 divisors mapping to D_1 resp. D_2 under ι can then be parametrised as follows, see Lemma 1.2.4:

$$\iota_{X_0(35)}^{-1}(D_1) = \{D_1 + 2 \cdot \infty + \mathrm{div}(t_0 f_0 + \ldots t_n f_n) \mid (t_0 : \ldots : t_n) \in \mathbb{P}^n(\mathbb{Q})\} \text{ and}$$
$$\iota_{X(\mathrm{s3},\mathrm{b7})}^{-1}(D_2) = \{D_2 + 2 \cdot \infty + \mathrm{div}(s_0 g_0 + \ldots s_m g_m) \mid (s_0 : \ldots : s_m) \in \mathbb{P}^m(\mathbb{Q})\}.$$

By the Riemann–Roch theorem, when $D_1 \neq 0$ and $D_2 \neq 0$, we have $n = m = 1$. This agrees with our intuition because $1 = \dim Y^{(4)} - \dim J(Y)$. When $D_1 = 0$ and $D_2 \neq 0$ (or the other way around), we have $n = 2$ and $m = 1$ (resp. $m = 2$ and $n = 1$). Thanks to Proposition 4.3.5, we do not need to worry about the final possibility $D_1 = D_2 = 0$.

We now base-change the curves to $\mathbb{Q}(t_0, \ldots, t_n)$ and $\mathbb{Q}(s_0, \ldots, s_m)$ respectively. Write $\mathbf{t} = (t_0, \ldots, t_n)$ and $\mathbf{s} = (s_0, \ldots, s_m)$. We consider the divisors

$$D_1(\mathbf{t}) := D_1 + 2 \cdot \infty + \mathrm{div}(t_0 f_0 + \ldots + t_n f_n) \text{ and}$$
$$D_2(\mathbf{s}) := D_2 + 2 \cdot \infty + \mathrm{div}(s_0 g_0 + \ldots + s_m g_m).$$

For each $Y \in \{X_0(35), X(\mathrm{s3}, \mathrm{b7})\}$, let α_Y be the map $Y \to X_0(7)$. Next, we define

$$S_{D_1,D_2} \subset \mathbb{P}^n \times \mathbb{P}^m$$

to be the subscheme determined as those $\mathbf{t} \in \mathbb{P}^n$ and $\mathbf{s} \in \mathbb{P}^m$ such that

$$(\alpha_{X_0(35)})_* D_1(\mathbf{t}) = (\alpha_{X(\mathrm{s3},\mathrm{b7})})_* D_2(\mathbf{s}).$$

Proposition 4.3.6. *There are exactly two pairs (P, Q) of $\mathbb{Q}$-rational degree 4 divisors P on $X_0(35)$ and Q on $X(\mathrm{s3}, \mathrm{b7})$ with irreducible pushforward to $X_0(7)$, such that $P = D_1(\mathbf{t})$ and $Q = D_2(\mathbf{s})$ for some $(D_1, D_2) \in J(X_0(35))(\mathbb{Q}) \times J(X(\mathrm{s3}, \mathrm{b7}))(\mathbb{Q}) \setminus \{(0, 0)\}$ and $(\mathbf{t}, \mathbf{s}) \in S_{D_1,D_2}(\mathbb{Q})$. Each of those pairs has quadratic j-invariant $632000 \pm 282880\sqrt{5}$.*

Remark 4.3.7. If this j-invariant looks familiar, that is because we found the same j-invariant for the quartic points on $X_0(105)$ determined in Proposition 4.2.10 (v). The corresponding elliptic curve has complex multiplication by $\mathbb{Z}[\sqrt{-5}]$. It determines a point on $X_0(105)$ because $\sqrt{-5}$, $1 + \sqrt{-5}$ and $3 + \sqrt{-5}$ define isogenies of degrees 5, 6 and 14 respectively. As for the point R on $X_0(37)$ in Section 3.5, this quartic point is defined over $\mathbb{Q}(\sqrt{5}, i)$ because that is the Hilbert class field of $\mathbb{Q}(\sqrt{5})$.

Proof. We enumerate the possibilities for (D_1, D_2) using Proposition 4.3.3. For each pair (D_1, D_2), we need to compute $S_{D_1,D_2}(\mathbb{Q})$. To that end, we compute the push-forward of $D_1(\mathbf{t})$ over the field $\mathbb{Q}(\mathbf{t})$. Because $X_0(7) = \mathbb{P}^1_{u,v}$, we view $X_0(35) \to X_0(7)$ as an element of the function field of $X_0(35)$. At each irreducible component of $D_1(\mathbf{t})$ over $\mathbb{Q}(\mathbf{t})$, we evaluate this function, and we determine the minimal polynomial (over $\mathbb{Q}(\mathbf{t})$) of the result. This gives us (after homogenising) the monic degree 4 equation

$$p_{\mathbf{t}}(u, v) := u^4 + a_3(\mathbf{t})u^3v + a_2(\mathbf{t})u^2v^2 + a_1(\mathbf{t})uv^3 + a_0(\mathbf{t})v^4 = 0,$$

defining $(\alpha_{X_0(35)})_* D_1(\mathbf{t})$, with coefficients in $\mathbb{Q}(\mathbf{t})$. We do the same for $D_2(\mathbf{s})$, which yields a monic degree 4 equation $q_{\mathbf{s}}(u, v) := u^4 + b_3(\mathbf{s})u^3v + \ldots + b_0(\mathbf{s})v^4 = 0$. Then we equate each of the four coefficients of $p_{\mathbf{t}}$ and $q_{\mathbf{s}}$. We note that each coefficient is a *rational* function in $\mathbf{t}$, resp. $\mathbf{s}$. So when equating coefficients we need to multiply by denominators. This yields 4 equations in $t_0, \ldots, t_n$ and $s_0, \ldots, s_m$ defining a scheme T_{D_1,D_2} such that $S_{D_1,D_2} \subset T_{D_1,D_2} \subset \mathbb{P}^n \times \mathbb{P}^m$. Indeed, by construction $S_{D_1,D_2} \subset T_{D_1,D_2}$. However, if $\mathbf{t}$ is a zero of the denominator of $a_i(\mathbf{t})$ for some i, and similarly $\mathbf{s}$ is a zero of the denominator of $b_i(\mathbf{s})$, then the equation $a_i(\mathbf{t}) = b_i(\mathbf{s})$ is automatically satisfied, regardless of whether $D_1(\mathbf{t})$ and $D_2(\mathbf{s})$ have the same pushforward to $X_0(7)$. This can lead to extra irreducible components on T_{D_1,D_2} that do not occur on S_{D_1,D_2}.

Next, we decompose T_{D_1,D_2} into irreducible components. We find that each component is at most 1-dimensional. In every case where a component is 1-dimensional, we find that indeed the denominator d of one of the $a_i(\mathbf{t})$ or $b_i(\mathbf{s})$ vanishes identically on that component. This means that $(\alpha_{X_0(35)})_* D_1(\mathbf{t})$ or $(\alpha_{X(\mathrm{s3},\mathrm{b7})})_* D_2(\mathbf{s})$ is reducible, because $d \cdot p_{\mathbf{t}}$, resp. $d \cdot q_{\mathbf{s}}$, is divisible by v. Reducible on $X_0(7)$ means that the j-invariant takes rational, quadratic or cubic values, and we can thus ignore such components.

On each 0-dimensional component of T_{D_1,D_2}, we determine all rational points explicitly. Again we remove points $(\mathbf{s},\mathbf{t})$ where a denominator of a coefficient vanishes, and for the same reason those where $a_0(\mathbf{t})$ or $b_0(\mathbf{s})$ vanishes. From the values of $\mathbf{s}$ and $\mathbf{t}$ we find two explicit pairs of divisors. With the `SmallModularCurves` package in `Magma`, we compute the j-invariant function on $X_0(35)$ and evaluate it at the two points. $\square$

Finally, Propositions 4.3.5 and 4.3.6 together prove Theorem 4.3.1.

4.4 $X(\mathrm{b5},\mathrm{ns7})$

4.4.1 Overview

Next, we turn our attention to the curve $X(\mathrm{b5},\mathrm{ns7})$. We first note that there are morphisms $X(\mathrm{b3},\mathrm{b5},\mathrm{e7}) \to X(\mathrm{b5},\mathrm{e7})$ and $X(\mathrm{s3},\mathrm{b5},\mathrm{e7}) \to X(\mathrm{b5},\mathrm{e7})$ forgetting the level 3 structure. We studied the curve $X(\mathrm{b5},\mathrm{e7})$ in Section 2.4. Recall that it admits an Atkin–Lehner involution w_5 and an involution ϕ_7, such that $X(\mathrm{b5},\mathrm{ns7}) = X(\mathrm{b5},\mathrm{e7})/\phi_7$. These involutions commute, giving rise to a commuting diagram of degree 2 maps between modular curves:

$$\begin{tikzcd}
 & X(\mathrm{b5},\mathrm{e7}) \arrow[dl] \arrow[d] \arrow[dr] & \\
X(\mathrm{b5},\mathrm{ns7}) \arrow[dr, "\rho"] & X(\mathrm{b5},\mathrm{e7})/\phi_7 w_5 \arrow[d] & X(\mathrm{b5},\mathrm{e7})/w_5 \arrow[dl] \\
 & X(\mathrm{b5},\mathrm{ns7})/w_5 &
\end{tikzcd} \cdot$$

Now each quartic point on $X(\mathrm{b3},\mathrm{b5},\mathrm{e7})$ or $X(\mathrm{s3},\mathrm{b5},\mathrm{e7})$ maps to a quartic point on $X(\mathrm{b5},\mathrm{ns7})$, so it would suffice to determine all quartic points on this curve instead.

The curve $X(\mathrm{b5},\mathrm{ns7})$ was studied by Le Hung [LH14], and later by Derickx, Najman and Siksek [DNS20], who found a planar model for $X(\mathrm{b5},\mathrm{ns7})$ in $\mathbb{P}^2_{u,v,w}$ given by

$$\begin{aligned} X(\mathrm{b5},\mathrm{ns7})\colon\ & 5u^6 - 50u^5v + 206u^4v^2 - 408u^3v^3 + 321u^2v^4 + 10uv^5 - 100v^6 + 9u^4w^2 \\ & - 60u^3vw^2 + 80u^2v^2w^2 + 48uv^3w^2 + 15v^4w^2 + 3u^2w^4 - 10uvw^4 + 6v^2w^4 - w^6 = 0. \end{aligned}$$

Here the Atkin–Lehner involution w_5 maps $(u:v:w) \mapsto (u:v:-w)$. The curve has genus 6 and its Jacobian's Mordell–Weil group has rank 2. Its quotient $C := X(\mathrm{b5},\mathrm{ns7})/w_5$ is hyperelliptic of genus 2 with Jacobian also of Mordell–Weil rank 2. Recall from Theorem 2.4.1 that it has a model given by

$$C:\ y^2 = x^6 + 2x^5 + 7x^4 - 4x^3 + 3x^2 - 10x + 5. \tag{4.1}$$

Given the genus and the rank of $X(\mathrm{b5},\mathrm{ns7})$, one might suspect $X(\mathrm{b5},\mathrm{ns7})^{(4)}(\mathbb{Q})$ to be finite; the degree 2 map $\rho\colon X(\mathrm{b5},\mathrm{ns7}) \to C$ disproves this, however: $C^{(2)}(\mathbb{Q})$ is infinite. The best we can hope for, is the following.

Theorem 4.4.1. *For each $i \in \{0, \dots, 4\}$, let $\mathcal{P}_i$ be the effective divisor that is the sum of P_i and its Galois conjugates, where $P_0, \dots, P_4$ are defined in Table 4.1. The set $X(\mathrm{b5}, \mathrm{ns7})^{(4)}(\mathbb{Q})$ equals*

$$\{\mathcal{P}_1, w_5^*\mathcal{P}_1, \dots, \mathcal{P}_4, w_5^*\mathcal{P}_4\} \cup (\mathcal{P}_0 + \rho^* C(\mathbb{Q})) \cup (w_5^*\mathcal{P}_0 + \rho^* C(\mathbb{Q})) \cup \rho^* C^{(2)}(\mathbb{Q}).$$

None of the fields of definition of $P_1, \dots, P_4$ is totally real.

Remark 4.4.2. Note that the elliptic curves corresponding to $P_2, w_5(P_2), P_3, w_5(P_3)$ are modular because they have complex multiplication. On $X_0(105)$ and $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$, we showed that all quartic points correspond to modular elliptic curves, but here we do need to use the totally real condition to exclude P_1, $w_5(P_1)$, P_4 and $w_5(P_4)$.

Name	minpol(θ)	Coordinates	j-invariant	CM
P_0	$x^2 - 5$	$(\theta - 5 : \theta - 3 : 2)$	1728	-4
$w_5(P_0)$	$x^2 - 5$	$(-\theta + 5 : -\theta + 3 : 2)$	$-98457455093 76\theta + 22015749613248$	-100
P_1	$x^4+x^3+2x^2-1$	$(\theta + 1 : \theta : 1)$	$-8795637219 11\theta^3 - 2256564598 26\theta^2 - 15913642742 27\theta + 1183091832488$	NO
$w_5(P_1)$	$x^4+x^3+2x^2-1$	$(\theta + 1 : \theta : -1)$	$-323691852 33\theta^3 - 1117079335 54\theta^2 - 175433680 31\theta + 35398801591$	NO
P_2	$x^4 - 5$	$(11\theta^3 + 24\theta^2 - 35\theta - 82 : (7\theta^3 + 4\theta^2 - 11\theta - 24) : -62)$	287496	-16
$w_5(P_2)$	$x^4 - 5$	$(11\theta^3 + 24\theta^2 - 35\theta - 82 : (7\theta^3+4\theta^2-11\theta-24) : 62)$	$-1449571301391224380091546 88\theta^3 + 2167614678828625929715921 92\theta^2 - 3241339968143613185790171 84\theta + 4846933770887181794613460 56$	-400
P_3	$x^4 - x^3 + x^2 + 4x - 4$	$(3\theta^3 - 3\theta^2 + 5\theta + 10 : \theta^3 - \theta^2 + 3\theta + 2) : -4)$	-32768	-11
$w_5(P_3)$	$x^4 - x^3 + x^2 + 4x - 4$	$(3\theta^3 - 3\theta^2 + 5\theta + 10 : \theta^3 - \theta^2 + 3\theta + 2) : 4)$	$-7084562494756740890624\theta^3 + 1098708046310747471872\theta^2 - 615624737982621627187 2\theta - 3353975688810419427737 6$	-275
P_4	$x^4 - x^3 + 2x^2 - x - 2$	$(2\theta^2 - 2\theta : \theta^3 - \theta^2 + 2\theta - 3 : -2)$	$(3826190688474785295\theta^3 + 7498461721986733375\theta^2 + 8549180309143366704\theta + 6398434116827442268)/128$	NO
$w_5(P_4)$	$x^4 - x^3 + 2x^2 - x - 2$	$(2\theta^2 - 2\theta : \theta^3 - \theta^2 + 2\theta - 3 : 2)$	$(-2489746184923633393\theta^3 + 4129898311646775999\theta^2 - 7699447555542820000\theta + 756153558218027868)/34359738368$	NO

Table 4.1: All isolated quadratic and all isolated quartic points on $X(\mathrm{b5}, \mathrm{ns7})$, up to Galois conjugacy.

Corollary 4.4.3. *Each quartic point on $X(\mathrm{b5}, \mathrm{e7})$ whose image in $X(\mathrm{b5}, \mathrm{ns7})$ is not a Galois conjugate of P_1, $w_5(P_1)$,…,P_4 or $w_5(P_4)$ maps to a quadratic point on one of $X(\mathrm{b5}, \mathrm{ns7})$, $X(\mathrm{b5}, \mathrm{e7})/w_5$, $X(\mathrm{b5}, \mathrm{e7})/\phi_7 w_5$.*

Proof. Apply Lemma 4.2.6 to $X(\mathrm{b5}, \mathrm{e7})$ with involutions w_5 and ϕ_7, and use Theorem 4.4.1. □

We note that each quadratic point on $X(\mathrm{b5}, \mathrm{ns7})$ has quadratic j-invariant, and thus corresponds to a modular elliptic curve. So Theorem 4.4.1 reduces the study of

the quartic points on $X(\mathrm{b5}, \mathrm{e7})$ with totally real quartic j-invariants to the study of the quadratic points on the curves $X(\mathrm{b5}, \mathrm{e7})/w_5$ and $X(\mathrm{b5}, \mathrm{e7})/\phi_7 w_5$. These curves (of genera 5 and 8 respectively) are studied in Section 4.5. In the next sections, we use the new Chabauty method for symmetric powers developed in Chapter 3 in combination with the Mordell–Weil sieve introduced in Section 1.2.5 to prove Theorem 4.4.1. More precisely, in Sections 4.4.3 and 4.4.4, we determine the input of the sieve, after which we prove Theorem 4.4.1 in Section 4.4.5.

4.4.2 Quadratic points

First, for completeness we mention the quadratic points on $X(\mathrm{b5}, \mathrm{ns7})$. Derickx, Najman and Siksek [DNS20] showed that $X(\mathrm{b5}, \mathrm{ns7})^{(3)}(\mathbb{Q}) = \{c_0, c_\infty\}$, where c_0 and c_∞ are the Galois orbits of the cusps. In coordinates, c_0 is the effective degree 3 divisor generated by

$$(4\eta^2 - 21\eta - 7 : \eta^2 - 7\eta : -14), \quad \eta = \zeta_7 + \zeta_7^{-1} \in \mathbb{Q}(\zeta_7)^+$$

and $c_\infty = w_5^* c_0$. In particular, $X(\mathrm{b5}, \mathrm{ns7})$ has no rational points. We find two isolated pairs of quadratic points P_0 and $w_5(P_0)$; let $\mathcal{P}_0$ be the sum of P_0 and its Galois conjugate. Each $\mathcal{P} \in X(\mathrm{b5}, \mathrm{ns7})^{(2)}(\mathbb{Q})$ satisfies $\mathcal{P} + \mathcal{P}_0 \in X(\mathrm{b5}, \mathrm{ns7})^{(4)}(\mathbb{Q})$, so it follows from Theorem 4.4.1 that $\mathcal{P} \in \{\mathcal{P}_0, w_5^* \mathcal{P}_0\} \cup \rho^* C(\mathbb{Q})$. We conclude (c.f. Remark 3.3.1) that

$$X(\mathrm{b5}, \mathrm{ns7})^{(2)}(\mathbb{Q}) = \{\mathcal{P}_0, w_5^* \mathcal{P}_0\} \cup \rho^* C(\mathbb{Q}).$$

Remark 4.4.4. In [FLHS15], Freitas, Le Hung and Siksek proved modularity of all elliptic curves over real quadratic fields by studying the quadratic points on seven modular curves. Now, thanks to the recent theorems of Thorne [Tho16] and Kalyanswamy [Kal18], it suffices by Theorem 4.1.2 to show that all real quadratic points on $X(\mathrm{b5}, \mathrm{ns7})$ and $X_0(35)$ correspond to modular elliptic curves, and separately prove that elliptic curves over $\mathbb{Q}(\sqrt{5})$ are modular. The latter two tasks are covered in [FLHS15], while we have just shown all quadratic points P on $X(\mathrm{b5}, \mathrm{ns7})$ to be modular: either P has CM, or P maps to a rational point on C and is therefore a $\mathbb{Q}$-curve (it satisfies $P^\sigma = w_5(P)$). This provides a shorter proof for modularity of elliptic curves over real quadratic fields.

Finally, we list the found rational points on C, together with the j-invariants of their inverse images on $X(\mathrm{b5}, \mathrm{ns7})$. These inverse images are in each case defined over a quadratic field (i.e. not rational), so the Galois orbit of this j-invariant is independent of the choice of inverse image.

Remark 4.4.5. The curve C has genus 2 and $J(C)(\mathbb{Q})$ has rank 2, making it infeasible to prove that $C(\mathbb{Q}) = \{Q_1, \ldots, Q_6\}$ using abelian Chabauty. A quadratic Chabauty method, however, might be successful, c.f. [Sik17], [BBB+] and [BDS+21].

4.4.3 The Mordell–Weil group

We first note that we can indeed apply the Chabauty method developed in Chapter 3. As $\mathrm{rk}(J(\mathrm{b5}, \mathrm{ns7})(\mathbb{Q})) = \mathrm{rk}(J(C)(\mathbb{Q})) = 2$ (see [DNS20]), we can use Proposition 3.3.7

Name	Coordinates	j-invariant of inverse image in $X(\mathrm{b5}, \mathrm{ns7})$	CM
Q_1	∞^-	287496	-16
Q_2	∞^+	$(85995\sqrt{5} - 191025)/2$	-15
Q_3	$(1, -2)$	-32768	-11
Q_4	$(1, 2)$	$18406806674317737984 0\sqrt{5} - 41158870972471296 0000$	-235
Q_5	$(1/2, -7/2)$	1728	-4
Q_6	$(1/2, 7/2)$	$(-16554983445\sqrt{5} + 37018076625)/2$	-60

Table 4.2: The found rational points on $X(\mathrm{b5}, \mathrm{ns7})/w_5$.

to explicitly verify the rank condition of Theorem 3.2.6 for $X = X(\mathrm{b5}, \mathrm{ns7})$ and $C = X/w_5$. (In particular, we obtain vanishing differentials with trace zero from the kernel of $1 + w_5^* \colon H^0(X, \Omega) \to H^0(X, \Omega)$.) We shall use this information as input for the Mordell–Weil sieve.

Before applying the sieve, however, we need knowledge of the Mordell–Weil group and a list of known points. In [DNS20], it was shown that $J(\mathrm{b5}, \mathrm{ns7})(\mathbb{Q}) \simeq \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, where the torsion subgroup $\mathbb{Z}/7\mathbb{Z}$ is generated by the difference $D_{\mathrm{tor}} := c_0 - c_\infty$ of the two degree 3 Galois orbits of cusps. Since $J(C)(\mathbb{Q})$ is hyperelliptic of genus 2, we can use an algorithm of Stoll [Sto02] to compute generators

$$d_1 := [(-1, -2) - \infty^-] \text{ and } d_2 := [(-1/2, -7/2) - \infty^-]$$

for $J(C)(\mathbb{Q}) \simeq \mathbb{Z}^2$. Pulling these back under ρ, we obtain $D_1 = \rho^* d_1$ and $D_2 = \rho^* d_2$. Finally, by Proposition 1.2.2, the group

$$G = \mathbb{Z}/7\mathbb{Z} \cdot D_{\mathrm{tor}} \oplus \mathbb{Z} \cdot D_1 \oplus \mathbb{Z} \cdot D_2$$

satisfies $2 \cdot J(\mathrm{b5}, \mathrm{ns7})(\mathbb{Q}) \subset G$. We find that the reductions of D_2 and $D_1 + D_2$ mod 19 are not doubles in $J(\mathrm{b5}, \mathrm{ns7})(\mathbb{F}_{19})$, so D_2 and $D_1 + D_2$ also cannot be doubles.

We define the maps $\iota : X(\mathrm{b5}, \mathrm{ns7})^{(4)}(\mathbb{Q}) \to J(\mathrm{b5}, \mathrm{ns7})(\mathbb{Q})$ given by $\iota(D) = 2 \cdot [D - D_0]$, where $D_0 = \rho^* d_0$ and $d_0 = \infty^+ + \infty^-$, and

$$\phi : \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}^2 \longrightarrow J(\mathrm{b5}, \mathrm{ns7})(\mathbb{Q}), \quad (a, b, c) \mapsto aD_{\mathrm{tor}} + bD_1 + 2cD_2.$$

Then by the previous discussion, $\mathrm{Im}(\iota) \subset \mathrm{Im}(\phi)$, c.f. (iii) in Section 1.2.5.

4.4.4 Finding the points

We distinguish between three types of points on $X(\mathrm{b5}, \mathrm{ns7})^{(4)}$:

- *pullbacks*: points in $\rho^* C^{(2)}(\mathbb{Q})$,
- *partial pullbacks*: points of the form $\mathcal{P} + \mathcal{Q}$ for $\mathcal{P} \in X(\mathrm{b5}, \mathrm{ns7})^{(2)}(\mathbb{Q}) \setminus \rho^* C(\mathbb{Q})$ and $\mathcal{Q} \in \rho^* C(\mathbb{Q})$, and
- *isolated points*: elements of $X(\mathrm{b5}, \mathrm{s7})^{(4)}(\mathbb{Q})$ that are neither a pullback nor a partial pullback.

We note that each of these types is treated slightly differently by Theorem 3.2.6. We first consider the pullbacks and partial pullbacks, and then describe how we found $P_0, \ldots, P_4 \in X(\mathrm{b5}, \mathrm{ns7})$. The curve $X(\mathrm{b5}, \mathrm{ns7})$ has finitely many quadratic points, so there are finitely many partial pullbacks, whereas the pullbacks $\rho^* C^{(2)}(\mathbb{Q})$ form an infinite set. For the Mordell–Weil sieve to work, we need to find all isolated points and partial pullbacks, and use a sufficiently large finite subset of $\rho^* C^{(2)}(\mathbb{Q})$. In this case, however, we can speed up the sieve by discarding all pullbacks thanks to the work of Derickx, Najman and Siksek.

Proposition 4.4.6. *Suppose that $D \in X(\mathrm{b5}, \mathrm{ns7})^{(4)}(\mathbb{Q})$ satisfies*

$$w_5^*(2[D - D_0]) = 2[D - D_0].$$

Then $D \in \rho^* C^{(2)}(\mathbb{Q})$.

Proof. Derickx, Najman and Siksek [DNS20] showed that $X(\mathrm{b5}, \mathrm{ns7})$ has no degree 4 map to $\mathbb{P}^1$, other than ρ followed by the hyperelliptic covering map x (and the composition of $x \circ \rho$ with automorphisms of $\mathbb{P}^1$). In particular, each degree 4 map $f : X(\mathrm{b5}, \mathrm{ns7}) \to \mathbb{P}^1$ satisfies $f \circ w_5 = f$.

Since the torsion subgroup has odd size, we find $w_5^*[D - D_0] = [D - D_0]$. As $w_5^* D_0 = D_0$ by construction, we conclude that $w_5^* D \sim D$. If $D \neq w_5^* D$, there exists a non-constant $f \in L(D)$ satisfying $\mathrm{div}_0(f) = w_5^* D$ and $\mathrm{div}_\infty(f) = D$. Then f defines a degree 4 map $\overline{f} : X(\mathrm{b5}, \mathrm{ns7}) \to \mathbb{P}^1$ such that $\overline{f} \circ w_5 \neq \overline{f}$. We conclude that $D = w_5^* D$. Now $D \in \rho^* C^{(2)}(\mathbb{Q})$ unless one of the points in the support of D is fixed by w_5. We compute the fixed points of w_5 explicitly in `Magma`, and find that each of them is defined over a field of degree 6. □

Conversely, note that all pullbacks $D \in \rho^* C^{(2)}(\mathbb{Q})$ also satisfy $w_5^*(D - D_0) = (D - D_0)$. Define $W = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}^2 \setminus (\{0\} \times \mathbb{Z}^2)$ and $S = X(\mathrm{b5}, \mathrm{ns7})^{(4)}(\mathbb{Q}) \setminus \rho^* C^{(2)}(\mathbb{Q})$. Since $w_5^* D_{\mathrm{tor}} = -D_{\mathrm{tor}}$, $w_5^* D_1 = D_1$ and $w_5^* D_2 = D_2$, this proposition means that $\iota(S) \subset \phi(W)$. In practice, this means that we will be able to disregard pullbacks altogether and sieve in W, c.f. Section 1.2.5.

Next, we recall that Derickx, Najman and Siksek already showed $X(\mathrm{b5}, \mathrm{ns7})^{(3)}(\mathbb{Q}) = \{c_0, c_\infty\}$; in particular, the curve has no rational points. The quotient C has (at least) 6 rational points $Q_1, \ldots, Q_6$ defined in Tabel 4.2, pulling back to 6 quadratic points. It remains to find the isolated quadratic and quartic points on $X(\mathrm{b5}, \mathrm{ns7})$. We found the quadratic points P_0 and $w_5^* P_0$ by intersecting with hyperplanes, as explained in Section 1.2.6. To find the quartic points $P_1, \ldots, P_4$, we used the sieve method also outlined in Section 1.2.6. Finally, we define $T := \{Q_1, \ldots, Q_6\}$,

$$\mathcal{L}' := \{\mathcal{P}_1, w_5^* \mathcal{P}_1, \ldots, \mathcal{P}_4, w_5^* \mathcal{P}_4\} \cup (\mathcal{P}_0 + \rho^* T) \cup (w_5^* \mathcal{P}_0 + \rho^* T),$$

and

$$\mathcal{L} := \{\mathcal{P}_1, w_5^* \mathcal{P}_1, \ldots, \mathcal{P}_4, w_5^* \mathcal{P}_4\} \cup (\mathcal{P}_0 + \rho^* C(\mathbb{Q})) \cup (w_5^* \mathcal{P}_0 + \rho^* C(\mathbb{Q})) \supset \mathcal{L}'.$$

4.4.5 The proof of Theorem 4.4.1

We apply the Mordell–Weil sieve defined in Section 1.2.5 with $V = X(\mathrm{b5}, \mathrm{ns7})^{(4)}$, $\mathcal{A} = J(\mathrm{b5}, \mathrm{ns7})$, $B = \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}^2$, ϕ and ι as defined at the end of Section 4.4.3 and S, W and $\mathcal{L}$ as defined in Section 4.4.4. For each prime $p \geq 17$, we define $\mathcal{N}_p \subset \widetilde{X}(\mathrm{b5}, \mathrm{ns7})(\mathbb{F}_p)$ to be the reductions of the points in $\mathcal{L}'$ satisfying the condition of Theorem 3.2.6. When $p < 17$, let $\mathcal{N}_p = \emptyset$. Then we set

$$\mathcal{M}_p = \iota_p^{-1}(\phi_p(W)) \setminus \mathcal{N}_p.$$

All assumptions for the sieve are then satisfied, and we run it with the primes $p_1 = 11$, $p_2 = 13$, $p_3 = 17$, $p_4 = 23$, $p_5 = 53$, $p_6 = 29$, $p_7 = 71$, $p_8 = 43$, $p_9 = 37$ and $p_{10} = 31$. This terminates, and by Proposition 1.2.9 we have thus proved Theorem 4.4.1.

4.4.6 The j-invariants

While Le Hung's fibred product model for $X(\mathrm{b5}, \mathrm{ns7})$ comes with a j-map by construction, this is not the case for the planar Derickx–Najman–Siksek model for $X(\mathrm{b5}, \mathrm{ns7})$, where no explicit j-map was previously known. So instead, to compute the j-invariant of the points in Table 4.1, we use Section 2.4. Here a different (canonical) model for $X(\mathrm{b5}, \mathrm{ns7})$ is computed, together with the morphism from this model to the planar model, and with the j-invariant. We thus pull back the effective degree 4 divisors of Table 4.1 to this canonical model, and evaluate the j-invariant there.

4.5 $X(\mathrm{b3}, \mathrm{b5}, \mathrm{e7})$ and $X(\mathrm{s3}, \mathrm{b5}, \mathrm{e7})$

By Corollary 4.4.3 and subsequent remarks, it suffices now to determine the quadratic points on

$$X_1 := X(\mathrm{b5}, \mathrm{e7})/w_5 \text{ and } X_2 := X(\mathrm{b5}, \mathrm{e7})/\phi_7 w_5.$$

Recall from Section 2.4 that both curves admit a map $\rho_i : X_i \to C = X(\mathrm{b5}, \mathrm{ns7})/w_5$ of degree 2. We also recall that C is a hyperelliptic curve of genus 2 whose Mordell–Weil group has rank 2, so determining $C(\mathbb{Q})$ with abelian Chabauty is unlikely to succeed, c.f. Remark 4.4.5. Consequently, we cannot expect to be able to determine $\rho_i^* C(\mathbb{Q}) \subset X_i^{(2)}(\mathbb{Q})$ using abelian Chabauty. Instead, therefore, we shall attempt to describe $X_i^{(2)}(\mathbb{Q}) \setminus \rho_i^* C(\mathbb{Q})$ using, again, relative symmetric Chabauty and the Mordell–Weil sieve. This suffices, as rational points on C come from rational or quadratic points on $X(\mathrm{b5}, \mathrm{ns7})$ and therefore have rational or quadratic j-invariants.

4.5.1 Overview

The curves X_1 and X_2 have genera 8 and 5 respectively.

Unlike for $X(\mathrm{b5}, \mathrm{ns7})$, each $J(X_i)(\mathbb{Q})$ appears to have rank strictly greater than $2 = \mathrm{rk}(J(C)(\mathbb{Q}))$. Compared to $X(\mathrm{b5}, \mathrm{ns7})$, this causes two extra difficulties when attempting to use Chabauty:

- We do not obtain a finite index subgroup of $J(X_i)(\mathbb{Q})$ by pulling back generators of $J(C)(\mathbb{Q})$, making it hard to sieve effectively.
- We do not obtain vanishing differentials with trace zero (defined in Section 3.2.2) from the kernel of $1 + w_i^*$, where w_i is the involution on X_i such that $C = X_i/w_i$.

We instead use cusp forms to find vanishing differentials in Section 4.5.3, while the Mordell–Weil group issue is addressed in the remainder of this section.

Recall from Section 1.2.5 that rather than the Jacobian, all we really need for sieving is a morphism $X_i^{(2)} \to A$ for some abelian variety A. As a start, we can try to take $A = J(C)$. Then $X_i^{(2)} \to J(C)$ is the Abel–Jacobi map composed with the push-forward $(\rho_i)_*$. Sieving in $J(C)(\mathbb{Q})$ is unlikely to work, however, because both $\#X_i^{(2)}(\mathbb{F}_p)$ and $\#J(C)(\mathbb{F}_p)$ have size close to p^2, c.f. Remark 1.2.10. Which other Jacobians, of which we know the Mordell–Weil group, does $X_i^{(2)}$ map to?

$$\begin{tikzcd}
 & X(*3,\mathrm{b5},\mathrm{e7}) \arrow[dl, dashed] \arrow[d, dashed] \arrow[ddr, dashed, bend left] \arrow[ddrr, dashed, bend left, "\text{if } *=\mathrm{b}"] & & \\
X(*3,\mathrm{b5}) \arrow[dd] & X(\mathrm{b5},\mathrm{e7}) \arrow[dl, dashed] \arrow[d, dashed] \arrow[dr, dashed] & & \\
 & X(\mathrm{b5},\mathrm{ns7}) \arrow[dl] \arrow[dr] \arrow[ddrr, bend right] & X_1 \arrow[d] & X_2 \arrow[dl] & X(\mathrm{b3},\mathrm{ns7}) \arrow[d] \arrow[ddl] \\
X(\mathrm{b5}) & & X(\mathrm{b5},\mathrm{ns7})/w_5 & X(\mathrm{e7}) \arrow[d] & X(\mathrm{b3},\mathrm{ns7})/w_3 \\
 & & & X(\mathrm{ns7}) &
\end{tikzcd}$$

Figure 4.2: Maps between modular curves, where $* \in \{\mathrm{b}, \mathrm{s}\}$. A full line means we have computed this map explicitly, whereas a dotted line has not been computed.

One answer is $J(\mathrm{e7})$. The curve $X(\mathrm{e7})$ is an elliptic curve of rank 0, and $X_i^{(2)}$ has a map to its Jacobian $J(\mathrm{e7})$. Indeed, each degree 2 effective divisor $D \in X_i^{(2)}$ pulls back to a degree 4 effective divisor on $X(\mathrm{b5},\mathrm{e7})$, then pushes forward to a degree 4 effective divisor on $X(\mathrm{e7})$. This then has an Abel–Jacobi map into $J(\mathrm{e7})$. In particular, demanding that each $D \in X_i^{(2)}(\mathbb{F}_p)$ maps into the image of $J(\mathrm{e7})(\mathbb{Q})$ in $J(\mathrm{e7})(\mathbb{F}_p)$, we obtain a stronger sieve (with $A = J(C) \times J(\mathrm{e7})$). Now $\dim(A) = 3 > 2 = \dim(X_i^{(2)})$, making A potentially large enough for sieving. In practice, however, this sieve still does not terminate fast enough.

We thus use the final trump card we have been dealt but neglected so far: the information at the prime 3. We are only interested in those quadratic points on X_i that are the image of a quartic point on $X(\mathrm{s3},\mathrm{b5},\mathrm{e7})$ or $X(\mathrm{b3},\mathrm{b5},\mathrm{e7})$. The curves $X(\mathrm{s3},\mathrm{b5})$ and $X(\mathrm{b3},\mathrm{b5}) = X_0(15)$ are also elliptic curves of rank 0, and we can make use of their Mordell–Weil groups. More precisely, we apply the sieve from Section 1.2.5 to the four varieties

$$Y_{*,i} := X_i^{(2)} \times_{X(\mathrm{b5})^{(4)}} X(*3,\mathrm{b5})^{(4)} \quad \text{for } i \in \{1,2\},\ * \in \{\mathrm{b},\mathrm{s}\}$$

using the abelian variety $A = J(C) \times J(\mathrm{e7}) \times J(*3, \mathrm{b5})$ and a relative symmetric Chabauty method. Note that the map $X_i^{(2)} \to X(\mathrm{b5})^{(4)}$ is defined by first pushing forward to C, then pulling back to $X(\mathrm{b5}, \mathrm{ns7})$ and then pushing forward to $X(\mathrm{b5})$, see Figure 4.2. This sieve is successful for three of the four cases: for $i = 1$ and $* = \mathrm{b}$, the sieve does not terminate.

The reason is that C is hyperelliptic. Denote by $x : C \to \mathbb{P}^1$ the map to $\mathbb{P}^1$. All $D \in x^*\mathbb{P}^1(\mathbb{Q}) \subset C^{(2)}(\mathbb{Q})$ have the same image $O \in J(C)(\mathbb{Q})$. So in order to "remove" in the sieve a class $(O, a, b) \in J(C) \times J(\mathrm{e7}) \times J(\mathrm{b3}, \mathrm{b5})$ as a possible image of an unknown element of $X_1^{(2)}(\mathbb{Q})$, we need, modulo a prime p, all $p + 1$ such pullbacks $x^*\mathbb{P}^1(\mathbb{F}_p)$ to be discounted simultaneously by the sieve; for one such class (O, a, b) this does not happen when $i = 1$ and $* = \mathrm{b}$.

We therefore add yet another curve and yet another Mordell–Weil group. The curve $X(\mathrm{b3}, \mathrm{ns7})$ has genus 5, and its quotient $C_2 := X(\mathrm{b3}, \mathrm{ns7})/w_3$ is a genus 2 hyperelliptic curve whose Mordell–Weil group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2$. We thus redefine

$$Y_{\mathrm{b},1} := X(\mathrm{b3}, \mathrm{ns7})^{(4)} \times_{X(\mathrm{ns7})^{(4)}} X_1^{(2)} \times_{X(\mathrm{b5})^{(4)}} X(\mathrm{b3}, \mathrm{b5})^{(4)}$$

and sieve in $A = J(C_2) \times J(C) \times J(\mathrm{e7}) \times J(\mathrm{b3}, \mathrm{b5})$. This works.

Theorem 4.5.1. *The sets $Y_{*,i}(\mathbb{Q})$, for $* \in \{\mathrm{b}, \mathrm{s}\}$ and $i \in \{1, 2\}$, consist entirely of points of which the image in $X_i^{(2)}(\mathbb{Q})$ is in $\rho_i^* C(\mathbb{Q})$.*

Together with Corollary 4.4.3 and subsequent remarks, Theorem 4.5.1 shows that all quartic points on $X(\mathrm{b3}, \mathrm{b5}, \mathrm{e7})$ and $X(\mathrm{s3}, \mathrm{b5}, \mathrm{e7})$ either have quadratic or rational j-invariant, correspond to a $\mathbb{Q}$-curve, or have non-totally real j-invariant displayed in Table 4.1. Together with Theorems 4.2.1 and 4.3.1, this finally proves Theorem 4.1.5.

To prove Theorem 4.5.1, we note that it remains necessary to use a relative Chabauty method on top of the sieve, because each $Q \in C(\mathbb{Q})$ determines for each $i \in \{1, 2\}$ a point on $Y_{*,i}(\mathbb{Q})$ for at least one $* \in \{\mathrm{b}, \mathrm{s}\}$.

4.5.2 Models and maps

In this section, we give explicit descriptions for the models and maps in Figure 4.2, as well as the known Mordell–Weil groups.

The map $X(\mathrm{b3}, \mathrm{b5}) \to X(\mathrm{b5})$

We begin on the left-hand side. A model for the elliptic curve $X(\mathrm{b3}, \mathrm{b5}) = X_0(15)$, together with the map to $X(\mathrm{b5}) = X_0(5) = \mathbb{P}^1$, can be computed by built-in functions of the Small Modular Curves package in `Magma`:

$$X(\mathrm{b3}, \mathrm{b5}) : \; y^2 + xy + y = x^3 + x^2 - 10x - 10,$$

and the degree 4 map to $X(\mathrm{b5}) = \mathbb{P}^1$ is given by

$$(x : y : z) \mapsto (-6x^2 + xy + 6xz + 10yz + 12z^2 : x^2 + 2xz + z^2),$$

where $(x : y : z)$ are the coordinates in $\mathbb{P}^2$. The Mordell–Weil group is

$$J(\mathrm{b3}, \mathrm{b5})(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \cdot (-1, 0) \oplus \mathbb{Z}/4\mathbb{Z} \cdot (-2, -2).$$

The map $X(\mathrm{s3}, \mathrm{b5}) \to X(\mathrm{b5})$

The curve $X(\mathrm{s3}, \mathrm{b5})$ is isomorphic to $X_0(45)/w_9$ by Example 1.1.12. For the latter, the `ModularCurveQuotient` function in `Magma` can compute a model using modular forms. However, for such quotients, the map to $X_0(5)$ is not built in.

Instead, we compute a canonical model for the non-hyperelliptic genus 3 curve $X_0(45)$ in $\mathbb{P}^2$, by finding equations between three linearly independent weight 2 cusp forms f_1, f_2, f_3. On $X_0(45)$, we compute a matrix for the action of w_9 on these cusp forms (and hence on this model), and by taking the quotient, we obtain explicitly the map $X_0(45) \to X_0(45)/w_9$, and find

$$X(\mathrm{s3}, \mathrm{b5}) : \ y^2 + xy + y = x^3 + x^2 - 5x + 2.$$

This map describes x and y as rational functions in terms of f_1, f_2 and f_3, so we obtain q-expansions $x(q)$, $y(q)$ for the functions x and y on $X(\mathrm{s3}, \mathrm{b5})$. Now using the `qExpansionsOfGenerators` function in `Magma`, we find the q-expansion $h(q)$ of a Hauptmodul on $X(\mathrm{b5})$.

Finally, we compute $X(\mathrm{s3}, \mathrm{b5}) \to X(\mathrm{b5})$ using the method of Section 1.2.2. We do not display this degree 6 map here for brevity reasons, but invite the curious reader to use the `Magma` code.

The Mordell–Weil group is

$$J(\mathrm{s3}, \mathrm{b5})(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \cdot (3/4, -7/8) \oplus \mathbb{Z}/4\mathbb{Z} \cdot (0, -2).$$

The map $X(\mathrm{e7}) \to X(\mathrm{ns7})$

This map was determined by Freitas, Le Hung and Siksek [FLHS15] using the j-invariant map on $X(\mathrm{ns7}) = \mathbb{P}^1$ computed by Chen [Che96]. They found $X(\mathrm{e7})$ to be an elliptic curve given by

$$X(\mathrm{e7}) : \ y^2 = 7(16x^4 + 68x^3 + 111x^2 + 62x + 11)$$

with the map $X(\mathrm{e7}) \to X(\mathrm{ns7})$ being simply a projection $(x : y : z) \mapsto (x : z)$.

The Mordell–Weil group is

$$J(\mathrm{e7})(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \cdot [(-1/3, -14/3) - (-1/3, 14/3)].$$

The curves X_1, X_2 and $X(\mathrm{b5}, \mathrm{ns7})$

Canonical models for these curves, as well as the map $X(\mathrm{b5}, \mathrm{ns7}) \to X(\mathrm{ns7})$, were computed in Section 2.4. Note that the map to $X(\mathrm{ns7})$ was also computed using Chen's j-map and is therefore compatible with $X(\mathrm{e7}) \to X(\mathrm{ns7})$.

The strategy described in Section 1.2.2 for determining morphisms of modular curves did not succeed in determining the map $X(\mathrm{b5},\mathrm{ns7}) \to X(\mathrm{b5})$, however, since the degree of this map (which is 21) is too large for such a computation. Instead, note that the map to $X(\mathrm{b5}) = \mathbb{P}^1$ corresponds to an element $g \in \mathbb{Q}(X(\mathrm{b5},\mathrm{ns7}))$. Denote by $j \in \mathbb{Q}(X(\mathrm{b5},\mathrm{ns7}))$ the function corresponding to the j-invariant, computed via the map to $X(\mathrm{ns7})$ and Chen's j-map on $X(\mathrm{ns7})$. The j-invariant j_5 on $X(\mathrm{b5})$ is a rational function of degree 6 such that

$$j_5(g) - j = 0 \in \mathbb{Q}(X(\mathrm{b5},\mathrm{ns7}))(g).$$

Multiplying this equation by the denominator of $j_5(g)$, we obtain a degree 6 polynomial equation in g, of which `Magma` can find the single root in $\mathbb{Q}(X(\mathrm{b5},\mathrm{ns7}))$. This root yields the map $X(\mathrm{b5},\mathrm{ns7}) \to X(\mathrm{b5})$. We do not display the map here for brevity reasons.

The curve $X(\mathrm{b3},\mathrm{ns7})$

This curve has genus 5. We compute a model, as well as the action of w_3, via cusp forms using Algorithm 2.3.13. This yields the following model in $\mathbb{P}^4$:

$$\begin{aligned} 10528X_0^2 - 21X_1X_2 - 112X_2^2 - 1136X_0X_3 - 17X_3^2 - 1016X_0X_4 + 273X_3X_4 - 176X_4^2 &= 0, \\ 47X_1^2 + 58X_1X_2 - 4X_2^2 - 336X_0X_3 - 9X_3^2 - 560X_0X_4 - 2X_3X_4 - 60X_4^2 &= 0, \\ 40X_0X_1 + 8X_0X_2 + X_1X_3 + 3X_2X_3 - 7X_1X_4 &= 0. \end{aligned}$$

We find that the Atkin–Lehner involution w_3 acts by

$$w_3 : \ (X_0 : \ldots : X_4) \mapsto (X_0 : -X_1 : -X_2 : X_3 : X_4).$$

The quotient by this automorphism yields the genus 2 hyperelliptic curve

$$C_2 = X(\mathrm{b3},\mathrm{ns7})/w_3 : \ y^2 = x^6 + 6x^5 - x^4 - 46x^3 - 43x^2 - 12x.$$

Using Stoll's algorithm [Sto02], we compute its Mordell–Weil group $J(X(\mathrm{b3},\mathrm{ns7})/w_3)(\mathbb{Q})$:

$$\mathbb{Z} \cdot [(-1,3) - \infty^-] \oplus \mathbb{Z} \cdot [(0,0) - \infty^-] \oplus \mathbb{Z}/2\mathbb{Z} \cdot [(0,0) - (-4,0)].$$

Recall that we used Chen's j-map in Section 2.4 to find the q-expansion of a Hauptmodul on $X(\mathrm{ns7})$. We now use the q-expansions of the cusp forms used to compute our model for $X(\mathrm{b3},\mathrm{ns7})$ and of this Hauptmodul on $X(\mathrm{ns7})$ to compute $X(\mathrm{b3},\mathrm{ns7}) \to X(\mathrm{ns7})$ via the method of Section 1.2.2. This yields

$$(X_0 : \ldots : X_4) \mapsto (3X_1 + 6X_2 + 5X_3 + 6X_4 : 56X_0 - 6X_1 - 4X_2 - 6X_3 + 4X_4).$$

Remark 4.5.2. While we will use the Mordell–Weil group $J(C_2)(\mathbb{Q})$ for sieving, we could also instead use a subgroup $G \subset J(\mathrm{b3},\mathrm{ns7})(\mathbb{Q})$ satisfying $2 \cdot J(\mathrm{b3},\mathrm{ns7})(\mathbb{Q}) \subset G$, c.f. Remark 1.2.8. This would result in a stronger sieve. We can construct such G as follows. By [Che96, Theorem 1], $J(\mathrm{b3},\mathrm{ns7})$ is isogenous to the new part of $J(X(\mathrm{b3},\mathrm{b49})/w_{49})$. In `Magma`, we

can compute the newforms corresponding to this new part of the Jacobian, and find that it is isogenous to $A_f \times A_g \times A_h$, where f, g, h are newforms, $A_f = J(C_2)$, and A_g and A_h have dimensions 1 and 2 respectively. Here A_k is the $\mathbb{Q}$-simple abelian variety attached to the newform k. We compute that $L(g,1) \neq 0$ and $L(h,1) \neq 0$, which by Kolyvagin–Logachëv [KL89] implies that $A_g(\mathbb{Q})$ and $A_h(\mathbb{Q})$ are torsion, so that $J(\mathrm{b3}, \mathrm{ns7})(\mathbb{Q})$ and $J(C_2)(\mathbb{Q})$ have equal rank. Pulling back $J(C_2)(\mathbb{Q})$ to $J(\mathrm{b3}, \mathrm{ns7})$ under the quotient map thus yields a subgroup $H \subset J(\mathrm{b3}, \mathrm{ns7})(\mathbb{Q})$ satisfyng $2 \cdot J(\mathrm{b3}, \mathrm{ns7})(\mathbb{Q}) \subset H$ modulo torsion by Proposition 1.2.2. Finally, composing the map $X(\mathrm{b3}, \mathrm{ns7}) \to X(\mathrm{ns7})$ with the j-map on the latter, we find the j-map on $X(\mathrm{b3}, \mathrm{ns7})$. Its poles consist of two irreducible degree 3 divisors c_0 and c_∞: the cuspidal divisors. The difference $[c_0 - c_\infty]$ has order 7 in the Mordell–Weil group, and reduction modulo primes shows that $2 \cdot J(\mathrm{b3}, \mathrm{ns7})(\mathbb{Q})_{\mathrm{tors}} \subset \langle [c_0 - c_\infty] \rangle$. The group G generated by $[c_0 - c_\infty]$ and the pullbacks of the generators of $J(C_2)(\mathbb{Q})$ displayed above thus satisfies $2 \cdot J(\mathrm{b3}, \mathrm{ns7}) \subset G$.

4.5.3 The vanishing differentials on X_1 and X_2

In order to apply a Chabauty method, we need to determine the vanishing differentials as defined in Section 3.2.2. In Section 2.4.3, we defined the newforms f_{49} (level 49), f_{35} (level 35), g_{35} (level 35), f_0 (level 245), f_1 (level 245) and f_2 (level 245) of trivial Nebentypus character. Also recall that $G(\mathrm{b5}, \mathrm{e7}) \subset \mathrm{GL}_2(\mathbb{Z}/35\mathbb{Z})$ is the intersection of the inverse images of $G(\mathrm{e7}) \subset \mathrm{GL}_2(\mathbb{F}_7)$ and $B_0(5) \subset \mathrm{GL}_2(\mathbb{F}_5)$ under the reduction maps, and $X(\mathrm{b5}, \mathrm{e7}) = X_{G(\mathrm{b5},\mathrm{e7})}$. Define the fixed spaces

$$S_1 = S_2(\Gamma_0(5 \cdot 7^2) \cap \Gamma_1(7), \mathbb{Q}(\zeta_7)^+)^{\langle G(\mathrm{b5},\mathrm{e7}), w_5 \rangle} \text{ and}$$
$$S_2 = S_2(\Gamma_0(5 \cdot 7^2) \cap \Gamma_1(7), \mathbb{Q}(\zeta_7)^+)^{\langle G(\mathrm{b5},\mathrm{e7}), \phi_7 w_5 \rangle},$$

where the action of $G(\mathrm{b5}, \mathrm{e7})$ was defined in Section 2.2.1. Despite containing cusp forms with Fourier coefficients in $\mathbb{Q}(\zeta_7)^+$, both S_1 and S_2 are $\mathbb{Q}$-vector spaces. Then the map $f(q) \mapsto f(q)(\mathrm{d}q)/q$ defines isomorphisms $S_i \simeq H^0(X_i, \Omega)$ for $i \in \{1, 2\}$. We computed in Section 2.4 canonical models for X_1 and X_2 by finding equations satisfied by the q-expansions of bases for S_1 and S_2 respectively. We describe the isomorphism $S_i \simeq H^0(X_i, \Omega^1)$ explicitly.

Lemma 4.5.3. *Suppose that X is a non-hyperelliptic curve of genus at least 2, and $f_0, \ldots, f_n$ is a basis for $H^0(X, \Omega^1)$. We obtain a canonical map $\phi : X \to \mathbb{P}^n$, $x \mapsto (f_0(x) : \ldots : f_n(x))$ which is an isomorphism onto its image Z. Consider $Q \in X$ with local coordinate q at Q. Then for each i we have a power series expansion $f_i(q) = (\sum_{j \geq 1} a_{ij} q^j)(\mathrm{d}q)/q$ at Q. Let $x_0, \ldots, x_n$ be the variables of $\mathbb{P}^n$, and consider $\omega \in H^0(Z, \Omega^1)$. Then $\omega = g(x_0, \ldots, x_n)\mathrm{d}(x_0/x_n)$, where g is a quotient of homogeneous polynomials of equal degree. The expansion of $\phi^*\omega$ at Q is*

$$\phi^*\omega(q) = g(f_0(q), \ldots, f_n(q)) \frac{\mathrm{d}(f_0/f_n)}{\mathrm{d}q} \mathrm{d}q.$$

Proof. This follows directly from the definitions. □

Given our model for X_i, we compute a basis for $H^0(X_i, \Omega)$, leading to an explicit isomorphism $H^0(X_i, \Omega) \simeq S_i$. We use this to determine the 1-form on X_i corresponding to a given q-expansion of a cusp form in S_i.

Denote by B_d the operator on modular forms mapping $q \mapsto q^d$ and by χ the Dirichlet character $\chi : (\mathbb{Z}/7\mathbb{Z})^\times \to \mathbb{C}^\times$ given by $\chi(3) = -e^{2\pi i/3}$. For X_2, we found in Section 2.4.5 a basis for S_2 consisting of five cusp forms h_0, h_1, h_2, h_3, h_4, where

$$h_0 \in V_{49} := \mathrm{Span}_{\overline{\mathbb{Q}}}\{f_{49}, f_{49} \otimes \chi^2, f_{49} \otimes \chi^4, f_{49}|B_5, (f_{49} \otimes \chi^2)|B_5, (f_{49} \otimes \chi^4)|B_5\}$$
$$h_1 \in \mathrm{Span}_{\overline{\mathbb{Q}}}\{f_{35}, f_{35} \otimes \chi^2, f_{35} \otimes \chi^4, f_{35}|B_7\}, \quad h_4 \in \mathrm{Span}_{\overline{\mathbb{Q}}}\{f_0 \otimes \chi, f_0 \otimes \chi^3, f_0 \otimes \chi^5\}.$$

Here, when f is a newform and ϵ a Dirichlet character, we denote by $f \otimes \epsilon$ the newform (at some level) satisfying $a_n(f \otimes \epsilon) = a_n(f)\epsilon(n)$ for all n coprime to the level of f and the conductor of ϵ. The forms h_2 and h_3 are fixed by the remaining involution on X_2 and thus correspond to the 1-forms on the quotient C. They are linear combinations of $f_1, f_1 \otimes \chi^2, f_1 \otimes \chi^4$ and their Galois conjugates.

For X_1, the chosen basis of S_1 was $g_0, g_1, \ldots, g_7$, where $g_4 = h_2$, $g_5 = h_3$, and

$$\begin{aligned}
&g_0 \in V_{49}, \qquad g_1, g_2 \in \mathrm{cSpan}_{\overline{\mathbb{Q}}}\{g_{35}, g_{35} \otimes \chi^2, g_{35} \otimes \chi^4, g_{35}|B_7\},\\
&g_3 \in \mathrm{Span}_{\overline{\mathbb{Q}}}\{f_0, f_0 \otimes \chi^2, f_0 \otimes \chi^4\},\\
&g_6, g_7 \in \mathrm{cSpan}_{\overline{\mathbb{Q}}}\{f_2, f_2 \otimes \chi^2, f_2 \otimes \chi^4, (f_2 \otimes \chi^2)|B_7, (f_2 \otimes \chi^4)|B_7\},
\end{aligned}$$

where $\mathrm{cSpan}(A)$ denotes the span of A and the Galois conjugates of elements in A.

By studying these twists of eigenforms, we will show that h_1, h_4 and g_1, g_2, g_6 and g_7 correspond to vanishing differentials on X_2 and X_1 respectively. These differentials can then be determined explicitly in terms of the models for X_1 and X_2 using Lemma 4.5.3.

In Section 2.4, it was shown that the modular curve

$$Y := X(\Gamma_0(5 \cdot 7^2) \cap \Gamma_1(7))$$

admits a morphism $\pi_i : Y \to X_i$ for each $i \in \{1, 2\}$. While both Y and X_i are defined over $\mathbb{Q}$, this morphism is defined over $K = \mathbb{Q}(\zeta_7)^+$, the real subfield of $\mathbb{Q}(\zeta_7)$. Moreover, $H^0(Y_K, \Omega^1) \simeq S_2(\Gamma_0(5 \cdot 7^2) \cap \Gamma_1(7), K)$, and the embedding $\pi_i^* : H^0((X_i)_K, \Omega^1) \to H^0(Y_K, \Omega^1)$ corresponds to the inclusion map on modular forms

$$S_i \otimes K \subset S_2(\Gamma_0(5 \cdot 7^2) \cap \Gamma_1(7), K).$$

Lemma 4.5.4. *Let K be a number field, and choose a prime $\mathfrak{p}$ of $\mathcal{O}_K$. Suppose that $\pi : X \to Z$ is a non-constant morphism of curves over K, and $\omega \in H^0(Z, \Omega^1)$ is such that $\pi^*\omega$ is a vanishing differential. Then ω is a vanishing differential.*

Proof. Consider $D \in J(Z)(K)$. We first note that $\pi_*(J(X)(K)) \subset J(Z)(K)$ has finite index (for $D \in J(Z)(K)$, we have $\deg(\pi)D = \pi_*\pi^*D \in \pi_*J(X)(K)$). So after multiplying

by an integer, we may suppose that $D = \pi_* E$ for some $E \in J(X)(K)$. Then

$$\int_{\pi_* E} \omega = \int_E \pi^* \omega = 0$$

by Proposition 3.2.3 (vi). $\square$

If we can find $f \in S_i$ corresponding to a vanishing differential on Y_K, then f corresponds to a vanishing differential on $(X_i)_K$ (hence on $X_i/\mathbb{Q}$) by the previous lemma. To this end, we make use of rank 0 quotients. Now let g be an eigenform in $S_2(\Gamma_0(5 \cdot 7^2) \cap \Gamma_1(7), \overline{\mathbb{Q}})$. By Eichler–Shimura theory, we obtain a morphism $\pi_g \colon J(Y) \to A_g$, where A_g is the Abelian variety associated to g by Eichler and Shimura. Let $\iota \colon Y \to J(Y)$ be the Abel–Jacobi map. Then $\iota^* \pi_g^* H^0((A_g)_{\overline{\mathbb{Q}}}, \Omega)$ is the space of 1-forms generated by the forms corresponding to g and its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates. Let us assume that $A_g(K)$ has rank zero. Then each element in $A_g(K)$ is torsion, and for each $\omega \in H^0(A_g, \Omega^1)$ and each $D \in J(Y)(K)$, we thus have an equality of Coleman integrals

$$\int_D \iota^* \pi_g^* \omega = \int_{(\pi_g)_* D} \omega = 0$$

by Proposition 3.2.3 (v) and (vi). To prove that g corresponds to a vanishing differential on Y_K, it thus suffices to show that $A_g(K)$ has rank 0, for which we use Proposition 1.2.1. Note that the group of characters on $\mathrm{Gal}(K/\mathbb{Q})$ is generated by χ^2.

Corollary 4.5.5. *The cusp forms h_1 and h_4 correspond to vanishing differentials on X_2 with trace zero to C. The forms g_1, g_2, g_6 and g_7 correspond to vanishing differentials on X_1 with trace zero to C.*

Proof. Let $\Psi := \{h_1, h_4, g_1, g_2, g_6, g_7\}$. Each element of Ψ is a linear combination of the newforms in $\Phi := \{f_{35}, f_{35} \otimes \chi^2, f_{35} \otimes \chi^4, g_{35}, g_{35} \otimes \chi^2, g_{35} \otimes \chi^4, f_0 \otimes \chi^3, f_0 \otimes \chi, f_0 \otimes \chi^5, f_2, f_2 \otimes \chi^2, f_2 \otimes \chi^4\}$ and their Galois conjugates. By Lemmas 4.5.3 and 4.5.4, the discussion below the latter and Proposition 1.2.1, to prove that the cusp forms in Ψ are vanishing differentials, it suffices to show that f_{35}, $f_0 \otimes \chi^3$, g_{35} and f_2 have no CM and no inner twists, and that each $f \in \Phi$ satisfies $L(f, 1) \neq 0$. We verified this in `Sage`, which uses an algorithm of Tim Dokchitser [Dok04] to evaluate $L(f, 1)$.

It remains to show that each element of Ψ corresponds to a differential on X_i with trace zero to C. Consider the map $\pi_C \colon Y \to C$ (which factors via X_1 and X_2). It suffices to show that each element of Φ corresponds to a differential ω on Y with $\pi_{C,*}(\omega) = 0$. Now $\pi_C^* H^0(C_K, \Omega)$ is the space generated by the 1-forms corresponding to $h_2 = g_4$ and $h_3 = g_5$, each of which is a linear combination of $f_1, f_1 \otimes \chi^2, f_1 \otimes \chi^4$ and their conjugates. The pushforward map $\pi_{C,*} \colon J(Y) \to J(C)$ thus factors via

$$\pi_{f_1} \colon J(Y) \to A_{f_1} \times A_{f_1 \otimes \chi^2} \times A_{f_1 \otimes \chi^4}.$$

As Φ consists of eigenforms unequal to (conjugates of) f_1, $f_1 \otimes \chi^2$ and $f_1 \otimes \chi^4$, indeed $\pi_{f_1}(\omega) = 0$ for each $\omega \in H^0(Y, \Omega)$ corresponding to an eigenform in Φ, from which it follows that also $\pi_{C,*}(\omega) = 0$, as desired. $\square$

4.5.4 Proof of Theorem 4.5.1

When $(*, i) \in \{(\mathrm{b}, 2), (\mathrm{s}, 1), (\mathrm{s}, 2)\}$, we apply the Mordell–Weil sieve described in Section 1.2.5 with $V = X_i^{(2)} \times_{X(\mathrm{b5})^{(4)}} X(*3, \mathrm{b5})^{(4)}$ and $A = J(C) \times J(\mathrm{e7}) \times J(*3, \mathrm{b5})$. When $(*, i) = (\mathrm{b}, 1)$, we apply the sieve with $V = X(\mathrm{b3}, \mathrm{ns7})^{(4)} \times_{X(\mathrm{ns7})^{(4)}} X_1^{(2)} \times_{X(\mathrm{b5})^{(4)}} X(\mathrm{b3}, \mathrm{b5})^{(4)}$ and $A = J(C) \times J(\mathrm{e7}) \times J(\mathrm{b3}, \mathrm{b5}) \times J(X(\mathrm{b3}, \mathrm{ns7})/w_3))$. In all cases, the map $\iota : V \to A$ is determined by the Abel–Jacobi maps on $C^{(2)}$, $X(*3, \mathrm{b5})^{(4)}$, $X(\mathrm{e7})^{(4)}$ and $(X(\mathrm{b3}, \mathrm{ns7})/w_3)^{(4)}$, and we let $\mathcal{L}$ be the set of points in $V(\mathbb{Q})$ mapping into $\{\rho_i^*(Q_j) \mid j \in \{1, \ldots, 6\}\}$ on $X_i^{(2)}$. (In particular, we find no other rational points on V.) When $(*, i) \in \{(\mathrm{b}, 2), (\mathrm{s}, 1), (\mathrm{s}, 2)\}$, we let $B = (\mathbb{Z}^2) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})$ and define $\phi\colon B \to A(\mathbb{Q})$ via the generators for $J(C)(\mathbb{Q})$, $J(\mathrm{e7})(\mathbb{Q})$ and $J(*3, \mathrm{b5})(\mathbb{Q})$ given in Section 4.5.2. Similarly, when $(*, i) = (\mathrm{b}, 1)$, we take $B = (\mathbb{Z}^2) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2)$ and ϕ is defined via the generators.

For a prime $p \geq 3$ of good reduction for V, we define $\mathcal{N}_p \subset \widetilde{V}(\mathbb{F}_p)$ to be the reductions of the points in $\mathcal{L}$ whose image in $X_i^{(2)}$ satisfies the rank condition in Theorem 3.2.6. This means we apply Theorem 3.2.6 to the pullbacks $\rho_i^* Q_j$ on X_i. We note that the most general form of Theorem 3.2.6 is not required for this; in fact, it suffices to use [Sik09, Theorem 4.3] instead. By Corollary 4.5.5, we can verify the rank condition in Theorem 3.2.6 or [Sik09, Theorem 4.3] using the vanishing differentials corresponding to h_1, h_4 (when $i = 2$) and g_1, g_2, g_6 and g_7 (when $i = 1$) under the isomorphism of Lemma 4.5.4. Then, as before, $\mathcal{M}_p = \iota_p^{-1}(\phi_p(B)) \setminus \mathcal{N}_p$. In each of the four sieves, the primes 13, 23, 43, 53, 67, 83, 71, 89, 97, 79 and 181 suffice to obtain an empty intersection, so we are done by Proposition 1.2.9.

4.6 Further study

4.6.1 Quartic fields containing $\sqrt{5}$

When considering quartic fields containing $\sqrt{5}$, we can no longer use Thorne's theorem (Theorem 4.1.3 (ii)). Instead, we can use [FLHS15, Proposition 2.1], to obtain the following theorem.

Theorem 4.6.1. *Suppose that K is any totally real quartic field. If an elliptic curve E/K is not modular, then E gives rise to a K-point on one of the curves*

$$X(\mathrm{u3}, \mathrm{v5}, \mathrm{w7}), \quad u \in \{\mathrm{b}, \mathrm{s}\},\ v \in \{\mathrm{b}, \mathrm{s}, \mathrm{ns}\},\ w \in \{\mathrm{b}, \mathrm{e}\}.$$

It was noted in [FLHS15, Remark (iii) in Section 4.2] that we cannot do any better than this at 5 without stronger modularity lifting results for fields containing $\sqrt{5}$. Instead of 4 curves, we thus need to consider 16 curves, a monumental task. An advantage is that instead of quartic points, we now need to study quadratic points over $\mathbb{Q}(\sqrt{5})$.

On the other hand, we lose an important $\mathbb{Q}$-curve argument used multiple times in Sections 4.2 and 4.3: on many curves to consider, only one Atkin–Lehner involution exists. For example, the quotient of $X(\mathrm{b3}, \mathrm{ns5})$ (genus 2) by w_3 is $\mathbb{P}^1$ and the quotient of $X(\mathrm{ns5}, \mathrm{b7})$ (genus 5) by w_7 is an elliptic curve with infinitely many $\mathbb{Q}(\sqrt{5})$-points. These

$\mathbb{Q}(\sqrt{5})$-points on the quotients pull back to infinitely many quadratic points over $\mathbb{Q}(\sqrt{5})$ on $X(\mathrm{b3}, \mathrm{ns5})$ and $X(\mathrm{ns5}, \mathrm{b7})$. Those points correspond to $\mathbb{Q}(\sqrt{5})$-curves, which, unlike $\mathbb{Q}$-curves, are not known to be modular.

Another complicating factor is that an analysis of the Jacobians of $X(\mathrm{u3}, \mathrm{v5}, \mathrm{b7})$ for $u \in \{\mathrm{b}, \mathrm{s}\}$ and $v \in \{\mathrm{s}, \mathrm{ns}\}$ (using the methods outlined in Section 1.2.3) revealed multiple 1-dimensional factors corresponding to elliptic curves with positive rank over $\mathbb{Q}(\sqrt{5})$, particularly in the ns5 case.

4.6.2 Quintic fields

After quartic fields, one naturally wonders what is possible for quintic fields. An apparent advantage is that quintic points on modular curves, unlike quartic points, do not arise as inverse images of lower degree points under degree 2 maps, which are abundant on modular curves due to the Atkin–Lehner involutions.

However, other problems do arise due to the increased degree. The Chabauty method for quartic points on $X(\mathrm{b5}, \mathrm{ns7})$ does not work for quintic points, as the Chabauty condition $r < g - (d - 1)$ is not satisfied when $r = 2$, $g = 6$ and $d = 5$. Other quotients of $X(\mathrm{b3}, \mathrm{b5}, \mathrm{e7})$ and $X(\mathrm{s3}, \mathrm{b5}, \mathrm{e7})$ that do satisfy the Chabauty condition and have small genus do not appear to exist. For $X(\mathrm{b3}, \mathrm{b5}, \mathrm{b7}) = X_0(105)$, its handy genus 5 quotient $X_0(105)/w_5$ has infinitely many quintic points (we computed multiple Riemann–Roch spaces to be 2-dimensional, c.f. Section 1.2.4). Similarly, the method for computing quartic points on $X(\mathrm{s3}, \mathrm{b5}, \mathrm{b7})$ used in Section 4.3 also fails in practice for quintic points.

While not necessarily infeasible, it is clear that new ideas are required for quintic fields.

Bibliography

[ACGH85] Enrico Arbarello, Maurizio Cornalba, Phillip A. Griffiths, and Joseph Harris. *Geometry of algebraic curves. Vol. I*, volume 267 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1985.

[AL70] A. O. L. Atkin and Joseph Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[AL78] A. O. L. Atkin and Wen Ch'ing Winnie Li. Twists of newforms and pseudo-eigenvalues of W-operators. *Invent. Math.*, 48(3):221–243, 1978.

[Ass20] Eran Assaf. Computing Classical Modular Forms for Arbitrary Congruence Subgroups. *arXiv e-prints*, page arXiv:2002.07212, February 2020.

[Bal15] Jennifer S. Balakrishnan. Coleman integration for even-degree models of hyperelliptic curves. *LMS J. Comput. Math.*, 18(1):258–265, 2015.

[Bar10] Burcu Baran. Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem. *J. Number Theory*, 130(12):2753–2772, 2010.

[Bar14] Burcu Baran. An exceptional isomorphism between modular curves of level 13. *J. Number Theory*, 145:273–300, 2014.

[BBB+] Jennifer S. Balakrishnan, Alex Best, Francesca Bianchi, Brian Lawrence, Steffen Müller, Nicholas Triantafillou, and Jan Vonk. Two recent p-adic approaches towards the (effective) mordell conjecture. To appear in *Arithmetic L-Functions and Differential Geometric Methods, Springer, ISBN 9783030652029, 2021.*

[BBK10] Jennifer S. Balakrishnan, Robert W. Bradshaw, and Kiran S. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 16–31. Springer, Berlin, 2010.

[BC] Barinder S. Banwait and John E. Cremona. Computing the modular curves $X_s(13)$, $X_{ns}(13)$ and $X_{A_4}(13)$ using modular symbols in Sage (annotated Sage code). *ancillary file to arXiv:1306.6818, see also https://github.com/JohnCremona/X13/blob/main/X13.ipynb.*

[BC14] Barinder S. Banwait and John E. Cremona. Tetrahedral elliptic curves and the local-global principle for isogenies. *Algebra Number Theory*, 8(5):1201–1229, 2014.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. volume 24, pages 235–265. 1997. Computational algebra and number theory (London, 1993).

[BD14] Christophe Breuil and Fred Diamond. Formes modulaires de Hilbert modulo p et valeurs d'extensions entre caractères galoisiens. *Ann. Sci. Éc. Norm. Supér. (4)*, 47(5):905–974, 2014.

[BDS+21] Jennifer S. Balakrishnan, Netan Dogra, Jan Steffen Müller, Jan Tuitman, and Jan Vonk. Quadratic Chabauty for modular curves: Algorithms and examples. *arXiv e-prints*, page arXiv:2101.01862, January 2021.

[BEL+19] Abbey Bourdon, Ozlem Ejder, Yuan Liu, Frances Odumodu, and Bianca Viray. On the level of modular curves that give rise to isolated j-invariants. *Advances in Mathematics*, 357:106824, 12 2019.

[BGG21] Josha Box, Stevan Gajović, and Pip Goodman. Cubic and quartic points on modular curves using generalised symmetric Chabauty. *arXiv e-prints*, page arXiv:2102.08236, February 2021.

[BL20] Josha Box and Samuel Le Fourn. Bounding integral points on the Siegel modular variety A_2(2). *arXiv e-prints*, page arXiv:2007.14422, July 2020.

[BN15] Peter Bruin and Filip Najman. Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields. *LMS J. Comput. Math.*, 18(1):578–602, 2015.

[BN20] François Brunault and Michael Neururer. Fourier expansions at cusps. *The Ramanujan Journal*, 53, 11 2020.

[Box21a] Josha Box. Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular. *arXiv e-prints*, page arXiv:2103.13975, March 2021.

[Box21b] Josha Box. Models for quotients of modular curves. *arXiv e-prints*, page arXiv:2101.03797, January 2021.

[Box21c] Josha Box. Quadratic points on modular curves with infinite Mordell–Weil group. *Math. Comp.*, 90(327):321–343, 2021.

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll. Generalized explicit descent and its application to curves of genus 3. *Forum Math. Sigma*, 4:Paper No. e6, 80, 2016.

[BS10] Nils Bruin and Michael Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010.

[BT20] Jennifer S. Balakrishnan and Jan Tuitman. Explicit Coleman integration for curves. *Math. Comp.*, 89(326):2965–2984, 2020.

[CDT99] Brian Conrad, Fred Diamond, and Richard Taylor. Modularity of certain potentially Barsotti-Tate Galois representations. *J. Amer. Math. Soc.*, 12(2):521–567, 1999.

[Cha41] Claude Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *C. R. Acad. Sci. Paris*, 212:1022–1024, 1941.

[Che96] Imin Chen. *The Jacobian of Modular Curves Associated to Cartan Subgroups (Ph.D. thesis)*. Oxford University, 1996.

[CN79] John Conway and Simon Norton. Monstrous moonshine. *Bull. London Math. Soc.*, 11(3):308–339, 1979.

[CN20] John E. Cremona and Filip Najman. $\mathbb{Q}$-curves over odd degree number fields. *arXiv e-prints*, page arXiv:2004.10054, April 2020.

[Col85a] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[Col85b] Robert F. Coleman. Torsion points on curves and p-adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985.

[Cre] John E. Cremona. Qcurves.py. `Sage` code available at https://github.com/JohnCremona/ecnf-data/blob/master/sage/Qcurves.py.

[Cre97] John E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[Der16] Maarten Derickx. *Torsion points on elliptic curves over number fields of small degree (Ph.D. thesis)*. Universiteit Leiden, 2016.

[DEv+20] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown. Sporadic Cubic Torsion. *arXiv e-prints*, pages arXiv:2007.13929, to appear in *Algebra Number Theory*, July 2020.

[DKSS17] Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll. Torsion points on elliptic curves over number fields of small degree. *arXiv e-prints*, page arXiv:1707.00364, July 2017.

[DNS20] Maarten Derickx, Filip Najman, and Samir Siksek. Elliptic curves over totally real cubic fields are modular. *Algebra Number Theory*, 14(7):1791–1800, 2020.

[Dok04] Tim Dokchitser. Computing special values of motivic L-functions. *Experiment. Math.*, 13(2):137–149, 2004.

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. pages 143–316. Lecture Notes in Math., Vol. 349, 1973.

[Dri73] Vladimir Drinfeld. Two theorems on modular curves. *Funkcional. Anal. i Priložen.*, 7(2):83–84, 1973.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[FLHS15] Nuno Freitas, Bao V. Le Hung, and Samir Siksek. Elliptic curves over real quadratic fields are modular. *Invent. Math.*, 201(1):159–206, 2015.

[Gal02] Steven D. Galbraith. Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}$-curves. *J. Théor. Nombres Bordeaux*, 14(1):205–219, 2002.

[GJG10] Enrique González-Jiménez and Xavier Guitart. On the modularity level of modular abelian varieties over number fields. *J. Number Theory*, 130(7):1560–1570, 2010.

[GQ14] Xavier Guitart and Jordi Quer. Modular abelian varieties over number fields. *Canad. J. Math.*, 66(1):170–196, 2014.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[Hes02] Florian Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.

[JM08] Frazer Jarvis and Jayanta Manoharmayum. On the modularity of supersingular elliptic curves over certain totally real number fields. *J. Number Theory*, 128(3):589–618, 2008.

[Kal18] Sudesh Kalyanswamy. Remarks on automorphy of residually dihedral representations. *Math. Res. Lett.*, 25(4):1285–1304, 2018.

[Kam92] Sheldon Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[Kat81] Nicholas M. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1981.

[Ken81] Monsur Kenku. On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$. *J. London Math. Soc. (2)*, 23(3):415–427, 1981.

[Kim05] Minhyong Kim. The motivic fundamental group of $\mathbb{P}^1\setminus\{0,1,\infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[KL89] Victor A. Kolyvagin and Dmitry Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[Kla93] Matthew James Klassen. *Algebraic points of low degree on curves of low rank (Ph.D. thesis)*. The University of Arizona, 1993.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[KM88] Monsur Kenku and Fumiyuki Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988.

[LH14] Bao Viet Le Hung. *Modularity of some elliptic curves over totally real fields (Ph.D. thesis)*. Harvard University, 2014.

[Lin97] San Ling. On the $\mathbb{Q}$-rational cuspidal subgroup and the component group of $J_0(p^r)$. *Israel J. Math.*, 99:29–54, 1997.

[LLL82] Arjen Lenstra, Hendrik Lenstra, Jr., and László Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[LN64] Joseph Lehner and Max Newman. Weierstrass points of $\Gamma_0(n)$. *Ann. of Math. (2)*, 79:360–368, 1964.

[LT02] Dino Lorenzini and Thomas J. Tucker. Thue equations and the method of Chabauty-Coleman. *Invent. Math.*, 148(1):47–77, 2002.

[Man72] Ju. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

[Mat89] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[Maz77] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Maz78] Barry Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[MP12] William McCallum and Bjorn Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012.

[MSD74] Barry Mazur and Peter Swinnerton-Dyer. Arithmetic of Weil curves. *Invent. Math.*, 25:1–61, 1974.

[Ogg74] Andrew P. Ogg. Hyperelliptic modular curves. *Bull. Soc. Math. France*, 102:449–462, 1974.

[OS19] Ekin Ozman and Samir Siksek. Quadratic points on modular curves. *Math. Comp.*, 88(319):2461–2484, 2019.

[Par99] Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.

[Rib80] Kenneth A. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.*, 253(1):43–62, 1980.

[Rib04] Kenneth A. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 241–261. Birkhäuser, Basel, 2004.

[Rub97] Karl Rubin. Modularity of mod 5 representations. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 463–474. Springer, New York, 1997.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Sik09] Samir Siksek. Chabauty for symmetric powers of curves. *Algebra Number Theory*, 3(2):209–236, 2009.

[Sik17] Samir Siksek. Quadratic Chabauty for Modular Curves. *arXiv e-prints*, page arXiv:1704.00473, April 2017.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Ste00] William Arthur Stein. *Explicit approaches to modular abelian varieties (Ph.D. thesis)*. University of California, Berkely, 2000.

[Sto02] Michael Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104(2):165–182, 2002.

[Sto17] Michael Stoll. Chabauty without the Mordell-Weil group. In *Algorithmic and experimental methods in algebra, geometry, and number theory*, pages 623–663. Springer, Cham, 2017.

[SV88] Karl-Otto Stöhr and Paulo Viana. A variant of Petri's analysis of the canonical ideal of an algebraic curve. *Manuscripta Math.*, 61(2):223–248, 1988.

[Tay89] Richard Taylor. On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98(2):265–280, 1989.

[Tho16] Jack A. Thorne. Automorphy of some residually dihedral Galois representations. *Math. Ann.*, 364(1-2):589–648, 2016.

[Tin75] David J. Tingley. *Elliptic curves uniformized by modular functions (Ph.D. thesis)*. University of Oxford, 1975.

[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[Wet97] Joseph Loebach Wetherell. *Bounding the number of rational points on certain curves of high rank (Ph.D. thesis)*. University of California, Berkeley, 1997.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[Zyw15] David Zywina. Possible indices for the Galois image of elliptic curves over Q. *arXiv e-prints*, page arXiv:1508.07663, August 2015.

[Zyw20] David Zywina. Computing actions on cusp forms. *arXiv e-prints*, page arXiv:2001.07270, January 2020.