2023

Triangular modular curves of low genus and geometric quadratic Chabauty

Juanita Duque Rosero
Dartmouth College, Juanita.Duque.Rosero.GR@Dartmouth.edu

TRIANGULAR MODULAR CURVES OF LOW GENUS AND GEOMETRIC QUADRATIC CHABAUTY

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

in

Mathematics

by Juanita Duque Rosero

DARTMOUTH COLLEGE

Hanover, New Hampshire

May 15, 2023

Examining Committee:

John Voight, Chair

Asher Auel

Pete Clark

Rosa Orellana

F. Jon Kull, Ph.D.
Dean of the Guarini School of Graduate and Advanced Studies

Abstract

This manuscript consists of two parts. In the first part, we study generalizations of modular curves: triangular modular curves. These curves have played an important role in recent developments in number theory, particularly concerning hypergeometric abelian varieties and approaches to solving generalized Fermat equations. We provide a new result that shows that there are only finitely many Borel-type triangular modular curves of any fixed genus, and we present an algorithm to list all such curves of a given genus.

In the second part of the manuscript, we explore the problem of computing the set of rational points on a smooth, projective, geometrically irreducible curve of genus $g > 1$ over $\mathbb{Q}$. We study the geometric quadratic Chabauty method, which is an effective method for producing a finite set of p-adic points containing the rational points of the curve. This method is due Edixhoven and Lido [36]. We overview the method and discuss explicit algorithms for finding rational points. We also present a comparison is with the classical (cohomological) quadratic Chabauty method.

Acknowledgments

I would like to express my gratitude to my Ph.D. advisor, John Voight, for his support, guidance, and encouragement throughout my journey at Dartmouth. His wisdom, dedication, and passion for mathematics have been a constant source of inspiration.

I would also like to thank Sachi Hashimoto and Pim Spelier for being such great collaborators and bringing joy into writing the second part of this manuscript.

I am grateful to Rachel Pries for her mentorship and teachings.

Muchas gracias a mi madre y a mi padre por todo su amor y apoyo incondicional. Sin ustedes, nada sería posible.

I also want to thank all the amazing women who have inspired me and given me a community. Your presence has been essential in my life.

Finally, I would like to thank the people who became my family in this country: Alex McCleary, Alina Glaubitz, and Lara Kassab. Your friendship and support have been crucial in my journey.

Contents

Abstract . . . ii

Acknowledgments . . . iii

1 Introduction 1

1.1 Triangular modular curves . . . 1

1.2 Geometric quadratic Chabauty . . . 8

I Triangular modular curves of low genus 13

2 Preliminaries 14

2.1 Triangle groups . . . 14

2.2 Quaternions . . . 18

2.3 Principal congruence subgroups . . . 20

2.4 Triangular modular curves, first encounter . . . 21

3 Triangular modular curves 23

3.1 Galois case . . . 23

3.2 Congruence subgroups: matrix case . . . 25

3.3 Image and admissibility . . . 28

3.4 Hyperbolic triples reducing to non-hyperbolic triples 30
3.5 Borel-type subgroups 34

4 Triangular modular curves of prime level **36**
4.1 Setup 36
4.2 Cycle structure and genus formula 38
4.3 Algorithm 42
4.4 Bounds from fixed genus 43
4.5 Enumerating curves of low genus and prime level 45
4.6 Triangular modular curves $X_1(a,b,c;\mathfrak{p})$ 47

5 Triangular modular curves of composite level **53**
5.1 Extra setup 54
5.2 Admissibility 61
5.3 Congruence subgroups 66
5.4 Algorithm 69
5.5 Triangular modular curves $X_1(a,b,c;\mathfrak{N})$ 74
5.6 Main theorem 76
5.7 Future work: computing monodromy with embedding numbers 77

II Geometric quadratic Chabauty **83**

6 Preliminaries **84**
6.1 Overview and Setup 84
6.2 The Poincaré torsor $\mathcal{P}$ 88
6.3 The biextension $\mathcal{M}$ 90

6.4 The trivial biextension $\mathcal{N}$ 93

6.5 The torsor T_f 97

6.6 The torsor T 102

7 Construction of the line bundle **104**

7.1 Construction of T 105

7.2 Embedding the curve 113

7.3 Integer points of the torsor 117

8 Main results **123**

8.1 The geometric quadratic Chabauty algorithm 123

8.2 The comparison theorem 126

8.3 Example: $X_0(67)^+$ 135

A Tables **150**

B Equations **162**

References **169**

Chapter 1

Introduction

This manuscript consists of two parts. In both parts, we study curves and rational points.

The first part of this thesis consists of joint work with John Voight. The main results from chapters 3 and 4 are published in [35], and chapter 5 contains new results. The second part of this thesis is joint work with Sachi Hashimoto and Pim Spelier that can be found in the preprint [32].

Section 1.1

Triangular modular curves

Modular curves are of immense significance in arithmetic geometry. They have been the focus of extensive research for over a century and have played a crucial role in understanding elliptic curves and solutions to Diophantine equations. In this first part of the thesis, we study generalizations of modular curves called *triangular modular curves.* These curves are quotients of the (completed) complex upper-half plane by congruence subgroups of triangle groups in the sense of Clark–Voight; note the corresponding groups, in general, are not arithmetic. In particular, we focus on classifying triangular modular curves by genus and enumerating the ones with low genus. One of the primary motivations for this work is that the study of triangular modular curves has the potential to contribute to the field of arithmetic geometry, similar to classical modular curves.

Low genus problems

For an integer $N \geq 1$, let $\Gamma_0(N), \Gamma_1(N) \leq \mathrm{SL}_2(\mathbb{Z})$ be the usual congruence subgroups and let $X_0(N), X_1(N)$ be the corresponding quotients of the completed upper half-plane. The genera of $X_0(N)$ and $X_1(N)$ as compact Riemann surfaces can be computed using the Riemann–Hurwitz formula [31, p. 66], and it can readily be seen that there are only finitely many of any given genus $g \geq 0$.

The study of modular curves of small genus goes back at least to Fricke [39, p. 357]. At the end of the twentieth century, Ogg enumerated and studied elliptic [57] and hyperelliptic [59] modular curves; the resulting Diophantine study [58] informed Mazur's classification of rational isogenies of elliptic curves [53], where the curves of genus 0 are precisely the ones with infinitely many rational points. This explicit study continues today, extended to include all quotients of the upper half-plane by congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$; the list up to genus 24 was computed by Cummins–Pauli [28]. Recent papers have studied curves with infinitely many rational points in the context of Mazur's *Program B*—see Rouse–Sutherland–Zureick-Brown [61] for further references and recent results in this direction.

Given this rich backdrop, it is worthwhile to pursue generalizations. For example, replacing $\mathrm{SL}_2(\mathbb{Z})$ with its quaternionic cousins, Voight [72] enumerated all Shimura curves of the form $X_0^1(\mathfrak{D}, \mathfrak{M})$ of genus at most 2. In a similar direction, Long–

Maclachlan–Reid [49] enumerated all maximal arithmetic Fuchsian groups of genus 0 over $\mathbb{Q}$. These groups correspond to quotients of Shimura curves by the full group of Atkin–Lehner involutions.

Setup

Let $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ and define

$$\chi(a, b, c) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$$

so that $\chi(a, b, c)\pi$ measures the difference from π of the sum of the angles of a triangle with angles $\pi/a, \pi/b, \pi/c$. If $\chi(a, b, c) \geq 0$, then such a triangle is drawn on the sphere or Euclidean plane, and these are very classical. Otherwise, we have $\chi(a, b, c) < 0$, and we say that the triple (a, b, c) is *hyperbolic*, as then the triangle lies in the (completed) upper half-plane $\mathcal{H}$. We focus on the hyperbolic case. Let $\Delta(a, b, c) \leq \mathrm{PSL}_2(\mathbb{R})$ be the subgroup of orientation-preserving isometries of the group generated by reflections in the sides of the triangle described above. Then $\Delta(a, b, c)$ can be presented as

$$\Delta(a, b, c) := \langle \delta_a, \delta_b, \delta_c \,|\, \delta_a^a = \delta_b^b = \delta_c^c = \delta_a\delta_b\delta_c = 1 \rangle,$$

where δ_s corresponds to a counterclockwise rotation at the vertex with angle $2\pi/s$.

Because of the associated map $\Delta(a, b, c) \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$, the group $\Delta(a, b, c)$ acts by isometries on $\mathcal{H}$. Then we define the triangular modular curve $X(a, b, c)$ as the quotient of $\mathcal{H}$ by the action of $\Delta(a, b, c)$ as above. In more generality, a triangular modular curve is the quotient of $\mathcal{H}$ by a congruence subgroup of $\Delta(a, b, c)$ as follows.

The first step is to define level structure. For $s \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, let $\zeta_s := \exp(2\pi i/s)$

and let $\lambda_s := \zeta_s + 1/\zeta_s = 2\cos(2\pi/s)$, with $\zeta_\infty = 1$ and $\lambda_\infty = 2$ by convention. Let $E = E(a,b,c) := \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c, \lambda_{2a}\lambda_{2b}\lambda_{2c})$ be the invariant trace field. For every nonzero ideal $\mathfrak{N}$ of $\mathbb{Z}_E$ not dividing $2abc$, there is a homomorphism

$$\varpi_{\mathfrak{N}} : \Delta(a,b,c) \to \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N}).$$

Intuitively, this homomorphism can be thought of as reducing matrix entries modulo $\mathfrak{N}$, but it has a rigorous quaternionic interpretation. If the image of the generators of $\Delta(a,b,c)$ has orders $(a',b',c') \neq (a,b,c)$, then $\varpi_{\mathfrak{N}}$ factors through $\Delta(a',b',c')$. This isomorphism is the reason why we only focus on *admissible* triples (a,b,c) for $\mathfrak{N}$, triples such that the order of the image of the generators under $\varpi_{\mathfrak{N}}$ are exactly a, b, and c.

We define $\Gamma(a,b,c;\mathfrak{N}) := \ker \pi_{\mathfrak{N}}$ as the *principal congruence subgroup of level* $\mathfrak{N}$ and

$$X(a,b,c;\mathfrak{N}) := \Gamma(a,b,c;\mathfrak{N})\backslash\mathcal{H}$$

as the *principal* triangular modular curve of level $\mathfrak{N}$. Following the analogy with classical modular curves, we also consider quotients of $\mathcal{H}$ by subgroups $\Gamma_0(a,b,c;\mathfrak{N})$ and $\Gamma_1(a,b,c;\mathfrak{N})$ coming from upper-triangular matrices. These quotients give rise to the *Borel–type triangular modular curves* $X_0(a,b,c;\mathfrak{N})$ and $X_1(a,b,c;\mathfrak{N})$. These are the main objects of study in this part of the thesis.

Some interesting features of triangular modular curves are the following. There are only finitely many arithmetic triangle groups [69, 68]. Hence, most triangular modular curves are not arithmetic, falling outside the Langlands program's scope. The Galois group and field of definition of these curves is characterized in [21], following the work of Macbeath [50]. It turns out that, triangular modular curves are not necessarily defined over $\mathbb{Q}$ [21, Theorem B].

Main result

In [21], Clark and Voight study the existence, construction, and properties of triangular modular curves. We build upon this work and show there are finitely many Borel–type triangular modular curves of any fixed genus. The main theorem is as follows.

Theorem A (Theorem 5.6.1)**.** *For any $g \in \mathbb{Z}_{\geq 0}$ there are finitely many triangular modular curves $X_0(a,b,c;\mathfrak{N})$ and $X_1(a,b,c;\mathfrak{N})$ of genus g with nontrivial admissible level $\mathfrak{N}$. Moreover, we present an algorithm to list all such curves of a given genus.*

We implemented the algorithm presented in Theorem A in Magma [17]; the code is available online [34].

We run this algorithm to enumerate all triangular modular curves $X_0(a,b,c;\mathfrak{N})$ and $X_1(a,b,c;\mathfrak{N})$ of genus g with nontrivial admissible level $\mathfrak{N}$ of genus 0, 1, and 2. The list in computer-readable format with additional data can be found in [34]. For the list with $g = 0, 1$ and prime level, see appendix A.

The number of curves of genus at most 2 are as follows:

	genus		
	0	1	2
$X_0(a,b,c;\mathfrak{N})$	76	268	485
$X_1(a,b,c;\mathfrak{N})$	7	9	13

Applications

Our theorem has potential applications in arithmetic geometry analogous to classical modular curves. Just as the quotient of the upper half-plane by $\mathrm{PSL}_2(\mathbb{Z})$ is the set of complex points of the moduli space of elliptic curves (parametrized by the affine j-line), Cohen–Wolfart [22, section 3.3] and Archinard [1] showed that the curves $X(a, b, c)$ over $\mathbb{C}$ naturally parametrize *hypergeometric abelian varieties*, certain Prym varieties of cyclic covers of $\mathbb{P}^1$ branched over ≤ 4 points.

More generally, in the same way as classical modular curves parametrize elliptic curves equipped with level structure, triangular modular curves parametrize hypergeometric abelian varieties equipped with level structure: see upcoming work of Kucharczyk–Voight [47]. In this light, our work classifies those situations where we might parametrize *infinitely many* such varieties with (nontrivial Borel-type) level structure.

As a final possible Diophantine application, we recall the work of Darmon [29]: he provides a dictionary between finite index subgroups of the triangle group $\Delta(a, b, c)$ and approaches to solve the generalized Fermat equation $x^a + y^b + z^c = 0$. From this vantage point, the triangular modular curves of low genus "explain" situations where the associated mod $\mathfrak{N}$ Galois representations are reducible.

Future work

In future work, we plan to compute equations for these curves (as Belyi maps) using the methods of Klug–Musty–Schiavone–Voight [45] and then study their rational points. Even without these equations, we have verified that all but a handful of the genus zero curves necessarily have a ramified rational point (hence are isomorphic to $\mathbb{P}^1$ over any field of definition).

To conclude, we peek ahead to more general triangular modular curves, allowing other congruence subgroups $\Gamma \leq \Gamma(a, b, c; \mathfrak{N})$ (prescribing other possible images of the corresponding Galois representations). For the case $\Delta = \mathrm{PSL}_2(\mathbb{Z})$, the story is a long and beautiful one, originating with a conjecture of Rademacher that there are only finitely many genus 0 congruence subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. Thompson [70] proved this for any genus g. The list of Cummins–Pauli for curves of up to genus 24 relies upon intricate and delicate p-adic methods of Cox–Parry [27] for an explicit bound on the level in terms of the genus. We propose the following conjecture, which predicts a similar result for triangular modular curves.

Conjecture B. *For all $g \in \mathbb{Z}_{\geq 0}$, there are only finitely many admissible triangular modular curves of genus g.*

We consider our main result (Theorem A) as partial progress towards this conjecture. The Borel–type subgroups are the family with the smallest growing index, thus likely to have the smallest genera. It would be interesting to see if the rather delicate p-adic methods of Cox–Parry can be generalized from $\mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ to groups of the form $\mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{N})$, as this would imply Conjecture B effectively.

Organization

We start in chapter 2 by introducing triangle groups, their relation with quaternion algebras, and the definition of congruence subgroups of triangle groups. This chapter concludes with the first encounter with triangular modular curves. In chapter 3, we focus on the definitions of Borel-type congruence subgroups for triangular modular curves of prime level. We prove Proposition 3.2.6, where we define the relevant matrix representation of Δ, and Theorem 3.3.1, describing its image building on work of Clark–Voight [21]. Moving on to chapter 4, we present some of the main building blocks of our work. We prove Theorem 4.2.4, which uses Riemann-Hurwitz to explicitly compute the genus of the triangular modular curves $X_0(a, b, c; \mathfrak{p})$ for $\mathfrak{p}$ a prime ideal. Then we can show that there are finitely many admissible curves $X_0(a, b, c; \mathfrak{p})$ of bounded genus for any $g \geq 0$ in Corollary 4.4.6 and present an algorithm to enumerate them in Algorithm 4.5.2. We use these ideas to show similar results for curves $X_1(a, b, c; \mathfrak{p})$. Finally, chapter 5 generalizes the results of the previous chapters to curves $X_0(a, b, c; \mathfrak{N})$ and $X_1(a, b, c; \mathfrak{N})$ of composite level, and it ends with the proof of Theorem A in section 5.6.

Section 1.2

Geometric quadratic Chabauty

Let $X_{\mathbb{Q}}$ be a smooth, projective, geometrically irreducible curve of genus $g > 1$ over $\mathbb{Q}$. The problem of describing $X_{\mathbb{Q}}(\mathbb{Q})$, the set of rational points of $X_{\mathbb{Q}}$, has fascinated mathematicians for centuries. Mordell's famous conjecture states that for $g > 1$, the set $X_{\mathbb{Q}}(\mathbb{Q})$ is finite. In [38], Faltings proves this conjecture and the result is known as Faltings's theorem. However, Faltings's theorem is not effective, meaning it does not give a method to determine the set of rational points. In this part of the thesis, we focus on studying the geometric quadratic Chabauty method [36]. This algebro-geometric method describes the rational points on curves with specific properties (as explained below).

Computing (finite) sets of rational points

There is still an ongoing effort to find explicit methods to compute the finite set $X_{\mathbb{Q}}(\mathbb{Q})$ when $g > 1$. Chabauty's theorem [20] gives a finiteness result for $X_{\mathbb{Q}}(\mathbb{Q})$ on certain curves by using p-adic analysis. This was made effective by Coleman [23] through the development of Coleman integration; he gave a method to find p-adic power series that vanish on a superset of $X_{\mathbb{Q}}(\mathbb{Q})$ for the curves Chabauty considered. This breakthrough is the starting point for the Chabauty–Kim program [44] of p-adic methods for proving the finiteness of $X_{\mathbb{Q}}(\mathbb{Q})$ generalizing Chabauty and Coleman's method. The quadratic Chabauty method [7, 9, 10, 36, 13] is an effective instance of the Chabauty–Kim method, first developed by Balakrishnan and Dogra, for studying the rational points of $X_{\mathbb{Q}}$.

Quadratic Chabauty

Let $J_{\mathbb{Q}}$ be the Jacobian of $X_{\mathbb{Q}}$, with Mordell–Weil rank r and Néron–Severi rank $\rho := \operatorname{rk} \mathrm{NS}(J_{\mathbb{Q}}) > 1$. Let $p > 2$ be a prime, not necessarily of good reduction for $X_{\mathbb{Q}}$. Quadratic Chabauty is an effective p-adic method for producing a finite set of p-adic points containing the rational points of $X_{\mathbb{Q}}$. There are several approaches to the quadratic Chabauty method. The (original) cohomological quadratic Chabauty method [9, 10] studies $X_{\mathbb{Q}}(\mathbb{Q})$ using p-adic height functions and works in certain Selmer varieties (for p of good reduction). This method is effective when $g = r$ and has been applied to determine the rational points on many modular curves [2, 11], including the cursed curve [3], a famously difficult problem. The geometric quadratic Chabauty method [36] is an algebro-geometric method for quadratic Chabauty, which can be applied when $r < g + \rho - 1$. The computations take place in $\mathbb{G}_m^{\rho-1}$-torsors over $J_{\mathbb{Q}}$.

Main results

We compare the geometric and cohomological methods for quadratic Chabauty in the cases where both methods can be applied. We prove the following theorem.

Theorem C (Comparison Theorem (Theorem 8.2.5))**.** *Assume that p is a prime of good reduction for $X_{\mathbb{Q}}$. Assume that $r = g$, $\rho > 1$, and furthermore the p-adic closure $\overline{J_{\mathbb{Q}}(\mathbb{Q})}$ is finite index in $J_{\mathbb{Q}}(\mathbb{Q}_p)$. Assume there exists a rational base point $b \in X_{\mathbb{Q}}(\mathbb{Q})$. Let $X_{\mathbb{Q}}(\mathbb{Q}_p)_{\mathrm{Coh}}$ be the finite set of p-adic points defined under these assumptions in [9, Theorem 1.2]. Let $X_{\mathbb{Q}}(\mathbb{Z}_p)_{\mathrm{Geo}}$ be the finite set of p-adic points obtained with the geometric Chabauty method. Then we have the inclusions*

$$X_{\mathbb{Q}}(\mathbb{Q}) \subseteq X_{\mathbb{Q}}(\mathbb{Z}_p)_{\mathrm{Geo}} \subseteq X_{\mathbb{Q}}(\mathbb{Q}_p)_{\mathrm{Coh}} \subseteq X_{\mathbb{Q}}(\mathbb{Q}_p),$$

and we can explicitly characterize $X_{\mathbb{Q}}(\mathbb{Q}_p)_{\mathrm{Coh}} \setminus X_{\mathbb{Q}}(\mathbb{Z}_p)_{\mathrm{Geo}}$.

In [41], Hashimoto and Spelier show that the classical Chabauty–Coleman method [24] and the geometric linear Chabauty method [63] are related by a similar comparison theorem.

Description of the method

The geometric quadratic Chabauty method studies the Poincaré torsor, the universal $\mathbb{G}_m$-biextension over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}$. By pulling back the Poincaré torsor by a nontrivial trace zero morphism $f : J_{\mathbb{Q}} \to J_{\mathbb{Q}}$, we can construct a nontrivial torsor T over the Néron model of $J_{\mathbb{Q}}$ whose restriction to $X_{\mathbb{Q}}$ is trivial. This allows us to embed $X_{\mathbb{Q}}$ into T through a section. The idea of the geometric quadratic Chabauty method is to intersect the image of the integer points on a regular model of $X_{\mathbb{Q}}$ with the p-adic closure of the integer points $\overline{T(\mathbb{Z})}$. This intersection contains $X_{\mathbb{Q}}(\mathbb{Q})$.

Suppose that p is a prime of good reduction for $X_{\mathbb{Q}}$. We give new algorithms for geometric quadratic Chabauty that work mainly in the trivial biextension $\mathbb{Q}_p^g \times \mathbb{Q}_p^g \times \mathbb{Q}_p$. Working on the trivial biextension translates the geometric quadratic Chabauty method into the language of Coleman–Gross heights [25] and Coleman integrals [23]. The main contribution of this paper is to explicitly give this translation into the language of heights and Coleman integrals. This translation allows us to prove the comparison theorem between the cohomological quadratic Chabauty method and the geometric quadratic Chabauty method. We also give an algorithm to compute the local heights away from p associated with the curve $X_{\mathbb{Q}}$. These heights are also studied in [15].

We further leverage the language of p-adic heights to compute the embedding of $X_{\mathbb{Q}}$ into T and the integer points $\overline{T(\mathbb{Z})}$ as convergent power series. Then determining up to finite p-adic precision, a finite set containing $X_{\mathbb{Q}}(\mathbb{Q})$ reduces to solving simple polynomial equations. Theoretically, by working modulo p^k for large enough $k \in \mathbb{N}$, the geometric quadratic Chabauty method will always produce a finite set of p-adic points with precision k containing $X_{\mathbb{Q}}(\mathbb{Q})$.

Algorithms and example

In this manuscript, we also describe algorithms for finding the finite set of p-adic points obtained by applying the geometric quadratic Chabauty method. These algorithms are practical when $X_{\mathbb{Q}}$ is a hyperelliptic curve. Our Magma [17] code implementing these algorithms can be found in [33].

Finally, we present an example of our new method applied to the modular curve $X_0(67)^+$ and a trace zero endomorphism f arising from the Hecke operator T_2. Even though the rational points on this curve have already been determined [2], this provides a new way of analyzing the set of rational points and comparing both methods.

Organization

In chapter 6, we provide background on the Poincaré torsor and its realizations. Then in chapter 7, we give an algorithm to construct the unique line bundle associated with the endomorphism f from a divisor in $U \times X$ satisfying specific properties described in Lemma 7.1.3. Using this line bundle, we write a formula for the trivializing section $\widetilde{j_b}\colon U \to T$. We give an algorithm for computing the convergent power series describing the embedding of a residue disk of the curve into the biextension $\mathcal{N}$ in section 7.2. In section 7.3, we give formulas for computing integer points in the biextension $\mathcal{N}$ that are the image of generating sections of certain residue disks of $\mathcal{M}$.

In chapter 8, we tie everything together. In section 8.1, we present the algorithm for geometric quadratic Chabauty in a residue disk $U(\mathbb{Z})_{\overline{P}}$. The comparison theorem appears in section 8.2. Theorem 8.2.5 states that the finite set of points found by the cohomological quadratic Chabauty method is a superset of the points found by the geometric method and gives an explicit description of the points in their difference. Finally, section 8.3 shows a worked example of the algorithms applied to the curve $X_0(67)^+$.

Part I

Triangular modular curves of low genus

Chapter 2

Preliminaries

This chapter presents basic definitions related to triangle groups, principal congruence subgroups, and their associated quaternion algebras. We build upon this theory to arrive at our first encounter with triangular modular curves in section 2.4. We base this introduction on the work of Clark and Voight from [21]. We expand on joint work with John Voight, published in [35].

Section 2.1

Triangle groups

Let $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. Then consider a triangle with angles π/a, π/b, and π/c. This triangle can be drawn on the Euclidean plane, sphere, or hyperbolic plane, depending on the values of a, b, and c. The triangle group $\Delta(a, b, c)$ is the subgroup of orientation-preserving isometries of the group generated by reflections in the sides of the triangle described above, drawn in the appropriate geometry. Then we have a presentation

$$\Delta(a, b, c) := \langle \delta_a, \delta_b, \delta_c \mid \delta_a^a = \delta_b^b = \delta_c^c = \delta_a\delta_b\delta_c = 1\rangle. \tag{2.1.1}$$

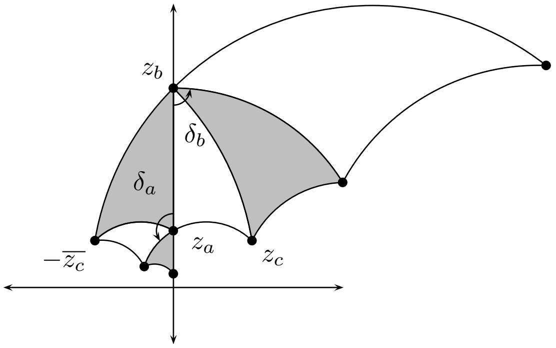

Figure 2.1: Triangle group (a, b, c) generated by $\delta_a, \delta_b, \delta_c$ (from [46, Figure 1]).

where δ_s corresponds to a counterclockwise rotation at the vertex with angle $2\pi/s$. In Figure 2.1, we see what these generators correspond to for a triangle in the hyperbolic plane.

Example 2.1.2. The triangle group $\Delta(2, 3, 3)$ is isomorphic to the symmetry group of the tetrahedron since these groups are both isomorphic to A_4.

Example 2.1.3. The triangle group $\Delta(2, 3, \infty)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{Z})$. Indeed, it is a classical result that $\mathrm{PSL}_2(\mathbb{Z})$ is generated by the elements

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

(see for example [74, Lemma 35.1.12]). We note that the order of ST is 3 and that $S(ST)T = I$, so we can choose $\delta_2 = S$, $\delta_3 = (ST)$, and $\delta_\infty = T$.

By cyclic permutation and inversion [21, Remark 2.2], we can reorganize the generators and suppose without loss of generality that

$$a \leq b \leq c. \tag{2.1.4}$$

All of the triples $(a, b, c) \in (\mathbb{Z} \cup \{\infty\})^3$ that we consider in this manuscript are such that $a \le b \le c$.

To decide on the appropriate geometry of the triangle, we let

$$\chi(a, b, c) := \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 \tag{2.1.5}$$

so that $\chi(a, b, c)\pi$ measures difference from π of the sum of the angles of a triangle with angles $\pi/a, \pi/b, \pi/c$. If $\chi(a, b, c) < 0$, then such a triangle is drawn on the sphere and if $\chi(a, b, c) = 0$, then the triangle is drawn on the Euclidean plane; these are very classical. Otherwise, $\chi(a, b, c) < 0$ and we say that the triple (a, b, c) is hyperbolic, as then the triangle lies in the (completed) upper half-plane $\mathcal{H}$. We now prove a well-known lemma that will be essential in future chapters.

Lemma 2.1.6. *For a hyperbolic triple* (a, b, c)*, we have*

$$\chi(a, b, c) \le \chi(2, 3, 7) = -\frac{1}{42} \tag{2.1.7}$$

bounded away from zero.

Proof. To maximize $\chi(a, b, c)$ with $a, b, c \in \mathbb{Z}_{\ge 2} \cup \{\infty\}$, the values of a, b, c need to be minimal. We have that $\chi(2, 3, 7) = -1/42$. Also, we compute $\chi(a, b, c)$ for $2 \le a \le b \le c \le 7$ with (a, b, c) hyperbolic and conclude that the maximum value of $\chi(a, b, c)$ for a hyperbolic triple is attained when $(a, b, c) = (2, 3, 7)$. □

From now on, we suppose that the triple (a, b, c) is hyperbolic. Then there is an associated map $\Delta(a, b, c) \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$, unique up to conjugation. We will often suppress the dependence on the triple from notation, writing for example $\Delta = \Delta(a, b, c)$.

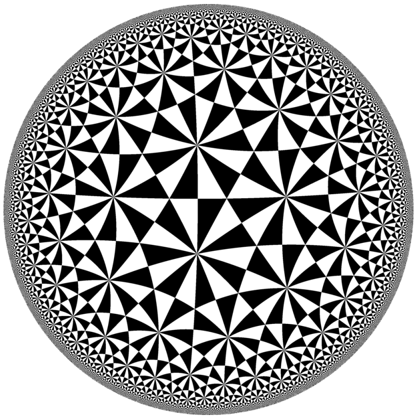

Figure 2.2: Tiling of $\mathcal{H}$ by the triangle $(2,3,7)$ (from public domain).

The group Δ is said to be cocompact if the quotient of the upper half-plane by Δ is compact, else we say Δ is noncocompact. We have Δ noncocompact if and only if at least one of a,b,c is equal to ∞.

Let $\Delta^{(2)}$ denote the subgroup of Δ generated by the set of squares $\{\delta^2 : \delta \in \Delta\}$. Then $\Delta^{(2)} \trianglelefteq \Delta$ is a normal subgroup, in fact [21, (5.9)] the quotient $\Delta/\Delta^{(2)}$ is generated by the elements δ_s with $s \in \{a,b,c\}$ such that either $s = \infty$ or $s \in \mathbb{Z}_{\geq 2}$ is even. Hence

$$\Delta/\Delta^{(2)} \simeq \begin{cases} \{0\}, & \text{if at least two of } a,b,c \text{ are odd integers;} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if exactly one of } a,b,c \text{ is an odd integer;} \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if all of } a,b,c \text{ are even integers or } \infty. \end{cases} \tag{2.1.8}$$

Lemma 2.1.9. *The group $\Delta^{(2)}$ is generated by the set*

$$\{\delta_s^{-1}\delta_t^2\delta_s : s,t \in \{a,b,c\}\} \cup \{\delta_s\delta_t\delta_s^{-1}\delta_t^{-1} : s,t \in \{a,b,c\}\}. \tag{2.1.10}$$

Proof. Follows from Takeuchi [69, Lemma 3, Proposition 5]: the generating set presented there is smaller (depending on cases), whereas we collect these and symmetrize to make a uniform statement. □

Section 2.2

Quaternions

For $s \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, let $\zeta_s := \exp(2\pi i/s)$ and let $\lambda_s := \zeta_s + 1/\zeta_s = 2\cos(2\pi/s)$, with $\zeta_\infty = 1$ and $\lambda_\infty = 2$ by convention. Define the tower of fields

$$\begin{tikzcd} F = F(a,b,c) := \mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c}) \arrow[d, dash] \\ E = E(a,b,c) := \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c, \lambda_{2a}\lambda_{2b}\lambda_{2c}). \end{tikzcd} \tag{2.2.1}$$

The extension $F \supseteq E$ is abelian of exponent at most 2 (since $\lambda_{2s}^2 = \lambda_s + 2$) and has degree at most 4. Let $\mathbb{Z}_F \supseteq \mathbb{Z}_E$ be the corresponding rings of integers, and let $\mathfrak{d}_{F|E}$ be the relative discriminant of $F \,|\, E$. The field F is the trace field of the image of Δ in $\mathrm{PSL}_2(\mathbb{R})$, and E the trace field for $\Delta^{(2)}$, also called the invariant trace field (see Maclachlan–Reid [51, section 5.5]).

Example 2.2.2. The fields E and F can be equal. For example,

$$F(2,3,7) = E(2,3,7) = \mathbb{Q}(\lambda_7).$$

As in section 2.1, we have a map $\Delta \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$; the F-subalgebra $B := F\langle\Delta\rangle \leq \mathrm{M}_2(\mathbb{R})$ generated by any lift of the image (well-defined, since $-1 \in F$) is a quaternion algebra, similarly $\mathcal{O} := \mathbb{Z}_F\langle\Delta\rangle$ is a $\mathbb{Z}_F$-order in B [67, Propositions 2–3]. The reduced discriminant of $\mathcal{O}$ is a principal ideal of $\mathbb{Z}_F$ generated by [21, Lemma 5.4]

$$\beta(a,b,c) := \lambda_{2a}^2+\lambda_{2b}^2+\lambda_{2c}^2+\lambda_{2a}\lambda_{2b}\lambda_{2c}-4 = \lambda_a+\lambda_b+\lambda_c+\lambda_{2a}\lambda_{2b}\lambda_{2c}+2 \in \mathbb{Z}_E. \tag{2.2.3}$$

The same construction applies to $\Delta^{(2)}$, yielding a quaternion E-algebra A and a $\mathbb{Z}_E$-order Λ. Let $\mathcal{O}^1 := \{\gamma \in \mathcal{O} : \operatorname{nrd}(\gamma) = 1\}$ be the elements of reduced norm 1 in $\mathcal{O}$, and define Λ^1 similarly. Then we have a commutative square of group homomorphisms

$$\begin{tikzcd}
\Delta^{(2)} \arrow[r, hook] \arrow[d, hook] & \Lambda^1/\{\pm 1\} \arrow[d, hook] \\
\Delta \arrow[r, hook] & \mathcal{O}^1/\{\pm 1\}
\end{tikzcd} \tag{2.2.4}$$

In fact, the bottom map descends to the *normalizer* $N_A(\Lambda)$ of Λ in A, as follows.

Lemma 2.2.5. *The composition of the maps*

$$\Delta \hookrightarrow \frac{\mathcal{O}^1}{\{\pm 1\}} \hookrightarrow \frac{N_B(\mathcal{O}^\times)}{F^\times}$$

factors via the map

$$\begin{aligned}
\Delta &\hookrightarrow \frac{N_A(\Lambda^\times)}{E^\times} \\
\delta_s &\mapsto \begin{cases} \delta_s^2+1 = \lambda_{2s}\delta_s, & \text{if } s \neq 2; \\ (\delta_c^2+1)(\delta_b^2+1) = \lambda_{2b}\lambda_{2c}\delta_a, & \text{if } s = a = 2; \end{cases}
\end{aligned} \tag{2.2.6}$$

followed by the natural inclusion $N_A(\Lambda^\times)/E^\times \hookrightarrow N_B(\mathcal{O}^\times)/F^\times$.

Proof. See Clark–Voight [21, Proposition 5.13]. (The description fails to be uniform when $a = 2$ because $\lambda_4 = 0$; since $a \leq b \leq c$ we must have $b > 2$, else (a,b,c) is not hyperbolic. The map is nevertheless uniquely determined, since $\delta_a\delta_b\delta_c = 1$.) □

Section 2.3

Principal congruence subgroups

We now define congruence subgroups. Let $\mathfrak{N} \subseteq \mathbb{Z}_E$ be a nonzero ideal. Then reducing elements modulo $\mathfrak{N}$, as in (2.2.4) we obtain a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \Gamma^{(2)}(\mathfrak{N}) \arrow[r] \arrow[d, hook] & \Delta^{(2)} \arrow[r] \arrow[d, hook] & (\Lambda/\mathfrak{N}\Lambda)^1/\{\pm 1\} \arrow[d, hook] \\
1 \arrow[r] & \Gamma(\mathfrak{N}) \arrow[r] & \Delta \arrow[r, "\varpi_{\mathfrak{N}}"] & (\mathcal{O}/\mathfrak{N}\mathcal{O})^1/\{\pm 1\}
\end{tikzcd} \tag{2.3.1}$$

but now with kernels in the rows: in particular, we have a group homomorphism

$$\varpi_{\mathfrak{N}} \colon \Delta \to (\mathcal{O}/\mathfrak{N}\mathcal{O})^1/\{\pm 1\} \tag{2.3.2}$$

with kernel

$$\Gamma(\mathfrak{N}) := \ker \varpi_{\mathfrak{N}} = \{\delta \in \Delta : \delta \equiv \pm 1 \pmod{\mathfrak{N}\mathcal{O}}\} \trianglelefteq \Delta \tag{2.3.3}$$

called the principal congruence subgroup of level $\mathfrak{N}$.

We define congruence subgroups of Δ to be those that contain a principal congruence subgroup.

Remark 2.3.4. One could work more generally with ideals of $\mathbb{Z}_F$ instead, arriving at the same definition of congruence subgroups but with a different notion of level. In light of what follows, especially the robust failure of $\varpi_{\mathfrak{N}}$ to be surjective, we prefer to work with levels in $\mathbb{Z}_E$.

Since Δ normalizes $\Delta^{(2)}$ and therefore Λ and $\mathfrak{N}\Lambda$, there is descent to the normalizer as in Lemma 2.2.5. However, the precise description of $\Gamma(\mathfrak{N})$ depends on the ramification behavior of the primes dividing $\mathfrak{N}$ in the extension $F\,|\,E$ and in the algebras A and B (and this already introduces some subtleties when $\mathfrak{N}$ is composite). We pursue this in Theorem 3.3.1 and Theorem 5.2.8.

Section 2.4

Triangular modular curves, first encounter

A triangular modular curve is a quotient of the (completed) upper half-plane by a congruence subgroup of a triangle group. For example

$$X(\mathfrak{N}) = X(a,b,c;\mathfrak{N}) := \Gamma(\mathfrak{N})\backslash\mathcal{H} \tag{2.4.1}$$

are called the principal triangular modular curves.

Example 2.4.2. We recall from Example 2.1.3 that $\Delta(2,3,\infty) \simeq \mathrm{PSL}_2(\mathbb{Z})$. We also note that $E(2,3,\infty) = \mathbb{Q}$, so ideals of $\mathbb{Z} = \mathbb{Z}_{\mathbb{Q}}$ can be represented by positive integers N. From this, we recover classical modular curves:

$$X(N) = X(2,3,\infty;N\mathbb{Z}).$$

Looking forward to chapter 3 and following the analogy with modular curves, we will define Borel–type congruence subgroups $\Gamma_0(a,b,c;\mathfrak{N})$ and $\Gamma_1(a,b,c;\mathfrak{N})$ and get corresponding triangular modular curves $X_0(a,b,c;\mathfrak{N})$ and $X_1(a,b,c;\mathfrak{N})$.

Example 2.4.3. Let $\mathfrak{p}_7$ be a prime of $\mathbb{Z}_{E(2,3,7)}$ above 7. The curve $X(2,3,7;\mathfrak{p}_7)$ is the Klein quartic, a genus 3 curve [21, section 10]. One of the most striking properties of this curve is that its automorphism group has size 168, the maximum for its genus. For more on this fact and the arithmetic properties of the curve, see [37].

Chapter 3

Triangular modular curves

We now study triangular modular curves that generalize classical modular curves. The main results of the chapter are Proposition 3.2.6, where we define the relevant matrix representation of Δ; and Theorem 3.3.1, describing its image building on work of Clark–Voight [21]. Throughout, we retain our notation from the previous chapter. This chapter is all joint work with John Voight published in [35].

Section 3.1

Galois case

Before proceeding, as a warmup we consider the curves $X(a,b,c;\mathfrak{N})$ defined in section 2.4 corresponding to principal congruence subgroups. The fundamental domain of the action of $\Delta(a,b,c)$ is two copies of the triangle with angles $\pi/a, \pi/b, \pi/c$ glued together, so $X(a,b,c) \simeq \mathbb{P}^1$. By construction, there is a cover

$$X(a,b,c;\mathfrak{N}) \to X(a,b,c) \simeq \mathbb{P}^1.$$

It also follows from the construction that this is a Galois Belyi map.

Quite generally, for any Galois (Belyi) map with group G, the ramification indices above each ramification point are equal. Without loss of generality, we may suppose that a, b, c are also the orders of the ramification points. Thus the Riemann-Hurwitz formula gives

$$2g(X) - 2 = -2(\#G) + \sum_{s=a,b,c} \frac{\#G}{s}(s-1) \tag{3.1.1}$$

which simplifies to

$$g(X) = 1 - \frac{\#G}{2}\chi(a,b,c). \tag{3.1.2}$$

From this genus formula and Lemma 2.1.6, we can conclude that, for any fixed genus $g_0 \geq 0$, there are finitely many hyperbolic G-Galois Belyi maps with genus g_0.

Following the analogy with modular curves, we are of course interested in the special case where

$$G = \Gamma(\mathfrak{p})\backslash\Delta \simeq \mathrm{PXL}_2(\mathbb{F}_\mathfrak{p})$$

where $\mathbb{F}_\mathfrak{p} := \mathbb{Z}_E/\mathfrak{p}$ is the residue field and $\mathrm{PXL}_2(\mathbb{F}_\mathfrak{p})$ denotes either $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ or $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$. (The major task in the next section is to precisely investigate this arithmetically.) Plugging $G = \mathrm{PXL}_2(\mathbb{F}_q)$ into the above:

$$84(g_0 - 1) \geq \#G = q(q+1)(q-1) \cdot \begin{cases} 1/2, & \text{if } G = \mathrm{PSL}_2(\mathbb{F}_q) \text{ and } q \text{ is odd;} \\ 1, & \text{otherwise.} \end{cases}$$

Thus, there are no curves $X(a,b,c;\mathfrak{p})$ of genus at most 1. For genus 2, we can use the inequality to see that q must be less than 6, so $\#G \leq 60$ and, if $g(X(a,b,c;\mathfrak{p})) = 2$, then

$$-\frac{1}{\chi(a,b,c)} \leq 30.$$

This inequality implies that $a \leq b \leq c \leq 7$ and, by checking the genera of these possibilities with (3.1.2), we conclude that there are no curves $X(a,b,c;\mathfrak{p})$ of genus 2.

In fact, the smallest genus for a hyperbolic triple with $a,b,c \in \mathbb{Z}_{\geq 2}$ is genus 3 for $(a,b,c) = (2,3,7)$, yielding the famed Klein quartic curve as in Example 2.4.3. More generally, see Clark–Voight [21, Table 10.5] for examples up to genus 24.

Section 3.2

Congruence subgroups: matrix case

We return to (2.3.1), and identify matrix groups. The goal is to define congruence subgroups of triangle groups that "come from matrices", just like with classical modular curves. We recall the setup from section 2.2. Let B be the F-subalgebra $F\langle\Delta\rangle \leq M_2(\mathbb{R})$ and we consider $\mathcal{O} = \mathbb{Z}_F\langle\Delta\rangle$ a $\mathbb{Z}_F$-order in B. Recalling (2.2.3), we first suppose that $\beta = \operatorname{discrd}\mathcal{O}$ is coprime to $\mathfrak{N}$, so all primes $\mathfrak{p} \mid \mathfrak{N}$ are unramified in B but more strongly we have $(\mathcal{O}/\mathfrak{N}\mathcal{O})^1/\{\pm 1\} \simeq \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)/\{\pm 1\}$.

We recall that $A = E\langle\Delta^{(2)}\rangle$ is a quaternion algebra, containing the $\mathbb{Z}_E$-order $\Lambda = \mathbb{Z}_E\langle\Delta^{(2)}\rangle$. For this order, we have Lemma 2.1.9: given a,b,c, we can compute its $\mathbb{Z}_E$-module span in A and therefore a $\mathbb{Z}_E$-pseudobasis for Λ, hence its reduced discriminant. Since $\Lambda\mathbb{Z}_F \subseteq \mathcal{O}$, we have $\beta \mid \operatorname{discrd}(\Lambda)$ [21, Corollary 5.17].

So we make the stronger assumption that $\mathfrak{N}$ is coprime to $\operatorname{discrd}(\Lambda)$. Then from

(2.2.4) we get

$$\begin{tikzcd}
\Delta^{(2)} \arrow[r] \arrow[d, hook] & (\Lambda/\mathfrak{N}\Lambda)^1/\{\pm 1\} \arrow[r, "\sim"] \arrow[d, hook] & \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \\
\Delta \arrow[r, "\pi_{\mathfrak{N}}"] & (\mathcal{O}/\mathfrak{N}\mathcal{O})^1/\{\pm 1\} \arrow[r, "\sim"] & \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)/\{\pm 1\}
\end{tikzcd} \qquad (3.2.1)$$

To descend the bottom map to the normalizer as in Lemma 2.2.5, we restrict our scope taking $\mathfrak{N} = \mathfrak{p}$ prime and work just a little bit more.

Let

$$\mathbb{Z}_{E,(\mathfrak{p})} := \{\alpha \in E : \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0\} \subseteq E \tag{3.2.2}$$

be the localization of $\mathbb{Z}_E$ at the ideal $\mathfrak{p}$ (all elements not in $\mathfrak{p}$ become units).

Lemma 3.2.3. *Suppose that $\mathfrak{p} \nmid \mathfrak{d}_{F|E}$. Then for $s = a, b, c$, we can write*

$$\lambda_s + 2 = \upsilon_s \theta_s^2 \in E^\times \tag{3.2.4}$$

with:

- $\upsilon_s \in \mathbb{Z}_{E,(\mathfrak{p})}^\times$, *well-defined up to multiplication by an element of* $\mathbb{Z}_{E,(\mathfrak{p})}^{\times 2}$, *i.e., up to the square of an element of* $\mathbb{Z}_{E,(\mathfrak{p})}^\times$, *and*
- $\theta_s \in E^\times$, *well-defined up to* $\mathbb{Z}_{E,(\mathfrak{p})}^\times$.

If $\mathfrak{p}$ is coprime to $2abc$, then we may take $\theta_s = 1$ and $\upsilon_s = \lambda_s + 2$.

Moreover, the prime $\mathfrak{p}$ (necessarily unramified in F) splits completely in F if and only if the Kronecker symbols $(\upsilon_s \,|\, \mathfrak{p}) = 1$ are trivial for all $s = a, b, c$.

Proof. First, a bit of generality: for $\alpha \in E^\times$ with even valuation at all primes $\mathfrak{p} \mid \mathfrak{N}$, by weak approximation in E we can write

$$\alpha = \upsilon\theta^2 \in E^\times \tag{3.2.5}$$

with υ, θ as in the statement of the lemma.

Now to apply this, we observe that $F = E(\lambda_{2a}, \lambda_{2b}, \lambda_{2c})$ and recall that $\lambda_{2s}^2 = \lambda_s + 2$. By hypothesis, we have $\mathfrak{p} \nmid \mathfrak{d}_{F|E}$; in particular the elements $\lambda_s + 2$ must have even (nonnegative) valuation at $\mathfrak{p}$. Thus (3.2.5) applies, giving (3.2.4). The final statement follows from the usual splitting criterion in quadratic fields. □

We obtain the following result.

Proposition 3.2.6. *Suppose that* $\mathfrak{p} \nmid \operatorname{discrd}(\Lambda)\mathfrak{d}_{F|E}$. *Then there is a commutative diagram*

$$\begin{tikzcd}
\Delta^{(2)} \arrow[r] \arrow[d, hook] & \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{p})/\{\pm 1\} \arrow[d] \\
\Delta \arrow[r, "\pi_{\mathfrak{N}}"] & \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p})
\end{tikzcd} \tag{3.2.7}$$

and the map $\pi_{\mathfrak{N}} \colon \Delta \to \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$ *factors through* $\varpi_{\mathfrak{N}}$.

We let $G_{\mathfrak{p}} := \pi_{\mathfrak{p}}(\Delta) \leq \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p})$ be the image of $\pi_{\mathfrak{p}}$.

Proof. Combine (3.2.1) with Lemma 3.2.3. □

Remark 3.2.8. A similar argument works when $\mathfrak{N}$ is composite; however the right-hand vertical map $\mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \to \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$ may no longer be injective when $\mathfrak{N}$ is composite. This leads to certain ambiguities about the definition which we will return to in chapter 5.

Section 3.3

Image and admissibility

Theorem 3.3.1 (Clark–Voight)**.** *We have* $\pi_{\mathfrak{p}}(G_{\mathfrak{p}}^{(2)}) = \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{p})$ *and*

$$\pi_{\mathfrak{p}}(G_{\mathfrak{p}}) = \mathrm{PXL}_2(\mathbb{Z}_E/\mathfrak{p})$$

where PXL_2 *denotes* PSL_2 *or* PGL_2 *according as* $\mathfrak{p}$ *splits in* $F \supseteq E$ *or not.*

Proof. We refer to Clark–Voight [21, Theorem A] for the case where $\mathfrak{p} \nmid 2abc$; but examining the argument given [21, Remark 5.24, proof of Theorem 9.1] in light of the above, we see that it extends when $\mathfrak{p} \nmid \operatorname{discrd}(\Lambda)\beta\mathfrak{d}_{F|E}$. □

It can and does happen that two different triangular modular curves are isomorphic (as curves and as covers of $\mathbb{P}^1$). The issue is simply that in the homomorphism $\pi_{\mathfrak{N}}$ from $\Delta(a, b, c)$ to a matrix group, the generators δ_s need not have order s in the image (for $s = a, b, c$). In other words, the reduction homomorphism factors through a triangle group with a smaller triple. This happens for example when $s = \infty$, as the order of $\pi_{\mathfrak{N}}(\delta_s)$ is always finite! To illustrate this phenomena, we present the following example.

Example 3.3.2. Consider the triples $(2, 3, c)$ with $c = p^k$, where $k \geq 1$ and $p \geq 5$ is prime. Then

$$E_k := E(2, 3, c) = F(2, 3, c) = \mathbb{Q}(\lambda_{2c}) = \mathbb{Q}(\zeta_{2c})^+ \tag{3.3.3}$$

and $\beta(2, 3, c) = \lambda_c - 1 \in \mathbb{Z}_{E_k}^\times$. The prime p is totally ramified in F and $\mathfrak{p}_k$ is the unique prime ideal above p, so $\mathbb{F}_{\mathfrak{p}_k} \simeq \mathbb{F}_p$. Thus $X(2, 3, p^k; \mathfrak{p}_k) \simeq X(2, 3, p; \mathfrak{p}_1)$.

To avoid this redundancy, we make the following definition.

Definition 3.3.4. Given a triple (a,b,c), a prime ideal $\mathfrak{p} \subseteq \mathbb{Z}_{E(a,b,c)}$ is admissible for (a,b,c) if

- $\mathfrak{p} \nmid \operatorname{discrd}(\Lambda)\mathfrak{d}_{F|E}$, and
- the order of $\pi_{\mathfrak{p}}(\delta_s)$ is equal to s for all $s = a,b,c$.

When we consider inadmissible triples, it is useful to talk about the order of $\pi_{\mathfrak{p}}(\delta_s)$, and we will denote this order by $s^\sharp$ for $s \in \{a,b,c\}$.

Proposition 3.3.5 ([21]). *Let (a,b,c) be a hyperbolic triple with $a,b,c \in \mathbb{Z} \cup \{\infty\}$ and let $\mathfrak{p}$ be a prime ideal of $E(a,b,c)$ with p the prime number below $\mathfrak{p}$. Let $s \in \{a,b,c\}$, then*

$$s^\sharp = \begin{cases} s & \text{if } s \neq \infty \text{ and } p \nmid s; \\ s_0 & \text{if } s \neq \infty \text{ and } s = s_0 p^k \text{ with } s_0 \neq 1 \text{ and } k \geq 1; \\ p & \text{otherwise.} \end{cases}$$

Proof. Follows from the proof of [21, Theorem 9.1] (not mentioned in the statement, but proven as a claim in the course of the proof). When $p \nmid s$ or $s = s_0 p^k$ with , the order of the matrix is uniquely determined by its trace. If $s = s_0 p^k$ with $s_0 \neq 1$ and $k \geq 1$, then $\lambda_2 s \equiv \lambda_2 s_0 \pmod{\mathfrak{p}}$ and the order must be s_0. Otherwise, the element must be unipotent, so it must have order p. □

Remark 3.3.6. When studying triangular modular curves, we can focus on admissible triples without loss of generality. Let (a,b,c) be an inadmissible triple, let $\mathfrak{p} \subseteq \mathbb{Z}_{E(a,b,c)}$ be a prime ideal, and assume that $\mathfrak{p} \nmid \operatorname{discrd}(\Lambda)\mathfrak{d}_{F|E}$. Then, there is a unique admissible triple $(a^\sharp, b^\sharp, c^\sharp)$, and a prime ideal $\mathfrak{p}' \subseteq \mathbb{Z}_{E(a^\sharp,b^\sharp,c^\sharp)}$ such that the cover $X(a,b,c;\mathfrak{p}) \to \mathbb{P}^1$ is isomorphic to $X(a^\sharp,b^\sharp,c^\sharp;\mathfrak{p}') \to \mathbb{P}^1$.

Section 3.4

Hyperbolic triples reducing to non-hyperbolic triples

In considering admissible triples, we may lose the hypothesis that (a, b, c) is hyperbolic; however, this situation is easy to characterize. We note that in most cases, these groups do not contain $\mathrm{PSL}_2(\mathbb{F}_q)$, so they are not considered in this manuscript.

Proposition 3.4.1. *Suppose $(a^\sharp, b^\sharp, c^\sharp)$ is not hyperbolic. Then $(a, b, c; p, q)$ is one of the elements listed in the following table. In the table, p lies below $\mathfrak{p}$ and q is the residue field degree of $\mathfrak{p}$. In addition, we distinguish the Galois groups $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ by writing 1 and -1 in the PXL column, respectively.*

$\boldsymbol{(a,b,c)}$	***conditions***	$\boldsymbol{p}$	$\boldsymbol{q}$	**PXL**	$\boldsymbol{E(a^\sharp,b^\sharp,c^\sharp)}$
$(2^{k_a}, 2^{k_b}, 3\cdot 2^{k_c})$, $(3\cdot 2^{k_c}, \infty, \infty)$, $(2^{k_a}, 3\cdot 2^{k_c}, \infty)$	$1 \le k_a < k_b \le k_c$	2	2	1	$\mathbb{Q}$
$(3^{k_a}, 3^{k_b}, 3^{k_c})$, $(3^{k_a}, \infty, \infty)$, $(3^{k_a}, 3^{k_b}, \infty)$, (∞, ∞, ∞)	$1 \le k_a \le k_b < k_c$	3	3	1	$\mathbb{Q}$
$(2\cdot 3^{k_a}, 3^{k_b}, 3^{k_c})$, $(2\cdot 3^{k_a}, 3^{k_b}, \infty)$, $(2\cdot 3^{k_a}, \infty, \infty)$	$1 \le k_b \le k_c,\ k_ak_bk_c \neq 1$	3	3	1	$\mathbb{Q}$
$(2\cdot 3^{k_a}, 3^{k_b}, 4\cdot 3^{k_c})$, $(2\cdot 3^{k_a}, 4\cdot 3^{k_b}, \infty)$	$1 \le k_b,\ k_ak_bk_c \neq 1$	3	3	-1	$\mathbb{Q}$
$(2^{k_a}, 3\cdot 2^{k_b}, 5\cdot 2^{k_c})$, $(3\cdot 2^{k_b}, 5\cdot 2^{k_c}, \infty)$	$1 \le k_a,\ k_ak_bk_c \neq 1$	2	4	1	$\mathbb{Q}(\sqrt{5})$
$(2\cdot 5^{k_a}, 3\cdot 5^{k_b}, 5^{k_c})$, $(2\cdot 5^{k_a}, 3\cdot 5^{k_b}, \infty)$	$1 \le k_c,\ k_ak_bk_c \neq 1$	5	5	1	$\mathbb{Q}(\sqrt{5})$

(3.4.2)

Furthermore, the curves $X(a,b,c;\mathfrak{p})$ with $(a,b,c;\mathfrak{p})$ as above all have genus 0.

Proof. We make a case by case study. The only triples $(a,b,c) \in (\mathbb{Z}_{\ge 0} \cup \{\infty\})^3$ that are not hyperbolic are

$$(2,2,n) \text{ for } n>1,\ (2,3,3),\ (2,3,4),\ (2,3,5),\ (2,3,6),\ (2,4,4),\ \text{ or } (3,3,3).$$

Assume first that $(a^\sharp, b^\sharp, c^\sharp) = (2,2,c)$ for $c > 1$. The image of $\pi_{\mathfrak{p}}\colon \Delta(2,2,c) \to \mathrm{PGL}_2(\mathbb{F}_q)$ must be dihedral because of the presentation of $\Delta(2,2,c)$. The only dihedral group that is isomorphic to $\mathrm{PXL}_2(\mathbb{F}_q)$ for any q is $D_6 \simeq \mathrm{PSL}_2(\mathbb{F}_2)$. Thus, we only have the triple $(a^\sharp, b^\sharp, c^\sharp) = (2,2,3)$ and prime $\mathfrak{p}_2$.

The group $\Delta(2,3,6)$ is solvable since it fits in the exact sequence:

$$1 \to \mathbb{Z}^2 \to \Delta(2,3,6) \to \mathbb{Z}/6\mathbb{Z} \to 1.$$

The only solvable groups of the form $\mathrm{PXL}_2(\mathbb{F}_q)$ are $S_4 \simeq \mathrm{PGL}_2(\mathbb{F}_3)$ and $A_4 \simeq \mathrm{PSL}_2(\mathbb{F}_3)$. The triple $(2,3,6)$ is inadmissible for $q = 2$ or $q = 3$, so $(2,3,6)$ does not arise from any prime ideal $\mathfrak{p}$. With the same analysis, we can rule out $(2,4,4)$. We also have that the group $\Delta(3,3,3)$ is solvable. Hence, the image of $\pi_{\mathfrak{p}} : \Delta(3,3,3) \to \mathrm{PXL}_2(\mathbb{F}_q)$ must be solvable. The only solvable groups of this form are $A_4 \simeq \mathrm{PSL}_2(\mathbb{F}_3)$ and $S_4 \simeq \mathrm{PGL}_2(\mathbb{F}_3)$. Thus, the only option is that $\mathfrak{p}$ is a prime above 3 with residue field $\mathbb{F}_3$.

The last triples to consider are $(2,3,3)$, $(2,3,4)$ and $(2,3,5)$. These triples are all *exceptional*. The only projective linear groups that can arise from exceptional triples [21, Remark 8.4] are the following:

$$\mathrm{PSL}_2(\mathbb{F}_3), \mathrm{PGL}_2(\mathbb{F}_3), \mathrm{PGL}_2(\mathbb{F}_4), \mathrm{PSL}_2(\mathbb{F}_5).$$

We now use this fact to finish the analysis. When $(a^\sharp, b^\sharp, c^\sharp) = (2,3,3)$, the admissible prime ideals $\mathfrak{p}$ have residue field degree $3, 4$, and 5. The field $E(2,3,3)$ is the rational field, so $\mathbb{Z}_E/\mathfrak{p}_2 \simeq \mathbb{F}_2$. In addition, the ideal $2\mathbb{Z}_E$ is totally ramified in any field $E(2 \cdot 2^{k_a}, 3 \cdot 2^{k_b}, 3 \cdot 2^{k_c})$, so $q \neq 4$. The only options then are $q = 3$ and $q = 5$. A quick Magma [17] calculation shows that elements with these orders cannot generate $\mathrm{PSL}_2(\mathbb{F}_5)$.

Similarly, when $(a^\sharp, b^\sharp, c^\sharp) = (2,3,4)$, the only possibilities for q with image containing $\mathrm{PSL}_2(\mathbb{F}_q)$ and admissible for $\mathfrak{p}$ are $q = 3$ or $q = 5$. However, the field $E(2,3,4)$ is the rational field and 5 is inert in F, so we would have $G_{5\mathbb{Z}_E} \simeq \mathrm{PGL}_2(\mathbb{F}_5)$, which is not on the list of possible groups. The same happens for $(a^\sharp, b^\sharp, c^\sharp) = (2,3,5)$; the options of q for an admissible prime $\mathfrak{p}$ are $q = 2, 3, 4, 5$. The ideal $2\mathbb{Z}_E$ is inert in $E(2,3,5)$, an extension of $\mathbb{Q}$ of degree 2, thus $q = 2$ is not possible. The ideal $3\mathbb{Z}_E$ is also inert in $E(2,3,5)$, so an isomorphism with $\mathrm{PXL}_2(\mathbb{F}_3)$ is not possible. The only options for q are $q = 4$ and $q = 5$.

For all of the possible triples $(a^\sharp, b^\sharp, c^\sharp)$ and primes $\mathfrak{p}$ described above, we certify that such map is possible by exhibiting passports for each curve. We then describe the options for (a, b, c) using Proposition 3.3.5. Finally, we use (3.1.2) to compute the genus of each of these curves, finding that they all have genus 0. □

Section 3.5

Borel-type subgroups

Now that we found a way to going back to matrices, we are ready to define congruence subgroups that mirror the constructions from classical modular curves. Let

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z}_E/\mathfrak{p} \text{ and } ad \in (\mathbb{Z}_E/\mathfrak{p})^\times \right\} \leq \mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{p}) \tag{3.5.1}$$

be the upper-triangular matrices in $\mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{p})$, and let $H_{0,\mathfrak{p}}$ be its image in the projection to $\mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p})$. Similarly, let

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}_E/\mathfrak{p} \right\} \leq \mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{p}) \tag{3.5.2}$$

be the upper unipotent subgroup and $H_{1,\mathfrak{p}}$ again its image in $\mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p})$.

We then define the subgroups

$$\begin{aligned} \Gamma_0(a,b,c;\mathfrak{p}) &:= \varphi_{\mathfrak{p}}^{-1}(H_{0,\mathfrak{p}}), \\ \Gamma_1(a,b,c;\mathfrak{p}) &:= \varphi_{\mathfrak{p}}^{-1}(H_{1,\mathfrak{p}}). \end{aligned} \tag{3.5.3}$$

and the corresponding quotients

$$\begin{aligned} X_0(a,b,c;\mathfrak{p}) &:= \Gamma_0(a,b,c;\mathfrak{p})\backslash\mathcal{H} = H_{0,\mathfrak{p}}\backslash X'(a,b,c;\mathfrak{p}) \\ X_1(a,b,c;\mathfrak{p}) &:= \Gamma_1(a,b,c;\mathfrak{p})\backslash\mathcal{H} = H_{1,\mathfrak{p}}\backslash X(a,b,c;\mathfrak{p}). \end{aligned} \tag{3.5.4}$$

Then we have natural quotient maps

$$X(a,b,c;\mathfrak{p}) \to X_1(a,b,c;\mathfrak{p}) \to X_0(a,b,c;\mathfrak{p}) \to X(a,b,c;1) \simeq \mathbb{P}^1. \tag{3.5.5}$$

These curves will be our main object of study in the following chapter.

Chapter 4

Triangular modular curves of prime level

In this chapter, we exhibit a formula for the genus of the Borel-type triangular modular curves $X_0(a,b,c;\mathfrak{p})$ for $\mathfrak{p}$ prime (see Theorem 4.2.4). Using this formula, we show that there are only finitely many such curves with bounded genus in Corollary 4.4.6, which is the main result of the chapter. We then present an algorithm that enumerates all such curves of bounded genus (see Algorithm 4.5.2). We then build up with these ideas to provide similar results for curves $X_1(a,b,c;\mathfrak{p})$. This chapter is from joint work with John Voight published in [35].

Section 4.1

Setup

Let (a,b,c) be a hyperbolic triple and $\mathfrak{p}$ be an admissible prime of $E = E(a,b,c)$ with residue field $\mathbb{F}_\mathfrak{p}$. Let $q := \#\mathbb{F}_\mathfrak{p}$, so $\mathbb{F}_\mathfrak{p} \simeq \mathbb{F}_q$. Because E is Galois over $\mathbb{Q}$, all primes $\mathfrak{p}$ have the same ramification and splitting type; it follows that the genus of $X_0(a,b,c;\mathfrak{p})$

only depends on the prime number $p \in \mathbb{Z}$ below $\mathfrak{p}$ (and the inertial degree of $\mathfrak{p}$ over p), i.e. only on q.

Let $G := G_{\mathfrak{p}}$ be as in Theorem 3.3.1. Then the group $H_0 = H_{0,\mathfrak{p}}$ consists of the image in G of the upper-triangular matrices of $\mathrm{SL}_2(\mathbb{F}_q)$ or $\mathrm{GL}_2(\mathbb{F}_q)$, depending on G. By construction, the curves $X_0(a, b, c; \mathfrak{p})$ and $X(a, b, c; \mathfrak{p})$ fit in the following diagram.

$$\begin{tikzcd}
X(a,b,c;\mathfrak{p}) \arrow[dd, "G"'] \arrow[dr, "H_0"] & \\
 & X_0(a,b,c;\mathfrak{p}) \arrow[dl] \\
\mathbb{P}^1 &
\end{tikzcd}$$

We first compute the index $[G : H_0]$, which corresponds to the degree of the cover $X_0(a, b, c; \mathfrak{p}) \to \mathbb{P}^1$. If $G = \mathrm{PGL}_2(\mathbb{F}_q)$, up to multiplication by a scalar matrix, it is possible to choose representatives of elements of H_0 that have 1 on the first entry of the matrix. Thus, $\#H_0 = q(q - 1)$ and $[G : H_0] = q + 1$. When q is even, we have an isomorphism $\mathrm{PSL}_2(\mathbb{F}_q) \simeq \mathrm{PGL}_2(\mathbb{F}_q)$, so the index $[G : H_0]$ is the same as above. Finally, if $G = \mathrm{PSL}_2(\mathbb{F}_q)$ with q odd, then representatives can be chosen to have 1 on the first entry of the matrix as above. Also, the upper triangular matrices are defined up to multiplication by -1. Hence $\#H_0 = \frac{1}{2}q(q - 1)$ and $[G : H_0] = q + 1$.

Via the projection of the first column of the matrix to $\mathbb{P}^1(\mathbb{F}_q)$, the set of cosets G/H_0 is naturally in bijection with $\mathbb{P}^1(\mathbb{F}_q)$. With this bijection, the action of $\pi_{\mathfrak{p}}(\Delta)$ on G/H_0 becomes simply matrix multiplication. The ramification of the cover of $\mathbb{P}^1$ coming from $X_0(a, b, c; p)$ then depends on the cycle decomposition of the corresponding elements (in G) as an element of $\mathrm{Sym}(\mathbb{P}^1(\mathbb{F}_q)) \simeq S_{q+1}$.

Section 4.2

Cycle structure and genus formula

The following lemma describes the cycle structure defined in the previous section. The main feature of this Lemma is that it only uses the order of the elements. Recall we write PXL_2 for either PSL_2 or PGL_2.

Lemma 4.2.1. *Let $G = \mathrm{PXL}_2(\mathbb{F}_q)$ with $q = p^r$ for a prime number p. Let $\overline{\sigma}_s \in G$ have order $s \geq 2$, and if $s = 2$ suppose $p = 2$. Then the action of $\overline{\sigma}_s$ on $\mathbb{P}^1(\mathbb{F}_q)$ has:*

(i) *two fixed points and $(q-1)/s$ orbits of length s if $s \mid (q-1)$;*

(ii) *one fixed point and q/p orbits of length p if $s = p$ (this is the case when $s \mid q$); and*

(iii) *(no fixed points and) $(q+1)/s$ orbits of length s if $s \mid (q+1)$.*

Proof. We note that each class in G is represented by matrices that are diagonalizable over $\mathbb{F}_q$, diagonalizable only over $\mathbb{F}_{q^2}$, or not diagonalizable. We prove the Lemma by studying in detail each case. Let σ_s be an element of $\mathrm{GL}_2(\mathbb{F}_q)$ whose projection to G is $\overline{\sigma}_s$. If σ_s is diagonalizable, then we say that $\overline{\sigma}_s$ is split semisimple, and σ_s is conjugate to say the diagonal matrix with diagonal $[u, v]$. We must have $u \neq v$ because otherwise $\overline{\sigma}_s$ would be the identity in G, contradicting that $s \geq 2$. The order of $\overline{\sigma}_s$ is s, so s is the order of uv^{-1} in $\mathbb{F}_q^\times$. To find the orbits of the action of $\overline{\sigma}_s$ on $\mathbb{P}^1(\mathbb{F}_q)$, we use that

$$\begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \begin{pmatrix} 1 \\ .. \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ .. \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \begin{pmatrix} x \\ .. \\ 1 \end{pmatrix} = \begin{pmatrix} uv^{-1}x \\ .. \\ 1 \end{pmatrix},$$

for any $x \in \mathbb{F}_q$. Hence, the action of $\overline{\sigma}_s$ has two fixed points: $\begin{pmatrix}1\\ \cdot\cdot\\ 0\end{pmatrix}$ and $\begin{pmatrix}0\\ \cdot\cdot\\ 1\end{pmatrix}$, and $(q-1)/s$ orbits with s elements.

The element $\overline{\sigma}_s$ is unipotent if and only if it is conjugate to an upper triangular matrix with diagonal values equal to 1 and upper-right entry $u \in \mathbb{F}_q^{\times}$. This is the case when the characteristic polynomial of σ_s has two equal roots and σ_s is not diagonalizable over $\mathbb{F}_q^2$. This happens if and only if $s = p$. In this case, we have

$$\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\begin{pmatrix}1\\ \cdot\cdot\\ 0\end{pmatrix} = \begin{pmatrix}1\\ \cdot\cdot\\ 0\end{pmatrix}, \qquad \begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\begin{pmatrix}x\\ \cdot\cdot\\ 1\end{pmatrix} = \begin{pmatrix}x+u\\ \cdot\cdot\\ 1\end{pmatrix},$$

where $x \in \mathbb{F}_q$. There is only one fixed point and there are q/p orbits of size p.

If the characteristic polynomial of σ_s does not split in $\mathbb{F}_q$, we call $\overline{\sigma}_s$ non-split semisimple. The action of $\overline{\sigma}_s$ has no fixed points because this would imply that σ_s has an eigenvector. The splitting field of the characteristic polynomial of σ_s is $\mathbb{F}_{q^2}$. Let $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be the roots of this polynomial. Then σ_s is conjugate to the diagonal matrix $[\alpha_1, \alpha_2]$ with $\sigma_s = T^{-1}[\alpha_1, \alpha_2]T$ for some invertible matrix T. For all $m \in \mathbb{N}$ such that $\overline{\sigma}_s^m$ fixes $(x : y)^t \in \mathbb{P}^1(\mathbb{F}_q)$, we have that

$$\begin{pmatrix}\alpha_1^m & 0\\ 0 & \alpha_2^m\end{pmatrix}\left(T\begin{pmatrix}x\\ \cdot\cdot\\ y\end{pmatrix}\right) = \left(T\begin{pmatrix}x\\ \cdot\cdot\\ y\end{pmatrix}\right).$$

From the analysis of the split semisimple case, we conclude that every orbit has length s. Thus, the action of σ_s on $\mathbb{P}^1(\mathbb{F}_q)$ has $(q+1)/s$ orbits of length s. □

The previous lemma does not consider the case when $s = 2$ and q is odd. The ambiguity arises since if $s = 2$ then $s \mid (q-1)$ and $s \mid (q+1)$, so $\overline{\sigma}_2$ can be either split or non-split (semisimple).

Example 4.2.2. For $(a,b,c) = (2,3,8)$ and $G = \mathrm{PGL}_2(\mathbb{F}_7)$, we have σ_2 split and it belongs to the conjugacy class of

$$\begin{pmatrix} 6 & 0 \\ 0 & 1 \end{pmatrix}.$$

On the other hand, for $(2,6,6)$ and $G = \mathrm{PGL}_2(\mathbb{F}_7)$, we have σ_2 non-split, belonging to the conjugacy class of

$$\begin{pmatrix} 0 & 6 \\ 1 & 0 \end{pmatrix}.$$

The following lemma solves this problem when $G = \mathrm{PSL}_2(\mathbb{F}_q)$.

Lemma 4.2.3. *Let $G = \mathrm{PSL}_2(\mathbb{F}_q)$ with q odd, and let $\overline{\sigma}_2 \in G$ be an element of order 2. Then the action of $\overline{\sigma}_2$ on $\mathbb{P}^1(\mathbb{F}_q)$ has:*

(i) *two fixed points and $(q-1)/2$ orbits of size 2 if -1 is a square modulo q; and*

(ii) *(no fixed points and) $(q+1)/2$ orbits of size 2, otherwise.*

Proof. Let $\overline{\sigma}_2$ be a matrix of order 2 in $\mathrm{PSL}_2(\mathbb{F}_q)$. Pick a lift $\sigma_2 \in \mathrm{SL}_2(\mathbb{F}_q)$ of $\overline{\sigma}_2$. Because σ_2^4 is the identity, its characteristic polynomial must be a quadratic polynomial dividing $x^4 - 1$. In addition, the constant of this polynomial must be 1 since this is the determinant of σ_2. The only possibility for such a polynomial is $x^2 + 1$. If $-1 \in \mathbb{F}_q^{\times 2}$, then this characteristic polynomial splits with distinct roots, so we are in the split semisimple case of Lemma 4.2.1. Otherwise, -1 is not a square and we are in the non-split semisimple case. □

Now we are ready to give a formula for the genus g of $X_0(a,b,c;p)$. For $x \in \mathbb{R}$, we write $\lfloor x \rceil$ for the rounding down of x, so $\lfloor 3/2 \rceil = 1$.

Theorem 4.2.4. *Let (a,b,c) be a hyperbolic admissible triple and $\mathfrak{p}$ be a prime of E above a rational prime p. Then the genus of $X_0(a,b,c;\mathfrak{p})$ is given by*

$$g(X_0(a,b,c;\mathfrak{p})) = -q + \frac{1}{2}\sum_{s\in\{a,b,c\}} \left\lfloor \frac{q}{s} \right\rceil (s-1) + \epsilon(a,b,c;\mathfrak{p}), \tag{4.2.5}$$

where q is as before and $\epsilon(a,b,c;\mathfrak{p}) \in \{0,1/2\}$ is uniquely determined by the genus $g(X_0(a,b,c;\mathfrak{p}))$ being an integer. Moreover, we have $\epsilon(a,b,c;\mathfrak{p}) = 0$ unless $a = 2$ and q is odd.

In the latter case ($a = 2$ and q odd), Lemma 4.2.3 implies that when $G = \mathrm{PSL}_2(\mathbb{F}_q)$, we have $\epsilon(a,b,c;\mathfrak{p}) = 0$ if and only if $q \equiv 1 \pmod 4$ (case (i)).

Proof. Consider elements $\overline{\sigma}_a$, $\overline{\sigma}_b$, $\overline{\sigma}_c \in \mathrm{PXL}_2(\mathbb{F}_q)$ of orders a, b, and c, respectively, such that $\sigma_a\sigma_b\sigma_c = 1$. We recall that the map $X_0(a,b,c;\mathfrak{p}) \to X(1)$ has degree $q+1$ since $[G : H_0] = q+1$. The Riemann–Hurwitz formula implies

$$2g - 2 = -2(q+1) + \epsilon_a + \epsilon_b + \epsilon_c, \tag{4.2.6}$$

where ϵ_s is the ramification index at each of the branch points corresponding to $s \in \{a,b,c\}$. We can compute ϵ_s from Lemma 4.2.1 and Lemma 4.2.3, with $\epsilon_s = k_s(s-1)$, where

$$k_s = \begin{cases} (q-1)/s, & \text{if } s \mid (q-1); \\ q/s, & \text{if } s \mid q; \\ (q+1)/s & \text{if } s \mid (q+1); \end{cases} \tag{4.2.7}$$

if $s \neq 2$ or ($s = a = 2$ and q is even); whereas if $s = a = 2$ and q is odd, then either $k_2 = (q+1)/2$ or $k_2 = (q-1)/2$ is determined by the fact that $g \in \mathbb{Z}$, since they differ by 1. □

Remark 4.2.8. Instead of using parity, in the $\mathrm{PGL}_2(\mathbb{F}_q)$ and q odd case, we can always explicitly compute elements $\overline{\sigma}_2$, $\overline{\sigma}_b$, $\overline{\sigma}_c \in G$, of orders 2, b, and c respectively, such that $\overline{\sigma}_2\overline{\sigma}_b\overline{\sigma}_c = 1$. We can then decide if $\overline{\sigma}_2$ is split or non-split and use Lemma 4.2.1 to compute the ramification.

Section 4.3

Algorithm

We present an implementation of Theorem 4.2.4.

Algorithm 4.3.1 (Compute the genus of $X_0(a, b, c; \mathfrak{p})$)**.**
Input: a hyperbolic triple $(a, b, c) \in (\mathbb{Z} \cup \{\infty\})^3$ *and a nonzero prime ideal* $\mathfrak{p} \subseteq \mathbb{Z}_{E(a,b,c)}$.
Output: the genus of $X_0(a, b, c; \mathfrak{p})$ *and the Galois group* $G_{\mathfrak{p}}$ *of the cover* $X(a, b, c; \mathfrak{p}) \to \mathbb{P}^1$.

1. *Compute the residue field of* $\mathfrak{p}$ *and set* $q := \#\mathbb{F}_{\mathfrak{p}}$.

2. *Compute the residue field* $\mathbb{Z}_F/\mathfrak{p}_F$*, where* $\mathfrak{p}_F$ *is a prime of* $F(a, b, c)$ *above* $\mathfrak{p}$*. If* $\mathbb{F}_q \simeq \mathbb{Z}_F/\mathfrak{p}_F$*, then* $G = \mathrm{PSL}_2(\mathbb{F}_q)$*. Otherwise set* $G = \mathrm{PGL}_2(\mathbb{F}_q)$.

3. *Compute* g *using Theorem 4.2.4.*

Proof of correctness. Correctness follows from the formula in Theorem 4.2.4. Steps 1 and 2 can be performed by constructing the algebraic number field; it can also be done purely in terms of the prime number p below $\mathfrak{p}$. □

Section 4.4

Bounds from fixed genus

Our goal remains to show that, for fixed genus g_0, there are finitely many admissible curves $X_0(a,b,c;\mathfrak{p})$ of genus $g \leq g_0$. We first characterize the hyperbolic triples (a,b,c) such that the curve $X(a,b,c;\mathfrak{p})$ has Galois group $\mathrm{PXL}_2(\mathbb{F}_q)$, for a given q.

In the prime case, the notion of admissible ideal can be turned around, as follows.

Definition 4.4.1. Let $q := p^r$ be a power of a prime number p. A hyperbolic triple (a,b,c) is q-admissible if s divides at least one integer in the set $\{q-1,\ p,\ q+1\}$ for all $s \in \{a,b,c\}$, not including ∞.

Lemma 4.4.2. *For any triangular modular curve $X_0(a,b,c;\mathfrak{p})$ with $q := \operatorname{Nm}\mathfrak{p}$ and $\mathfrak{p}$ admissible for (a,b,c), the triple (a,b,c) is q-admissible.*

Proof. As shown in the proof of Lemma 4.2.1, the order of every element in $\mathrm{PXL}_2(\mathbb{F}_q)$ needs to divide one of $\{q-1,p,q+1\}$. □

Proposition 4.4.3. *Let g be the genus of the triangular modular curve $X_0(a,b,c;\mathfrak{p})$ and set $q := \mathbb{Z}_E/\mathfrak{p}$. Then,*

$$q \leq 84(g+1)+1.$$

Proof. Recall that $s^\sharp$ denotes the order of $\pi_\mathfrak{p}(\delta_s)$. The cases where $(a^\sharp,b^\sharp,c^\sharp)$ is not hyperbolic are handled in Proposition 3.4.1: we get $g=0$, and the inequality holds. So we may suppose without loss of generality that $s^\sharp = s$ for $s = \{a,b,c\}$, and still that (a,b,c) is hyperbolic.

We study the Belyi map $X_0(a,b,c;\mathfrak{p}) \to \mathbb{P}^1$. Let $\epsilon_a, \epsilon_b, \epsilon_c$ be as before. Using

Lemma 4.2.1, we have that for $s \in \{a, b, c\}$,

$$(q-1) - \frac{q-1}{s} = \frac{(s-1)(q-1)}{s} \leq \epsilon_s \leq \frac{(s-1)(q+1)}{s} = (q+1) - \frac{q+1}{s}. \quad (4.4.4)$$

Because of these bounds and (4.2.6),

$$\begin{aligned} g(X_0(a,b,c;\mathfrak{p})) &\geq -(q+1) + \frac{(a-1)(q-1)}{2a} + \frac{(b-1)(q-1)}{2b} + \frac{(c-1)(q-1)}{2c} + 1 \\ &= (q-1)\left(-1 + \frac{3}{2} - \frac{1}{2a} - \frac{1}{2b} - \frac{1}{2c}\right) - 1 \\ &= \frac{q-1}{2}\,|\chi(a,b,c)| - 1, \end{aligned} \quad (4.4.5)$$

where $\chi(a, b, c)$ is as in (2.1.5). The result then follows from the previous inequality and the upper bound for $\chi(a, b, c)$ given in Lemma 2.1.6. □

Corollary 4.4.6. *For a fixed genus $g_0 \in \mathbb{Z}_{\geq 0}$, there are only finitely many hyperbolic triples (a, b, c) and admissible primes $\mathfrak{p}$ such that the curves $X_0(a, b, c; \mathfrak{p})$ have genus $g \leq g_0$.*

Proof. By Proposition 4.4.3, we obtain an upper bound on the rational prime p given by $q \leq 84(g_0 + 1) + 1$. Also, for (a, b, c) to be q-admissible, necessarily $s \leq q + 1$ for all $s \in \{a, b, c\}$. This leaves only finitely many possibilities. □

Remark 4.4.7. To make computations more efficient, we can consider a bound on q that depends on $\chi(a, b, c)$. For the genus of $X_0(a, b, c; \mathfrak{p})$ to be less than or equal to g_0, it is necessary that

$$q \leq \frac{2(g_0+1)}{|\chi(a,b,c)|} + 1. \quad (4.4.8)$$

This inequality also shows that

$$0 < |\chi(a,b,c)| \leq \frac{2(g_0+1)}{q-1}. \tag{4.4.9}$$

Therefore, we can bound a, b, and c whenever g_0 and q are fixed.

Section 4.5

Enumerating curves of low genus and prime level

Now we present the main algorithms that use the theory developed in the previous sections. We will effectively enumerate the curves $X_0(a,b,c;\mathfrak{p})$ of bounded genus. Note we already know that the number of curves is finite from Corollary 4.4.6. As explained in section 3.3, if $\mathfrak{p}$ is admissible for (a,b,c), then $G = G_{\mathfrak{p}}$ is given by $\mathrm{PXL}_2(\mathbb{F}_q)$. The first condition (coprimality) in admissibility can be expensive to check, so we first check the easier necessary (but not sufficient) condition that $\mathfrak{p} \nmid \beta(a,b,c)$.

Algorithm 4.5.1 (Relatively prime to β)**.**

Input: a hyperbolic triple (a,b,c) and a prime number p.

Output: returns `true` *if there exists a prime $\mathfrak{p} \subseteq \mathbb{Z}_{E(a,b,c)}$ above p such that $\mathfrak{p} \nmid \beta(a,b,c)$ and* `false` *otherwise.*

1. *If $p \nmid 2abc$, then return* `true`*.*

2. *Find $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q$, where $\mathfrak{p}$ is any prime of E above p.*

3. *Set $m := \mathrm{lcm}(a,b,c)$. Construct $\mathbb{F}_q(\zeta_{2m})$. Set $z := \zeta_{2m}$.*

4. *For every $i \in (\mathbb{Z}/2m\mathbb{Z})^\times$, and set $l_{2s} := z^{im/s} + 1/z^{im/s}$ for $s \in \{a, b, c\}$. Compute*

$$\beta_i := l_{2a}^2 + l_{2b}^2 + l_{2c}^2 + l_{2a}l_{2b}l_{2c} - 4.$$

If $\beta_i \neq 0$ and whenever $p \mid s$ we have $s = p$, then return `true`*. Otherwise, return* `false`*.*

Proof of correctness. Let $\mathfrak{p}$ be a prime of $\mathbb{Z}_{E(a,b,c)}$ above p. If $p \nmid 2abc$ then $\mathfrak{p} \nmid \beta(a, b, c)$ [21, Lemma 5.5]. When $\mathfrak{p} \mid abc$, checking that $\mathfrak{p}$ does not divide $\beta(a, b, c)$ is more involved. We do this in steps 2 to 4 by computing β in the residue field of $\mathfrak{p}$. This computation is independent of the prime $\mathfrak{p}$ chosen above p because E is Galois over $\mathbb{Q}$. □

Now we are ready to present the main algorithm that ties the results of this chapter into an explicit enumeration.

Algorithm 4.5.2 (Enumerate curves $X_0(a, b, c; \mathfrak{p})$ of bounded genus)**.**
Input: an integer $g_0 \in \mathbb{Z}_{\geq 0}$.
Output: a list `lowGenus` *of all hyperbolic triples $(a, b, c) \in \mathbb{Z}^3_{\geq 2}$ and norms of prime ideals $\mathfrak{p}$ of $E(a, b, c)$ that are admissible and such that the genus of $X_0(a, b, c; \mathfrak{p})$ is at most g_0.*

1. *Loop over the list of possible powers $q = p^r$, where p is a prime number and $q \leq 84(g_0 + 1) + 1$.*

2. *For each q from step 1, find all q-admissible hyperbolic triples (a, b, c) (as in Definition 4.4.1).*

3. *For each q-admissible triple (a,b,c) from step 2, check if $\chi(a,b,c)$ satisfies (4.4.9) and if $\mathfrak{p}$ does not divide $\beta(a,b,c)$ using Algorithm 4.5.1. If yes, compute the candidate genus g of $X_0(a,b,c;\mathfrak{p})$ using Algorithm 4.3.1.*

4. *If $g \leq g_0$, check that $\mathfrak{p} \nmid \operatorname{discrd}(\Lambda)\mathfrak{d}_{F|E}$. If yes, add $(a,b,c;q)$ to the list* `lowGenus`*.*

Proof of correctness. For step 1, see Proposition 4.4.3. Every hyperbolic q-admissible triple gives rise to one such curve. The correctness of the rest of the algorithm follows from the work done in the previous sections of this chapter. □

We list the CPU time (in seconds) for our implementation to compute the list of curves $X_0(a,b,c;\mathfrak{p})$ of genus up to bounds 0, 1, and 2 on a standard laptop:

Genus bound	0	1	2
Time (s)	1.7	9.7	1110.3

Section 4.6

Triangular modular curves $X_1(a,b,c;\mathfrak{p})$

In this section, we conclude the chapter by translating our methods to genus computation of curves $X_1(a,b,c;\mathfrak{p})$, completing the proof of our main result.

We recall that $X_1(a,b,c;\mathfrak{p})$ is defined in (3.5.4) as the quotient of $\mathcal{H}$ by $\Gamma_1(a,b,c;\mathfrak{p})$.

Corollary 4.6.1. *For any integer $g_0 \geq 0$, there are finitely many triangular modular curves $X_1(a,b,c;\mathfrak{p})$ with $\mathfrak{p}$ admissible.*

Proof. For every triple $(a,b,c) \in (\mathbb{Z}_{\geq 2} \cup \{\infty\})^3$ and prime ideal $\mathfrak{p}$ of $E(a,b,c)$, there is a cover $X_1(a,b,c;\mathfrak{p}) \to X_0(a,b,c;\mathfrak{p})$. All curves $X_1(a,b,c;\mathfrak{p})$ of genus bounded above by g_0 cover curves $X_0(a,b,c;\mathfrak{p})$ of genus bounded above by g_0. Because of Corollary 4.4.6, there are finitely many admissible triples (a,b,c) and prime ideals $\mathfrak{p}$ that give rise to curves $X_0(a,b,c;\mathfrak{p})$ of genus bounded above by g_0. □

We now focus on explicitly enumerating all curves of bounded genus. The goal first is to prove group-theoretic results that describe the degree and ramification of the cover $X_1(\mathfrak{p}) \to X(1)$. We describe the structure of the quotient $\mathrm{PXL}_2(\mathbb{F}_q)$ modulo $H_{1,\mathfrak{p}}$ and then describe the action of $\pi_{\mathfrak{p}}(\delta_s)$ on this quotient. The main difference with section 4.1 is that the quotient $G/H_{0,\mathfrak{p}}$ does not depend on G being isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$, whereas the structure of $G/H_{1,\mathfrak{p}}$ depends on the choice of G as we describe now. Let $H_1 := H_{1,\mathfrak{p}}$.

Lemma 4.6.2. *Let $G = \mathrm{PXL}_2(\mathbb{F}_q)$, where $\mathbb{F}_q := \mathbb{Z}_E/\mathfrak{p}$. The quotient G/H_1 can be described as follows.*

(i) *If $G = \mathrm{PSL}_2(\mathbb{F}_q)$, then $G/H_1 \simeq (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\langle \pm 1\rangle$: explicitly, the class of $(x,z) \in \mathbb{F}_q \times \mathbb{F}_q$ maps to the coset of $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$, where $y, w \in \mathbb{F}_q$ satisfy $xw - yz = 1$.*

(ii) *If $G = \mathrm{PGL}_2(\mathbb{F}_q)$, then $G/H_1 \simeq (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\langle \pm 1\rangle \times \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$: explicitly, for $\mu \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$ the class of $((x,y),u) \in (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\}) \times \mathbb{F}_q^\times$ maps to the coset of $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$, where $z, w \in \mathbb{F}_q$ satisfy $xw - yz = 1$ if u is a square and $xw - yz = \mu$ otherwise.*

Proof. Let $G = \mathrm{PSL}_2(\mathbb{F}_q)$ with q odd. Because $\#H_1 = \#\mathbb{F}_q$, we have that $[G : H_1] = (q^2-1)/2$. The coset representatives of G/H_1 can be parameterized by $(x,z) \in$

$(\mathbb{F}_q \times \mathbb{F}_q)/\langle \pm 1\rangle$. Indeed, two elements in $\mathrm{PSL}_2(\mathbb{F}_q)$ are in the same coset of G/H_1 if and only if there is $\alpha \in \mathbb{F}_q$ such that

$$\pm \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \pm \begin{pmatrix} x & x\alpha + y \\ z & z\alpha + w \end{pmatrix} = \begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix}.$$

This is the case if and only if $(x,z) = \pm(x',z')$. Thus, the map defined by the parametrization $(\mathbb{F}_q \times \mathbb{F}_q) \setminus \{(0,0)\}/\langle \pm 1\rangle \to G/H_1$ is a well-defined, injective homomorphism. By a cardinality comparison it follows that it is an isomorphism.

Now we let $G = \mathrm{PGL}_2(\mathbb{F}_q)$, so $[G : H_1] = q^2 - 1$. We claim that the quotient G/H_1 is isomorphic to $(\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\{\pm 1\} \times \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$. To present this isomorphism, we fix a non-square $\mu \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$. For any $\pm(x,z) \in (\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\langle \pm 1\rangle$, and any $u \in \{1,\mu\} \simeq \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$, we choose values of $y, w \in \mathbb{F}_q$ such that $xw - yz = u$ and map $\pm(x,z)$ to the class of the matrix $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ in $\mathrm{PGL}_2(\mathbb{F}_q)$. Given two different choices $y, w \in \mathbb{F}_q$ and $y', w' \in \mathbb{F}_q$, if $x \neq 0$, then

$$\pm \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x & y' \\ z & w' \end{pmatrix} \begin{pmatrix} 1 & x^{-1}(y - y') \\ 0 & 1 \end{pmatrix}.$$

If $x = 0$, then $z \neq 0$ and $0 \neq u = yz = y'z$. Thus, $y = y'$. We also have

$$\pm \begin{pmatrix} 0 & y \\ z & w \end{pmatrix} = \begin{pmatrix} 0 & y \\ z & w' \end{pmatrix} \begin{pmatrix} 1 & z^{-1}(w - w') \\ 0 & 1 \end{pmatrix}.$$

Thus, the map $(\mathbb{F}_q \times \mathbb{F}_q \setminus \{(0,0)\})/\{\pm 1\} \times \mathbb{F}_q^\times/\mathbb{F}_q^{\times 2} \to G/H_1$ is a well defined homomorphism. In addition, multiplication by elements in H_1 does not change the square class of the determinant or the first column of the matrix, so the homomorphism described above is injective. Since the cardinalities of the domain and range are equal, we conclude that this is an isomorphism. □

We proceed to describe the ramification of the cover $X_1(a, b, c; \mathfrak{p}) \to \mathbb{P}^1$. This result is similar to Lemma 4.2.1. The main difference is that in certain cases there are more fixed points than strictly necessary.

Proposition 4.6.3. *Let $\overline{\sigma}_s \in G = \mathrm{PXL}_2(\mathbb{F}_q)$ and assume that the order of $\overline{\sigma}_s$ is s. The structure of the action of $\overline{\sigma}_s$ on G/H_1 is as follows:*

(i) *if σ_s is semisimple, then there are (no fixed points and) $[G : H_1]/s$ orbits of length s,*

(ii) *if σ_s is unipotent, then:*

  (a) *if $G = \mathrm{PSL}_2(\mathbb{F}_q)$ and q is odd, there are $(q-1)/2$ fixed points and $(q^2 - q)/(2p)$ orbits of length p,*

  (b) *otherwise, there are $q - 1$ fixed points and $(q^2 - q)/p$ orbits of length p.*

Proof. We use the description of the quotient G/H_1 given in Lemma 4.6.2. Let σ_s be any element of $\mathrm{GL}_2(\mathbb{F}_q)$ that maps to $\overline{\sigma}_s$ in the quotient to G.

If σ_s is split semisimple, then it is conjugate over $\mathbb{F}_q$ to a diagonal matrix with entries u, v. Because the order of $\overline{\sigma}_s$ is s, then s is the order of uv^{-1}. We pick a class in the quotient G/H_1 represented by a matrix M. If the class of M is fixed by the action of $\overline{\sigma}_s$, then the first column of M is, up to multiplication by ± 1, fixed by multiplication by the diagonal matrix. This implies that $(u, v) = \pm(1, 1)$, contradicting that $s \geq 2$. Thus, there are no fixed points of the action of $\overline{\sigma}_s$ on G/H_1. A similar argument shows that orbits of elements that are not fixed cannot have length less than s. Thus, every element belongs to an orbit of length s.

If σ_s is non-split semisimple, then σ_s is split in a quadratic extension of $\mathbb{F}_q$. We assume that $\sigma_s = T^{-1}[\alpha_1, \alpha_2]T$ in this extension. If σ_s^r fixes an element for $r \geq 1$, then we have

$$\pm \begin{pmatrix} \alpha_1^r & 0 \\ 0 & \alpha_2^r \end{pmatrix} T \begin{pmatrix} x & y \\ z & w \end{pmatrix} = T \begin{pmatrix} x & y' \\ z & w' \end{pmatrix}.$$

Multiplication by T does not change the equality in G/H_1. Thus, we are back to the split semisimple case and the orbits of the action of $\overline{\sigma}_s$ all have size s.

If σ_s is unipotent, then σ_s can be chosen (by multiplying by scalar matrices) to be conjugate to an upper diagonal matrix with ones in the diagonal. Then,

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x+uz & y+uw \\ z & w \end{pmatrix},$$

so the class of this matrix in G/H_1 is fixed by multiplication by σ_s if and only if $uz = 0$. Since $s \geq 2$, then z must be 0. We note that if $z \neq 0$, then the orbit of the element has length p. In $G = \mathrm{PSL}_2(\mathbb{F}_q)$ there are $(q-1)/2$ representatives for which $z = 0$, i.e. fixed points. Similarly, if $G = \mathrm{PGL}_2(\mathbb{F}_q)$, then there are $q-1$ fixed points. □

Corollary 4.6.4. *Let $(a,b,c) \in \mathbb{Z}^3_{\geq 2}$ be a q-admissible hyperbolic triple. Let $\mathfrak{p}$ be a prime ideal of $E(a,b,c)$ above a rational prime p. Then the genus of $X_1(a,b,c;\mathfrak{p})$ is given by*

$$g(X_1(a,b,c;\mathfrak{p})) = -[G : H_1] + 1 + \frac{1}{2} \sum_{s \in \{a,b,c\}} k_s(s-1),$$

where

$$k_s = \begin{cases} (q^2-q)/(2p), & \textit{if } s=p \textit{ and } G=\mathrm{PSL}_2(\mathbb{F}_q); \\ (q^2-q)/p, & \textit{if } s=p \textit{ and } G=\mathrm{PGL}_2(\mathbb{F}_q); \\ (q^2-1)/s, & \textit{if } s\neq p \textit{ and } G=\mathrm{PGL}_2(\mathbb{F}_q); \textit{ and} \\ (q^2-1)/(2s), & \textit{if } s\neq p \textit{ and } q \textit{ is odd and } G=\mathrm{PSL}_2(\mathbb{F}_q). \end{cases}$$

Proof. This formula is given by using the Riemann-Hurwitz formula on $X_1(\mathfrak{p}) \to \mathbb{P}^1$ and Proposition 4.6.3. □

Now we are ready to present an algorithm that enumerates all curves $X_1(a,b,c;\mathfrak{p})$.

Algorithm 4.6.5 (Enumerate curves $X_1(a,b,c;\mathfrak{p})$ of bounded genus)**.**

Input: an integer $g_0 \in \mathbb{Z}_{\geq 0}$.

Output: a list `lowGenusX1` *of all hyperbolic triples* (a,b,c) *and admissible ideals* $\mathfrak{p}$ *such that the genus of* $X_1(a,b,c;\mathfrak{p})$ *is* $g \leq g_0$.

1. *Loop over all hyperbolic triples* (a,b,c) *and prime ideals* $\mathfrak{p}$ *such that* $X_0(a,b,c;\mathfrak{p})$ *has genus bounded above by* g_0. *This list can be obtained from Algorithm 4.5.2.*

2. *For each triple* (a,b,c) *and ideal* $\mathfrak{p}$ *listed in the previous step, compute the genus* g *of* $X_1(a,b,c;\mathfrak{p})$ *with Corollary 4.6.4. If* $g \leq g_0$, *then add* $(a,b,c;\mathfrak{p})$ *to the list* `lowGenusX1`.

Proof of correctness. We show that the list is complete. For all triples (a,b,c) and prime ideals $\mathfrak{p}$ there are maps $X_1(a,b,c;\mathfrak{p}) \to X_0(a,b,c;\mathfrak{p})$. Thus, the only curves $X_1(a,b,c;\mathfrak{p})$ that can have genus $g \leq g_0$ must be covers of curves $X_0(a,b,c;\mathfrak{p})$ of genus bounded above by g_0. □

Chapter 5

Triangular modular curves of composite level

This chapter aims to generalize the results from chapters 3 and 4 about Borel-type triangular modular curves of prime level to the same curves with composite level. Our building blocks will be the curves with prime level. We use that for any $\mathfrak{p} \mid \mathfrak{N}$, we have covers $X_i(a,b,c;\mathfrak{N}) \to X_i(a,b,c;\mathfrak{p})$ for $i \in 0,1$. When the level $\mathfrak{N}$ is the product of distinct primes, the results follows by the Sun Zi Theorem (CRT). This chapter's challenge is dealing with level $\mathfrak{N} = \mathfrak{p}^e$, where $e > 1$ and $\mathfrak{p}$ is a prime ideal. In particular, most of the work at the beginning is done to characterize admissible triples in Corollary 5.2.7. Then, we present Algorithm 5.4.6, a generalization of Algorithm 4.5.2 to composite level. We proceed to extending the results to curves X_1 in section 5.5, and we prove the main theorem of this part of the thesis, Theorem 5.6.1. At the end of this chapter, we explore future work on computing the ramification of the covers $X_0 \to \mathbb{P}^1$ by using embedding numbers and strong approximation instead of a direct computation. This chapter contains unpublished joint work with John

Voight.

Section 5.1

Extra setup

In this section, we give some basic setup and notation, extending the work done for the prime level case in section 2.3 and section 3.2. We recall the setup from that section. Let B be the F-subalgebra $F\langle\Delta\rangle \leq M_2(\mathbb{R})$ and we consider $\mathcal{O} = \mathbb{Z}_F\langle\Delta\rangle$ a $\mathbb{Z}_F$-order in B. Recalling (2.2.3), we first suppose that $\beta = \operatorname{discrd}\mathcal{O}$ is coprime to $\mathfrak{N}$, so all primes $\mathfrak{p} \mid \mathfrak{N}$ are unramified in B but more strongly we have $(\mathcal{O}/\mathfrak{N}\mathcal{O})^1/\{\pm 1\} \simeq \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)/\{\pm 1\}$. From (2.3.1) we obtain

$$\varpi_{\mathfrak{N}} \colon \Delta \to \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)/\{\pm 1\}. \tag{5.1.1}$$

We recall Proposition 3.2.6, which states that if $\mathfrak{N}$ is prime and coprime to $\operatorname{discrd}(\Lambda)\mathfrak{d}_{F|E}$, then there is a commutative diagram

$$\begin{tikzcd}
\Delta^{(2)} \arrow[r] \arrow[d, hook] & \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \arrow[d] \\
\Delta \arrow[r, "\pi_{\mathfrak{N}}"] & \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})
\end{tikzcd} \tag{5.1.2}$$

and the map $\pi_{\mathfrak{N}} \colon \Delta \to \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$ factors through $\varpi_{\mathfrak{N}}$. As explained in Remark 3.2.8, the issue with composite level is that the right-hand vertical map may no longer be injective. The main effort of this section is to compute the kernel of this map.

Recall that $G_{\mathfrak{N}} := \pi_{\mathfrak{N}}(\Delta)$ is the image of (5.1.1). We need a bit more notation to show the corresponding statement for $A = E\langle\Delta\rangle$ (under an additional hypothesis). Let

$$\mathbb{Z}_{E,(\mathfrak{N})} := \{\alpha \in E : \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0 \text{ for all } \mathfrak{p} \mid \mathfrak{N}\} \subseteq E \tag{5.1.3}$$

be the localization of $\mathbb{Z}_E$ at the ideal $\mathfrak{N}$ (all elements coprime to $\mathfrak{N}$ become units).

We recall Lemma 3.2.3. Suppose that $\mathfrak{N}$ is coprime to $\beta\mathfrak{d}_{F|E}$. Then for $s = a, b, c$, we can write

$$\lambda_s + 2 = \upsilon_s\theta_s^2 \in E^\times \tag{5.1.4}$$

with:

- $\upsilon_s \in \mathbb{Z}_{E,(\mathfrak{N})}^\times$, well-defined up to multiplication by an element of $\mathbb{Z}_{E,(\mathfrak{N})}^{\times 2}$, and
- $\theta_s \in E^\times$, well-defined up to $\mathbb{Z}_{E,(\mathfrak{N})}^\times$.

If $\mathfrak{N}$ is coprime to $2abc$, then we may take $\theta_s = 1$ and $\upsilon_s = \lambda_s + 2$.

Moreover, a prime $\mathfrak{p} \mid \mathfrak{N}$ (necessarily unramified in F) splits completely in F if and only if the Kronecker symbols $(\upsilon_s \,|\, \mathfrak{p}) = 1$ are trivial for all $s = a, b, c$.

Proposition 5.1.5. *If $\mathfrak{p} \nmid \beta\mathfrak{d}_{F|E}$, then A is split at the prime $\mathfrak{p}$.*

Proof. For simplicity, we suppose that $a > 2$; when $a = 2$, the proof can be modified as in Lemma 2.2.5. Consider the completed order $\Lambda_{\mathfrak{p}} := \Lambda \otimes_{\mathbb{Z}_E} \mathbb{Z}_{E,\mathfrak{p}}$. We will find an order $\Lambda'_{\mathfrak{p}} \supseteq \Lambda_{\mathfrak{p}}$ with trivial reduced discriminant; this implies the statement.

Consider the $\mathbb{Z}_{E,\mathfrak{p}}$-submodule $\Lambda'_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$ generated by 1 and $\delta'_s := (\delta_s^2 + 1)/\theta_s$ for $s = a, b, c$ with θ_s as in (5.1.4). A direct calculation similar to that for Λ shows that $\Lambda'_{\mathfrak{p}}$ is a $\mathbb{Z}_{E,\mathfrak{p}}$-order. Recalling the calculation of the reduced discriminant [21, Lemma 5.4], we have

$$\mathrm{trd}([\delta_a, \delta_b]\delta_c) = \beta;$$

therefore $\operatorname{discrd}(\Lambda'_{\mathfrak{p}})$ is generated by

$$\operatorname{trd}([\delta'_a, \delta'_b]\delta'_c) = \frac{\lambda_{2a}\lambda_{2b}\lambda_{2c}}{\theta_a\theta_b\theta_c}\beta.$$

But $(\lambda_{2s}/\theta_s)^2 = \upsilon_s \in \mathbb{Z}_{E,\mathfrak{p}}^{\times}$, so $(\lambda_{2a}\lambda_{2b}\lambda_{2c})/(\theta_a\theta_b\theta_c) \in \mathbb{Z}_{E,\mathfrak{p}}^{\times}$ as well. We are given $\mathfrak{p} \nmid \beta$, so $\operatorname{ord}_{\mathfrak{p}}(\Lambda'_{\mathfrak{p}}) = 0$ and A is split at $\mathfrak{p}$. □

Remark 5.1.6. The coprimality hypothesis in Proposition 5.1.5 is natural. If $\mathfrak{p} \mid \beta$, then for any prime $\mathfrak{P}$ of $\mathbb{Z}_F$ over $\mathfrak{p}$, the local order $\mathcal{O}_{\mathfrak{P}} := \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{P}}$ is not isomorphic to $\mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{p}})$ (else it would have trivial reduced discriminant). Similarly, if $\mathfrak{p} \mid \mathfrak{d}_{F|E}$, then $\mathfrak{p} \mid \lambda_{2a}\lambda_{2b}\lambda_{2c}$ (and $\lambda_{2b}\lambda_{2c}$ if $a = 2$) and so $\mathfrak{p}$ may divide the reduced discriminant of Λ [21, Corollary 5.17].

From Proposition 5.1.5, the restriction of $\pi_{\mathfrak{N}}$ to $\Delta^{(2)}$ gives a map

$$\pi_{\mathfrak{N}} \colon \Delta^{(2)} \to \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\}. \tag{5.1.7}$$

Let $G_{\mathfrak{N}}^{(2)} := \pi_{\mathfrak{N}}(\Delta^{(2)})$ be the image and $\Gamma^{(2)}(\mathfrak{N}) = \ker \pi_{\mathfrak{N}} \cap \Delta^{(2)}$ the kernel (of the restriction).

Further, let

$$W_{\mathfrak{N}} := \Delta/\Delta^{(2)}\Gamma(\mathfrak{N}). \tag{5.1.8}$$

Corollary 5.1.9. *The following diagram is commutative and has exact rows and* *columns:*

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \Gamma^{(2)}(\mathfrak{N}) \arrow[r] \arrow[d] & \Gamma(\mathfrak{N}) \arrow[r] \arrow[d] & \Gamma(\mathfrak{N})/\Gamma^{(2)}(\mathfrak{N}) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \Delta^{(2)} \arrow[r] \arrow[d] & \Delta \arrow[r] \arrow[d, "\pi_{\mathfrak{N}}"] & \Delta/\Delta^{(2)} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & G_{\mathfrak{N}}^{(2)} \arrow[r] \arrow[d] & G_{\mathfrak{N}} \arrow[r] \arrow[d] & W_{\mathfrak{N}} \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd} \tag{5.1.10}$$

Proof. The proof is immediate. □

Let $G_{\mathfrak{N}} := \pi_{\mathfrak{N}}(\Delta) \leq \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$ be the image of $\pi_{\mathfrak{N}}$. Before we characterize $G_{\mathfrak{N}}$, we note one additional feature.

The right-hand vertical map in (5.1.2) has kernel the center $Z(\mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N}))/\{\pm 1\}$ consisting of unsigned scalar matrices of determinant 1, a group isomorphic to

$$Z_{\mathfrak{N}} := (\mathbb{Z}_E/\mathfrak{N})^\times/\{\pm 1\}(\mathbb{Z}_E/\mathfrak{N})^{\times 2}, \tag{5.1.11}$$

the quotient of $(\mathbb{Z}_E/\mathfrak{N})^\times$ by the subgroup generated by squares and ± 1. Let $\overline{\upsilon}_s \in Z_{\mathfrak{N}}$ be the image of υ_s for $s = a, b, c$, well-defined by Lemma 3.2.3.

Corollary 5.1.12. *If $G_{\mathfrak{N}} \leq \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$, then $\pi_{\mathfrak{N}}$ factors through a lift*

$$\pi_{\mathfrak{N},1} \colon \Delta \to \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\}.$$

Proof. We may take $\upsilon_s = 1$ in Lemma 3.2.3 for all $s = a, b, c$. □

Corollary 5.1.13. *Suppose that $\mathfrak{N}$ is coprime to $\mathfrak{d}_{F|E}$. Then there is a commutative diagram*

$$\begin{tikzcd}
1 \arrow[r] & G_{\mathfrak{N}}^{(2)} \arrow[r] \arrow[d] & G_{\mathfrak{N}} \arrow[r] \arrow[d, "\pi'_{\mathfrak{N}}"] & W_{\mathfrak{N}} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N}) \arrow[r] & \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N}) \arrow[r, "\det"] & (\mathbb{Z}_E/\mathfrak{N})^\times/(\mathbb{Z}_E/\mathfrak{N})^{\times 2} \arrow[r] & 1
\end{tikzcd} \tag{5.1.14}$$

and the map $\pi_{\mathfrak{N}}$ fits into a diagram

$$\begin{tikzcd}
\Delta \arrow[r, two heads, "\pi_{\mathfrak{N}}"] \arrow[dr, two heads, "\pi'_{\mathfrak{N}}"'] & G_{\mathfrak{N}} \leq \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)/\{\pm 1\} \arrow[d, two heads] \\
& G'_{\mathfrak{N}} \leq \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})
\end{tikzcd} \tag{5.1.15}$$

Proof. Returning to the proof of Lemma 3.2.3, we now rescale the map (2.3.1) by sending $\delta_s \mapsto (\delta_s^2+1)/\theta_s$ when $s \neq 2$ (modified similarly when $s = a = 2$); then

$$\mathrm{nrd}((\delta_s^2+1)/\theta_s) = \frac{\lambda_{2s}^2}{\theta_s^2} = \frac{\lambda_s+2}{\theta_s^2} = \upsilon_s \in \mathbb{Z}_{E,(\mathfrak{N})}^\times. \tag{5.1.16}$$

The reduction modulo $\mathfrak{N}$ yields the map $\pi'_{\mathfrak{N}} : \Delta \to G_{\mathfrak{N}}$. The restriction to $G_{\mathfrak{N}}^{(2)}$ maps to $\mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\}$ which surjects onto $\mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$. □

Remark 5.1.17. Understanding the bottom row of (5.1.10) turns out to be quite involved when $\mathfrak{N}$ is composite, owing to the following issues:

- We have equality $G_{\mathfrak{N}}^{(2)} = \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\}$ when $\mathfrak{N}$ is prime, but only an inclusion $G_{\mathfrak{N}}^{(2)} \leq \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\}$ when $\mathfrak{N}$ is not coprime to 6;
- The natural map $\mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \to \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$ (vertical maps in (5.1.14)) has a nontrivial kernel when $\mathfrak{N}$ is not prime, leaving several possible interpre-

tations of the Borel-type subgroups (coming from additional involutions).

We begin by describing the finite quotient $W_{\mathfrak{N}}$.

Lemma 5.1.18. *The following statements hold.*

(a) *The group $W_{\mathfrak{N}}$ is an elementary abelian 2-group of rank at most 2. More precisely, $W_{\mathfrak{N}}$ is isomorphic to the subgroup of $\mathrm{Gal}(F \,|\, E)$ generated by the set*

$$\{\mathrm{Frob}_{\mathfrak{p}} : \mathfrak{p} \mid \mathfrak{N} \text{ odd}\} \cup \{\mathrm{Frob}_{\mathfrak{p}} : \mathfrak{p} \mid \mathfrak{N} \text{ even and } \mathrm{ord}_{\mathfrak{p}}(\mathfrak{N}) > \mathrm{ord}_{\mathfrak{p}}(4)\}.$$

(b) *The group $W_{\mathfrak{N}} \leq (\mathbb{Z}/2\mathbb{Z})^2$ is effectively computable.*

(c) *Let $\mathfrak{N}_2 := \mathfrak{N}/(2\mathbb{Z}_E + \mathfrak{N})$. Suppose that $a \neq 2$ and for all $s = a, b, c$ we have $\lambda_{2s} \notin \mathfrak{N}_2\mathbb{Z}_F$. Then $W_{\mathfrak{N}} = \Delta/\Delta^{(2)}$.*

The exceptional levels $\mathfrak{N}$ in Lemma 5.1.18(b) where the hypotheses do not hold are $\mathrm{Gal}(F/E)$-invariant divisors classes of one of $2\lambda_{2s}$ for $s = a, b, c$, so the associated (a, b, c) are finite in number; we call such $\mathfrak{N}$ lamentable.

Proof. We recall that $F = E(\lambda_{2a}, \lambda_{2b}, \lambda_{2c})$ where $\lambda_{2s}^2 = \lambda_s + 2$. We start showing part (a). By hypothesis, the ideal $\mathfrak{p} \mid \mathfrak{N}$ is unramified in F. If $\mathfrak{p} \mid \mathfrak{N}$ is even then $\upsilon_s \equiv 1 \pmod{4\mathbb{Z}_E}$ for $s = \{a, b, c\}$. If $\mathfrak{p}^e \parallel \mathfrak{N}$ is odd, it follows that $\mu_s \in (\mathbb{Z}_E/\mathfrak{p}^e)^{\times 2}$ if and only if the element $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(E(\lambda_{2s}) \,|\, E)$ is trivial; and for $\mathfrak{p}^e \parallel \mathfrak{N}$, we automatically have $\mu_s \in (\mathbb{Z}_E/\mathfrak{p}^e)^{\times 2}$ whenever $e \leq \mathrm{ord}_{\mathfrak{p}}(4)$, and when $e > \mathrm{ord}_{\mathfrak{p}}(4)$, we have $\mu_s \in (\mathbb{Z}_E/\mathfrak{p}^e)^{\times 2}$ if and only if $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(E(\lambda_{2s}) \,|\, E)$ trivial. We conclude by the Sun Zi theorem (CRT).

For (b), we can compute the quaternion order $\mathcal{O}$ explicitly and compute the map (5.1.1) by recognizing the matrix ring [73]. The quotient is finite; hence we can compute the image of the subgroup of squares and then the quotient.

Finally, part (c) follows from part(a). □

Putting together Corollary 5.1.13 and Proposition 5.1.5, the right-hand vertical map of (5.1.2) sits in an exact sequence

$$1 \to \mu_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \to \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \to \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N}) \xrightarrow{\det} (\mathbb{Z}_E/\mathfrak{N})^{\times/\times 2} \to 1 \tag{5.1.19}$$

where $\mu_2(R) := \{x \in R^\times : x^2 = 1\}$ for a ring R.

Applying these to (2.3.1), we obtain the following corollary.

Corollary 5.1.20. *If $\mathfrak{p} \nmid \beta\mathfrak{d}_{F|E}$, the diagram*

$$\begin{tikzcd}
1 \arrow[r] & \Gamma^{(2)}(\mathfrak{N}) \arrow[r] \arrow[d, hook] & \Delta^{(2)} \arrow[r] \arrow[d, hook] & \mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\} \arrow[d, hook] \\
1 \arrow[r] & \Gamma(\mathfrak{N}) \arrow[r] & \Delta \arrow[r] & \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)/\{\pm 1\}
\end{tikzcd}$$

is commutative, with exact rows.

Proof. In the bottom row of (2.3.1), we have isomorphisms $\mathcal{O}/\mathfrak{N}\mathcal{O} \simeq \mathrm{M}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)$ and $(\mathcal{O}/\mathfrak{N}\mathcal{O})^1/\{\pm 1\} \simeq \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)/\{\pm 1\}$. The top row is similar, applying Proposition 5.1.5. □

Section 5.2

Admissibility

We recall the definition of admissibility (Definition 3.3.4). Given a triple (a, b, c), an ideal $\mathfrak{N} \subseteq \mathbb{Z}_{E(a,b,c)}$ is admissible for (a, b, c) if

- $\mathfrak{N}$ is coprime to $\operatorname{discrd}(\Lambda)\mathfrak{d}_{F|E}$, and
- the order of $\pi_{\mathfrak{N}}(\delta_s)$ is equal to s for all $s = a, b, c$.

In this section, we study admissible triples and, given an inadmissible triple, we find its corresponding admissible triple. To do so, we explicitly describe the order of the images of the $\Delta(a, b, c)$ generators under the map $\pi_{\mathfrak{N}}$ from (5.1.15). We record our findings in Proposition 5.2.4 and Corollary 5.2.7. In order to prove the proposition, we need the following technical lemmas.

Lemma 5.2.1. *Let p be an odd prime. Let F be an abelian number field which contains ζ_{p^k} but not $\zeta_{p^{k+1}}$ with $k \geq 1$. Let $\mathfrak{p}_F$ be a prime ideal of $\mathbb{Z}_F$ above p and $e \geq 1$. Then the smallest $r \geq 1$ for which $\zeta_{p^k}^r \equiv 1 \pmod{\mathfrak{p}_F^e}$ is*

$$\xi(p, k, e)p^k,$$

where

$$\xi(p, k, e) := p^{\min(0, \lceil \log_p(e) \rceil - k)}.$$

In particular, we have that $\zeta_{p^k} \equiv 1 \pmod{\mathfrak{p}_F^e}$ if and only if $e = 1$.

Proof. Let $s := p^k$. Since F is abelian over $\mathbb{Q}$, we can write it as a compositum $F = KL$, where $K := F \cap \mathbb{Q}(\zeta_{p^\infty})$ and L is such that $\mathbb{Q}(\zeta_{p^\infty}) \cap L = \mathbb{Q}$. In particular,

p does not ramify in L. Thus, the ramification of p in F is measured only by the ramification of p in K.

Let $\mathfrak{P}$ be a prime of K above p. We have $\mathfrak{P} = (\zeta_s - 1)$. Hence, $\zeta_s \equiv 1 \pmod{\mathfrak{P}}$ if and only if $e = 1$.

Now we assume that $e > 1$. The order of ζ_s modulo $\mathfrak{P}^e$ divides p^k. We have $\zeta_{p^k}^p$ is a p^{k-1}-th primitive root of unity in K. Thus, the element $\zeta_{p^k}^p - 1$ is a uniformizer in the subfield $K' := \mathbb{Q}(\zeta_{p^{k-1}})$. We have $[K : K'] = p$, and the prime above p is totally ramified in this extension. This implies that $\zeta_{p^k}^p - 1 \in \mathfrak{P}^p$. We can keep on going until the power of $\mathfrak{P}$ is larger than e, or until the subfield is $\mathbb{Q}(\zeta_p)$. Thus, the order of ζ_s modulo $\mathfrak{P}^e$ is $\xi(p, k, e)p^k$ as desired. □

Recall that given a number field L and a prime ideal $\mathfrak{p}$, we denote the completion of $\mathbb{Z}_L$ at $\mathfrak{p}$ by $\mathbb{Z}_{L,\mathfrak{p}}$.

Lemma 5.2.2. *Let $s \geq 1$, let L be a number field containing a primitive root of unity ζ_{2s} of order $2s$, let $\mathfrak{p}$ be a prime ideal of L, and let $M \in \mathrm{GL}_2(\mathbb{Z}_{L,\mathfrak{P}})$ be a matrix with characteristic polynomial $x^2 - \lambda_{2s}x + 1$. Then there is an (integral) change of basis such that M is conjugate over $\mathrm{GL}_2(\mathbb{Z}_{L,\mathfrak{P}})$ to*

$$\begin{pmatrix} \zeta_{2s} & -\zeta_{2s}^2 \\ 0 & \zeta_{2s}^{-1} \end{pmatrix}. \tag{5.2.3}$$

Proof. The regular representation gives an integral change of basis to the matrix in rational canonical form as

$$\begin{pmatrix} 0 & -1 \\ 1 & \lambda_{2s} \end{pmatrix}$$

(see [74, (30.5.4)]). We can (integrally) make a change of basis to get this matrix to be upper-triangular by conjugating by the matrix

$$\begin{pmatrix} \zeta_{2s} & 0 \\ 1 & \zeta_{2s}^{-1} \end{pmatrix}$$

to obtain the matrix in (5.2.3). □

Proposition 5.2.4. *Let (a,b,c) be a hyperbolic triple with $a,b,c \in \mathbb{Z}_{\geq 2}$. Let $\mathfrak{p}_F$ be a prime ideal of $\mathbb{Z}_F$ and $e \geq 2$. Let p be the prime below $\mathfrak{p}_F$ and assume that $p \neq 2$. Let $M_{2s} \in \mathrm{GL}(\mathbb{Z}_{F,\mathfrak{p}_F})$ be a matrix with characteristic polynomial $x^2 - \lambda_{2s}x + 1$ for $2s = s_0p^k$ with $p \nmid s_0$ and $k \geq 0$. Then the order of the reduction of M_{2s} modulo $\mathfrak{p}_F^e$ is*

$$\mathrm{ord}_p^e(M) := \begin{cases} s_0, & \text{if } e = 1 \text{ and } s \text{ is not a power of } p; \\ 2 \cdot p, & \text{if } e = 1 \text{ and } s \text{ is a power of } p; \\ 2 \cdot s \cdot \xi(p,k,e) & \text{if } e > 1 \text{ and } e \text{ is not a power of } p; \\ 2 \cdot s \cdot p \cdot \xi(p,k,e) & \text{if } e > 1 \text{ and } e \text{ is a power of } p. \end{cases}$$

where $\xi(p,k,e)$ is as before if $k \geq 1$ and $\xi(p,0,e) = 1$.

Proof. The case $e = 1$ follows from Proposition 3.3.5.

Let $\mathfrak{P}$ be a prime ideal of $F(\zeta_{2s})$ above $\mathfrak{p}_F$. We can use the injective group homomorphism

$$\mathrm{SL}_2(\mathbb{Z}_{F,\mathfrak{p}_F}) \hookrightarrow \mathrm{SL}_2(\mathbb{Z}_{F(\zeta_{2s}),\mathfrak{P}})$$

to consider M as en element of the ring $\mathbb{Z}_{E(\zeta_{2s}),\mathfrak{P}}$. This does not change the order of M because of injectivity.

We write $2s = s_0p^k$, where $p \nmid s_0$. By the Sin Zi theorem (CRT), the order of ζ_{2s}

modulo $\mathfrak{P}^e$ equals the product of the orders of ζ_{s_0} and ζ_{p^k} modulo $\mathfrak{P}^e$. Since $p \nmid s_0$, the order of ζ_{s_0} is s_0 modulo $\mathfrak{P}^e$. By Lemma 5.2.1, the order of ζ_{p^k} modulo $\mathfrak{P}^e$ is $\xi(p,k,e)p^k$. In total, the order of ζ_{2s} is

$$r := s_0\xi(p,k,e)p^k = s\xi(p,k,e).$$

By Lemma 5.2.2, we have that M is conjugate to the matrix

$$M := \begin{pmatrix} \zeta_{2s} & -\zeta_{2s}^2 \\ 0 & \zeta_{2s}^{-1} \end{pmatrix}. \tag{5.2.5}$$

Thus, the orders of M and M_{2s} are equal. By recursion, the matrix M^t has diagonal $[\zeta_{2s}^t, \zeta_{2s}^{-t}]$ and upper-right entry equal to

$$-\zeta_{2s}^3 \sum_{i=0}^{t-1} \left(\zeta_{2s}^2\right)^i.$$

Thus, the smallest power of M that has diagonal entries equal to 1 is r. In this case, the upper-right entry equals

$$-\zeta_{2s}^3 \frac{\left(\zeta_{2s}^2\right)^r - 1}{\zeta_{2s} - 1}.$$

Since $p \neq 2$, then $\left(\zeta_{2s}^2\right)^r - 1 = (\zeta_{2s} - 1)^r$. By the proof of Lemma 5.2.1, the quotient belongs to $\mathfrak{P}^e$ only when e is not a power of p. Otherwise, the proof of Lemma 5.2.1 allows us to conclude that the upper-right entry of M^{rp} is zero modulo $\mathfrak{P}^e$, so the order of M is rp. □

Remark 5.2.6. Proposition 5.2.4 does not deal with the case $s = \infty$. We believe that in this case, the order is the same as the order when $s = p^e$. We hope to show this in upcoming work.

Corollary 5.2.7. *Let (a, b, c) be a hyperbolic triple with $a, b, c \in \mathbb{Z}_{\geq 2}$. Let $\mathfrak{N}_F$ be an ideal of $\mathbb{Z}_F$ with $n\mathbb{Z} = \mathfrak{N}_F \cap \mathbb{Q}$ and $n = p_1^{e_1} \cdots p_r^{e_r}$ where $p_i \neq p_j$ for $i \neq j$. Recall the homomorphism $\pi_{\mathfrak{N}}$ from (5.1.15). Then the order of $\pi_{\mathfrak{N}}(\delta_s) \in \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N}\mathbb{Z}_F)$ is*

$$\mathrm{lcm}\left\{\mathrm{ord}_{p_i}^{e_i}(M)\right\}_{i=1}^{r}.$$

Proof. The result follows immediately from Proposition 5.2.4 and the Sun Zi theorem (CRT). □

The upshot of Corollary 5.2.7 is that redundancies like in Example 3.3.2 do not arise under the admissibility hypothesis.

Theorem 5.2.8 (Clark–Voight)**.** *Suppose that either*

- *(a, b, c) is arithmetic, or*
- *for all primes $\mathfrak{p} \mid \mathfrak{N}$ with $\mathrm{Nm}(\mathfrak{p}) \leq 3$ we have $\mathfrak{p} \parallel \mathfrak{N}$.*

Then $\pi_{\mathfrak{N}}(G_{\mathfrak{N}}^{(2)}) = \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$ and

$$\pi_{\mathfrak{N}}(G_{\mathfrak{N}}) = \{\nu \in \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N}) : \det(\nu) \in \langle \pm \overline{v}_s : s \neq 2 \rangle\}.$$

Proof. When $\mathfrak{p} \nmid \mathrm{discrd}(\Lambda)\beta\mathfrak{d}_{F|E}$, this follows from Theorem 3.3.1. The group $G_{\mathfrak{N}}$ maps onto $\mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{p})$ or $\mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p})$ for each $\mathfrak{p} \mid \mathfrak{N}$ according as $\mathfrak{p}$ splits in $F \supseteq E$ or not; but this is exactly measured by the group $\langle \pm \overline{v}_s : s \neq 2 \rangle$, by Lemma 3.2.3. □

Remark 5.2.9. We note that, in the same way as in section 3.4, some hyperbolic triples are inadmissible and reduce to non-hyperbolic triples. When considering composite level, the problem of characterizing these triples is more challenging, and this phenomenon is rare. Since these cases fall out of the scope of this project's interest, we do not study these triples.

Section 5.3

Congruence subgroups

In the same way as for the curves $X_i(a, b, c; \mathfrak{p})$ for $i = 0, 1$ and $\mathfrak{p}$ prime from section 3.5, we define curves $X_i(a, b, c; \mathfrak{N})$ for $\mathfrak{N}$ not prime and $i = 0, 1$. We stress some of the new features of this definition. We have analogous definitions of the Borel-type congruence subgroups Γ_0 and Γ_1 as follows.

Let

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z}_E/\mathfrak{N} \text{ and } ad \in (\mathbb{Z}_E/\mathfrak{N})^\times \right\} \leq \mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{N}) \tag{5.3.1}$$

be the upper-triangular matrices in $\mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{N})$, and let $H_{0,\mathfrak{N}}$ be its image in the projection to $\mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$. Similarly, let

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z}_E/\mathfrak{N} \text{ and } a^1 = 1 \right\} \leq \mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{N}) \tag{5.3.2}$$

be the upper unipotent subgroup and $H_{1,\mathfrak{N}'}$ again its image in $\mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$.

There is an essential difference that goes back to the issue presented in Remark 3.2.8. We define the subgroups

$$\begin{aligned} \Gamma_0(a, b, c; \mathfrak{N}) &:= \varphi_{\mathfrak{N}}^{-1}(H_{0,\mathfrak{N}}), \\ \Gamma_1'(a, b, c; \mathfrak{N}) &:= \varphi_{\mathfrak{N}}^{-1}(H_{1,\mathfrak{N}}'). \end{aligned} \tag{5.3.3}$$

We then get the corresponding quotients

$$\begin{aligned} X_0(a,b,c;\mathfrak{N}) &:= \Gamma_0(a,b,c;\mathfrak{N})\backslash\mathcal{H} = H_{0,\mathfrak{N}}\backslash X'(a,b,c;\mathfrak{N}) \\ X_1'(a,b,c;\mathfrak{N}) &:= \Gamma_1'(a,b,c;\mathfrak{N})\backslash\mathcal{H} = H_{1,\mathfrak{N}}'\backslash X'(a,b,c;\mathfrak{N}) \end{aligned} \tag{5.3.4}$$

and natural quotient maps

$$X(a,b,c;\mathfrak{N}) \to X_1'(a,b,c;\mathfrak{N}) \to X_0(a,b,c;\mathfrak{N}) \to X(a,b,c;1) \simeq \mathbb{P}^1. \tag{5.3.5}$$

The reason for the prime superscript is explained by the following lemma. Recall that for a subgroup $H \leq G$, the normal core is $\bigcap_{g\in G} g^{-1}Hg$, the largest normal subgroup of G contained in H.

Lemma 5.3.6. *The following statements hold.*

(a) *The normal core of the subgroup* (5.3.1) *in* $\mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{N})$ *is the central subgroup of scalar matrices, isomorphic to* $(\mathbb{Z}_E/\mathfrak{N})^\times$.

(b) *The normal core of the intersection of* $\mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})$ *with the subgroup* (5.3.1) *is*

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{Z}_E/\mathfrak{N} \textit{ and } a^2 = 1 \right\} \simeq \mu_2(\mathbb{Z}_E/\mathfrak{N}). \tag{5.3.7}$$

(c) *The normal core of* (5.3.2) *in* $\mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{N})$ *(and in* $\mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})$*) is trivial.*

Proof. For part (a), we see that every matrix in the normal core must be upper triangular with the duplicate entries in the diagonal by taking g as the identity in G. By taking g as a lower-triangular matrix with non-zero entries equal to 1, we conclude that any element in the normal core must be a scalar matrix. Moreover, scalar matrices are clearly in the normal core, so these sets must be equal. Part (b) follows immediately from this, and a similar argument gives part (c). □

By Galois theory, the normal closure of the fixed field of a subgroup $H \geq G$ in a G-Galois extension is the fixed field by the normal core of H. In our case, since the quotients by the normal core in cases (a) and (b) are $\mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$ and $\mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$, respectively, we can work directly with the reduction map $\pi_{\mathfrak{N}}$ for the curves $X_0(a,b,c;\mathfrak{N})$. The same is true for $X_1'(a,b,c;\mathfrak{N})$ when $\mu_2(\mathbb{Z}_E/\mathfrak{N}) = \{\pm 1\}$; this is why we did not encounter this issue for prime level in section 3.5.

In general, when $\mu_2(\mathbb{Z}_E/\mathfrak{N}) > \{\pm 1\}$, to define the curves $X_1(a,b,c;\mathfrak{N})$, we work as follows. Recalling Corollary 5.1.12, in the special case where $G_{\mathfrak{N}} \leq \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$, we have a lift to $\mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\}$, so we repeat all of the above definitions but take

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}_E/\mathfrak{N} \right\} \leq \mathrm{GL}_2(\mathbb{Z}_E/\mathfrak{N}) \tag{5.3.8}$$

and its the image $H_{1,\mathfrak{N}}$ in $\mathrm{SL}_2(\mathbb{Z}_E/\mathfrak{N})/\{\pm 1\}$ and define

$$X_1(a,b,c;\mathfrak{N}) := \Gamma_1(a,b,c;\mathfrak{N})\backslash\mathcal{H} = H_{1,\mathfrak{N}}\backslash X(a,b,c;\mathfrak{N}). \tag{5.3.9}$$

We obtain quotient maps as in (5.3.5) with the additional map

$$X_1(a,b,c;\mathfrak{N}) \to X_1'(a,b,c;\mathfrak{N}). \tag{5.3.10}$$

Our strategy to compute the genera of the curves $X_0(a,b,c;\mathfrak{N})$ and $X_1'(a,b,c;\mathfrak{N})$ will be similar to the one from the previous chapter. We first describe the ramification and degree of the cover $X_0(a,b,c;\mathfrak{N}) \to \mathbb{P}^1$ and then exploit that to describe the cover $X_1'(a,b,c;\mathfrak{N})$. The final step is studying the cover $X_1(a,b,c;\mathfrak{N}) \to X_1'(a,b,c;\mathfrak{N})$, a cover of at most degree 2.

Section 5.4

Algorithm

Let $\mathfrak{N} \subseteq \mathbb{Z}_E$ be a nonzero ideal. For any prime $\mathfrak{p} \mid \mathfrak{N}$ dividing $\mathfrak{N}$, there is a cover $X_0(\mathfrak{N}) \to X_0(\mathfrak{p})$, so by the Riemann–Hurwitz formula, if $X_0(a,b,c;\mathfrak{N})$ has genus bounded above by g then so does $X_0(a,b,c;\mathfrak{p})$. In this section, we present an algorithm to compute the genus of $X_0(a,b,c;\mathfrak{N})$. We also show that there are finitely many admissible curves $X_0(a,b,c;\mathfrak{N})$ of bounded genus.

The main difference with the prime level case is that the Galois group $G_{\mathfrak{N}}$ of the cover $X_0(\mathfrak{N}) \to \mathbb{P}^1$ is not necessarily isomorphic to $\mathrm{PXL}_2(\mathbb{F}_q)$ (see Theorem 5.2.8). We now present an algorithm to compute this group explicitly.

Algorithm 5.4.1 (Compute $G_{\mathfrak{N}}$)**.**

Input: a hyperbolic triple $(a,b,c) \in (\mathbb{Z}_{\geq 2} \cup \{\infty\})^3$ *and a nontrivial, admissible, nonzero ideal* $\mathfrak{N} \subseteq \mathbb{Z}_E$.

Output: returns `true` *and the group* $G_{\mathfrak{N}} := \pi_{\mathfrak{N}}(\Delta)$ *if* $\mathfrak{N}$ *is coprime to* $\operatorname{discrd}(\Lambda)$ *and* $\beta\mathfrak{d}_{F|E}$. *Otherwise, it returns* `false`.

1. *For every prime divisor* $\mathfrak{p}$ *of* $\mathfrak{N}$ *do the following. Compute the residue field degree of* $\mathfrak{p}|\mathfrak{N}$ *in* $E(a,b,c)$ *and the residue field degree of* $\mathfrak{p}'$ *in* $E(a^\sharp,b^\sharp,c^\sharp)$, *where* $\mathfrak{p}'$ *is an ideal of* $E(a^\sharp,b^\sharp,c^\sharp)$ *above* p. *If these are different, return false.*

2. *If* $\mathfrak{N}$ *is not coprime to* $\beta\mathfrak{d}_{F|E}$, *return false.*

3. *If* $\operatorname{discrd}(\Lambda)$ *is not coprime to* $\mathfrak{N}$*, return false.*

4. *For all prime powers exactly dividing* $\mathfrak{N}$ *(*$\mathfrak{p}^e \parallel \mathfrak{N}$*), compute a ring homomorphism* $\iota_{\mathfrak{p}} \colon \Lambda \to \mathrm{M}_2(\mathbb{Z}_E/\mathfrak{p}^e)$*.*

5. *For each* $\mathfrak{p} \mid \mathfrak{N}$*, find the (matrix) image of* $\iota_{\mathfrak{p}}(\delta_s)$ *for* $s = a, b, c$ *by using Lemma 3.2.3.*

6. *Using the Sun Zi Theorem (CRT)*

$$\iota_{\mathfrak{N}} \colon \Lambda \to \mathrm{M}_2(\mathbb{Z}_E/\mathfrak{N}) \simeq \prod_{\mathfrak{p}^e \parallel \mathfrak{N}} \mathrm{M}_2(\mathbb{Z}_E/\mathfrak{p}^e)$$

compute $\iota_{\mathfrak{N}}(\delta_s)$ *for* $s = a, b, c$*.*

7. *Let* $G_{\mathfrak{N}}$ *be the subgroup of* $\mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{N})$ *generated by the elements* $\iota_{\mathfrak{N}}(\delta)$*. If* $G_{\mathfrak{N}}$ *contains* $\mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$*, return* `true`*, else return* `false`*.*

Proof of correctness. This algorithm computes $G_{\mathfrak{N}}$ by definition. Step 1 ensures that the group is Borel-type (so the triple is admissible) and this step can be done in a finite field extension (see [56]). Step 4 can be computed following Voight [73, (IsMatrixRing)]. □

A Magma [17] implementation of this algorithm is available online [34]. With this algorithm, we can compute the image $G_{\mathfrak{N}}$ and thereby the genus of any curve $X_0(a, b, c; \mathfrak{N})$.

Algorithm 5.4.2 (Compute the genus of $X_0(a, b, c; \mathfrak{N})$)**.**
Input: a hyperbolic triple $(a, b, c) \in (\mathbb{Z}_{\geq 2} \cup \{\infty\})^3$ *and a nontrivial nonzero ideal* $\mathfrak{N} \subseteq \mathbb{Z}_{E(a,b,c)}$*.*

Output: returns `true` *and the genus of* $X_0(a,b,c;\mathfrak{N})$ *if* $\mathfrak{N}$ *is admissible. Otherwise, it returns* `false`*.*

1. *Run Algorithm 5.4.1 for* (a,b,c) *and* $\mathfrak{N}$*. If* `false`*, then return* `false`*. If* `true`*, let* $G_{\mathfrak{N}}$ *be the algorithm's output.*

2. *Find the action of each* $\bar{\delta}_s = \iota_{\mathfrak{N}}(\delta_s)$ *on* $G_{\mathfrak{N}}/H_0$ *for* $s \in \{a,b,c\}$*. This description gives the ramification of the degree* $\#G_{\mathfrak{N}}/H_0$ *cover* $X_0(a,b,c;\mathfrak{N}) \to \mathbb{P}^1$*.*

3. *Use Riemann-Hurwitz to compute the genus of* $X_0(a,b,c;\mathfrak{N})$*.*

Proof of correctness. Follows by the definition of $X_0(a,b,c;\mathfrak{N})$ and the Riemann–Hurwitz formula. □

This algorithm provides an independent way to check the results of section 4.5. Giving a formula for the composite case is more complicated since the structure of $G_{\mathfrak{N}}$ may be more complex, and the ramification behaves differently.

Lemma 5.4.3. *Let* $Y \to X$ *be a map of degree greater than 1 with* $\text{genus}(X) \geq 2$*. Then we have*

$$\text{genus}(Y) > \text{genus}(X). \tag{5.4.4}$$

Proof. Follows immediately from the Riemann-Hurwitz formula. □

Lemma 5.4.5. *Let* (a,b,c) *be a hyperbolic triple and let* $\mathfrak{N}$ *be a nontrivial ideal of* E*. If* $X_0(\mathfrak{N})$ *has genus* g*, then for all primes* $\mathfrak{p} \mid \mathfrak{N}$*, the curve* $X_0(\mathfrak{p})$ *has genus bounded above by* g*.*

Proof. It follows from the existence of the cover $X_0(\mathfrak{N}) \to X_0(\mathfrak{p})$ and the Riemann-Hurwitz formula. □

From Lemma 5.4.5 and Corollary 4.4.6 we can conclude that if the genus of $X_0(\mathfrak{N})$ is bounded by g, then the list of possible prime ideals that can divide $\mathfrak{N}$ is finite. The list of triples and prime divisors of $\mathfrak{N}$ can be computed explicitly using Algorithm 4.5.2. It remains to show that the power of the primes dividing $\mathfrak{N}$ can be bounded above.

Algorithm 5.4.6 (Enumerate curves $X_0(a, b, c; \mathfrak{N})$ of bounded genus)**.**
Input: an integer $g_0 \in \mathbb{Z}_{\geq 0}$.
Output: The list of all hyperbolic triples (a, b, c) *and admissible nontrivial ideals* $\mathfrak{N}$ *such that* $X_0(a, b, c; \mathfrak{N})$ *has genus bounded above by* g_0.

1. *Use Algorithm 4.5.2 to enumerate the finitely many hyperbolic triples* (a, b, c) *and admissible prime ideals* $\mathfrak{p}$ *that give rise to curves* $X_0(a, b, c; \mathfrak{p})$ *of genus* $g \leq g_0$. *Add to this list the triples* (3.4.1), *namely*

$$(3, 3, 3; \mathfrak{p}_3), (2, 3, 3; \mathfrak{p}_3), (2, 3, 4; \mathfrak{p}_3), (2, 3, 5; \mathfrak{p}_2), (2, 3, 5; \mathfrak{p}_5).$$

2. *For each* (a, b, c) *on the list, set* `Lprime`, `L`, *and* `lowGenus` *as the list of all prime ideals that appear on the list from Step 1 associated to* (a, b, c). *Then repeat the following step until the list* `L` *is empty.*

3. *Initialize the empty list* `Lnew`. *For each element* $\mathfrak{N}$ *of* `L` *do the following. For each prime ideal* $\mathfrak{p}$ *of* `Lprime`, *let* p *be the prime of* $\mathbb{Z}$ *below* $\mathfrak{p}$. *Use Algorithm 5.4.2 to compute the genus* g *of the curve* $X_0(a, b, c; \mathfrak{N} \cdot \mathfrak{p})$. *If* $g \leq g_0$, *then add* $(a, b, c; \mathfrak{N}\mathfrak{p})$ *to the lists* `lowGenus` *and* `Lnew`. *If* $\mathfrak{N} + \mathfrak{p} = \mathbb{Z}_E$, *then compute the genus* g_{e_a, e_b, e_c} *of the curves* $X_0(a \cdot p^{e_a}, b \cdot p^{e_b}, c \cdot p^{e_c}; \mathfrak{N} \cdot \mathfrak{p})$, *where* $e_s \in \{0, 1\}$

for $s \in \{a, b, c\}$. If $g_{e_a,e_b,e_c} \leq g_0$, then add $(a \cdot p^{e_a}, b \cdot p^{e_a}, c \cdot p^{e_a}; \mathfrak{N} \cdot \mathfrak{p})$ to the lists `lowGenus` *and* `Lnew`*. Once done with all possible products, set* `L` *equal to* `Lnew`*.*

4. *Return the list* `lowGenus`*.*

The following lemma is necessary to prove the correctness of the algorithm.

Lemma 5.4.7. *If Algorithm 5.4.6 terminates for $g_0 = 1$, then it terminates for all $g_0 \geq 0$.*

Proof. Given $g_0 \geq 2$, the genera of the curves $X_0(a, b, c; \mathfrak{N}\mathfrak{p})$ in Step 3 are 0, 1, or at least 2. However, there are only finitely many such curves with genus 0 or 1 by assumption. Lemma 5.4.5 implies that when the genus of $(a, b, c; \mathfrak{N})$ is $g \geq 2$, the genus of the new curve with level $\mathfrak{N} \cdot \mathfrak{p}$ must have strictly larger genus. Hence the process of multiplying by prime ideals in Step 3 will stop eventually. □

Proof of correctness of Algorithm 5.4.6. By Lemma 5.4.5, every curve $X_0(a, b, c; \mathfrak{N})$ with genus $g \leq g_0$ covers the curve $X_0(a, b, c; \mathfrak{p})$ with genus bounded above by g_0 and $\mathfrak{p}$ any prime ideal dividing $\mathfrak{N}$. This ensures that starting with the list in Step 1 allows us to enumerate all possibilities. By Corollary 5.2.7, if $\mathfrak{N}$ is admissible for (a, b, c), then $\mathfrak{N}\mathfrak{p}$ is admissible for $(ap^{e_a}, bp^{e_b}, cp^{e_c})$, where $e_s \in \{0, 1\}$ for $s \in \{a, b, c\}$.

We run a Magma [17] implementation of Algorithm 5.4.6 with $g_0 = 1$. This process terminates and gives a finite list of triples and ideals. Then Lemma 5.4.7 implies that the algorithm terminates for all $g_0 \geq 0$. □

Remark 5.4.8. Our Magma [17] implementation to enumerate curves $X_0(a, b, c; \mathfrak{N})$ of genus 0 and 1 is time and memory-consuming. For a faster algorithm, see the ideas in section 5.7.

Proposition 5.4.9. *For any integer $g_0 \geq 0$, there are finitely many triangular modular curves $X_0(a,b,c;\mathfrak{N})$ of genus bounded above by g_0 with $(a,b,c) \in (\mathbb{Z}_{\geq 2} \cup \{\infty\})^3$ hyperbolic and $\mathfrak{N}$ admissible.*

Proof. Running Algorithm 5.4.6 for $g_0 = 0$ and $g_0 = 1$, we find that the algorithm terminates (with finitely many curves output). The correctness then follows from Lemma 5.4.7. □

Our implementation of Algorithm 5.4.6 is available online [34].

Section 5.5

Triangular modular curves $X_1(a,b,c;\mathfrak{N})$

We first study the curves $X_1'(a,b,c;\mathfrak{N})$ and prove the finiteness result and corresponding enumeration algorithm for these curves. Afterwards, we recall that we have an additional map $X_1(a,b,c;\mathfrak{N}) \to X_1'(a,b,c;\mathfrak{N})$ as in (5.3.10). This map is at most a degree two cover and we completely characterize it in terms of (a,b,c) and $\mathfrak{N}$. This allows us to conclude with the same kind of results for curves $X_1(a,b,c;\mathfrak{N})$.

Algorithm 5.5.1 (Genus of $X_1'(a,b,c;\mathfrak{N})$)**.**
Input: a hyperbolic triple $(a,b,c) \in (\mathbb{Z}_{\geq 2} \cup \{\infty\})^3$ and a nontrivial nonzero ideal $\mathfrak{N}$ of E such that $\mathfrak{N} \nmid \beta\mathfrak{d}_{F|E}$.
Output: the genus of $X_1'(a,b,c;\mathfrak{N})$.

1. *Compute $G_{\mathfrak{N}}$ from Algorithm 5.4.1.*

2. *Find the action of each $\bar{\delta}_s$ on $G_{\mathfrak{N}}/H_1$ for $s \in \{a,b,c\}$. This gives the ramification of the cover $X_1'(a,b,c;\mathfrak{N}) \to \mathbb{P}^1$. The degree of this cover is $\#G_{\mathfrak{N}}/H_1$.*

3. *Use Riemann-Hurwitz to compute the genus of* $X_1'(a, b, c; \mathfrak{N})$.

Proof of correctness. Follows from the Riemann-Hurwitz formula. □

Algorithm 5.5.2 (Enumerate curves $X_1'(a, b, c; \mathfrak{N})$ of bounded genus)**.**

Input: an integer $g_0 \in \mathbb{Z}_{\geq 0}$.

Output: a list `lowGenusX1` *of all hyperbolic triples* (a, b, c)*, admissible ideals* $\mathfrak{N}$ *such that the genus of* $X_1'(a, b, c; \mathfrak{N})$ *is* $g \leq g_0$.

1. *Loop over all hyperbolic triples* (a, b, c) *and ideals* $\mathfrak{N}$ *such that* $X_0(a, b, c; \mathfrak{N})$ *has genus bounded above by* g_0. *This list can be obtained from Algorithm 4.5.2, Proposition 5.4.9, and Proposition 3.4.1.*

2. *For each triple* (a, b, c) *and ideal* $\mathfrak{N}$ *of the previous step, compute the genus* g *of* $X_1'(a, b, c; \mathfrak{N})$. *For this, use Corollary 4.6.4 if* $\mathfrak{N}$ *is prime, or Algorithm 5.5.1 otherwise. If* $g \leq g_0$*, add* $(a, b, c; \mathfrak{N})$ *to the list* `lowGenusX1`.

Proof of correctness. For all hyperbolic triples (a, b, c) and ideals $\mathfrak{N}$ there are maps $X_1'(a, b, c; \mathfrak{N}) \to X_0(a, b, c; \mathfrak{N})$ as in (5.3.5). Thus, the only curves $X_1'(a, b, c; \mathfrak{N})$ that can have genus $g \leq g_0$ must be covering curves $X_0(a, b, c; \mathfrak{N})$ of genus bounded above by g_0. □

Example 5.5.3. In fact, there are only two examples of potential genus ≤ 2 curves of the form $X_1'(a, b, c; \mathfrak{N})$ with $\mathfrak{N}$ composite: namely, with $(a, b, c) = (2, 3, 7)$ with $\mathfrak{N} = \mathfrak{p}^2$ with $\operatorname{Nm} \mathfrak{p} = 7$, and $(2, 4, 5)$ with $\mathfrak{N} = \mathfrak{p}^2$ with $\operatorname{Nm} \mathfrak{p} = 5$.

In the first case, we have $g(X_0(2, 3, 7; \mathfrak{p}^2)) = 1$ with elliptic points of order 3, and $g(X_1'(2, 3, 7; \mathfrak{p})) = 0$ with three elliptic points of order 7. It follows that $X_1'(2, 3, 7; \mathfrak{p}^2)$

has no elliptic points, so with the degree of the cover being $56 \cdot 21 = 1176$ we get

$$g(X_1'(2,3,7;\mathfrak{p}^2)) = 1 + \frac{1176}{2} \cdot \frac{1}{42} = 15.$$

A similar argument applies in the second case: for $X_0(2,4,5;\mathfrak{p}^2)$ we have genus 2 with two elliptic points of order 2 and for $X_1'(2,4,5;\mathfrak{p})$ we have genus $g = 0$ with four elliptic points of order 5; the degree is $30 \cdot 10 = 300$ and

$$g(X_1'(2,4,5;\mathfrak{p}^2)) = 1 + \frac{300}{2} \cdot \frac{1}{10} = 16.$$

Remark 5.5.4. As noted in section 5.3, the cover $X_1(a,b,c;\mathfrak{N}) \to X_1'(a,b,c;\mathfrak{N})$ is not an isomorphism only when the group $G_{\mathfrak{N}}$ is contained in $\mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$ and $\mu_2(\mathbb{Z}_E/\mathfrak{N}) \neq \{\pm 1\}$. This is, $\mathfrak{N}$ is the product of at least two distinct primes and for all primes $\mathfrak{p}|\mathfrak{N}$, we have $G_{\mathfrak{p}} \cong \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{p})$. In this case, we can use Lemma 5.3.6 to compute the degree of the cover and the genus of $X_1(a,b,c;\mathfrak{N})$.

Section 5.6

Main theorem

We are now ready to present the main result of this part of the thesis.

Theorem 5.6.1. *For any $g \in \mathbb{Z}_{\geq 0}$, there are only finitely many Borel-type triangular modular curves $X_0(a,b,c;\mathfrak{N})$ and $X_1(a,b,c;\mathfrak{N})$ of genus g with nontrivial admissible* *level* $\mathfrak{N} \neq (1)$. *The number of curves of genus at most* 2 *are as follows:*

Genus	0	1	2
$X_0(a,b,c;\mathfrak{N})$	71	190	153
$X_1(a,b,c;\mathfrak{N})$	28	51	36

Proof of Theorem 5.6.1. By Proposition 5.4.9, there are only finitely many curves $X_0(a,b,c;\mathfrak{N})$ with nontrivial admissible level $\mathfrak{N}$ and genus $g \leq g_0$. Since every curve $X_1'(a,b,c;\mathfrak{N})$ covers $X_0(a,b,c;\mathfrak{N})$, the same is true for $X_1'(a,b,c;\mathfrak{N})$ (see Corollary 4.6.1).

For the computation, we run Algorithm 4.5.2 with $g_0 = 2$, adding extra cases according to Proposition 3.4.1. The composite cases can be computed explicitly using Algorithm 5.4.2. To finish, we run Algorithm 4.6.5. We implement this enumeration in Magma [17], and the code is available in [34]. □

Section 5.7
Future work: computing monodromy with embedding numbers

We fix a hyperbolic triple (a,b,c) which is admissible for an ideal $\mathfrak{N}$. Algorithm 5.4.2, the algorithm to compute the genus of $X_0(\mathfrak{N})$, is intricate and computationally expensive. In contrast, for curves that are arithmetic, this computation is more straightforward: the ramification of the covers of $\mathbb{P}^1$ is entirely described by embedding numbers (for example, see [74, section 39.4]).

In this section, we suggest a method to show that the same is be valid for triangular modular curves; the genus of $X_0(\mathfrak{N})$ is also be described by embedding numbers. The primary tool we use is strong approximation. This section is work with John Voight.

To make notation in this section simpler, we define the following piece of notation. Given a group G and $x \in G$, we define

$$x^G := \{y^{-1}xy : y \in G\}.$$

We recall the task at hand is. By (5.3.5), there is a cover

$$X_0(\mathfrak{N}) = \Gamma_0(\mathfrak{N})\backslash\mathcal{H} \to \Delta\backslash\mathcal{H} = \mathbb{P}^1.$$

The ramification of this cover is described by the existence of nontrivial stabilizers (under conjugation) of subgroups of Δ of finite order. We note that from the structure of Δ, a subgroup of finite order is conjugate in Δ to $\langle\delta_s^i\rangle$ for $s \in \{a, b, c\}$ and $1 \leq i \leq s$. Thus, our task is to count the number of $\Gamma_0(\mathfrak{N})$-conjugacy classes of $(\delta_s^i)^\Delta$ for $s \in \{a, b, c\}$ and $1 \leq i \leq s$. The goal of using strong approximation is to bring this computation to a question about conjugacy of matrices over a ring.

Strong approximation

The main result we will use is the following.

Theorem 5.7.1 ([21], Theorem C)**.** *Let $\mathfrak{p} \nmid 2abc$ be a prime ideal of E. Recall the map $\iota_\mathfrak{p} : \Delta(a, b, c) \to \mathrm{PXL}_2(\mathbb{Z}_{E,\mathfrak{p}})$. Then the image of $\iota_\mathfrak{p}$ contains a dense subgroup of $\mathrm{PXL}_2(\mathbb{Z}_{E,\mathfrak{p}})$.*

Remark 5.7.2. Instead of working with the triangle group $\Delta(a, b, c)$, we can consider the theory of triangular modular curves by using extended triangle groups

$$\tilde{\Delta} := \langle \delta_a, \delta_b, \delta_c, -1 \mid \delta_a^a = \delta_b^b = \delta_c^c = \delta_a\delta_b\delta_c = -1,\ (-1)^2 = 1,\ \text{and}\ -1 \in Z(\tilde{\Delta})\rangle.$$

Proving strong approximation in this setting will allow us to avoid having to distinguish between the groups PSL and PGL.

For the rest of this section, we restrict to the case when there is a surjective map $\Delta \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z}_{E,\mathfrak{p}})$ for all $\mathfrak{p} \mid \mathfrak{N}$.

Lemma 5.7.3. *Let G be a group and let $\widetilde{H}$ and H be subgroups of G such that $\widetilde{H}$ is a subgroup of H and $\widetilde{H}$ is normal in G. Let $x \in G$, then the H-conjugacy classes in x^G are in bijection with the $H/\widetilde{H}$-conjugacy classes in $(xH)^{G/\widetilde{H}}$.*

Proof. We assume that $r \in G$ and that there is $h \in H$ with $h^{-1}xh = r^{-1}xr$. Then it is clear that $x\widetilde{H}$ is conjugate to $(r^{-1}\widetilde{H})(x\widetilde{H})(r\widetilde{H})$ by $h\widetilde{H}$. Now, we assume that $x\widetilde{H}$ and that there is $h\widetilde{H}$ with $h \in H$ such that

$$h^{-1}\widetilde{H}x\widetilde{H}h\widetilde{H} = g^{-1}\widetilde{H}x\widetilde{H}g\widetilde{H}.$$

Then, there is $\widetilde{H} \in \widetilde{H}$ with $(hg^{-1})^{-1}x(hg^{-1}) = \tilde{h}$. This implies that x and $g^{-1}hg$ are conjugate by $h \in H$, concluding our proof. □

Now we setup some notation for the next proposition. Let $R := \mathbb{Z}_{E,\mathfrak{N}}$ and let B be the quaternion algebra $\mathrm{M}_2(R)$ with order

$$\mathcal{O} = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{M}_2(R) : x, y, w \in R, z \in \mathfrak{N} \right\}.$$

Proposition 5.7.4. *Let δ_s be one of the generators of Δ with $s \in \{a, b, c\}$ and let $1 \leq i < s$. Then the $\Gamma_0(\mathfrak{N})$-conjugacy classes of $(\delta_s^i)^{\Delta}$ are in bijection with the $\mathcal{O}$-conjugacy classes of $(M_s^i)^{\mathcal{O}^1}$, where M_s is a matrix with characteristic polynomial $x^2 - \lambda_{2s}x + 1$.*

Proof. By strong approximation, there is a surjective map $\Delta \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$. Let H_0 be the image of $\Gamma_0(\mathfrak{N})$ and let M_s be the image of δ_s under this map. Then M_s has characteristic polynomial $x^2 - \lambda_{2s}x + 1$. Applying this map, we have that the number of $\Gamma_0(\mathfrak{N})$-conjugacy classes in $(\delta_s^i)^{\Delta/\Gamma_0(\mathfrak{N})}$ is equal to the number of H_0-conjugacy classes in $(M_s^i)^{\mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})}$. But $\mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$ is a quotient of $\mathrm{SL}_2(\mathbb{Z}_{E,\mathfrak{N}})$ (and under this quotient, H_0 is the quotient of $H_{0,\mathfrak{N}}$). Using Lemma 5.7.3, we conclude that the number of conjugacy classes we are seeking equals the number of $\mathcal{O}$-conjugacy classes of $(M_s^i)^{\mathcal{O}^1}$. □

Embedding numbers and monodromy

We maintain the assumption that there is a surjection $\Delta \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$. Before we prove our result, we present the basic theory of embedding numbers based on [74, section 30.3].

Let R be a local field. The theory of embeddings can be studied more generally for R a Dedekind domain, but focusing on local fields is enough for our purposes. Let π be the maximal ideal of R and let $k := R/\mathfrak{p}$ be its residue field. Assume $F := \mathrm{Frac}(R)$ and let B be a quaternion algebra over F. Let K be a separable quadratic F-algebra such that $K \hookrightarrow B$. We are interested in studying a special set of embeddings $\varphi : K \hookrightarrow B$. For that, we need to consider $\mathcal{O} \subseteq B$ a quaternion R-order and $S \subseteq K$ a quadratic R-order. We denote $\mathrm{Emb}_R(S, \mathcal{O})$ as the set of embeddings of S into $\mathcal{O}$ as R-algebras. We note that an embedding $S \hookrightarrow \mathcal{O}$ gives an embedding

$K \hookrightarrow B$ by extending scalars.

Since R is local, the R-order S is free, so $S = R[\gamma]$ for some $\gamma \in S$. Let $f_\gamma(x) := x^2 - t_\gamma x + n_\gamma$ be the minimal polynomial of γ and let d_γ be its discriminant.

Definition 5.7.5. An R-algebra embedding $\varphi : S \hookrightarrow \mathcal{O}$ is optimal if

$$\varphi(K) \cap \mathcal{O} = \varphi(S).$$

Let Γ be an order such that $\mathcal{O}^1 \leq \Gamma \leq N_{B^\times}(\mathcal{O})$. Then we have an action of Γ on $\mathrm{Emb}_R(S, \mathcal{O})$. For any $\gamma \in \Gamma$ and any optimal embedding $\varphi \in \mathrm{Emb}_R(S, \mathcal{O})$, we have

$$\alpha \mapsto \gamma^{-1}\varphi(\alpha)\gamma.$$

Then we define $\mathrm{Emb}(S, \mathcal{O}; \Gamma)$ as the set of Γ-conjugacy classes of optimal embeddings $S \hookrightarrow \mathcal{O}$. Since we will be interested in counting them, we define

$$m(S, \mathcal{O}; \Gamma) := \#\mathrm{Emb}(S, \mathcal{O}; \Gamma).$$

To see formulas for computing optimal embedding numbers, see for example [74, section 30.4].

Now we are ready to come back to our problem of computing ramification.

Proposition 5.7.6. *Let $M_s \in \mathrm{SL}_2(\mathbb{Z}_{E,\mathfrak{N}})$ be a matrix with characteristic polynomial $x^2 - \lambda_{2s}x + 1$. Then the number of $\mathcal{O}$-conjugacy classes of $(M_s)^{\mathcal{O}^1}$ is given by a sum of optimal embedding numbers:*

$$\sum_{S \supseteq R[M_s]} m(S, \mathcal{O}; \mathcal{O}^1)$$

Proof. By definition, the number of $\mathcal{O}$-conjugacy classes of $(M_s)^{\mathcal{O}^1}$ equals the number of embeddings from $R[M_s]$ to $\mathcal{O}$ up to conjugation by $\mathcal{O}^1$. Now, let $\varphi : R[M_s] \hookrightarrow \mathcal{O}$ be an embedding. Then, $S := \varphi^{-1}(\varphi(R) \cap \mathcal{O})$ is the unique order such that S can be optimally embedded to $\mathcal{O}$ up to conjugating by $\mathcal{O}^1$. □

We conclude with a computation of the ramification of the cover $X_0(\mathfrak{N}) \to \mathbb{P}^1$.

Corollary 5.7.7. *Let (a, b, c) be a hyperbolic triple which is admissible for an ideal $\mathfrak{N}$. Assume that there is a map $\Delta \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{N})$. Then the ramification of the cover $X_0(\mathfrak{N}) \to \mathbb{P}^1$ above the point corresponding to $s \in \{a, b, c\}$ is given by*

$$\sum_{1 \neq t | s} (t-1) \sum_{\substack{S \supseteq R[M_t] \\ \#S^\times/R^\times = s}} m\left(S, \mathcal{O}; \mathcal{O}^1\right), \tag{5.7.8}$$

where $M_s \in \mathcal{O}$ is a matrix with characteristic polynomial $x^2 - \lambda_{2s} x + 1$.

Proof (sketch). Let m_t be the number of cycles of order t and assume that $m_t > 0$. The order of each subgroup is determined by the trace of its generator. If $\gcd(i, n) = 1$, then the the trace of δ_s^i is the same as the trace of δ_s modulo $\mathfrak{N}$. This is why we restrict to divisors of s. Now, to ensure that the cycles have exactly order t, we require $\#S^\times/R^\times = s$. Then, the result follows from the previous discussion. □

Part II

Geometric quadratic Chabauty

Chapter 6

Preliminaries

We first present an overview of the geometric quadratic Chabauty method and introduce different incarnations of the Poincaré torsor. This work is joint with Sachi Hashimoto and Pim Spelier and is part of [32].

Section 6.1

Overview and Setup

We first set up some notation and give a broad overview of the geometric quadratic Chabauty method, then outline the contents of this part.

Let $X_{\mathbb{Q}}$ be any smooth, projective, geometrically irreducible curve over $\mathbb{Q}$ with a proper regular model X of $X_{\mathbb{Q}}$ over the integers and a fixed base point $b \in X_{\mathbb{Q}}(\mathbb{Q}) = X(\mathbb{Z})$. Let X^{sm} denote the open subscheme of X consisting of points at which X is smooth over $\mathbb{Z}$; then $X^{\mathrm{sm}}(\mathbb{Z}) = X(\mathbb{Z})$. Let $J_{\mathbb{Q}}$ denote the Jacobian of $X_{\mathbb{Q}}$ and let J denote the Néron model of $J_{\mathbb{Q}}$ over the integers. Suppose $J_{\mathbb{Q}}$ has Mordell–Weil rank r and Néron–Severi rank $\rho = \rho(J_{\mathbb{Q}})$. Let p be a prime greater than 2 not necessarily of good reduction for $X_{\mathbb{Q}}$.

The goal in geometric quadratic Chabauty is to lift X into a non-trivial $\mathbb{G}_m^{\rho-1}$-torsor T over J through a section $\widetilde{j_b}$ lying over the Abel–Jacobi embedding $j_b\colon X^{\mathrm{sm}} \to J$. Over $\mathbb{Q}$ we find this section $\widetilde{j_b}$ by giving a trivializing section of the $\mathbb{G}_m^{\rho-1}$-torsor $j_b^* T_{\mathbb{Q}}$ over $X_{\mathbb{Q}}$. If we want to spread this out over $\mathbb{Z}$, there is an obstruction coming from the multidegree.

Definition 6.1.1. The multidegree of a line bundle $\mathcal{L}$ on a curve C with geometrically irreducible components $(C_i)_{i\in I}$ over $\overline{\mathbb{Q}}$ is $(\deg \mathcal{L}|_{C_i})_{i \in I}$.

The map $\mathrm{Pic}(X) \to \mathrm{Pic}(X_{\mathbb{Q}})$ is not, in general, an isomorphism, and $j_b^* T$ is not in general trivial over X since its multidegree over the fibers $X_{\mathbb{F}_\ell}$ of X might be non-zero. This is the only obstruction: the torsor can be trivialized over an open $U \subset X^{\mathrm{sm}}$ constructed by picking one geometrically irreducible component in each fiber $X_{\mathbb{F}_\ell}$ and removing the other irreducible components. We call these fiberwise geometrically irreducible open $U \subset X^{\mathrm{sm}}$ simple open sets. By [64, Tag 04KV] every irreducible component of $X_{\mathbb{F}_\ell}$ admitting a smooth $\mathbb{F}_\ell$-point is geometrically irreducible. Hence every point $P \in X^{\mathrm{sm}}(\mathbb{Z})$ is contained in $U(\mathbb{Z})$ for a unique simple open U. There is a finite number $(U_i)_{i\in I}$ of simple open sets that cover $X^{\mathrm{sm}}(\mathbb{Z})$. For every such open, the map $\mathrm{Pic}(U) \to \mathrm{Pic}(X_{\mathbb{Q}})$ is an isomorphism. We fix a simple open U and obtain a trivialization $\widetilde{j_b}\colon U \to T$ lying over j_b.

Because $\mathbb{G}_m(\mathbb{Z}) = \{\pm 1\}$ is finite, we can expect the closure of $T(\mathbb{Z})$ inside the $(g + \rho - 1)$-dimensional p-adic manifold $T(\mathbb{Z}_p)$ to be of dimension at most r. The image of the p-adic points of U, namely $\widetilde{j_b}(U(\mathbb{Z}_p))$, is of dimension 1. Given this T, we see the analog of the classical Chabauty's theorem that applies to curves satisfying the inequality $r < g$ [20].

Theorem 6.1.2. *[36, section 9.2] When $r < g + \rho - 1$, the intersection*

$$\widetilde{j}_b(U(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})} \subset T(\mathbb{Z}_p)$$

is finite.

Definition 6.1.3. The geometric quadratic Chabauty set $X(\mathbb{Z}_p)_{\text{Geo}}$ is defined to be the union over the simple open sets $i \in I$ of $\widetilde{j}_b^*(\widetilde{j}_b(U_i(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})}) \subset U_i(\mathbb{Z}_p) \subset X(\mathbb{Z}_p)$.

The geometric quadratic Chabauty method computes this finite set $X(\mathbb{Z}_p)_{\text{Geo}}$, working in one simple open $U \subset X$ and one residue disk of $U(\mathbb{Z}_p)$ at a time. In Algorithm 8.1.1 we give an algorithm to determine $\widetilde{j}_b(U(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})}$ to finite precision.

To construct the $\mathbb{G}_m^{\rho-1}$-torsor T over J we start with the universal $\mathbb{G}_m$-torsor. In our calculations, this takes the form of the Poincaré torsor $\mathcal{M}^\times$ over $J \times J^0$ (this is a pullback of the Poincaré torsor over $J \times J^{\vee 0}$; for more details see chapter 6. Here $J^{\vee 0}$ is the fiberwise connected component of $J^\vee$ containing 0.

Remark 6.1.4. When p is a prime of good reduction for X, we have $J^0_{\mathbb{Z}_{(p)}} = J_{\mathbb{Z}_{(p)}}$ and $J^{\vee 0}_{\mathbb{Z}_{(p)}} = J^\vee_{\mathbb{Z}_{(p)}}$.

By the universality of $\mathcal{M}^\times$, we want to construct T by pulling back $\mathcal{M}^\times$ along morphisms $(\mathrm{id}, \alpha_i)\colon J \to J \times J^0$ for $i = 1, \ldots, \rho - 1$. Define

$$m := \mathrm{lcm}\{\exp\left((J/J^0)(\overline{\mathbb{F}}_q)\right) \mid q \text{ prime}\}, \tag{6.1.5}$$

where $\exp(G) \in \mathbb{N}_{\geq 1}$ is the exponent of a finite group G. Note that $m\cdot\colon J \to J^0$ is a well-defined morphism. Any morphism of schemes $J \to J$ can be written as a translation composed with an endomorphism, and hence we choose our morphisms

$\alpha_i\colon J \to J^0$ to be of the form $m \cdot \circ \operatorname{tr}_{c_i} \circ f_i$ with $c_i \in J(\mathbb{Z})$ and $f_i\colon J \to J$ a morphism of group schemes.

The torsor T is the product $T = \prod_{i=1}^{\rho-1} (\mathrm{id}, \alpha_i)^* \mathcal{M}^{\times}$ as a fiber product over J. We also let $\mathcal{M}^{\times,\rho-1}$ be the product taken as a fiber product over J via the first projection map $\mathcal{M}^{\times} \to J \times J^0 \to J$. In order to embed U through a section $\widetilde{j}_b\colon U \to T$, the torsor T pulled back to U must be trivial: that is $j_b^*(\mathrm{id}, \alpha_i)^* \mathcal{M}^{\times}$ must be trivial over U. The torsor $(\mathrm{id}, \alpha_i)^* \mathcal{M}^{\times}$ over J can be thought of as the total space of a line bundle without its zero section, and the condition that its pullback $L_{\alpha_i} := j_b^*(\mathrm{id}, \alpha_i)^* \mathcal{M}^{\times}$ to U is trivial forces the corresponding line bundle to be degree 0. Equivalently, the trace of f_i must be 0. The condition that L_{α_i} is trivial uniquely determines c_i.

$$\begin{tikzcd}
 & T \arrow[r] \arrow[d] & \mathcal{M}^{\times,\rho-1} \arrow[d] \\
U \arrow[ur, "\widetilde{j}_b"] \arrow[r, "j_b"] & J \arrow[r, "(\mathrm{id}, m\cdot\circ \operatorname{tr}_{c_i} \circ f_i)_i"] & J \times (J^0)^{\rho-1}
\end{tikzcd} \tag{6.1.6}$$

Because the Néron–Severi rank of $J_{\mathbb{Q}}$ is ρ, the Jacobian J has $\rho - 1$ independent non-trivial endomorphisms of trace 0.

Definition 6.1.7. For Y a scheme, S a ring with residue field $\operatorname{Spec} \mathbb{F}_p \to \operatorname{Spec} S$ and $Q \in Y(\mathbb{F}_p)$, we define the residue disk over Q, denoted by $Y(S)_Q := \{y \in Y(S) \mid \overline{y} = Q\}$, to be the set of all S-points specializing to Q.

Let $\overline{P} \in U(\mathbb{F}_p)$. The residue disk $U(\mathbb{Z}_p)_{\overline{P}}$ embeds into the residue disk $T(\mathbb{Z}_p)_{\widetilde{j}_b(\overline{P})}$ of T through the section $\widetilde{j}_b$. Since $p > 2$, we have that 1 and -1 reduce to different points modulo p and hence the map $T(\mathbb{Z})_{\widetilde{j}_b(\overline{P})} \to J(\mathbb{Z})_{j_b(\overline{P})}$ is a bijection. By [60, Proposition 2.3] and the fact that $p > 2$ the residue disk $J(\mathbb{Z})_{j_b(\overline{P})}$ is up to a translation isomorphic to $\mathbb{Z}_p^r$. In [36, Theorem 4.10] this bijection $T(\mathbb{Z})_{\widetilde{j}_b(\overline{P})} \to J(\mathbb{Z})_{j_b(\overline{P})}$ is upgraded to a morphism $\kappa\colon \mathbb{Z}_p^r \to T(\mathbb{Z}_p)_{\widetilde{j}_b(\overline{P})}$ with image exactly $\overline{T(\mathbb{Z})}_{\widetilde{j}_b(\overline{P})}$.

In this part of the manuscript, we explain how to make the geometric quadratic Chabauty method explicit in the case where p is of good reduction by giving algorithms to compute $\widetilde{j}_b$ and κ in a residue disk as polynomials in parameters up to finite precision. This process translates the geometric Chabauty method into solving simple polynomial equations. We also give algorithms to work in residue disks of T explicitly using p-adic heights and Coleman integrals. Moreover, by writing the geometric quadratic Chabauty method in terms of p-adic heights and Coleman integrals, we can prove Theorem C.

Section 6.2

The Poincaré torsor $\mathcal{P}$

A crucial object of study in this part of the thesis is the Poincaré torsor. This has four incarnations, which we introduce in this section, section 6.3, section 6.4, and section 6.5. In this section, we present the first incarnation of the Poincaré torsor $\mathcal{P}_{\mathbb{Q}}^{\times}$ over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, its biextension structure, and the torsor $\mathcal{P}^{\times}$ over the integers. For more details on the Poincaré torsor and biextensions, see [54, section I.2.5] or Grothendieck's Exposés VII and VIII [40].

Given a line bundle $\mathcal{L}$ over a scheme S, there is an associated $\mathbb{G}_m$-torsor $\mathcal{L}^{\times}$ defined by taking the sheaf of non-vanishing sections, and similarly given a $\mathbb{G}_m$-torsor Y there is an associated line bundle $Y \otimes_{\mathcal{O}_S^{\times}} \mathcal{O}_S$. Applying these associations to the Poincaré bundle, we obtain the universal $\mathbb{G}_m$-torsor $\mathcal{P}_{\mathbb{Q}}^{\times}$ over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, called the Poincaré torsor.

Alternatively,

$$\mathcal{P}_{\mathbb{Q}}^{\times} = \mathrm{Isom}_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}}(\mathcal{O}_{J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}}, \mathcal{P}_{\mathbb{Q}}),$$

i.e. for a scheme $S/(J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee})$ we have that $\mathcal{P}_{\mathbb{Q}}^{\times}(S)$ consists of isomorphisms of line bundles $\mathcal{O}_S \to (\mathcal{P}_{\mathbb{Q}})_S$. This set $\mathcal{P}_{\mathbb{Q}}^{\times}(S)$ is an $\mathcal{O}_S(S)^{\times}$-pseudotorsor: either empty or an $\mathcal{O}_S(S)^{\times}$-torsor.

The Poincaré torsor $\mathcal{P}_{\mathbb{Q}}^{\times}$ has the structure of a biextension over $J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee}$, as we will now explain. Addition in $J_{\mathbb{Q}}^{\vee}$ corresponds to tensoring line bundles on $J_{\mathbb{Q}}$. This, along with the theorem of the square, induces a partial group law on $\mathcal{P}_{\mathbb{Q}}^{\times}$. Let S be a scheme over $\mathbb{Q}$. For $x \in J_{\mathbb{Q}}(S)$ and $y_1, y_2 \in J_{\mathbb{Q}}^{\vee}(S)$ we have a tensor product which is an isomorphism of $\mathbb{G}_m$-torsors

$$(x, y_1)^* \mathcal{P}_{\mathbb{Q}}^{\times} \otimes (x, y_2)^* \mathcal{P}_{\mathbb{Q}}^{\times} \to (x, y_1 + y_2)^* \mathcal{P}_{\mathbb{Q}}^{\times}$$

that we denote by $\otimes_2$ because we are adding on the second coordinate (while the first coordinate stays fixed). Similarly since $(J_{\mathbb{Q}}^{\vee})^{\vee}$ is canonically identified with $J_{\mathbb{Q}}$, we also have the tensor product

$$(x_1, y)^* \mathcal{P}_{\mathbb{Q}}^{\times} \otimes (x_2, y)^* \mathcal{P}_{\mathbb{Q}}^{\times} \to (x_1 + x_2, y)^* \mathcal{P}_{\mathbb{Q}}^{\times}$$

called $\otimes_1$. These two partial group laws are compatible. Let $x_1, x_2 \in J_{\mathbb{Q}}(S)$, $y_1, y_2 \in J_{\mathbb{Q}}^{\vee}(S)$, and $z_{ij} \in (x_i, y_j)^* \mathcal{P}_{\mathbb{Q}}^{\times}(S)$, for $i, j \in \{1, 2\}$. Then

$$(z_{11} \otimes_2 z_{12}) \otimes_1 (z_{21} \otimes_2 z_{22}) = (z_{11} \otimes_1 z_{21}) \otimes_2 (z_{12} \otimes_1 z_{22}).$$

In other words, tensoring points in the biextension is not order-dependent. Together with this compatibility, the structure of these two partial group laws over the product $J_{\mathbb{Q}} \times J^{\vee}_{\mathbb{Q}}$ make $\mathcal{P}^{\times}_{\mathbb{Q}}$ a $\mathbb{G}_m$-biextension over $J_{\mathbb{Q}} \times J^{\vee}_{\mathbb{Q}}$.

For our applications, we need to work over the integers. Let J^0 be the fiberwise connected component of J containing 0. This represents line bundles on C that are fiberwise of multidegree 0. Let $J^{\vee}$ be the Néron model of $J^{\vee}_{\mathbb{Q}}$ and similarly let $J^{\vee 0}$ be the fiberwise connected component of $J^{\vee}$ containing 0. The Poincaré torsor extends to a biextension $\mathcal{P}^{\times}$ over $J \times J^{\vee 0}$. In particular, the integer points of $\mathcal{P}^{\times}$ lying over $(x, y) \in (J \times J^{\vee 0})(\mathbb{Z})$ form a $\mathbb{G}_m(\mathbb{Z})$-torsor, i.e. a $\{\pm 1\}$-torsor. So there is exactly one integer point lying over (x, y), up to sign.

Section 6.3
The biextension $\mathcal{M}$

To work with explicit computations of points in the Poincaré torsor in practice, we need a few modifications of $\mathcal{P}^{\times}$. We introduce two torsors over $J \times J^0$ given by the biextension $\mathcal{M}^{\times}$ and the trivial biextension $\mathcal{N}$.

We first discuss the construction of $\mathcal{M}^{\times}$ and the generating sections of its residue disks. The Abel–Jacobi embedding induces an isomorphism $j_b^*\colon J^{\vee} \to J$ and hence an isomorphism $j_b^*\colon J^{\vee 0} \to J^0$. We define

$$\mathcal{M}^{\times} := (\mathrm{id}, j_b^{*,-1})^* \mathcal{P}^{\times}. \tag{6.3.1}$$

For the torsor $\mathcal{M}^{\times}$, we have an explicit description of the fibers. Let S be a scheme, $x \in J(S)$ be a point corresponding to a line bundle $\mathcal{L}$, and $y \in J^0(S)$ be a point with representing divisor $E = E^+ - E^-$ such that E^+ and E^- are effective and of the same multidegree. We denote the fiber $(x,y)^*\mathcal{M}^\times$ of $\mathcal{M}^\times$ over $(x,y) \in (J \times J^0)(S)$ by $\mathcal{M}^\times(x,y)$. This fiber $\mathcal{M}^\times(x,y)$ is the $\mathbb{G}_m$-torsor

$$E^*\mathcal{L}^\times := \operatorname{Norm}_{E^+/S}\left(\mathcal{L}^\times\,|_{E^+}\right) \otimes \operatorname{Norm}_{E^-/S}\left(\mathcal{L}^\times\,|_{E^-}\right)^{-1}, \tag{6.3.2}$$

which we also denote by $\operatorname{Norm}_{E/S}\mathcal{L}^\times$. When $S = \operatorname{Spec}\mathbb{Z}$ we also write simply $\operatorname{Norm}_E \mathcal{L}^\times$. This fiber can be thought of as the aggregate of how $\mathcal{L}$ looks around E.

This description of the fiber is proven in [36, Proposition 6.8.7], and more general facts about these norms can be found in [36, section 6]. Because equation (6.3.2) may seem opaque, we provide some examples of how to apply the formula in practice.

Definition 6.3.3. Let S be a scheme. Let D and E be two relative Cartier divisors on X_S/S. We say D and E are disjoint over S if their support is disjoint as closed subschemes of X_S. In particular, it is not enough to have disjoint S-points if D or E does not split completely over S.

Example 6.3.4. Let S be a scheme, $[D] \in J(S)$, and $[E] \in J^0(S)$ be points of J and J^0 with representing divisors D and E where E has multidegree 0. Assume D and E are disjoint over S, and write $E = E^+ - E^-$ with E^+, E^- effective. Then the $\mathbb{G}_m$-torsor $E^*\mathcal{O}_X(D)^\times$ is generated by $\operatorname{Norm}_{E^+/S}(1) \otimes \operatorname{Norm}_{E^-/S}(1)^{-1}$ where 1 is here seen as a section of $\mathcal{O}_X(D)^\times|_{E^{\pm 1}}$. We also denote this generator by E^*1.

Example 6.3.5. Suppose the fiber of $X^{\mathrm{sm}}/\mathbb{Z}$ over 2 is geometrically irreducible. Let $[D] \in J(\mathbb{Z})$ and $[E] \in J^0(\mathbb{Z})$ be points of J and J^0 with representing divisors D and E. Assume D and E are disjoint over $\mathbb{Z}[\frac{1}{2}]$ and meet with multiplicity 1 over 2. Then

$E^*\mathcal{O}_X(D)^\times$ is generated by $2^{-1}E^*1$.

Remark 6.3.6. Let S be a scheme. If $D = \operatorname{Div} g \in \operatorname{Div}^0(X_S/S)$ is the principal divisor of a rational function g and is disjoint from $E \in \operatorname{Div}^0(X_S/S)$, then the isomorphism $\mathcal{O}_X(D) \to \mathcal{O}_X$ given by multiplication by g induces an isomorphism $E^*\mathcal{O}_X(D)^\times \to E^*\mathcal{O}_X^\times$ sending E^*1 to $E^*g(E)$ where $g(E) \in \mathbb{G}_m(S)$.

Remark 6.3.7. In general, if $[D] \in J(\mathbb{Z})$, $[E] \in J^0(\mathbb{Z})$, and we have a choice of representing divisors D and E that are disjoint over $\mathbb{Q}$, using intersection theory we can determine $n \in \mathbb{Q}^\times$ unique up to sign, such that $\operatorname{Norm}_E \mathcal{O}_X(D)^\times$ is generated by $n \cdot E^*1$. If E is not of multidegree 0, there is a unique vertical divisor $V \subset C$ with $V + E$ of multidegree 0. In this case, one can compute the unique integer a up to sign such that $(E+V)^*\mathcal{O}_X(D)^\times = a \operatorname{Norm}_E \mathcal{O}_X(D)^\times$. This is treated in detail in [36, section 6.9].

The partial group laws on $\mathcal{M}^\times$ are also very explicit: let $[E], [E_1], [E_2] \in J^0(S)$ and $\mathcal{L}, \mathcal{L}_1, \mathcal{L}_2 \in J(S)$, then the group laws are given by the morphisms

$$E_1^*\mathcal{L}^\times \otimes E_2^*\mathcal{L}^\times \to (E_1 + E_2)^*\mathcal{L}^\times \tag{6.3.8}$$

corresponding to $\otimes_2$ and

$$E^*\mathcal{L}_1^\times \otimes E^*\mathcal{L}_2^\times \to E^*(\mathcal{L}_1 \otimes \mathcal{L}_2)^\times \tag{6.3.9}$$

corresponding to $\otimes_1$.

Example 6.3.10. Let $x_1, x_2 \in J(\mathbb{Z})$ and $y_1, y_2 \in J^0(\mathbb{Z})$. Let $z_{ij} \in \mathcal{M}^\times(\mathbb{Z})$ be points above (x_i, y_j) for $i \in \{1, 2\}$. Then for $n_1, n_2, m_1, m_2 \in \mathbb{Z}$ we can construct points above $(n_1x_1 + n_2x_2, m_1y_1 + m_2y_2)$ by the formula

$$\left(z_{11}^{\otimes_2 m_1} \otimes_2 z_{12}^{\otimes_2 m_2}\right)^{\otimes_1 n_1} \otimes_1 \left(z_{21}^{\otimes_2 m_1} \otimes_2 z_{22}^{\otimes_2 m_2}\right)^{\otimes_1 n_2}.$$

This allows us to construct many integer points of $\mathcal{M}^\times$ by starting with a few points that lie over generators of the Jacobian and then applying the partial group laws. In section 7.3, we will use this idea to determine the integer points of the torsor T landing in a specific residue disk of T.

Section 6.4

The trivial biextension $\mathcal{N}$

In practice, we often translate between $\mathcal{M}$, introduced in section 6.3, and the trivial biextension $\mathcal{N}$ where we do our computations. We explain how to make this translation following [36, section 9.3]. From now on, we assume $p > 2$ is a prime of good reduction for $X_\mathbb{Q}$.

Let $[D] \in J(\mathbb{Q}_p)$ and $[E] \in J^0(\mathbb{Q}_p)$ be divisor classes with a choice of representing divisors D and E that are disjoint over $\mathbb{Q}_p$. Then $E^*\mathcal{O}_X(D)^\times$ is a $\mathbb{Q}_p^\times$-torsor, trivial with generator E^*1 by Example 6.3.4. Let h_p be the cyclotomic Coleman–Gross local height at p with respect to an isotropic splitting $H^1_{\mathrm{dR}}(X) = H^0(X, \Omega^1_X) \oplus W$ of the Hodge filtration [25, Section 5]. Choose a branch of the logarithm with $\log p = 0$ so that it is compatible with h_p. The height h_p is a biadditive, symmetric pairing on disjoint divisors of degree 0, taking values in $\mathbb{Q}_p$. For f, a rational function and $\operatorname{Div} f$ its associated divisor, it also satisfies the equality $h_p(D, \operatorname{Div} f) = \log f(D)$.

Remark 6.4.1. The assumption that p is a prime of good reduction for X is used to define the logarithm of $J_{\mathbb{Z}_p}$ and to compute the Coleman–Gross height and iterated Coleman integrals. There is a more general construction using Vologodsky integrals to construct the Coleman–Gross height [12]. However, currently there is no known way to compute this more general height for a prime of bad reduction.

We define a map

$$\begin{aligned} \psi \colon \mathcal{M}^{\times}(\mathbb{Z}_p) &\to \mathbb{Q}_p \\ E^*\lambda \in E^*\mathcal{O}_X(D)^{\times} &\mapsto \log\lambda + h_p(D,E). \end{aligned} \tag{6.4.2}$$

We define $\mathcal{N}$ to be the trivial $\mathbb{Q}_p$-biextension $J(\mathbb{Q}_p)\times J(\mathbb{Q}_p)\times\mathbb{Q}_p$ over $J(\mathbb{Q}_p)\times J(\mathbb{Q}_p)$. By definition, the partial group laws in $\mathcal{N}$ are just addition keeping one coordinate fixed. Let $[D],[D_1],[D_2]\in J(\mathbb{Q}_p)$ and $[E],[E_1],[E_2]\in J^0(\mathbb{Q}_p)$ and $v_1,v_2\in\mathbb{Q}_p$. The first group law is

$$([D_1],[E],v_1) +_1 ([D_2],[E],v_2) = ([D_1]+[D_2],[E],v_1+v_2).$$

The second group law is

$$([D],[E_1],v_1) +_2 ([D],[E_2],v_2) = ([D],[E_1]+[E_2],v_1+v_2).$$

Definition 6.4.3. We define the morphism of biextensions

$$\Psi \colon \mathcal{M}^{\times}(\mathbb{Z}_p) \to \mathcal{N}$$

to be the projection $\mathcal{M}^{\times}(\mathbb{Z}_p)\to J(\mathbb{Q}_p)\times J(\mathbb{Q}_p)$ on the first two factors and ψ on the last factor.

Remark 6.4.4. Since $\log(-1) = 0$, the morphism Ψ sends the two integer points of $\mathcal{M}^{\times}(\mathbb{Z})$ above a fixed integer point of $J \times J^0$ to the same point.

The following proposition appears in [36, Section 9.3] but is not proven.

Proposition 6.4.5. *The map $\Psi\colon \mathcal{M}^{\times}(\mathbb{Z}_p) \to \mathcal{N}$ is a morphism of biextensions.*

Proof. First, we show that Ψ is well-defined. For divisor classes $[D] \in J(\mathbb{Q}_p)$ and $[E] \in J^0(\mathbb{Q}_p)$ we can always choose representing divisors D and E with disjoint support over $\mathbb{Q}_p$; we show that the choice of representing divisors D and E does not matter. Suppose $D = D' + \operatorname{Div} g$ for some rational function g with $\operatorname{Div} g$ disjoint from E. Multiplication by g induces an isomorphism $\mathcal{O}_X(D) \to \mathcal{O}_X(D')$ sending $E^*1 \mapsto E^*g(E)$ by Remark 6.3.6. Under ψ, the section $E^*\lambda$ in $E^*\mathcal{O}_X(D)$ maps to $\log\lambda + h_p(D, E)$ while $E^*g(E)\lambda$ in $E^*\mathcal{O}_X(D')$ maps to $\log\lambda + \log g(E) + h_p(D', E)$. But since $h_p(\operatorname{Div} g, E) = \log g(E)$ we have the equality $h_p(D', E) + \log g(E) = h_p(D, E)$, so the choice of representing divisor for $[D]$ does not change the value of Ψ. By symmetry of the norm [36, section 6.5], we can also conclude that Ψ does not depend on the choice of representing divisor for $[E]$.

Finally we show that Ψ preserves the two group laws (6.3.8) and (6.3.9). Consider $[D_1], [D_2] \in J(\mathbb{Q}_p)$, and $[E] \in J^0(\mathbb{Q}_p)$ with E disjoint from D_1 and D_2. Let $E^*\lambda_1 \in E^*\mathcal{O}_X(D_1)$ and $E^*\lambda_2 \in E^*\mathcal{O}_X(D_2)$. Under ψ, the section $E^*\lambda_i$ maps to $\log\lambda_i + h_p(D_i, E)$ for $i = 1, 2$. The group law $\otimes_1$ in $\mathcal{M}^{\times}$ sends the sections to $E^*(\lambda_1\lambda_2)$ in $E^*\mathcal{O}_X(D_1 + D_2)$. Under the map ψ, the section $E^*(\lambda_1\lambda_2)$ is sent to

$$\log(\lambda_1\lambda_2) + h_p(D_1 + D_2, E) = \log\lambda_1 + \log\lambda_2 + h_p(D_1, E) + h_p(D_2, E).$$

Therefore Ψ preserves $\otimes_1$. By symmetry of the norm, it also preserves $\otimes_2$. □

The following proposition relates this to the global p-adic height.

Proposition 6.4.6. *Let $[D] \in J(\mathbb{Z})$ and $[E] \in J^0(\mathbb{Z})$ with representing divisors D and E that have disjoint support over $\mathbb{Z}_{(p)}$. Let F be the unique vertical divisor such that $F + E$ has multidegree 0 on all fibers $X_{\mathbb{F}_q}$. Let $z \in \mathcal{M}^\times([D], [E+F])(\mathbb{Z})$. Then $\psi(z) = h([D], [E])$ where $h(\cdot, \cdot)$ denotes the global p-adic height.*

Proof. Let $\mathcal{L} = \mathcal{O}_X(D)$. Write $F = \sum_q F_{\mathbb{F}_q}$ where q ranges over the primes of bad reduction for X and $F_{\mathbb{F}_q}$ has support in $X_{\mathbb{F}_q}$. Then by [36, Proposition 6.9.3] we have the equation

$$\mathcal{M}^\times([D], [E]) = \prod_q q^{-F_{\mathbb{F}_q} \cdot D} \operatorname{Norm}_E(\mathcal{L}^\times)$$

where q ranges over the bad primes.

Recall that $\operatorname{Norm}_E(\mathcal{L}^\times)$ is by definition $\operatorname{Norm}_{E/\operatorname{Spec}\mathbb{Z}}(\mathcal{L}^\times|_E)$; this torsor is canonically identified with $\mathcal{O}_{\operatorname{Spec}\mathbb{Z}}(\prod_q q^{-(E\cdot D)_q})^\times$ and hence has generator $\prod_q q^{-(E\cdot D)_q}$, where $(E \cdot D)_q$ denotes the intersection number of E and D over $\mathbb{Z}_{(q)}$ taking values in $\mathbb{Z}$.

In total, we see that under these identifications $\mathcal{M}^\times([D], [E+F])$ is generated by the element $E^* \prod_q q^{-((E+F)\cdot D)_q}$. By definition, for $q \neq p$, we have that $h_q(D, E)$ is $-((E+F) \cdot D)_q \log q$, and hence we get

$$\begin{aligned} &= \sum_{q \neq p} h_q(D, E) + h_p(D, E) \\ &= h([D], [E]) \end{aligned}$$

as we wanted. □

Section 6.5
The torsor T_f

We now are ready to define a $\mathbb{G}_m$-torsor over J. We first set up some notation. Recall from section 6.1 that we have fixed a simple open set $U \subset X^{\mathrm{sm}}$ that contains the smooth points of one geometrically irreducible component of each fiber. Let f be a trace 0 endomorphism of J. Recall the integer m from (6.1.5). The map $m \cdot \circ f$ is a morphism $J \to J^0$. Let $c \in J(\mathbb{Z})$ denote the unique element such that $j_b^*(\mathrm{id}, m \cdot \circ \operatorname{tr}_c \circ f)^* \mathcal{M}^\times$ is trivial over U. Let $\alpha_f := m \cdot \circ \operatorname{tr}_c \circ f$. Let $\xi_f \colon T_f \to J$ denote the $\mathbb{G}_m$-torsor $(\mathrm{id}, \alpha_f)^* \mathcal{M}^\times$ over J. The trivialization of $j_b^*(\mathrm{id}, m \cdot \circ \operatorname{tr}_c \circ f)^* \mathcal{M}^\times$ then gives us a morphism $\widetilde{j_{b,f}} \colon U \to T_f$ of schemes over J.

Remark 6.5.1. If f is identically zero, then T_f is isomorphic to the trivial $\mathbb{G}_m$-torsor over J. If $r < g$ this reduces to the geometric linear Chabauty case, see [63, 41] for more details, but when $r = g$ this trivial torsor contains no information.

As discussed in the overview, we work on the curve residue disk by residue disk, and hence we will describe the residue disks of T_f, culminating in Lemma 6.5.9. Throughout the rest of this section, fix a $\bar{t} \in T_f(\mathbb{F}_p)$. We work inside the residue disk $T_f(\mathbb{Z}_p)_{\bar{t}}$. Since T_f is trivial on fibers, the residue disk $T_f(\mathbb{Z}_p)_{\bar{t}}$ is isomorphic to $J(\mathbb{Z}_p)_{\xi_f(\bar{t})} \times \mathbb{G}_m(\mathbb{Z}_p)_u$ for some unit $u \in \mathbb{F}_p$. We would like to parametrize this residue disk.

Definition 6.5.2. Let Y be a smooth scheme over $\mathbb{Z}_p$ of relative dimension d, and let $y \in Y(\mathbb{F}_p)$. We say $t_1, \ldots, t_d$ are parameters of Y at y if they are elements of the local ring $\mathcal{O}_{Y,y}$ such that the maximal ideal is given by $(p, t_1, \ldots, t_d)$.

Define $t_i' := t_i/p$. Then evaluation of t', the vector $(t_1', \ldots, t_d')$, gives a bijection

$t' \colon Y(\mathbb{Z}_p)_y \to \mathbb{Z}_p^d$. We call t' a parametrization given by parameters t_i.

Example 6.5.3. Take $Y = \mathbb{G}_m = \operatorname{Spec} \mathbb{Z}_p[x, x^{-1}]$ over $\mathbb{Z}_p$; this is of relative dimension 1. Let $y = 1 \in \mathbb{G}_m(\mathbb{F}_p)$. Then $x - 1$ is a parameter at y; it induces a parametrization $\theta \colon \mathbb{G}_m(\mathbb{Z}_p)_y \to \mathbb{Z}_p$ given by $u \mapsto (u-1)/p$. Note that the map log, defined by its power series $\log(1+x) = x - \frac{x^2}{2} + \cdots$ also induces a bijection $\varphi = \log / p \colon \mathbb{G}_m(\mathbb{Z}_p)_y \to \mathbb{Z}_p$, but this is *not* a parametrization; it is not given by evaluating elements of the maximal ideal, and is not even fully algebraic in nature. However, there is a relation between φ and θ, in that $\theta \circ \varphi^{-1}$ is given by the power series $\frac{1}{p}\big(xp - \frac{(xp)^2}{2} + \cdots\big) \in \mathbb{Z}_p[[x]]$.

In [36, Lemma 6.6.8] the residue disk $T_f(\mathbb{Z}_p)_{\bar{t}}$ is parametrized using parameters at $\bar{t}$. However, this parametrization can be difficult to work with because it uses parameters in J. The group law of J expressed in these parameters is given by complicated converging power series. It is possible to use this parametrization in practice: see for example [52], where the Khuri-Makdisi representation [43] is generalized in order to work with points of the Jacobian up to the required p-adic precision and compute parameters of them; however, with this representation other steps of the algorithm, like computing the image under an endomorphism, would be more difficult. Here, we opt to use the logarithm of J instead to give a bijection between the residue disk $T_f(\mathbb{Z}_p)_{\bar{t}}$ and $\mathbb{Z}_p^{g+1}$ that is not a parametrization in the sense of Definition 6.5.2. For a definition of this logarithm, see [42]. To describe the relationship between this bijection and the parametrization of this residue disk we need the framework of convergent power series.

Definition 6.5.4. Let $n \in \mathbb{N}$. The ring of convergent power series in n variables is defined as

$$\mathbb{Q}_p\langle x_1, \ldots, x_n\rangle := \left\{ \sum_{I \in \mathbb{N}^n} a_I \mathbf{x}^I \in \mathbb{Q}_p[[x_1, \ldots, x_n]] \mid \lim_{I \to \infty} |a_I| = 0 \right\},$$

where $\mathbf{x} = (x_1, \ldots, x_n)$ is the vector of variables. An element of this ring is called an integral convergent power series if it lies inside $\mathbb{Z}_p[[x_1, \ldots, x_n]]$. The convergent power series are those power series converging on all of $\mathbb{Z}_p^n$. Unlike formal power series, one can always compose two (integral) convergent power series, since by definition the resulting infinite sum inside the ring of (integral) convergent power series converges.

Remark 6.5.5. Let Y be a smooth scheme over $\mathbb{Z}_p$ of relative dimension d, let $y \in Y(\mathbb{F}_p)$, and let $\theta, \theta' \colon Y(\mathbb{Z}_p)_y \to \mathbb{Z}_p^d$ be two parametrizations. Then the composite $\theta' \circ \theta^{-1} \colon \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ is given by (multivariate) integral convergent power series that are linear modulo p, and in fact are of degree at most M modulo p^M.

Lemma 6.5.6. *Let G be a smooth, commutative group scheme over $\mathbb{Z}_p$ of relative dimension d. Let $G(\mathbb{Z}_p)_0$ be the residue disk containing the unit $0 \in G(\mathbb{Z}_p)$. Let $\theta \colon G(\mathbb{Z}_p)_0 \to \mathbb{Z}_p^d$ be a parametrization, and let $\log \colon G(\mathbb{Z}_p)_0 \to p\mathbb{Z}_p^d$ be a choice of logarithm. Then $\log \circ \theta^{-1} \colon \mathbb{Z}_p^d \to p\mathbb{Z}_p^d$ is given by d integral convergent power series in d variables. For $n \geq 0$ the coefficient of a degree n monomial in one of these power series has valuation at least $\max(1, n - v_p(n))$.*

Proof. By [63, Lemma 3.7] the function $\log \circ \theta^{-1}$ is given by integral convergent power series. There the third author gives the vector-valued formula

$$\log = \sum_{I \in \mathbb{N}^d \setminus (0,\ldots,0)} a_I c_{|I|} \mathbf{x}^I$$

where $\mathbf{x} = (x_1, \dots, x_d)$ is the vector of variables, the coefficients a_I lie in $\mathbb{Z}_p$, the notation $|I|$ means $i_1 + \cdots + i_d$ where $I = (i_1, \dots, i_d)$, and $c_n = p^n/n$. (In this paper we do not divide by p in the log, unlike in [63]). The result follows immediately from the observation that $v_p(c_{|I|}) = |I| - v_p(|I|)$. □

The following result establishes the analyticity of the map ψ on residue disks of $\mathcal{M}^\times$.

Lemma 6.5.7 ([36, Section 9.3])**.** *Let $\overline{z} \in \mathcal{M}^\times(\mathbb{F}_p)$. Let $\widetilde{z}$ be a lift of $\overline{z}$ to $\mathcal{M}^\times(\mathbb{Z}_p)$. Let $\Theta\colon \mathbb{Z}_p^{2g+1} \to \mathcal{M}^\times(\mathbb{Z}_p)_{\overline{z}}$ be a parametrization. Consider the map*

$$\begin{aligned} \psi_{\overline{z}}\colon \mathcal{M}^\times(\mathbb{Z}_p)_{\overline{z}} &\to \mathbb{Q}_p \\ z &\mapsto \frac{\psi(z) - \psi(\widetilde{z})}{p}. \end{aligned}$$

Then $\psi_{\overline{z}} \circ \Theta$ is given by a convergent power series.

As discussed above, we can now find a bijection between residue disks of T_f and $\mathbb{Z}_p^{g+1}$. We use the logarithm of the Jacobian, which gives an isomorphism $\log\colon J(\mathbb{Z}_p)_0 \to p\mathbb{Z}_p^g$ by choosing a basis of $H^0(J_{\mathbb{Z}_p}, \Omega^1)$ as well as the map ψ defined in (6.4.2). For ease of notation, we suppress the monomorphism $T_f \to \mathcal{M}^\times$ in our notation, and apply ψ directly to $T_f(\mathbb{Z}_p)$.

Definition 6.5.8. Recall that we fixed a $\overline{t} \in T_f(\mathbb{F}_p)$. Choose $\widetilde{t} \in T_f(\mathbb{Z}_p)_{\overline{t}}$ to be a lift of $\overline{t}$. Let $\varphi_f\colon T_f(\mathbb{Z}_p)_{\overline{t}} \to \mathbb{Z}_p^g \times \mathbb{Q}_p$ be defined by

$$\varphi_f(z) = ((\log \xi_f(z) - \log \xi_f(\widetilde{t}))/p, (\psi(z) - \psi(\widetilde{t}))/p)$$

where ψ is defined in (6.4.2) and the map $\xi_f\colon T_f \to J$ is the structure morphism of

T_f. We call φ_f a pseudoparametrization of the residue disk $T_f(\mathbb{Z}_p)_{\bar{t}}$.

Similarly to Example 6.5.3, this is not a parametrization; it shares some of the properties of a parametrization, notably the property in Remark 6.5.5, as the following lemma shows.

Lemma 6.5.9. *The pseudoparametrization φ_f is injective, and for any parametrization $\theta\colon T_f(\mathbb{Z}_p)_{\bar{t}} \to \mathbb{Z}_p^{g+1}$ the resulting map $\varphi_f \circ \theta^{-1}\colon \mathbb{Z}_p^{g+1} \to \mathbb{Z}_p^g \times \mathbb{Q}_p$ is given by $g+1$ convergent power series. The valuation of the coefficient of any degree n monomial occurring in one of the first g convergent power series is at least $\max(0, n-1-v_p(n))$. The valuation of the coefficient of any degree n monomial occurring in the last convergent power series is at least $n-1+v-2\lfloor \log_p n\rfloor$ (and at least 0 if $n=0$) where v is the constant from Lemma 6.5.7.*

Proof. By Lemma 6.5.6 and Lemma 6.5.7 the pseudoparametrization is given by convergent power series and the valuations of the coefficients behave in the required way. It remains to prove that it is a bijection onto its image. First, note that the maps $\frac{1}{p}\log\colon J(\mathbb{Z}_p)_0 \to \mathbb{Z}_p^g$ and $\frac{1}{p}\log\colon \mathbb{G}_m(\mathbb{Z}_p)_1 \to \mathbb{Z}_p$ are bijections.

Let $[D], m(f([D])+c) \in J(\mathbb{Z}_p)_0$ with disjoint representing divisors D and E, and let $\lambda_0, \lambda_1 \in \mathbb{G}_m(\mathbb{Z}_p)$ such that for $i = 0, 1$ we have $([D],[E],\lambda_i) \in T_f(\mathbb{Z}_p)_{\bar{t}}$. Assume that $\varphi_f(([D],[E],\lambda_0)) = \varphi_f(([D],[E],\lambda_1))$. Then we have that $\log\lambda + h_p(D,E) = \log\lambda' + h_p(D,E)$ so, because $\frac{1}{p}\log$ is injective on residue disks, then $\lambda = \lambda'$, and φ_f is injective.

By Lemma 6.5.6 the result follows. □

Section 6.6

The torsor T

Let $f_1, \dots, f_{\rho-1}$ be a basis for the trace 0 endomorphisms of J. We simplify our notation by setting $c_i \coloneqq c_{f_i}$, $\alpha_i \coloneqq \alpha_{f_i}$, $T_i \coloneqq T_{f_i}$, and $\xi_i \coloneqq \xi_{f_i} \colon T_i \to J$.

Now we define $\xi \colon T \to J$ to be the $\mathbb{G}_m^{\rho-1}$-torsor given by the fiber product

$$T \coloneqq T_1 \times_J T_2 \times_J \cdots \times_J T_{\rho-1}.$$

Finally, let $\widetilde{j_b} \colon U \to T$ be a choice of morphism (well defined up to the choice of $\rho-1$ signs) coming from the morphisms $\widetilde{j_{b,f_i}} \colon U \to T_i$.

As in section 6.5, we can pseudoparametrize residue disks of T.

Definition 6.6.1. Recall that we fixed a $\overline{t} \in T(\mathbb{F}_p)$. We also fix $\widetilde{t} = (\widetilde{t}_1, \dots, \widetilde{t}_{\rho-1}) \in T(\mathbb{Z}_p)_{\overline{t}}$ a lift of $\overline{t}$. Let $\varphi \colon T(\mathbb{Z}_p)_{\overline{t}} \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$be the map which sends $(z_1, \dots, z_{\rho-1})$ to

$$((\log \xi_1(z_1) - \log \xi_1(\widetilde{t}_1))/p, (\psi(z_1) - \psi(\widetilde{t}_1)/p), \dots, (\psi(z_{\rho-1}) - \psi(\widetilde{t}_{\rho-1})/p)),$$

where ψ is defined in (6.4.2). We call φ a pseudoparametrization of the residue disk $T(\mathbb{Z}_p)_{\overline{t}}$. (Recall that $\xi_i(z_i)$ and $\xi_i(\widetilde{t}_i)$ are independent of i, since T is a fibered product over J.)

Corollary 6.6.2. *The pseudoparametrization map φ is a bijection onto its image, and for any parametrization $\theta \colon T(\mathbb{Z}_p)_{\overline{t}} \to \mathbb{Z}_p^{g+\rho-1}$ the resulting map $\varphi \circ \theta^{-1} \colon \mathbb{Z}_p^{g+\rho-1} \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$ is given by $g+\rho-1$ convergent power series.*

For any of the first g power series, the valuation of the coefficient of a degree n

monomial is at least $n-1-v_p(n)$*, and for any of the last* $\rho - 1$ *power series, the valuation of the coefficient is at least* $n-1+v-2\lfloor \log_p n \rfloor$*, where* v *is a (possibly negative) constant.*

Proof. This is a corollary of Lemma 6.5.9. □

The main advantage of this method is that for φ_f we need only to compute the map ψ defined in (6.4.2); it is this fact that allows to us to mainly work in $\mathcal{N}$ and only translate back to the image of the residue disk under φ when needed.

Chapter 7

Construction of the line bundle

We now focus on describing how to explicitly construct the nontrivial $\mathbb{G}_m$-torsor T introduced in section 7.1.17 and give a formula for the trivializing section $\widetilde{j}_b : U \to T$ in (8.3.10). Moreover, in section 7.1 we present explicit algorithms for working with T by using endomorphisms of J. Then we proceed to give a description and explicit algorithms for defining a parametrization $\kappa : \mathbb{Z}_p^r \to T(\mathbb{Z}_p)_{\widetilde{j}_b(\overline{P}}$ with image exactly $\overline{T(\mathbb{Z})}_{\widetilde{j}_b(\overline{P}}$ in section 7.3. These results will be essential in chapter 8. Recall that $p > 2$ is henceforth a prime of good reduction. This chapter only contains joint work with Sachi Hashimoto and Pim Spelier that can be found in the preprint [32].

Remark 7.0.1. To work with divisors on U, X or $U \times X$ explicitly, we use equations for a projective regular model of X. There are multiple ways to do this. On a theoretical level, a regular model itself is projective over $\mathbb{Z}$ because it is a repeated blowup of the projective closure of its generic fiber. On a practical level, this process could embed the regular model in a high-dimensional projective space, and it is easier to work on affine patches. In this case we give divisors on each of the affine patches by Groebner bases, compatible with the glueing data. For a practical implementation, we recommend this latter method. This is, for example, implemented in Magma [17]. The methods in the rest of the section are agnostic to the exact implementation. Throughout this section, we assume we can represent effective divisors on the regular model by a Groebner basis, and we represent general divisors by a difference between two effective divisors.

Section 7.1 Construction of T

As explained in section 6.6, to construct the torsor T, we need $\rho - 1$ independent trace zero endomorphisms $(f_i)_{i=1}^{\rho-1} \colon J \to J$. (In general one only needs n independent nontrivial trace zero endomorphisms where n is such that $r < g+n$, but one expects to obtain a smaller superset of p-adic points containing $X(\mathbb{Z})$ for higher n. In fact, if we use n nontrivial independent endomorphisms such that $r < g+n-1$, then we expect to cut out $X(\mathbb{Z})$ exactly unless there is some geometric reason for extra points.) To work with any endomorphism $f \colon J \to J$ explicitly, we recall some facts about correspondences, as can be found in [62]. A correspondence on $X \times X$ is a divisor D on $X \times X$.

Write $D = \sum_i n_i D_i$ as a sum of prime divisors. Denote by $\pi_1^{D_i} \colon D_i \to X$ the projection onto the first factor of $X \times X$ and similarly $\pi_2^{D_i}$ for projection onto the second factor. The correspondence D induces an endomorphism of the Jacobian $\xi_D = \sum_i n_i \pi_{2,*}^{D_i} \pi_1^{D_i,*}$. In particular, it sends the Jacobian point $[x-y]$ to $\mathcal{O}_X(D|_{x \times X} - D|_{y \times X})$.

Example 7.1.1. Consider negation $-1 \cdot \colon J \to J$ on a hyperelliptic curve of the form $y^2 = h(x,z)$ in weighted projective space. If we give $X \times X$ the projective coordinates

x, y, z, x', y', z', then a correspondence representing $-1\cdot$ is given by the homogeneous equation $y = -y'$.

The aim of this section is to describe, given correspondences for all f_i, how to calculate the morphism $\widetilde{j_b} \colon U \to T$. For this goal, we partially follow [36, Section 7].

In the case where $X_{\mathbb{Q}}$ is a classical modular curve we can construct many trace zero endomorphisms using the Hecke algebra. See for example the computation leading to (8.3.8) in section 8.3.

Algorithms

We now focus on the computations for a single trace zero endomorphism $f \colon J \to J$. We can compute equations for a correspondence $D_{f,\mathbb{Q}} \subset X_{\mathbb{Q}} \times X_{\mathbb{Q}}$ inducing f using the code of Costa, Mascot, Sijsling, and Voight [26]. The input of that algorithm is the $g \times g$ matrix giving the representation of the morphism f on a basis of differential forms $H^0(X_{\mathbb{Q}}, \Omega^1)$.

Algorithm 7.1.2 (Compute A_α)**.**

Input: $D_{f,\mathbb{Q}} \subset X_{\mathbb{Q}} \times X_{\mathbb{Q}}$ *a divisor.*

Output: a divisor A_α *on* $X^{\mathrm{sm}} \times X$.

1. *Spread out* $D_{f,\mathbb{Q}}$ *to* D'_f *over* $X^{\mathrm{sm}} \times X$ *by clearing denominators of the generators of the Groebner basis.*

2. *Set* $B := D'_f|_{X^{\mathrm{sm}} \times b}$ *and* $C := D'_f|_{\Delta_{X^{\mathrm{sm}}}}$.

3. *Set* $A_\alpha := m\left(D'_f - B \times X + X^{\mathrm{sm}} \times B - X^{\mathrm{sm}} \times C\right)$, *where* m *is the integer defined in* (6.1.5).

4. *Return* A_α, *as a Groebner basis over* $\mathbb{Z}$.

Lemma 7.1.3. *The divisor A_α on $X^{\text{sm}} \times X$ given by Algorithm 7.1.2 is the unique divisor on $X^{\text{sm}} \times X$ with the following properties:*

(a) *the endomorphism of J induced by the correspondence A_α is $m \cdot \circ f$;*

(b) *$\mathcal{O}_{X^{\text{sm}}}(A_\alpha|_{U \times b})$ is rigidified with trivializing section 1;*

(c) *$\mathcal{O}_{X^{\text{sm}}}(A_\alpha|_\Delta)$ is rigidified, compatible with the previous rigidification;*

(d) *the degree of A_α restricted to fibers of the first projection is 0.*

Proof. By [62, Theorem 3.4.7], any divisor inducing the endomorphism $m \cdot \circ f$ is of the form $mD_f + F$ such that F is a sum of vertical or horizontal divisors, so then (a) holds. Conditions (b) and (c) force F to be $m(-B \times X + X^{\text{sm}} \times B - X^{\text{sm}} \times C)$. Finally, by [16, Proposition 11.5.2] and the important fact that the trace of f is zero we have that $\deg(A_\alpha|_{P \times X}) = 0$ and (d) holds. So A_α is the desired divisor. □

Remark 7.1.4. Conditions (b) and (d) are defined the other way from the order chosen in Edixhoven–Lido, in order to agree with the convention in [26]. (That is, in Edixhoven–Lido, they require that the fibers of the *second* projection are degree 0.)

This divisor A_α determines a line bundle $\mathcal{L}_\alpha = \mathcal{O}_{X^{\text{sm}} \times X}(A_\alpha)$ on $X^{\text{sm}} \times X$, rigidified on $X^{\text{sm}} \times b$, of degree 0 on the fibers of the first projection, and such that $\Delta^*\mathcal{L}_\alpha$ is trivial. This induces the endomorphism $m \cdot \circ f$ by

$$[x - y] \mapsto (\mathcal{L}_\alpha)_{x \times X} \otimes (\mathcal{L}_\alpha)^{-1}_{y \times X}. \tag{7.1.5}$$

Corollary 7.1.6. *Let $c := [(\mathcal{L}_{\alpha,\mathbb{Q}})_{b \times X}] \in J(\mathbb{Q}) = J(\mathbb{Z})$. Let $\alpha = m \cdot \circ \operatorname{tr}_c \circ f$ be the morphism $\alpha \colon J \to J^0$. Then $j_b^*(\operatorname{id}, \alpha)^*\mathcal{M}^\times$ is trivial over U.*

Proof. This follows directly from [36, Proposition 7.2] □

The rest of this section will be dedicated to computing α, and computing the trivialization of $j_b^*(id, \alpha)^*\mathcal{M}^\times$.

Algorithm 7.1.7 (Compute c)**.**

Input: equations for a correspondence A_α output by Algorithm 7.1.2, inducing the morphism $m \cdot \circ f \colon J \to J$.

Output: a divisor representing $c = [(\mathcal{L}_\alpha)_{b\times X}] \in J(\mathbb{Q}) = J(\mathbb{Z})$.

1. *Set $A_f := A_\alpha/m$ (recall that A_α was defined as m times a different correspondence, so this is well-defined).*

2. *Compute the generic fiber $A_{f,\mathbb{Q}}$ of A_f.*

3. *Compute equations for the divisor $A_{f,\mathbb{Q}}|_{b\times X}$ by specializing the equations of $A_{f,\mathbb{Q}}$ to b in the first copy of C.*

4. *Return a Groebner basis for $A_{f,\mathbb{Q}}|_{b\times X}$ over $\mathbb{Q}$.*

Algorithm 7.1.8 (Compute f_*)**.**

Input: a morphism of projective schemes $f \colon X \to Y$ given as a graded ring morphism $f^* \colon S \to R$, where $X = \operatorname{Proj} R$ and $Y = \operatorname{Proj} S$; an irreducible subvariety Z of X given by a Groebner basis for its defining ideal J in R.

Output: the pushforward $f_*([Z])$, given by a Groebner basis.

1. *Let B be a set of generators of S.*

2. *Set $I \subset S \otimes R$ to be the ideal generated by $\{b \otimes 1 - 1 \otimes f^*(b) \mid b \in B\}$ and $1 \otimes J$.*

3. *Compute a Groebner basis B for I with respect to the lexicographical ordering on $S \otimes R$.*

4. *Set $K := I \cap S$ with Groebner basis $B \cap S$.*

5. *Compute the degree $d := \deg(f|_Z \colon \operatorname{Proj} R/J \to \operatorname{Proj} S/K)$.*

6. *Return a Groebner basis for K^d.*

Proof. By construction, K is the defining ideal for the image of Z. The pushforward of Z is then exactly $(\deg f|_Z) \cdot [\operatorname{im} f|_Z]$. □

Remark 7.1.9. In Step 5, we need to compute the degree of a morphism between projective schemes. There are algorithms to compute the degree of a rational map between two projective schemes. See for example [65] for a discussion on an implementation in Macaulay2.

Algorithm 7.1.10 (Apply f)**.**
Input: a ring S and two effective divisors D_+ and D_- on X_S^{sm} of the same degree; the correspondence A_α from Algorithm 7.1.2 inducing the morphism $m \cdot f \colon J \to J$.
Output: the Jacobian point $m \cdot f([D_+ - D_-]) \in J(S)$.

1. *For $D \in \{D_+, D_-\}$ do:*

   (i) Compute a Groebner basis for $A_\alpha|_{D \times X}$ as a divisor on $D \times X$.

   (ii) Write $D = \sum_i n_i D_i$ as a sum of irreducible components using primary decomposition.

   (iii) Compute the Groebner basis for the pushforward $E(D_i) := n_i f_*(D_i)$ on X using Algorithm 7.1.8 for every D_i.

(iv) Set $E(D) := \sum_i E(D_i)$.

2. *Return* $E(D_+) - E(D_-)$.

Remark 7.1.11. In the case where one can write $[D_+ - D_-]$ as a sum $\left[\sum_{i=1}^k n_i P_i\right]$ of S-points, one can use the isomorphism $P_i \times X \cong X$ to simply compute $A_\alpha|_{P_i \times X}$ on X and take the linear combination $\left[\sum_{i=1}^k n_i A_\alpha|_{P_i \times X}\right]$.

Finally, we discuss the section $\widetilde{j_b}\colon U \to T$ lying above the Abel–Jacobi map $j_b\colon U \to J$ with base point b. Let $\bar{z} \in X(\mathbb{F}_p)$. Since the pullback j_b^*T is trivial, there is a morphism $\widetilde{j_b}\colon U \to T$ embedding each residue disk $U(\mathbb{Z}_p)_{\bar{z}}$ into the $(g+\rho-1)$-dimensional residue disk $T(\mathbb{Z}_p)_{\widetilde{j_b}(\bar{z})}$, where $z \in U(\mathbb{Z}_p)$. To compute this map, we follow [36, section 7]. Let n be the product of all primes of bad reduction. We first need to compute the numbers W_q and V_q mentioned in [36, Proposition 7.8] for $q \mid n$. These numbers have an involved definition in general. Nevertheless, they can be explicitly computed in our case, and we explain their meaning below.

By Lemma 7.1.3 the line bundles $\Delta^*(\mathcal{L}_\alpha)$ and $(\mathrm{id}, b)^*(\mathcal{L}_\alpha)$ are trivial with trivializing sections $\ell = 1$. Then W_q is defined as the valuation of this section ℓ on $U_{\mathbb{F}_q}$. In our case, these are always 0. It remains to compute V_q. We recall the definition. Note that $\mathcal{L}_\alpha$ has degree 0 on the fibers of the projection $U \times X \to U$, but it might not have multidegree 0.

Definition 7.1.12. We define V to be the unique vertical divisor on $U \times X$ having support disjoint from $U \times b$ such that $\mathcal{L}_\alpha(V)$ has multidegree 0 on all fibers of the projection. Write $V_{\mathbb{F}_q}$ as a sum of irreducible components of $U_{\mathbb{F}_q} \times X_{\mathbb{F}_q}$, i.e., as a linear combination of $U_{\mathbb{F}_q} \times Y_{\mathbb{F}_q}$ where $Y_{\mathbb{F}_q}$ is an irreducible component of $X_{\mathbb{F}_q}$. For $q \mid n$ define $V_q \in \mathbb{Z}$ to be the coefficient of the component $(U_{\mathbb{F}_q} \times U_{\mathbb{F}_q})$ in $V_{\mathbb{F}_q}$.

Lemma 7.1.13. *The number V_q is equal to the intersection number $-((z-b)\cdot A_\alpha|_{z\times X})_q$ over $\mathbb{Z}_q$ for any $z \in U(\mathbb{Z}_q)$.*

Proof. Since $A_\alpha + V$ has multidegree 0 on all fibers of the projection, we have that $((z-b)\cdot(A_\alpha+V)|_{z\times X})_q = 0$. It remains to show that $((z-b)\cdot V|_{z\times X})_q = V_q$. This follows from Definition 7.1.12 and the fact that V has support disjoint from $U \times b$. □

To compute these numbers, we give the following algorithm.

Algorithm 7.1.14 (Calculate V_q)**.**

Input: the curve X, a bad prime q dividing n, the open set U such that $U(\mathbb{F}_q) \neq \emptyset$, and the divisor A_α on $X \times X$.

Output: the integer V_q.

1. *Pick a point $\overline{Q} \in U(\mathbb{F}_q)$.*
2. *Compute $A_\alpha|_{\overline{Q}\times X}$.*
3. *Compute the multidegree of $A_\alpha|_{\overline{Q}\times X}$.*
4. *Compute the multidegree of the irreducible components of $X_{\mathbb{F}_q}$.*
5. *Compute the unique linear combination $D \subset X_{\mathbb{F}_q}$ of these irreducible components such that D does not meet $\overline{b}$ and such that $A_\alpha|_{\overline{Q}\times X} + D$ has multidegree 0 at the fiber over q.*
6. *Set V_q to be the coefficient of the irreducible component containing $U_{\mathbb{F}_q}$ in D.*
7. *Return V_q.*

Remark 7.1.15. If $U(\mathbb{F}_q)$ is empty for some prime q, we can discard U. Integer points reduce to smooth points, so $U(\mathbb{Z}) = \emptyset$ in this case.

Remark 7.1.16. These local heights can also be computed using harmonic analysis on the dual graph, see [15, section 12]. Even though both the geometric method and the harmonic method can be realized as combinatorics on the dual graph, it is not clear how to compare the two computations of local heights.

Let R be a ring and $z \in U(R)$. By [36, Proposition 7.5] we have

$$\begin{aligned} T_f(j_b(z)) &= \mathcal{M}^{\times}(j_b(z), \alpha(j_b(z))) = z^*(z, \mathrm{id})^*(\mathcal{L}_\alpha)^{\times} \otimes b^*(z, \mathrm{id})^*(\mathcal{L}_\alpha)^{\times,-1} \\ &= (\mathcal{L}_\alpha)^{\times}(z,z) \otimes (\mathcal{L}_\alpha)^{\times}(z,b)^{-1} = (\mathcal{L}_\alpha)^{\times}(z,z). \end{aligned}$$

We apply [36, Proposition 7.8] to give a formula for $\widetilde{j_b}(z)$ when $R \subset \mathbb{Z}_p$. We have that

$$\widetilde{j_b}(z) = \prod_{q|n} q^{-V_q}(z^*1) \otimes (b^*1)^{-1} = (z-b)^* \prod_{q|n} q^{-V_q} \in (z-b)^*\mathcal{O}_X(A_\alpha|_{z\times X}) \quad (7.1.17)$$

is a trivializing section over the curve. The image in $\mathcal{N}$ is given by

$$\psi(\widetilde{j_b}(z)) = h_p(z-b, A_\alpha|_{z\times X}) - \sum_{q|n} V_q \log q. \quad (7.1.18)$$

Corollary 7.1.19. *The function $\Psi \circ \widetilde{j_b} \colon U(\mathbb{Z}_p) \to \mathcal{N}$ is given by*

$$z \mapsto ([z-b], [A_\alpha|_{z\times X}], h_p(z-b, A_\alpha|_{z\times X}) - \sum_{q|n} V_q \log q).$$

Section 7.2

Embedding the curve

We now describe how to compute the embedding of the curve into the torsor through the evaluation of the trivializing section $\widetilde{j_b}$ on a residue disk of the point $\overline{P} \in U(\mathbb{F}_p)$. Recall the pseudoparametrization $\varphi\colon T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^g \oplus \mathbb{Q}_p^{\rho-1}$ from Definition 6.6.1. Let $\mathbb{Z}_p \to U(\mathbb{Z}_p)_{\overline{P}}$ be a parametrization of the residue disk. Define the map $\lambda\colon \mathbb{Z}_p \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ to be the composite of this parametrization $\mathbb{Z}_p \to U(\mathbb{Z}_p)_{\overline{P}}$ and $\widetilde{j_b}$. In this section, we show how to apply the following proposition.

Proposition 7.2.1. *The map $\varphi \circ \lambda : \mathbb{Z}_p \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$ is given by convergent power series. Let ν be a coordinate for $\mathbb{Z}_p$. For any of the first g power series, the valuation of the coefficient of ν^n is at least $n - 1 - v_p(n)$, and for any of the last $\rho - 1$ power series, the valuation of the coefficient is at least $n - 1 + v - 2\lfloor \log_p n \rfloor$, where v is a (possibly negative) constant.*

The image $\operatorname{im}(\varphi \circ \lambda)$ inside $\operatorname{im} \varphi$ is cut out by equations $g_1 = \cdots = g_{g+\rho-2} = 0$ where $g_1, \ldots, g_{g+\rho-2} \in \mathbb{Z}_p\langle x_1, \ldots, x_{g+\rho-1}\rangle$ are integral convergent power series.

Proof. This follows from Corollary 6.6.2 and [18, Corollary 2, III.4.5]. □

For actual calculations with the convergent power series $\varphi \circ \lambda$, we need to lower bound the valuation of the coefficients.

Proposition 7.2.2. *Let ν be a coordinate for $\mathbb{Z}_p$. Consider the $g + \rho - 1$ convergent power series given by $\varphi \circ \lambda\colon \mathbb{Z}_p \to \mathbb{Z}_p^g \times \mathbb{Q}_p^{\rho-1}$. For any of the first g convergent power series, the valuation of the coefficient of ν^n is at least $n - 1 - v_p(n)$. For any of the last $\rho - 1$ power series, the valuation of the coefficient is at least $n - 1 - 2\lfloor \log_p n \rfloor + v$, where v is an explicit (possibly negative) constant.*

Proof. The result about the coefficients of the first g power series follows from Corollary 6.6.2.

Let $Z_1, \ldots Z_{\rho-1}$ be a basis for $\ker(\mathrm{NS}(J) \to \mathrm{NS}(X))$. Then [11, Lemma 4.5] states that the Nékovar height $h_{i,p}^{\mathrm{Nek}} : X \to \mathbb{Q}_p$ corresponding to Z_i is analytic on residue disks. Furthermore, they show that the valuation of the coefficient of ν^n is at least $n - 1 - 2\lfloor \log_p n \rfloor + v$, where $v = \min(\mathrm{ord}_p(\gamma_{\mathrm{Fil}}), c_2 + c_3)$ and γ_{Fil}, c_2, and c_3 are explicit constants defined in [11, Section 4], depending on Z_i among other things. (The valuation of ν^n stated in [11, Lemma 4.5] differs by 1 from the value given here, because our coordinates differ from theirs by a factor of p.)

In Section 8.2 we go more into detail about this Nékovar height. In particular, in Theorem 8.2.10 together with Proposition 8.2.11 we show that $h_p^{\mathrm{Nek}}(z)$ and $h_p(z - b, A_\alpha|_{z \times X})$ differ by a factor of $-m$. The result follows from Corollary 7.1.19. □

Remark 7.2.3. In the example of Section 8.3, we calculate that the constant v is 0 for the residue disk of the curve we consider there. We suspect that this constant can often be taken to be 0, at least in the cases $p > 2g - 1$ and $p \nmid \#J(\mathbb{F}_p)$.

We first present a general algorithm to compute the trivializing section $\varphi \circ \lambda$. For example, if $p > 3$ and $v = 0$, to compute $\widetilde{j}_b(P_\nu)$ in $\mathcal{N}$ modulo p, it suffices to compute $\widetilde{j}_b$ on two values, for example $\widetilde{j}_b(P_0)$ and $\widetilde{j}_b(P_1)$. Since the embedding must be linear in ν on $U(\mathbb{Z}/p^2\mathbb{Z})_{\overline{P}}$, we can interpolate between these values to determine the map. In general, to compute $\varphi \circ \lambda$ to finite precision, it is enough to determine the map on $\mathbb{Z}/p^k\mathbb{Z}$-points for some large enough k. We give an algorithm to compute $\widetilde{j}_b(P)$ when P is a $\mathbb{Z}/p^k\mathbb{Z}$-point.

Algorithm 7.2.4 (The trivializing section)**.**

Input: A point $P_\nu \in U(\mathbb{Z}/p^k\mathbb{Z})_{\overline{P}}$*.*

Output: the value $\varphi \circ \lambda(P_\nu)$ *to a finite precision.*

1. *Calculate the Coleman integral* $\log(P_\nu - b)$*.*

2. *Compute* $A_{\alpha_i}|_{P_\nu \times X}$ *for each* $i = 1, \ldots, (\rho - 1)$ *using Algorithm 7.1.10.*

3. *Calculate all* $h_p(P_\nu - b, A_{\alpha_i}|_{P_\nu \times X})$*.*

4. *Compute* $c_U := \sum_{q|n} V_q \log q$ *using Algorithm 7.1.14, where* n *is the product of the primes of bad reduction for* X*.*

5. *Return*

$$(\varphi \circ \lambda)(\nu) = (\log(P_\nu - P_0), h_p(P_\nu - b, A_{\alpha_1}|_{P_\nu \times X}), \ldots, h_p(P_\nu - b, A_{\alpha_{\rho-1}}|_{P_\nu \times X})) + c_U.$$

For the rest of this section, we describe a practical algorithm to do Step (3) of Algorithm 7.2.4 in the case where X is a hyperelliptic curve of the form $y^2 = H(x)$. For hyperelliptic curves where H has odd degree, there is an algorithm to compute the local Coleman–Gross height at p of two disjoint divisors given as a sum of points [6, Algorithm 5.7]. Forthcoming work of Gajović extends this algorithm to even degree models.

For any $i = 1, \ldots, (\rho - 1)$ since the divisor $A_{\alpha_i}|_{P_\nu \times X}$ on $X_{\mathbb{Q}_p}$ may not split as a sum of points, we instead consider multiples of this divisor $nA_{\alpha_i}|_{P_\nu \times X}$ for $n \in \mathbb{N}$. We can hope some large enough multiple splits as a sum of points. Therefore, we must explicitly describe arithmetic in the Jacobian. For hyperelliptic curves, this process can be done via Cantor's algorithm [19]. The main idea is to use the Mumford representations of divisors. We use the implementation of Cantor's algorithm done by Sutherland in [66, section 3]. The only extra step is to keep track of the function that realizes the linear equivalence with a Mumford representation of the sum. Even though Sutherland works with even degree models for hyperelliptic curves, the algorithms still apply to our odd degree model hyperelliptic curves (see [66, p. 433]).

Remark 7.2.5. In practice, we represent divisors with ideals of polynomial rings. We can translate from a Groebner basis of an ideal to a Mumford representation in the following way. Let Y be a hyperelliptic curve over a field k given by $y^2 = H(x)$. Let $\pi\colon Y \to \mathbb{P}^1$ be the degree two morphism forgetting y. Let D be an effective divisor on the affine chart $k[x,y]/(y^2 - H(x))$ of Y, given by a Groebner basis. We assume that D and $\iota(D)$ are disjoint. Then we can find a Mumford representation for D by simply taking a Groebner basis with respect to the lexicographical ordering $y \leq x$. If D and ιD are not disjoint, one can explicitly compute an effective divisor E on $\mathbb{P}^1$ such that $D - \pi^*E$ is disjoint from $\iota(D - \pi^*E)$, and hence find a Mumford representation for $D - \pi^*E$.

We can now give a practical algorithm to compute the local heights at p in Step (3) of Algorithm 7.2.4. When X is a hyperelliptic curve of the form $y^2 = H(x)$, given $P_\nu \in U(\mathbb{Z}/p^k\mathbb{Z})$ we can apply Algorithm 7.1.10 to obtain $A_{\alpha_i}|_{P_\nu \times X}$ as a divisor on $X_{\mathbb{Q}_p}$.

Algorithm 7.2.6 (Local heights for the trivializing section on a hyperelliptic curve)**.**

Input: A point $P_\nu \in U(\mathbb{Z}/p^k\mathbb{Z})_{\overline{P}}$ on a hyperelliptic curve $Y\colon y^2 = H(x)$ and the Mumford representation of $A_{\alpha_i}|_{P_\nu \times Y}$ as a divisor on Y.

Output: the value $h_p(P_\nu - b, A_{\alpha_i}|_{P_\nu \times Y})$.

1. *Set $n := 1$.*

2. *Use Cantor's Algorithm to compute a Mumford representation* (u_n, v_n) *and a rational function* s_n *such that* $\operatorname{Div}(u_n, v_n) + \operatorname{Div} s_n = nA_{\alpha_i}|_{P_\nu \times Y}$ *[19].*

3. *Check if* u_n *factors completely over* $\mathbb{Q}_p$ *into linear factors.*

4. *If yes, set* x_i *to be the roots of* u_n *for* $i = 1, \ldots, \deg(u_n)$. *If no, increase* n *by* 1 *and go back to Step* (2).

5. *Set* $y_i := v_n(x_i)$.

6. *Set* $Q_i := (x_i, y_i) \in Y(\mathbb{Q}_p)$.

7. *Compute* $h_p(P_\nu - b, \sum_{i=1}^{\deg(u_n)} Q_i - \deg(u_n)\infty)$ *using [6, Algorithm 5.7].*

8. *Return* $(1/n)(h_p(P_\nu - b, \sum_{i=1}^{\deg(u_n)} Q_i - \deg(u_n)\infty) + \log(s_n(P_\nu - b)))$.

Algorithm 7.2.6 does not always terminate; we cannot guarantee that eventually the divisor $nA_{\alpha_i}|_{P_\nu \times Y}$ splits completely into a sum of points over $\mathbb{Q}_p$. In theory, we can split any divisor as a sum of points over some finite extension of $\mathbb{Q}_p$. However, working with these field extensions of $\mathbb{Q}_p$ is often currently not possible in practice.

Remark 7.2.7. Algorithms 7.2.4 and 7.2.6 take in a point P_ν of precision k, but their output can be of smaller precision. This depends on the precision loss in the computation of the p-adic height; see [6, section 6.2].

Section 7.3

Integer points of the torsor

Next we discuss the integer points of the torsor T. We give an algorithm to construct a map $\kappa \colon \mathbb{Z}_p^r \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ with image exactly $\overline{T(\mathbb{Z})}_{\widetilde{j_b}(\overline{P})}$.

In practice, to give an upper bound on $\#U(\mathbb{Z})_{\overline{P}}$, we only need to compute the image of the map κ in $T(\mathbb{Z}/p^2\mathbb{Z})_{\widetilde{j}_b(\overline{P})}$. This is because after composing with the pseudoparametrization φ from Definition 6.6.1 the map κ is given by convergent power series. In fact, in this section we will show that by virtue of our choice of pseudoparametrization, they are given by g linear polynomials and $\rho - 1$ quadratic polynomials.

Note that if the residue disk $T(\mathbb{Z})_{\widetilde{j}_b(\overline{P})}$ is empty, then its p-adic closure is also empty, and therefore we do not need to consider $\overline{P}$. If the disk is not empty, then we can find $\widetilde{t} \in T(\mathbb{Z})_{\widetilde{j}_b(\overline{P})}$ by arithmetic in the Jacobian. It is enough to consider if the corresponding residue disk $J(\mathbb{Z})_{j_b(\overline{P})}$ is empty. This is an instance of the Mordell–Weil sieve at p.

As an intermediate step, we need to compute integer points Q_{ij} on $\mathcal{N}$, the trivial biextension, that are the image under Ψ (defined in Definition 6.4.3) of generating sections on certain fibers of $\mathcal{M}^\times(\mathbb{Z})$.

We construct integer points on $\mathcal{N}$ that are the image of generating sections of residue disks of $\mathcal{M}^\times(\mathbb{Z})$ following the method in Example 6.3.10.

Algorithm 7.3.1 (Compute the Q_{ij})**.**

Input: $G_1, \ldots, G_{r'}$ a generating set of the Mordell–Weil group of J, a trace zero endomorphism $f\colon J \to J$.

Output: Integer points Q_{ij} on the trivial biextension $\mathcal{N}$ which are the image of the generating section of $\mathcal{M}^\times(G_i, f(G_j))(\mathbb{Z})$ and Q_{i0} that are the image of the generating section of $\mathcal{M}^\times(G_i, c)(\mathbb{Z})$ for $1 \leq i, j \leq r'$.

1. *Compute $E_1, \ldots E_{r'}$ representing divisors of $G_1, \ldots, G_{r'}$.*

2. *For each G_i, use Algorithm 7.1.10 to compute representing divisors $D_1, \ldots, D_{r'}$*

of $f(G_i)$.

3. *Use Algorithm 7.1.7 to compute a divisor D_0 whose class is the point $c \in J(\mathbb{Z})$.*

4. *Compute the local height $h_p(E_i, D_j)$ and $h_p(E_i, D_0)$ for $1 \leq i, j \leq r'$.*

5. *Using [71, section 2], compute the height $h_\ell(E_i, D_j)$ at $\ell \neq p$ and $h_\ell(E_i, D_0)$ at $\ell \neq p$ for $1 \leq i, j \leq r'$.*

6. *Return*

$$Q_{ij} := (G_i, f(G_j), \sum_{\ell \text{ prime}} h_\ell(E_i, D_j))$$

and

$$Q_{i0} := (G_i, c, \sum_{\ell \text{ prime}} h_\ell(E_i, D_0))$$

for $1 \leq i, j \leq r'$.

Let $G_1, \ldots, G_{r'}$ be a generating set for the full Mordell–Weil group, with $r' \geq r$. Let $\widetilde{G_i}$ be a basis for the kernel of reduction $J(\mathbb{Z}) \to J(\mathbb{F}_p)$ for $i = 1, \ldots, r$. (Note that the reduction map is injective when restricted to the torsion of $J(\mathbb{Z})$, so the kernel of reduction is a free $\mathbb{Z}$-module of rank r.) Write

$$\widetilde{G_i} = \sum_{j=1}^{r'} e_{ij} G_j$$

for some $e_{ij} \in \mathbb{Z}$. Let $\widetilde{G_t}$ denote the projection of $\tilde{t} \in T(\mathbb{Z})_{\widetilde{j_b}(\overline{P})}$ to $J_{j_b(\overline{P})}$. Write

$$\widetilde{G_t} = \sum_{i=1}^{r'} e_{0i} G_i$$

for some $e_{0i} \in \mathbb{Z}$. Using the biextension group laws and the points Q_{ij} we construct a series of points in $\mathcal{M}^\times(\mathbb{Z})$ living over certain points in $J \times J$ that are the image of generating sections of the corresponding residue disks in $\mathcal{M}^\times(\mathbb{Z})$.

A formula for the points P_{ij} over $(\widetilde{G_i}, f(m\widetilde{G_j}))$ is

$$P_{ij} := \sum_{k=1}^{r'}{}_1\, e_{ik} \cdot_1 \left(\sum_{\ell=1}^{r'}{}_2\, m \cdot_2 e_{j\ell} \cdot_2 Q_{k\ell} \right). \tag{7.3.2}$$

Here, $\cdot_i$ and $\sum_i$ for $i = 1, 2$ denote the biextension group laws (6.3.9) and (6.3.8).

A $\mathbb{Z}$-point $\tilde{t}$ living over $(\widetilde{G_t}, m\alpha(\widetilde{G_t}))$ can be constructed as

$$\tilde{t} := \sum_{k=1}^{r'}{}_1\, e_{0k} \cdot_1 \left(m \cdot_2 Q_{k0} +_2 \sum_{\ell=1}^{r'}{}_2\, m \cdot_2 e_{0\ell} \cdot_2 Q_{k\ell} \right). \tag{7.3.3}$$

Next $R_{i\tilde{t}}$ live over $(\widetilde{G_i}, m\alpha(\widetilde{G_t}))$ and hence

$$R_{i\tilde{t}} := \sum_{k=1}^{r'}{}_1\, e_{ik} \cdot_1 \left(m \cdot_2 Q_{k0} +_2 \sum_{\ell=1}^{r'}{}_2\, m \cdot_2 e_{0\ell} \cdot_2 Q_{k\ell} \right). \tag{7.3.4}$$

Finally, $S_{\tilde{t}j}$ live over $(\widetilde{G_t}, f(m\widetilde{G_j}))$ and so

$$S_{\tilde{t}j} := \sum_{k=1}^{r'}{}_1\, e_{0k} \cdot_1 \left(\sum_{\ell=1}^{r'}{}_2\, m \cdot_2 e_{j\ell} \cdot_2 Q_{k\ell} \right). \tag{7.3.5}$$

Remark 7.3.6. In $\mathcal{M}^\times(\mathbb{Z})$, these points are all unique up to sign. Since we are recording the image in $\mathcal{N}$, this sign does not matter.

For $n = (n_1, \ldots, n_r) \in \mathbb{Z}^r$ we can now construct the points $A_{\tilde{t}}(n)$, $B_{\tilde{t}}(n)$, $C_{\tilde{t}}(n)$, and $D_{\tilde{t}}(n)$ in $T(\mathbb{Z})$ given by [36, (4.2)-(4.4)]. The key property of this construction is that $D_{\tilde{t}}(n)$ lies above the point $\widetilde{j_b}(\overline{P}) \in J(\mathbb{F}_p)$. Furthermore, by [36, (4.6)-(4.9)], we have that $D_{\tilde{t}}((p-1)n)$ is in the residue disk $T(\mathbb{Z})_{\widetilde{j_b}(\overline{P})}$, allowing us to explicitly construct the map

$$\kappa_{\mathbb{Z}} \colon \mathbb{Z}^r \to T(\mathbb{Z})_{\widetilde{j_b}(\overline{P})}, \qquad (n_1, \ldots, n_r) \mapsto D_{\tilde{t}}((p-1)n_1, \ldots, (p-1)n_r), \tag{7.3.7}$$

Finally, by [36, Theorem 4.10], the map $\kappa_{\mathbb{Z}}$ extends continuously to a map

$$\kappa \colon \mathbb{Z}_p^r \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \tag{7.3.8}$$

with image $\overline{T(\mathbb{Z})}_{\widetilde{j_b}(\overline{P})}$.

Recall the pseudoparametrisation $\varphi \colon T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^{g+\rho-1}$ from Definition 6.6.1.

Proposition 7.3.9. *The map $\varphi \circ \kappa \colon \mathbb{Z}_p^r \to \mathbb{Z}_p^{g+\rho-1}$ is given by g linear polynomials and $\rho - 1$ quadratic polynomials.*

Proof. It is enough to show this for $\kappa_{\mathbb{Z}}$, since polynomials are continuous. Note that $\varphi \circ \kappa_{\mathbb{Z}} \colon \mathbb{Z}^r = J(\mathbb{Z})_{\widetilde{j_b}(\overline{P})}$ is given by

$$D \mapsto \log(D - D_0),$$

on the first g components, for a fixed $D_0 \in J(\mathbb{Z})_{j_b(\overline{P})}$. Since log is a group homomorphism, it follows the first g polynomials are linear as desired.

Now we fix one of the $\rho - 1$ trace zero endomorphisms $f \colon J \to J$. Let $\pi_f \colon \mathbb{Z}_p^{g+\rho-1} \to \mathbb{Z}_p$ be the projection onto the coefficient corresponding to f. Consider at the map $\tau \coloneqq \pi_f \circ \varphi \circ \kappa$. We write F for the linear map

$$\mathbb{Z}^r \cong J(\mathbb{Z})_{j_b(\overline{P})} \xrightarrow{f} J(\mathbb{Z})_{f(j_b(\overline{P}))} \cong \mathbb{Z}^r.$$

Then by formulas [36, (4.2)-(4.4)] we have that $\tau(n_1, \dots, n_r)$ is a sum of a constant term, a linear function in the n, a linear function in Fn and a bilinear form evaluated in (n, Fn). Since F is linear, we see that, in total, this gives a quadratic function in n. □

Chapter 8

Main results

We are now ready to present the main algorithm for explicit Geometric quadratic Chabauty and a comparison theorem with geometric Chabauty. The main algorithm is Algorithm 8.1.1 and the main theorem is Theorem 8.2.5. We then apply the geometric quadratic Chabauty method to the (classical) modular curve $X_0(67)^+$ as an example. This is joint work with Sachi Hashimoto and Pim Spelier from [32].

Section 8.1

The geometric quadratic Chabauty algorithm

In this section, we present the main algorithm of this paper for doing geometric quadratic Chabauty. This algorithm ties together the results of the previous sections.

Algorithm 8.1.1 (Geometric quadratic Chabauty in a single disk)**.**

Input:

- *$X_{\mathbb{Q}}/\mathbb{Q}$ a smooth, projective, geometrically irreducible curve over $\mathbb{Q}$ such that $X_{\mathbb{Q}}(\mathbb{Q}) \neq \varnothing$ with a regular model X of genus g and Mordell–Weil rank r, and* *with Jacobian of Néron–Severi rank $\rho > 1$, such that $r < g + \rho - 1$;*

- *$\rho - 1$ nontrivial independent trace 0 endomorphisms represented by $(g \times g)$-matrices giving the action on the sheaf of differentials with respect to a fixed basis;*

- *an open set $U \subset X^{\mathrm{sm}}$ containing the smooth points of one geometrically irreducible component of $X_{\mathbb{F}_q}$ for all primes q;*

- *a prime $p > 2$ of good reduction for X;*

- *a precision $k \in \mathbb{N}$;*

- *a base point $b \in X(\mathbb{Z})$;*

- *a point $\overline{P} \in U(\mathbb{F}_p)$;*

- *a generating set $G_1, \ldots, G_{r'}$ of the Mordell–Weil group of J.*

Output: $g + \rho - 2$ integral convergent power series in $\mathbb{Z}_p\langle z_1, \ldots, z_r\rangle$ up to precision k, defining $\widetilde{j_b}(U(\mathbb{Z}_p)_{\overline{P}}) \cap \overline{T(\mathbb{Z})}$ inside $\overline{T(\mathbb{Z})}$.

For each of the given trace 0 endomorphisms f do the following.

1. *Compute the correspondence A_α that induces the endomorphism $m \cdot \circ f\colon J \to J$ as given in Lemma 7.1.3.*

2. *Find the divisor representing $c = [(\mathcal{L}_\alpha)_{b \times X}] \in J(\mathbb{Z})$ using Algorithm 7.1.7.*

3. *Choose a local parameter ν to parameterize $(\mathbb{Z}_p)_{\overline{P}}$ as $\nu \mapsto P_\nu$. By Proposition 7.2.1 the map $\nu \mapsto \varphi \circ \lambda(P_\nu)$ is, modulo p^k, given by a polynomial with bounded degree. By calculating enough values, interpolate to find the polynomial*

expression. In particular, when $v = 0$ and $p > 3$, for $k = 1$, the degree bound is 1. In this case, compute $\varphi \circ \lambda(P_0), \varphi \circ \lambda(P_1)$ and interpolate the resulting line.

4. *With the generating set $G_1, \ldots, G_{r'}$, use Algorithm 7.3.1 to compute integer points $Q_{ij}, Q_{i0} \in \mathcal{N}$ up to precision k that are the images of the generating sections of $\mathcal{M}^\times(G_i, f(G_j))(\mathbb{Z})$ and $\mathcal{M}^\times(G_i, c)(\mathbb{Z})$ for $1 \leq i, j \leq r'$.*

5. *Using the elements Q_{ij}, find the map $\kappa_\mathbb{Z} \colon \mathbb{Z}^r \to T(\mathbb{Z})_{\tilde{j}_b(\bar{P})}$ as in (7.3.7) and extend it to the map $\kappa \colon \mathbb{Z}_p^r \to T(\mathbb{Z}_p)_{\tilde{j}_b(\bar{P})}$.*

6. *Compose with the pseudoparametrization φ to compute the linear and quadratic polynomials describing $\varphi \circ \kappa \colon \mathbb{Z}_p^r \to \mathbb{Z}_p^{g+\rho-1}$, as guaranteed by Proposition 7.3.9, up to precision k.*

7. *Use Lagrangian interpolation to compute the power series $\varphi \circ \lambda$ up to precision k.*

8. *Use Hensel lifting to compute the power series $f_1, \ldots, f_{g+\rho-2}$ defined in Proposition 7.2.1 that cut out $\operatorname{im} \varphi \circ \lambda$, up to precision k.*

9. *Return $g_i := f_i \circ (\varphi \circ \kappa)$ for $i = 1, \ldots, g + \rho - 2$.*

By iterating this over all simple opens U_i such that $(U_i(\mathbb{Z}))_{i \in I}$ covers $X(\mathbb{Z})$ (as in section 6.1), and also iterating over all $\mathbb{F}_p$-points of U_i, we obtain multivariate power series up to precision k cutting out $X(\mathbb{Z}_p)_{\text{Geo}}$.

Remark 8.1.2. By [36, section 9.2], the power series in the output of Algorithm 8.1.1 have at most finitely many zeros in $\mathbb{Z}_p$. In practice, one can solve these power series up to enough precision by using a multivariate Hensel's lemma [48, Theorem 25].

This assumes that the Jacobian matrix of the sequence of power series is invertible over $\mathbb{Q}_p$. We expect this to always happen unless there is a geometric obstruction.

Often solving these power series modulo p is enough to determine $X(\mathbb{Z}_p)_{\mathrm{Geo}}$. See for example [36, Theorem 4.12], which we use in section 8.3. Even if computations modulo p are not enough, one can increase the precision by considering the residue disks $U(\mathbb{Z}_p)_{\overline{P}}$, where $\overline{P} \in U(\mathbb{Z}/p^k\mathbb{Z})$ for some integer k. An example of the geometric Chabauty method with higher precision is given in Remark 8.3.19.

Remark 8.1.3. In practice, to run Algorithm 8.1.1 we need to be able to compute Coleman–Gross heights on the curve X. Currently, this has only been made algorithmic for hyperelliptic curves.

Section 8.2
The comparison theorem

In this section we give a comparison theorem between the geometric method and the cohomological quadratic Chabauty of [9, 10, 3, 11]. In Theorem 8.2.5, we show that the geometric method produces a refined set of points, as is the case for classical Chabauty–Coleman [41].

For this section we assume that p is a prime of good reduction, that $r = g$, and further, that $\overline{J(\mathbb{Z})}$ has finite index in $J(\mathbb{Z}_p)$. These assumptions are needed for constructing the cohomological quadratic Chabauty set. We do not require a semistable model for $X/\mathbb{Q}_q$, $q|n$ as is sometimes assumed; a semistable model can make explicit calculations of heights away from p easier, see [15] or [11, section 3.1]. By [14, Lemma 6.1.1] the local heights away from p factor through the component set of the minimal regular model.

Let $Z_1, \dots, Z_{\rho-1}$ be a basis for $\ker(\mathrm{NS}(J) \to \mathrm{NS}(X))$. In the cohomological method, from the transpose $Z_i^\top$ of such a correspondence[1] we are able to construct a quadratic Chabauty function $\sigma_i \colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ and a finite subset $\Omega_i \subset \mathbb{Q}_p$ described explicitly in terms of local heights at primes of bad reduction such that $\sigma_i(z) \in \Omega_i$ for all $z \in X(\mathbb{Q})$. This finite subset Ω_i consists of one constant $c_{U,i}$ for every simple open U.

We describe the construction of σ_i and the set Ω_i in more detail after we present the main theorem. The divisor Z_i is the correspondence of a trace zero endomorphism $f_i \colon J \to J$ of the Jacobian. In the geometric method, we work with the endomorphism $\alpha_i \coloneqq m \cdot \circ \operatorname{tr}_{c_i} \circ f_i$. This multiplication with m will result in all the heights in the trivial biextension $\mathcal{N}$ to be a factor m larger than in the cohomological case.

Definition 8.2.1. Define $X(\mathbb{Q}_p)_{\mathrm{Coh}} \coloneqq \bigcup_U \{x \in X(\mathbb{Q}_p) \mid \sigma_i(x) = c_{U,i}, \text{ for } i = 1, \dots, \rho - 1\}$ where the union is over all simple opens U.

Remark 8.2.2. As far as we know, the existing literature does not explicitly define the quadratic Chabauty set in the case of multiple endomorphisms. One can see Definition 8.2.1 as a special case of the finite set implicitly defined in [14, Theorem A], for the quotient of the fundamental group that is an extension of the abelianization by $\mathbb{Q}_p(1)^{\rho-1}$.

The alternative definition is $\bigcap_i \bigcup_U \{x \in X(\mathbb{Q}_p) \mid \sigma_i(x) = c_{U,i}\}$. Here the union and the intersection have been switched, and hence the resulting set can be bigger. The difference between the two sets consists exactly of points $x \in X(\mathbb{Q}_p)$ such that $\sigma_i(x) \in \Omega_i$ for every i, but such that there is no U with $\sigma_i(x) = c_{U,i}$ for every i. In

[1] Due to a difference of conventions of rigidifications for line bundles on $X \times X$, we have to take the transpose of Z_i for the methods to align perfectly. The transpose $Z_i^\top$ induces the same endomorphism of the Jacobian.

particular, the points in the difference do not lie in any of the simple opens U, and hence are not rational points.

Recall the definition of $X(\mathbb{Z}_p)_{\mathrm{Geo}}$ from Definition 6.1.3. Given a covering of X by simple opens U we have that

$$X(\mathbb{Z}_p)_{\mathrm{Geo}} := \bigcup_U \widetilde{j_b}^*(\widetilde{j_b}(U(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})}) \subset \bigcup_U U(\mathbb{Z}_p) = X(\mathbb{Z}_p).$$

The following definitions give terminology for two of the cases in which $X(\mathbb{Q}_p)_{\mathrm{Coh}}$ is strictly bigger than $X(\mathbb{Z}_p)_{\mathrm{Geo}}$.

Definition 8.2.3. We say that the Mordell–Weil group is of good reduction (modulo p) if the map $\overline{J(\mathbb{Z})}_0/p\overline{J(\mathbb{Z})}_0 \to J(\mathbb{Z}/p^2\mathbb{Z})_0$ is injective. Otherwise, we say that it is of bad reduction.

The Mordell–Weil group being of good reduction is equivalent to the map $\overline{J(\mathbb{Z})}_0 \to J(\mathbb{Z}_p)_0$ being an isomorphism. On the level of abstract groups, this map is always an embedding $\mathbb{Z}_p^g \to \mathbb{Z}_p^g$ with image of index some power of p. Another equivalent way of stating this is that the p-saturation of $\overline{J(\mathbb{Z})}_0$ in $J(\mathbb{Z}_p)_0$

$$\{x \in J(\mathbb{Z}_p)_0 \mid \exists k, p^k x \in \overline{J(\mathbb{Z})}_0\}$$

is always equal to $J(\mathbb{Z}_p)_0$, and the Mordell–Weil group is of bad reduction if and only if this p-saturation is bigger than $\overline{J(\mathbb{Z})}_0$.

Definition 8.2.4. For $Q \in X(\mathbb{F}_p)$, if $j_b(Q)$ is not in the image of the reduction map $J(\mathbb{Z}) \to J(\mathbb{F}_p)$, then we say Q fails the Mordell–Weil sieve (at p). In this case, the residue disk $X(\mathbb{Z}_p)_Q$ cannot contain a rational point. Otherwise, Q passes the

Mordell–Weil sieve (at p).

Our main theorem is the following comparison theorem.

Theorem 8.2.5. *There is an inclusion $X(\mathbb{Q}) \subseteq X(\mathbb{Z}_p)_{\mathrm{Geo}} \subseteq X(\mathbb{Q}_p)_{\mathrm{Coh}}$. For $P \in X(\mathbb{Q}_p)_{\mathrm{Coh}}$ we have $P \notin X(\mathbb{Z}_p)_{\mathrm{Geo}}$ if and only if one of the following conditions holds:*

(a) P fails the Mordell–Weil sieve at p;

(b) the Mordell–Weil group is of bad reduction at p and $j_b(P)$ does not lie in the p-adic closure of the Mordell–Weil group, but only in its p-saturation.

Remark 8.2.6. In [41], an analogous theorem is given for the comparison between the classical Chabauty–Coleman method, as in [24, 8], and the geometric linear Chabauty, as developed in [63] and [41]. The comparison theorem [41, Theorem 4.1] shows that the set of candidates found by the classical Chabauty–Coleman method contains the set found by geometric linear Chabauty method. Furthermore, the two sets differ by conditions analogous to (a) and (b).

Let $1 \leq i \leq \rho(J) - 1$. We briefly recall the constructions of σ_i and Ω_i from [11]. For more details, the reader can also consult [9, 3]. The cohomological method for quadratic Chabauty uses Nekovář's theory [55] of p-adic heights of certain Galois representations to construct a global height $h_i^{\mathrm{Nek}} \colon X(\mathbb{Q}) \to \mathbb{Q}_p$ by attaching a family of Galois representations to $X(\mathbb{Q})$ and $X(\mathbb{Q}_p)$. The Galois representation depends on the choice of base point b as well as the correspondence Z_i. We suppress this dependence on b in our notation. The global height also depends on a choice of splitting of the Hodge filtration and idèle class character, which we choose to be compatible with the choices made to construct the Coleman–Gross height h. In particular we choose the cyclotomic character. This global height h_i^{Nek} factors through

$h^{\mathrm{Nek}}\colon J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{Q}_p$ [11, section 2.3]. We can thus extend h^{Nek} on $J(\mathbb{Q}) \times J(\mathbb{Q})$ to a bilinear function on $J(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \to \mathbb{Q}_p$ and evaluate it on elements of $X(\mathbb{Q}_p)$.

This global height decomposes as a sum of local heights over finite places

$$h_i^{\mathrm{Nek}} = \sum_v h_{i,v}^{\mathrm{Nek}}$$

where $h_{i,v}^{\mathrm{Nek}}\colon X(\mathbb{Q}_v) \to \mathbb{Q}_p$. Define the quadratic Chabauty function

$$\sigma_i(z) := h_i^{\mathrm{Nek}}(z) - h_{i,p}^{\mathrm{Nek}}(z)$$

for $z \in X(\mathbb{Q}_p)$, recalling that the right hand side implicitly depends on Z_i. Then, for any $z \in X(\mathbb{Q})$, using the decomposition above we can write $h^{\mathrm{Nek}}(z) = h_p^{\mathrm{Nek}}(z) + \sum_{q \neq p} h_q^{\mathrm{Nek}}(z)$. The set $\Omega_i \subset \mathbb{Q}_p$ is defined by the local heights in the following way. Let

$$\Omega_{i,q} := \{h_{i,q}^{\mathrm{Nek}}(z) \mid z \in X(\mathbb{Q}_q)\}.$$

If $X_{\mathbb{F}_q}$ is geometrically irreducible, then $\Omega_{i,q} = \{0\}$. We can therefore define the finite set

$$\Omega_i := \{\sum_q w_q \mid w_q \in \Omega_{i,q}\}, \tag{8.2.7}$$

Hence, when $z \in X(\mathbb{Q})$, we have $\sigma_i(z) \in \Omega_i$ and so $X(\mathbb{Q}_p)_{\mathrm{Coh}} \supseteq X(\mathbb{Q})$.

Remark 8.2.8. The function $\sigma_i(z)$ is locally analytic [11, pp.6-10]. If X has sufficiently many rational points, then one can explicitly express the function $\sigma_i(z)$ as a power series in every residue disk, and for each $c \in \Omega_i$ and each residue disk of $X(\mathbb{Q}_p)$ find the roots of $\sigma_i(z) - c$ to explicitly solve for elements of $X(\mathbb{Q}_p)_{\mathrm{Coh}}$.

The following theorem relates the local height of the Galois representation associated to a point $P \in X(\mathbb{Q}_p)$ to a pairing with a divisor that is studied in [30].

Definition 8.2.9. Let $z \neq b$ be a point in $X(\mathbb{Q}_p)$. Define $D_{Z_i^\top}(z,b)$ to be the degree zero divisor on X given by $D_{Z_i^\top}(z,b) := Z_i|_\Delta - Z_i|_{X \times b} - Z_i|_{z \times X}$.

Theorem 8.2.10. *[9, Theorem 6.3] Let q be a prime and let $z \neq b$ be a point in $X(\mathbb{Q}_p)$. We have the equality of local heights $h_{i,q}^{\mathrm{Nek}}(z) = h_q(z - b, D_{Z_i^\top}(z,b))$ for $z \in X(\mathbb{Q}_q)$ and moreover $h_i^{\mathrm{Nek}}(z) = h(z - b, D_{Z_i^\top}(z,b))$ where h is the Coleman–Gross height.*

Proposition 8.2.11. *Let $z \in X(\mathbb{Z}_p)$ be such that $z \neq b$. We have $-mD_{Z_i^\top}(z,b) = A_{\alpha_i}|_{z \times X}$ and $-m[D_{Z_i^\top}(z,b)] = [\alpha_i(z - b)]$.*

Proof. Write $B = Z_i|_{X \times b}$ and $C = Z_i|_\Delta$. Then

$$D_{Z_i^\top}(z,b) = C - B - Z_i|_{z \times X}.$$

Define $A = Z_i - B \times X + X \times B - X \times C$. Then we see $A|_{z \times X} = Z_i|_{z \times X} + B - C = -D_{Z_i^\top}(z,b)$. Then by Lemma 7.1.3, mA is equal to A_{α_i} and the proposition follows. □

Definition 8.2.12. Define $\rho_{\mathcal{N}} \colon \mathcal{N} \to \mathbb{Q}_p$ by $(D_1, D_2, x) \mapsto h^{\mathrm{Nek}}(D_1, D_2) - x$.

Note that $\rho_{\mathcal{N}}$ does not depend on Z_i.

Lemma 8.2.13. *The function $\rho_{\mathcal{N}}$ vanishes on the image $\Psi(\mathcal{M}(\mathbb{Z}))$ in $\mathcal{N}$, and in particular, on $\Psi(T_i(\mathbb{Z}))$.*

Proof. This follows from Proposition 6.4.6. □

In order to characterise the difference between $X(\mathbb{Q}_p)_{\text{Geo}}$ and $X(\mathbb{Q}_p)_{\text{Coh}}$, we will use the following lemma.

Lemma 8.2.14. *The difference $Z(\rho_{\mathcal{N}}) \setminus \Psi(\overline{\mathcal{M}(\mathbb{Z})})$ consists of all the points (D, E, x) with $D, E \in J(\mathbb{Z}_p)$ such that*

(a) D or E fail the Mordell–Weil sieve, or;

(b) the Mordell–Weil group is of bad reduction, and at least one of D or E does not lie in the p-adic closure $\overline{J(\mathbb{Z})}$ of the Mordell–Weil group, and only lies in its p-saturation.

Proof. Note that $Z(\rho_{\mathcal{N}})$ is in bijection with $J(\mathbb{Z}_p) \times J(\mathbb{Z}_p)$. In contrast, $\Psi(\mathcal{M}(\mathbb{Z}))$ is in bijection with $J(\mathbb{Z}) \times J(\mathbb{Z})$. By assumption, $\overline{J(\mathbb{Z})}_0 \subset J(\mathbb{Z}_p)_0$ is a finite index $\mathbb{Z}_p$-submodule, and therefore has p-saturation $J(\mathbb{Z}_p)_0$. Hence $J(\mathbb{Z}_p) \setminus \overline{J(\mathbb{Z})}$ consists exactly of points failing the Mordell–Weil sieve and points that only lie in the p-saturation of $\overline{J(\mathbb{Z})}$ and not in $\overline{J(\mathbb{Z})}$ itself. This can only happen if $\overline{J(\mathbb{Z})_0}$ is a proper subgroup of $J(\mathbb{Z}_p)_0 \cong \mathbb{Z}_p^g$. A finite index $\mathbb{Z}_p$-submodule $G \subset \mathbb{Z}_p^g$ is a proper subgroup if and only if after tensoring with $\mathbb{F}_p$ the induced map $G/pG \to \mathbb{F}_p^g$ is not an isomorphism. This is equivalent to $G/pG \to \mathbb{F}_p^g$ not being injective. So the second condition can only happen if the Mordell–Weil group is of bad reduction. □

Definition 8.2.15. Let $U \subset X^{\text{sm}}$ be a simple open set of X^{sm}. Define $c_{U,i} \in \Omega_i \subset \mathbb{Q}_p$ to be $\sum_{q \neq p} h_q(z_q - b, D_{Z_i^\top}(z_q, b))$ for any $z_q \in U(\mathbb{Z}_q)$ with $z_q \neq b$.

Remark 8.2.16. By Lemma 7.1.13, the previous definition is well defined and $-mc_{U,i}$ is equal to $-\sum_q V_q \log q$, with V_q as defined in Definition 7.1.12. Here we use the local height $h_q(D,E)$ is $(D+F)\cdot E\cdot \log q$ where F is the unique vertical divisor on $X_{\mathbb{Z}_q}$ making $D+F$ have multidegree 0 on $X_{\mathbb{F}_q}$. Hence by (7.1.18) we have that $\psi \circ \widetilde{j_b}\colon U(\mathbb{Z}_p) \to \mathbb{Q}_p$ is given by $z \mapsto h_p(z-b, A_\alpha|_{z\times X}) - mc_{U,i}$ and $(\Psi\circ \widetilde{j_b})(z) = (z-b, A_\alpha|_{z\times X}, h_p(z-b, A_\alpha|_{z\times X}) - mc_{U,i})$.

Lemma 8.2.17. *The function $-m(\sigma_i(z)-c_{U,i})$ is the pullback along $\Psi\circ\widetilde{j_b}|_U\colon U(\mathbb{Z}_p)\to \mathcal{N}$ of $\rho_{\mathcal{N}}$.*

Proof. Let $z\in U(\mathbb{Z}_p)\subset X(\mathbb{Z}_p)$ with $z\neq b$. By Theorem 8.2.10 and Proposition 8.2.11 we have that

$$-mh_{i,q}^{\mathrm{Nek}}(z) = -mh_q(z-b, D_{Z_i^\top}(z,b)) = h_q(z-b, A_\alpha|_{z\times X}).$$

By [11, p. 12],

$$h_q(z-b, A_\alpha|_{z\times X}) = -((z-b)\cdot A_\alpha|_{z\times X})_q \log q$$

where the right hand side denotes the intersection number of the divisors over $\mathbb{Z}_{(q)}$. By Lemma 7.1.13, this is equal to $V_q\log q$.

Then

$$\begin{aligned} &-m(\sigma_i(z)-c_{U,i}) = -m(h^{\mathrm{Nek}}(z) - h_p^{\mathrm{Nek}}(z) - c_{U,i})\\ &= h(z-b, A_\alpha|_{z\times X}) - h_p(z-b, A_\alpha|_{z\times X}) + mc_{U,i}.\end{aligned}$$

This is equal to

$$\begin{aligned} &h(z-b, A_\alpha|_{z\times X}) - (h_p(z-b, A_\alpha|_{z\times X}) - mc_{U,i}) =\\ &\rho_{\mathcal{N}}((z-b, A_\alpha|_{z\times X}, h_p(z-b, A_\alpha|_{z\times X}) - mc_{U,i})) = \rho_{\mathcal{N}}(\widetilde{j_b}(z)).\end{aligned}$$

This last equality follows from Corollary 7.1.19. □

Proof of Theorem 8.2.5. Let $c \in \Omega_i$, and consider the function $\sigma_i - c$. By (8.2.7), Theorem 8.2.10 and Definition 8.2.15 there is a simple open $U \subset X$ such that $c = c_{U,i}$.

Let $\widetilde{j_{b,U,i}}$ denote the map $U \to T_i$. According to Lemma 8.2.17 we have that $-m(\sigma_i - c)\colon U(\mathbb{Z}_p) \to \mathbb{Q}_p$ is the composite

$$U(\mathbb{Z}_p) \xrightarrow{\widetilde{j_{b,U,i}}} T_i(\mathbb{Z}_p) \to \mathcal{M}^\times(\mathbb{Z}_p) \xrightarrow{\Psi} \mathcal{N} \xrightarrow{\rho_{\mathcal{N}}} \mathbb{Q}_p, \tag{8.2.18}$$

identifying $T_i(\mathbb{Z}_p)$ as a subset of $\mathcal{M}^\times(\mathbb{Z}_p)$. Define $g_{U,i} := -m(\sigma_i - c)$. Note that the first three maps in (8.2.18) are injections.

With this formulation we have

$$X(\mathbb{Q}_p)_{\mathrm{Coh}} = \bigcup_U \bigcap_i Z(g_{U,i}).$$

Similarly, we can write

$$X(\mathbb{Z}_p)_{\mathrm{Geo}} = \bigcup_U \bigcap_i \widetilde{j_{b,U,i}}^*(\widetilde{j_{b,U,i}}(U(\mathbb{Z}_p)) \cap \overline{T_i(\mathbb{Z})}).$$

By Lemma 8.2.13, the set $Z(g_{U,i})$ contains

$$\widetilde{j_{b,U,i}}^*(\widetilde{j_{b,U,i}}(U(\mathbb{Z}_p)) \cap \overline{T_i(\mathbb{Z})}).$$

Therefore, we get the containment $X(\mathbb{Z}_p)_{\mathrm{Geo}} \subseteq X(\mathbb{Q}_p)_{\mathrm{Coh}}$.

The difference $X(\mathbb{Q}_p)_{\mathrm{Coh}} \setminus X(\mathbb{Z}_p)_{\mathrm{Geo}}$ is

$$\bigcup_U \bigcap_i Z(g_{U,i}) \setminus \widetilde{j_{b,U,i}}^{\,*}(\widetilde{j_{b,U,i}}(U(\mathbb{Z}_p)) \cap \overline{T_i(\mathbb{Z})}).$$

By Lemma 8.2.14 the theorem follows. □

Section 8.3

Example: $X_0(67)^+$

We give an example of the implementation on the modular curve $X_0(67)^+$ of the algorithms presented. The rational points on this curve have already been determined [2] using quadratic Chabauty and a Mordell–Weil sieve, but we can also use the methods presented here to show the following proposition about the rational points of the curve in one residue disk. Magma [17] code that can be used to verify the computations here can be found in [33]. Let X be a regular model for $X_0(67)^+$ over the integers given by the homogenization of $y^2+(x^3+x+1)y = x^5-x$ in the weighted projective plane $\mathbb{P}^2_{(1,3,1)}$. Then $X(\mathbb{Q}) = X(\mathbb{Z})$ and we show the following.

Theorem 8.3.1. *The integer points of $X(\mathbb{Z})$ that do not reduce to $(1,4) \in X(\mathbb{F}_7)$ are contained in the set*

$$\begin{aligned}\big\{&[0,-1,1],\ [0,0,1],\ [1,0,1],\ [1,-3,1],\ [1,-1,0],\ [1,0,0],\\ &[4\cdot 7+O(7^2), 6+6\cdot 7+O(7^2), 1],\ [4\cdot 7+O(7^2), 3\cdot 7+O(7^2), 1],\\ &[1+2\cdot 7+O(7^2), 5\cdot 7+O(7^2), 1],\ [1+2\cdot 7+O(7^2), 4+O(7^2), 1],\\ &[1, 6+3\cdot 7+O(7^2), 3\cdot 7+O(7^2)],\ [1, 4\cdot 7+O(7^2), 4\cdot 7+O(7^2)]\big\}.\end{aligned}$$

Remark 8.3.2. The residue disk above $(1,4) \in X(\mathbb{F}_7)$ has at least two integer points, $[1,-3,2]$ and $[1,-10,2]$. Using geometric quadratic Chabauty modulo p^2, we cannot bound the size of this residue disk. After doing the necessary calculations, it turns out $\operatorname{im} \widetilde{j_b}(z) = \operatorname{im} \kappa(0, n_2)$. In this case, applying [36, Theorem 4.12], since the ring $\mathbb{F}_p[n_1, n_2]/(\overline{g_1}, \overline{g_2}) \simeq \mathbb{F}_p[n_2]$ is not finite, we cannot determine the solutions using calculations modulo p^2.

By increasing precision we are guaranteed a finite set of solutions in this residue disk. In practice, this requires computing heights of points that lie in residue disks at infinity which is not possible using current implementations of Coleman–Gross heights.

We present the computations in a single residue disk over $\overline{P} = (0,-1) \in X(\mathbb{F}_7)$ where we show the following.

Proposition 8.3.3. *The integer points of $X(\mathbb{Z})$ reducing to $(0,-1) \in X(\mathbb{F}_7)$ are contained in the set*

$$\{(0,-1), (4 \cdot 7 + O(7^2), 6 + O(7^2))\}.$$

By iterating the algorithm over the remaining residue disks, one can in principle determine a finite set of p-adic points containing $X(\mathbb{Q})$.

We first list some facts about this curve that will be useful in our computations. The curve X is a projective curve of genus 2 with Jacobian J. We recall some details about X and its Jacobian that are presented in [2, section 6]. The Jacobian J has Mordell–Weil rank 2 and $J_{\mathbb{Q}}$ has Néron–Severi rank 2. In addition, the only prime of bad reduction of X is 67. At 67, the special fiber is geometrically irreducible: it has one component with two nodes defined over $\mathbb{F}_{67^2}$. Hence, there are only geometrically irreducible fibers over every prime.

Remark 8.3.4. For this example curve, all of the fibers are geometrically irreducible, leading to a simplification in the notation used in the example compared to the notation in the preceding sections. In general, one needs to consider a distinction between J and J^0, where J^0 is the fiberwise connected component of 0 in J. We also omit the constant m which is the least common multiple of the exponents of all $J/J^0(\overline{\mathbb{F}}_p)$, with p ranging over all primes. Since $J = J^0$, we have $m = 1$. Let X^{sm} denote the open subscheme of X consisting of points at which X is smooth over $\mathbb{Z}$. Above, we consider the simple open subschemes U of X^{sm}. In this example, there is only one simple open to consider: the scheme X^{sm} obtained by removing the two Galois conjugate nodes in the fiber over 67. Since X is regular, $X^{\mathrm{sm}}(\mathbb{Z}) = X(\mathbb{Z})$.

Let ι be the hyperelliptic involution of X. We list some rational points on the curve that will be used in our computations:

$$\begin{aligned} P &:= [0,-1,1], & \iota P &:= [0,0,1], \\ Q &:= [-1,0,1], & \iota Q &:= [-1,1,1], \\ b &:= [1,0,1], & \iota b &:= [1,-3,1], \\ R &:= [1,-3,2], & \iota R &:= [1,-10,2], \\ \infty_+ &:= [1,0,0], & \infty_- &:= [1,-1,0]. \end{aligned} \tag{8.3.5}$$

These points turn out to be the only rational points on X, as proven in [2, Theorem 6.3] by a combination of quadratic Chabauty and the Mordell–Weil sieve.

Let $p = 7$. We first perform some local computations. There are 9 points on $X(\mathbb{F}_p)$. For each $\mathbb{F}_p$-point x of X^{sm}, we need an element in $T(\mathbb{Z})_{\widetilde{j_b}(x)}$, or equivalently an element in $J(\mathbb{Z})_{j_b(x)}$. Every residue disk of $X(\mathbb{Z}_p)$ contains an integer point; only

R and ιR reduce to the same point. Therefore, none of the residue disks $J(\mathbb{Z})_{j_b(x)}$ are empty. So we cannot rule out any residue disks of the torsor immediately; in fact, this calculation is a Mordell–Weil sieve at p, see [41, section 3.4] for more details.

This example presents the specific case of the residue disk corresponding to $X(\mathbb{Z})_{\overline{P}}$, where P is the point defined in (8.3.5). Because we can consider residue disks up to the hyperelliptic involution, this also gives us the analogous result for the residue disk corresponding to ιP.

Let $j_b\colon X^{\mathrm{sm}} \to J$ denote the Abel–Jacobi map with base point b defined in (8.3.5). We also have a set of generators for the Mordell–Weil group $J(\mathbb{Z})$ from the LMFDB,

$$\begin{aligned} G_1 &:= [P - \iota P], \\ G_2 &:= [P + Q - 2 \cdot \iota P]. \end{aligned} \tag{8.3.6}$$

Since X is a modular curve, its Jacobian has an action by the Hecke algebra. To describe the Hecke action on J explicitly, we fix the following basis for $H^0(X_{\mathbb{Q}}, \Omega^1_{X_{\mathbb{Q}}})$:

$$\left\{ \frac{dx}{2y - x^3 - x - 1}, \frac{xdx}{2y - x^3 - x - 1} \right\}. \tag{8.3.7}$$

We focus on the endomorphism given by the action of the Hecke operator T_2 on 1-forms of X. The Kodaira–Spencer map gives an isomorphism between $H^0(X_{\mathbb{Q}}, \Omega^1_{X_{\mathbb{Q}}})$ and $S_2(67)^+$. We choose a basis for $S_2(67)^+$ that is given by q-expansions with rational coefficients, as follows:

$$\begin{aligned} g_1 &:= q - 3q^3 - 3q^4 - 3q^5 + q^6 + 4q^7 + 3q^8 + O(q^9), \\ g_2 &:= q^2 - q^3 - 3q^4 + 3q^7 + 4q^8 + O(q^9). \end{aligned}$$

Then we choose the model for X where $\frac{du}{v}$ corresponds to $g_1\frac{dq}{q}$ and $u\frac{du}{v}$ corresponds to $g_2\frac{dq}{q}$, by setting $u = \frac{g_2}{g_1}$ and $v = q\frac{du}{g_1 dq}$. This allows us to find q-expansions for the monomials $\{v^2, 1, u, u^2, \ldots, u^5, u^6\}$ and use linear algebra to get an explicit equation for the new model of X,

$$v^2 = 9u^6 - 14u^5 + 9u^4 - 6u^3 + 6u^2 - 4u + 1.$$

Writing down an explicit change of model to the regular model, we can find the q-expansion of the forms in (8.3.7) and compute the Hecke action on these q-expansions. This gives us the matrix representation of the Hecke operator T_2 with respect to the basis on (8.3.7). The trace of this matrix is nonzero, so we let $f := 2T_2 + 3\,\mathrm{id}\colon J \to J$. The endomorphism f has trace zero and matrix representation

$$\begin{pmatrix} 1 & -2 \\ -2 & -1 \end{pmatrix} \tag{8.3.8}$$

with respect to the basis presented in (8.3.7). Using the work of [26], we can compute a divisor $D_f \subset X_{\mathbb{Q}} \times X_{\mathbb{Q}}$ inducing f. The equations that define this divisor are given in (B.0.1). Then Algorithm 7.1.2 produces the divisor A_α that satisfies the properties of Lemma 7.1.3.

We now use Algorithm 7.1.10 to calculate $f(G_1)$ and $f(G_2)$, where G_1 and G_2 are the generators of the Mordell–Weil group of J as in (8.3.6).

Since $J(\mathbb{Z}) = J(\mathbb{Q})$, the divisor $f(G_i)$ only needs to be computed over the rationals for $i = 1, 2$. For example, applying (7.1.5) we get $f(G_1) = \mathcal{O}_X(D_f|_{P\times X} - D_f|_{\iota(P)\times X})$ and we can compute an explicit divisor $f(G_1)$ using the equations for D_f. We find that

$$\begin{aligned} f(G_1) &= -G_1 + 2G_2 = [-(P - \iota P) + 2(P + Q - 2\iota P)] = [P + 2Q - 3\iota P], \qquad (8.3.9)\\ f(G_2) &= 2G_1 + G_2 = [2(P - \iota P) + 1(P + Q - 2\iota P)] = [3P + Q - 4\iota P]. \end{aligned}$$

Furthermore, we compute $c = [-11G_1 - 8G_2]$ using Algorithm 7.1.7.

We can parametrize the residue disk over $\overline{P}$ up to finite precision by

$$\mathbb{F}_p \to X(\mathbb{Z}/p^2\mathbb{Z})_{\overline{P}}, \qquad \nu \mapsto P_\nu \text{ such that } x(P_\nu)/p = \nu.$$

We now find the trivializing section $\varphi \circ \lambda$, following Section 7.2. By direct computation the constant v from Proposition 7.2.2 is 0, hence the pseudoparametrization φ has codomain $\mathbb{Z}_p^3$ (instead of $\mathbb{Z}_p^2 \times \mathbb{Q}_p$). This computation is done using code from the repository [4].

Since $p > 3$, by Proposition 7.2.2 the map $\varphi \circ \lambda : \mathbb{Z}_p \to \mathbb{Z}_p^3$ is linear modulo p. We will calculate $\widetilde{j}_b(P_0)$ and $\widetilde{j}_b(P_1)$ following Algorithm 7.2.4 and interpolate to determine the map. What the following computations show is that

$$\varphi \circ \lambda(\nu) \equiv (2\nu, 0, 6 - \nu) \mod p. \qquad (8.3.10)$$

By Proposition 7.2.1, the image of the map $\varphi \circ \lambda$ is cut out by two convergent power series. Giving $\mathbb{Z}_p^3$ the coordinates (x_1, x_2, x_3), we see the image of $\varphi \circ \lambda$ is cut out by the equations $g_1 = 0, g_2 = 0$ with $g_1 \equiv x_2 \mod p$, $g_2 \equiv 2x_3 + x_1 + 2 \mod p$.

Algorithm 7.2.4 relies on being able to compute Coleman–Gross local heights at p and at primes of bad reduction. We first note that, since the special fiber of X at 67 is geometrically irreducible, the heights at $\ell \neq p$ are all trivial, and we only have to consider the heights at p. Balakrishnan [5] has implemented Coleman–Gross local heights $h_p(D, E)$ for disjoint divisors of degree 0 on a curve Y with a few requirements:

(a) the hyperelliptic curve $Y\colon y^2 = H(x)$ is given by a monic odd degree model;

(b) the divisors D and E split as a sum of points $D = \sum_i n_i P_i$, $E = \sum_j m_j Q_j$ with $P_i, Q_j \in Y(\mathbb{Q}_p)$.

Remark 8.3.11. Suppose that $D = \sum_i n_i P_i$ and $E = \operatorname{Div} r + E'$ where $E' = \sum_j m_j Q_j$ with $P_i, Q_j \in Y(\mathbb{Q}_p)$. Then

$$h_p(D, E) = h_p(D, E' + \operatorname{Div} r) = h_p(D, E') + h_p(D, \operatorname{Div} r) = h_p(D, E') + \log(r(D))$$

so we can also compute $h_p(D, E)$.

Therefore we make a change of model when doing computations on $\mathcal{N}$. The even degree model of X is given by

$$y^2 = g(x) := x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1,$$

where $g(x)$ has a 7-adic zero $\beta = 4 + 3 \cdot 7 + 4 \cdot 7^2 + O(7^3)$. We can construct a degree

5 model:

$$\beta^6 y'^2 = g(\beta x'/(x'-1)) \cdot (x'-1)^6.$$

Letting $c_0 = 5 + 3 \cdot 7 + 3 \cdot 7^2 + O(7^3)$ be a 5th root of the leading coefficient of $g(\beta x'/(x'-1))$ we obtain an odd degree model over $\mathbb{Q}_p$ given by the coordinate transformation from the even degree model

$$(x, y) \mapsto (c_0 \cdot x/(x-\beta), \beta^3 y/(x-\beta)^3). \tag{8.3.12}$$

Remark 8.3.13. Forthcoming work of Gajović gives a practical algorithm and code for computing Coleman–Gross local heights $h_p(D, E)$ on even degree hyperelliptic curves.

We now compute for P the local height $\psi(\widetilde{j_b}(P)) = h_p(P - b, A_\alpha|_{P \times X})$. Let B, C be the divisors on X defined in Algorithm 7.1.2. One can check that $B \cap P_\nu$ is empty over $\mathbb{Z}/p^2\mathbb{Z}$ for all $\nu \in \mathbb{F}_p$, so we have $A_\alpha|_{P_\nu \times X} = D_f|_{P_\nu \times X} + B - C$; we denote $A_\alpha|_{P_0 \times X}$ by E_{P_0}. Over the rationals

$$E_{P_0} \sim [0, 0, 1] - [-1, 1, 1] + 2[-1, 0, 1] - 2[1, -3, 1] =: E'_{P_0},$$

with $E_{P_0} = E'_{P_0} + \operatorname{Div} g_{P_0}$ where g_{P_0} is computed explicitly as an element of the function field and given by equation (B.0.2). By Remark 8.3.11, we can decompose $h_p(P - b, E_{P_0}) = h_p(P - b, E'_{P_0}) + h_p(P - b, \operatorname{Div} g_{P_0})$. We compute

$$h_p(P - b, \operatorname{Div} g_{P_0}) = \log g_{P_0}(P)/g_{P_0}(b) = \log(4/9) \equiv 7 \mod 49.$$

We also compute

$$h_p(P-b, E'_{P_0}) = 5\cdot 7 + 3\cdot 7^2 + 3\cdot 7^3 + 6\cdot 7^4 + 7^5 + 5\cdot 7^6 + 2\cdot 7^7 + 6\cdot 7^8 + O(7^9).$$

So, $\psi(\widetilde{j_b}(P)) = 6\cdot 7 + O(7^2)$.

Unlike the P_0 case, the divisor $D_{P_1} := D_f|_{P_1\times X}$ is not a sum of two p-adic points. Instead we use the explicit Cantor's algorithm [19, 66] to get a linearly equivalent multiple which does split as a sum of p-adic points.

Let (u_1, v_1) be the Mumford representation for D_{P_1}. Then using [66, Algorithm Compose] we can compute (u_2, v_2), the Mumford representation for $2D_{P_1}$. Applying [66, Algorithm Reduce] we obtain the Mumford representation (u_3, v_3) for the reduction of $2D_{P_1}$ along with $r = (y - v_2(x))/u_3(x)$, satisfying the relationship

$$2D_{P_1} = \mathrm{Div}(u_1, v_1) = \mathrm{Div}((y - v_2(x))/u_3(x)) + \mathrm{Div}(u_3, v_3). \tag{8.3.14}$$

Remark 8.3.15. Since the computations for D_{P_1} were done on the regular model, we need to change the equations to the odd degree model. The Mumford divisor for D_{P_1} is a sum of 2 points over a totally ramified extension of $\mathbb{Q}_p$. Using the equations (8.3.12) for the change of model we can map the points to two points $(x_1, y_1), (x_2, y_2)$ on the odd degree model and construct the corresponding degree 2 Mumford divisor (u_1, v_1) vanishing on the x-coordinates using interpolation: $u_1(x) = (x - x_1)(x - x_2)$ and $v_1(x) = y_2 \cdot (x - x_1)/(x_2 - x_1) + y_1 \cdot (x - x_2)/(x_1 - x_2)$.

Then $2D_{P_1}$ is linearly equivalent to a divisor that splits into a sum of two points over the odd degree model. The splitting is given by $\{Q_1, Q_2\}$ equal to

$$\{(469610 \cdot 7 + O(7^9), -15018865 + O(7^9)), (499647 + O(7^9), -14480684 + O(7^9))\}.$$

By (8.3.14) we have

$$2D_{P_1} = Q_1 + Q_2 + \mathrm{Div}((y - v_2(x))/u_3(x)) + 2\infty,$$

where $v_2(x)$ is given by

$$-(462222 + O(7^8))x^3 + (73804 + O(7^8))x^2 + (1999391 + O(7^8))x - 1649234 + O(7^8)$$

and $u_3(x)$ by

$$(1 + O(7^8))x^2 + (1977884 + O(7^8))x + 297368 \cdot 7 + O(7^8).$$

With the splitting in hand, we can compute $\widetilde{j_b}(P_1)$:

$$\begin{aligned}\frac{1}{2}h_p(P_1 - b, 2D_{P_1}) + h_p(P_1 - b, B - C) = {} & h_p(P_1 - b, B - C) + \\ & \frac{1}{2}h_p(P_1 - b, Q_1 + Q_2 + 2\infty) + \\ & \frac{1}{2}h_p(P_1 - b, \mathrm{Div}((y - v_2(x))/u_3(x))).\end{aligned}$$

The divisor $B - C$ is not a sum of points, but we have that $B - C$ is linearly equivalent to $4\infty_- - \iota b - 5\iota Q + \mathrm{Div}(g_{P_1})$, where g_{P_1} is given by (B.0.3). Therefore $\psi(\widetilde{j_b}(P_1))$ is

$$\begin{aligned}
&h_p(P_1 - b, D_{P_1} + B - C)\\
&= \frac{1}{2}h_p(P_1 - b, Q_1 + Q_2 + 2\infty + 2(4\infty_- - \iota b - 5\iota Q))\\
&+ \frac{1}{2}\log((y - v_2)(P_1 - b)/u_3(P_1 - b)) + \log g_{P_1}(P_1 - b).
\end{aligned}$$

Then

$$\begin{aligned}
&\log g_{P_1}(P_1 - b) = 6 \cdot 7 + 3 \cdot 7^2 + 2 \cdot 7^3 + 2 \cdot 7^4 + O(7^5)\\
&\log(y - v_2)(P_1 - b)/u_3(P_1 - b)) = 7^2 + 3 \cdot 7^3 + 2 \cdot 7^4 + O(7^5))\\
&h_p(P_1 - b, Q_1 + Q_2 + 2\infty + 2(4\infty_- - \iota b - 5\iota Q)) = 5 \cdot 7 + 7^2 + 4 \cdot 7^3 + O(7^4)
\end{aligned}$$

So $\psi(\widetilde{j_b}(P_1)) = 5 \cdot 7 + O(7^2)$.

Now we can calculate $\widetilde{j_b}(P_1)$ in the bijection $\varphi\colon T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^3$ given in Definition 6.6.1. We can compute this using the logarithm, normalized by the logarithm at P:

$$\begin{aligned}
&\log(P_0 - b) - \log(P_0 - b) = (0, 0),\\
&\log(P_1 - b) - \log(P_0 - b) = (2 \cdot 7 + O(7^2), O(7^2)).
\end{aligned}$$

Hence we see $\varphi(\widetilde{j_b}(P_0)) = (0, 0, 6)$ and $\varphi(\widetilde{j_b}(P_1)) = (2, 0, 5)$. By interpolating these values we get (8.3.10).

We now discuss the map κ using formulas in section 7.3. We will show that the map $\varphi \circ \kappa\colon \mathbb{Z}_p^2 \to \mathbb{Z}_p^3$, which is by Proposition 7.3.9 given by two linear polynomials and one quadratic polynomial, is modulo p equal to

$$(n_1, n_2) \mapsto (n_1, -n_1 - 2n_2, -3n_1^2 - n_1 n_2 - n_1 + n_2 - 1). \tag{8.3.16}$$

We follow Algorithm 7.3.1 to construct the points of $\mathcal{M}^\times(G_i, f(G_j))(\mathbb{Z})$ and $\mathcal{M}^\times(G_i, c)(\mathbb{Z})$ for $i, j = 1, 2$ as in [36, section 8.3].

We work out the example $\mathcal{M}^\times(G_1, f(G_2))(\mathbb{Z})$ here in detail. Recall from (8.3.9) that we have $G_1 = [P - \iota P]$ and $f(G_2) = [3P + Q - 4\iota P]$. By (6.3.2), the $\mathbb{G}_m$-torsor $\mathcal{M}^\times(G_1, f(G_2))$ is $f(G_2)^* \mathcal{O}_X^\times(G_1)$. Since we want to work with the image in $\mathcal{N}$, and this representation of $f(G_2)$ is not disjoint from G_1 over $\mathbb{Q}$, we represent G_1 by the linearly equivalent divisor $\iota b - \infty_+ + \infty_- - Q$ and $f(G_2)$ by the linearly equivalent divisor $3(P - \iota P) + (P - \iota Q)$. These divisors are not disjoint over $\mathbb{Z}$ because $-\iota Q$ and ιb intersect over $\mathbb{Z}/2\mathbb{Z}$ so

$$\begin{aligned} h(P - \iota P, 3(P - \iota P) + (P - \iota Q)) = h_p(&\iota b - \infty_+ + \infty_- - Q, 3(P - \iota P) + (P - \iota Q)) \\ &+ \log(2). \end{aligned}$$

We can compute Q_{12}, which equals

$$([P - \iota P], [3(P - \iota P) + (P - \iota Q)], h(\iota b - \infty_+ + \infty_- - Q, 3(P - \iota P) + (P - \iota Q)).$$

This also equals $(G_1, f(G_1), 5 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + O(7^4))$.

The remaining Q_{ij} are:

$$\begin{aligned}
Q_{11} &= (G_1, f(G_1), 2\cdot 7 + 5\cdot 7^3 + O(7^4)),\\
Q_{21} &= (G_2, f(G_1), 4\cdot 7 + 3\cdot 7^2 + 2\cdot 7^3 + O(7^4)),\\
Q_{22} &= (G_2, f(G_2), 3\cdot 7^2 + 4\cdot 7^3 + O(7^4)),\\
Q_{10} &= (G_1, c, 3\cdot 7 + 4\cdot 7^2 + 5\cdot 7^3 + O(7^4)),\\
Q_{20} &= (G_2, c, 2\cdot 7 + 2\cdot 7^3 + O(7^4)).
\end{aligned}$$

Remark 8.3.17. In practice, since we will need to add Q_{ij} in $\mathcal{N} \simeq J(\mathbb{Q}_p)\times J(\mathbb{Q}_p)\times \mathbb{Q}_p$ we use the map $\log\colon J(\mathbb{Q}_p) \to \mathbb{Q}_p^g$ for $i,j = 1,2$ and for $j = 0$, we store Q_{ij} as the vector $(\log(G_i), \log(f(G_j)), h(G_i, f(G_j)))$. This allows us to add in $\mathbb{Q}_p^g$ instead of $J(\mathbb{Q}_p)$.

We proceed to compute the bijection $\kappa\colon \mathbb{Z}_p^2 \to T(\mathbb{Z}_p)_{\widetilde{j_b(\overline{P})}}$ of the integral points of T modulo p^2, as in [36, section 8.5]. The divisor $j_b(\overline{P}) \in J(\mathbb{F}_p)$ is equal to the image of

$$\widetilde{G_t} := G_1 + 3G_2$$

in $J(\mathbb{F}_p)$ and correspondingly we define $e_{01} := 1$ and $e_{02} := 3$.

Let $\widetilde{G_1}$ and $\widetilde{G_2}$ be a basis for the kernel of reduction $J(\mathbb{Z}) \to J(\mathbb{F}_p)$. Since

$$\widetilde{G_1} = -3G_1 + 7G_2, \quad \widetilde{G_2} = 7G_1 + 4G_2$$

we define $e_{11} = -3, e_{12} = 7, e_{21} = 7, e_{22} = 4$.

The map $\kappa_{\mathbb{Z}}$ is given in coordinates in $\mathcal{N}$ by sending (n_1, n_2) to

$$\begin{array}{l}
((7+7^2+7^3+O(7^4))\cdot n_1+(4\cdot 7^3+O(7^4))\cdot n_2+5\cdot 7+5\cdot 7^2+7^3+O(7^4),\\
(6\cdot 7+4\cdot 7^2+3\cdot 7^3+O(7^4))\cdot n_1+(5\cdot 7+O(7^4))\cdot n_2+5\cdot 7^2+3\cdot 7^3+O(7^4)),\\
((6\cdot 7+5\cdot 7^2+6\cdot 7^3+O(7^4))\cdot n_1+(2\cdot 7+2\cdot 7^2+6\cdot 7^3+O(7^4),\\
(4\cdot 7+3\cdot 7^2+3\cdot 7^3+O(7^4))\cdot n_1+(3\cdot 7+3\cdot 7^2+O(7^4))\cdot n_2+\\
4\cdot 7+2\cdot 7^3+O(7^4)),\\
(4\cdot 7+6\cdot 7^2+3\cdot 7^3+O(7^4))\cdot n_1^2+(6\cdot 7+7^2+4\cdot 7^3+O(7^4))\cdot n_2^2+\\
(6\cdot 7+3\cdot 7^2+2\cdot 7^3+O(7^4))\cdot n_1+(7+7^3+O(7^4))\cdot n_2+\\
6\cdot 7+6\cdot 7^2+3\cdot 7^3+O(7^4)),
\end{array}$$

where we apply the logarithm to the first two coordinates as in Remark 8.3.17.

Finally, by [36, Theorem 4.10], the map $\kappa_{\mathbb{Z}}$ extends to a bijection

$$\kappa\colon \mathbb{Z}_p^2 \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \tag{8.3.18}$$

with image $\overline{T(\mathbb{Z})}_{\widetilde{j_b}(\overline{P})}$. This map $\varphi\circ\kappa$ is polynomials $(\kappa_1, \kappa_2, \kappa_3) \in \mathbb{Q}_p[x_1, x_2]^3$, with κ_1, κ_2 linear and κ_3 at worst quadratic. Applying Corollary 6.6.2, we obtain the formula for $\varphi\circ\kappa$ given in (8.3.16).

We now have the tools to prove the upper bound on the number of points in the residue disk $\#X(\mathbb{Z})_{\overline{P}}$. We define

$$\overline{g_1} := (\varphi\circ\kappa)^*\overline{f_1} = -n_1 - 2n_2, \quad \overline{g_2} := (\varphi\circ\kappa)^*\overline{f_2} = n_1^2 - 2n_1n_2 - n_1 + 2n_2,$$

and $\overline{A} := \mathbb{F}_p[n_1, n_2]/(\overline{g_1}, \overline{g_2})$. The ring $\overline{A}$ is isomorphic to $\mathbb{F}_p[n_2]/(n_2^2 - 3n_2) \cong \mathbb{F}_p \times \mathbb{F}_p$, so by [36, Theorem 4.12] we have an upper bound of 2 on $\#X(\mathbb{Z})_{\overline{P}}$. Specifically, we see that there is at most one point reducing to P_0, namely P itself, and at most one point reducing to P_4 in $X(\mathbb{Z}/p^2\mathbb{Z})_{\overline{P}}$; the other P_ν have no rational points lying over them.

Remark 8.3.19. If we calculate κ and $\widetilde{j_b}$ with greater p-adic precision, we can compute the point reducing to P_4 with greater precision. This can be done by brute force, that is, trying all lifts of the found solution $n_1 = 1, n_2 = 3, \nu = 4$ and seeing when any of the calculated values of κ or $\widetilde{j_b}$ agree modulo the required precision. However, there is a more efficient way. We can look at the "higher residue disks" $X(\mathbb{Z}_p)_{P_4}$ and $T(\mathbb{Z}_p)_{\widetilde{j_b}(P_4)}$, consisting of points that reduce to a specified $\mathbb{Z}/p^2\mathbb{Z}$-point. We can parametrize $X(\mathbb{Z}_p)_{P_4}$ with the map $\mathbb{Z}_p \to X(\mathbb{Z}_p)_{P_4}$ sending μ to $P_{4+p\mu}$. With respect to our usual bijection $\varphi : T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^3$, we get a bijection of the higher residue disk of the torsor $T(\mathbb{Z}_p)_{\widetilde{j_b}(P_4)} \to (1,0,2)+p\mathbb{Z}_p^3$. Given these identifications, the inclusion $\widetilde{j_b}\colon X^{\mathrm{sm}}(\mathbb{Z}_p)_{P_4} \to T(\mathbb{Z}_p)_{\widetilde{j_b}(P_4)}$ is given by power series that are linear modulo p. Like in section 7.2, these can be found by interpolation. Similarly, κ restricted to $(1+p\mathbb{Z}_p) \times (3+p\mathbb{Z}_p)$ gives the inclusion $\kappa\colon \overline{T(\mathbb{Z})}_{\widetilde{j_b}(P_4)} \to T(\mathbb{Z}_p)_{\widetilde{j_b}(P_4)}$. For these identifications, κ is actually linear modulo p. Solving the resulting affine linear system of equations, we get that the only possible intersection of the image of κ and of $\widetilde{j_b}$ in the higher residue disk $T(\mathbb{Z}/p^3\mathbb{Z})_{\widetilde{j_b}(P_4)} \cong \mathbb{F}_p^3$ is $(5,1,5)$, corresponding to $P_{4+p\mu}$ with $\mu = 4$. This is the point $P_{32} \in X(\mathbb{Z}/p^3\mathbb{Z})_{P_4}$.

In total, we can strengthen Proposition 8.3.3 to say the residue disk $X(\mathbb{Z})_{\overline{P}}$ is contained in the set

$$\{P, (4\cdot 7 + 4\cdot 7^2 + O(7^3), 6 + 6\cdot 7 + 6\cdot 7^2 + O(7^3))\}.$$

Appendix A

Tables

We present tables of all hyperbolic triples (a, b, c) and admissible primes $\mathfrak{p}$ such that the curve $X_0(a, b, c; \mathfrak{p})$ has genus 0 or 1. The list with additional data is available online [34].

To record $\mathfrak{p}$, we list the prime number p below $\mathfrak{p}$. We describe the group $G = \mathrm{PXL}_2(\mathbb{F}_q)$ by presenting q and writing 1 in the PXL field if $G = \mathrm{PSL}_2(\mathbb{F}_q)$ and -1 if $G = \mathrm{PGL}_2(\mathbb{F}_q)$. We also record the information about the field $E(a, b, c)$ and the number of different prime ideals of E above p.

Nugent–Voight [56] define an invariant, the arithmetic dimension $\mathrm{adim}(a, b, c)$, to be the dimension of a quaternionic Shimura variety attached to $\Delta(a, b, c)$ given by the number of split real places of $E(a, b, c)$ of the quaternion algebra $A = E\langle\Delta^{(2)}\rangle$. In particular, the triangle group $\Delta(a, b, c)$ is arithmetic if and only if $\mathrm{adim}(a, b, c) = 1$.

One subtlety is that there can be an isomorphism between the cover coming from a nonarithmetic group and the cover coming from an arithmetic group. This can only happen when the arithmetic group is of noncompact type, with

$$(a, b, c) = (2, 3, \infty), (2, 4, \infty), (2, 6, \infty), (2, \infty, \infty), (3, 3, \infty), (3, \infty, \infty),$$
$$(4, 4, \infty), (6, 6, \infty), (\infty, \infty, \infty)$$

by Takeuchi [68]. All of these arise from finite-index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$, so they are related to classical modular curves, and are defined over $\mathbb{Q}$. The ramification of the curve $X_0(a, b, c; \mathfrak{p})$ for $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ replaces any occurrence of ∞ by p (see Proposition 3.3.5); this allows one to readily identify when this extra isomorphism applies. We record this by adding (1) to the arithmetic dimension entry on the table.

For the arithmetic triangle groups $\Delta(a, b, c)$ such that $\Delta \simeq \Lambda^1$, the corresponding list of curves is contained in [72, Tables 4.1–4.7]. We confirmed that the intersection is in agreement.

Finally, for noncocompact triples see Proposition 3.4.1.

Genus 0, $X_0(a,b,c;\mathfrak{p})$

This is a long table split into three tables (over the next three pages).

(a,b,c)	p	q	PXL	adim	$E(a,b,c)$	# of $\mathfrak{p}$
$(2,3,7)$	7	7	1	1	$\mathbb{Q}(\lambda_7)$	1
$(2,3,7)$	2	8	1	1	$\mathbb{Q}(\lambda_7)$	1
$(2,3,7)$	13	13	1	1	$\mathbb{Q}(\lambda_7)$	3
$(2,3,7)$	29	29	1	1	$\mathbb{Q}(\lambda_7)$	3
$(2,3,7)$	43	43	1	1	$\mathbb{Q}(\lambda_7)$	3
$(2,3,8)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2,3,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{8})$	1
$(2,3,8)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2,3,8)$	5	25	-1	1	$\mathbb{Q}(\sqrt{8})$	1
$(2,3,9)$	19	19	1	1	$\mathbb{Q}(\lambda_9)$	3
$(2,3,9)$	37	37	1	1	$\mathbb{Q}(\lambda_9)$	3
$(2,3,10)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,3,10)$	31	31	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,3,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$	2
$(2,3,12)$	5	25	1	1	$\mathbb{Q}(\sqrt{12})$	1
$(2,3,13)$	13	13	1	2 (1)	$\mathbb{Q}(\lambda_{13})$	1

⋮

(a,b,c)	p	q	PXL	adim	$E(a,b,c)$	# of $\mathfrak{p}$
$(2,3,15)$	2	16	1	2 (1)	$\mathbb{Q}(\lambda_{15})$	1
$(2,3,18)$	19	19	-1	1	$\mathbb{Q}(\lambda_9)$	3
$(2,4,5)$	5	5	-1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,4,5)$	3	9	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,4,5)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,5)$	41	41	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,6)$	5	5	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	7	7	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	13	13	-1	1	$\mathbb{Q}$	1
$(2,4,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{8})$	1
$(2,4,8)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2,4,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$	2
$(2,5,5)$	5	5	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,5,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,5,10)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,6,6)$	7	7	-1	1	$\mathbb{Q}$	1
$(2,6,6)$	13	13	1	1	$\mathbb{Q}$	1
$(2,6,7)$	7	7	-1	2 (1)	$\mathbb{Q}(\lambda_7)$	1

$\vdots$

(a,b,c)	p	q	PXL	adim	$E(a,b,c)$	# of $\mathfrak{p}$
$(2,8,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{8})$	1
$(3,3,4)$	7	7	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(3,3,4)$	3	9	1	1	$\mathbb{Q}(\sqrt{8})$	1
$(3,3,4)$	5	25	1	1	$\mathbb{Q}(\sqrt{8})$	1
$(3,3,5)$	2	4	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(3,3,6)$	13	13	1	1	$\mathbb{Q}(\sqrt{12})$	2
$(3,4,4)$	5	5	-1	1	$\mathbb{Q}$	1
$(3,4,4)$	13	13	-1	1	$\mathbb{Q}$	1
$(3,6,6)$	7	7	-1	1	$\mathbb{Q}$	1
$(4,4,4)$	3	9	1	1	$\mathbb{Q}(\sqrt{8})$	1

Genus 1, $X_0(a, b, c; \mathfrak{p})$

This long table is split into seven tables (over the next seven pages).

(a, b, c)	p	q	PXL	adim	E	# of $\mathfrak{p}$
$(2, 3, 7)$	3	27	1	1	$\mathbb{Q}(\lambda_7)$	1
$(2, 3, 7)$	41	41	1	1	$\mathbb{Q}(\lambda_7)$	3
$(2, 3, 7)$	71	71	1	1	$\mathbb{Q}(\lambda_7)$	3
$(2, 3, 7)$	97	97	1	1	$\mathbb{Q}(\lambda_7)$	3
$(2, 3, 7)$	113	113	1	1	$\mathbb{Q}(\lambda_7)$	3
$(2, 3, 7)$	127	127	1	1	$\mathbb{Q}(\lambda_7)$	3
$(2, 3, 8)$	23	23	-1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2, 3, 8)$	31	31	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2, 3, 8)$	41	41	-1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2, 3, 8)$	73	73	-1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2, 3, 8)$	97	97	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2, 3, 9)$	2	8	1	1	$\mathbb{Q}(\lambda_9)$	1
$(2, 3, 9)$	17	17	1	1	$\mathbb{Q}(\lambda_9)$	3
$(2, 3, 9)$	73	73	1	1	$\mathbb{Q}(\lambda_9)$	3
$(2, 3, 10)$	3	9	-1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2, 3, 10)$	19	19	1	1	$\mathbb{Q}(\sqrt{5})$	2

⋮

$(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$	$\boldsymbol{p}$	$\boldsymbol{q}$	**PXL**	**adim**	$\boldsymbol{E}$	# of $\mathfrak{p}$
$(2,3,10)$	41	41	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,3,10)$	61	61	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,3,11)$	11	11	1	1	$\mathbb{Q}(\lambda_5)$	1
$(2,3,11)$	23	23	1	1	$\mathbb{Q}(\lambda_5)$	5
$(2,3,12)$	11	11	-1	1	$\mathbb{Q}(\sqrt{12})$	2
$(2,3,12)$	37	37	-1	1	$\mathbb{Q}(\sqrt{12})$	2
$(2,3,12)$	7	49	1	1	$\mathbb{Q}(\sqrt{12})$	1
$(2,3,13)$	5	25	1	2	$\mathbb{Q}(\lambda_{13})$	3
$(2,3,13)$	3	27	1	2	$\mathbb{Q}(\lambda_{13})$	2
$(2,3,14)$	13	13	-1	1	$\mathbb{Q}(\lambda_7)$	3
$(2,3,14)$	29	29	1	1	$\mathbb{Q}(\lambda_7)$	3
$(2,3,14)$	43	43	-1	1	$\mathbb{Q}(\lambda_7)$	3
$(2,3,15)$	31	31	1	2	$\mathbb{Q}(\lambda_{15})$	4
$(2,3,16)$	17	17	-1	1	$\mathbb{Q}(\lambda_{16})$	4
$(2,3,17)$	2	16	1	2	$\mathbb{Q}(\lambda_{17})$	2
$(2,3,17)$	17	17	1	2	$\mathbb{Q}(\lambda_{17})$	1
$(2,3,18)$	37	37	1	1	$\mathbb{Q}(\lambda_9)$	3
$(2,3,19)$	19	19	1	3 (1)	$\mathbb{Q}(\lambda_{19})$	1

$\vdots$

(a,b,c)	p	q	PXL	adim	E	# of $\mathfrak{p}$
$(2,3,20)$	19	19	-1	2	$\mathbb{Q}(\lambda_{20})$	4
$(2,3,22)$	23	23	-1	2	$\mathbb{Q}(\lambda_5)$	5
$(2,3,24)$	5	25	-1	1	$\mathbb{Q}(\sqrt{2},\sqrt{3})$	2
$(2,3,26)$	3	27	-1	2	$\mathbb{Q}(\lambda_{13})$	2
$(2,3,30)$	31	31	-1	1	$\mathbb{Q}(\lambda_{15})$	4
$(2,4,5)$	19	19	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,5)$	29	29	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,5)$	31	31	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,5)$	7	49	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,4,5)$	61	61	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,6)$	11	11	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	17	17	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	19	19	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	29	29	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	31	31	-1	1	$\mathbb{Q}$	1
$(2,4,6)$	37	37	-1	1	$\mathbb{Q}$	1
$(2,4,7)$	7	7	1	1	$\mathbb{Q}(\lambda_7)$	1
$(2,4,7)$	13	13	-1	1	$\mathbb{Q}(\lambda_7)$	3

$\vdots$

(a,b,c)	p	q	PXL	adim	E	# of $\mathfrak{p}$
$(2,4,7)$	29	29	-1	1	$\mathbb{Q}(\lambda_7)$	3
$(2,4,8)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2,4,8)$	5	25	-1	1	$\mathbb{Q}(\sqrt{8})$	1
$(2,4,9)$	17	17	1	2	$\mathbb{Q}(\lambda_9)$	3
$(2,4,9)$	19	19	-1	2	$\mathbb{Q}(\lambda_9)$	3
$(2,4,10)$	3	9	-1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,4,10)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,4,11)$	11	11	-1	2 (1)	$\mathbb{Q}(\lambda_5)$	1
$(2,4,12)$	5	25	1	1	$\mathbb{Q}(\sqrt{12})$	1
$(2,4,13)$	13	13	-1	3 (1)	$\mathbb{Q}(\lambda_{13})$	1
$(2,4,14)$	13	13	-1	2	$\mathbb{Q}(\lambda_7)$	3
$(2,4,16)$	17	17	-1	2	$\mathbb{Q}(\lambda_{16})$	4
$(2,4,17)$	17	17	1	4 (1)	$\mathbb{Q}(\lambda_{17})$	1
$(2,5,5)$	3	9	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,5,5)$	31	31	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,5,5)$	41	41	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,5,6)$	5	5	-1	1	$\mathbb{Q}(\sqrt{5})$	1
$(2,5,6)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$	2

$\vdots$

(a,b,c)	p	q	PXL	adim	E	# of $\mathfrak{p}$
$(2,5,6)$	19	19	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,5,6)$	31	31	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,5,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{2},\sqrt{5})$	2
$(2,5,11)$	11	11	1	4 (2)	$\mathbb{Q}(\sqrt{5},\lambda_{11})$	2
$(2,5,12)$	11	11	-1	2	$\mathbb{Q}(\sqrt{3},\sqrt{5})$	4
$(2,5,15)$	2	16	1	2	$\mathbb{Q}(\lambda_{15})$	1
$(2,6,6)$	5	5	-1	1	$\mathbb{Q}$	1
$(2,6,6)$	19	19	-1	1	$\mathbb{Q}$	1
$(2,6,7)$	13	13	1	2	$\mathbb{Q}(\lambda_7)$	3
$(2,6,8)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$	2
$(2,6,9)$	19	19	-1	2	$\mathbb{Q}(\lambda_9)$	3
$(2,6,10)$	11	11	-1	2	$\mathbb{Q}(\sqrt{5})$	2
$(2,6,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$	2
$(2,6,13)$	13	13	1	4 (1)	$\mathbb{Q}(\lambda_{13})$	1
$(2,7,7)$	7	7	1	1	$\mathbb{Q}(\lambda_7)$	1
$(2,7,8)$	7	7	-1	2	$\mathbb{Q}(\sqrt{2},\lambda_7)$	2
$(2,7,9)$	2	8	1	3	$\mathbb{Q}(\lambda_7,\lambda_9)$	3
$(2,8,8)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$	2

⋮

$\boldsymbol{(a,b,c)}$	$\boldsymbol{p}$	$\boldsymbol{q}$	**PXL**	**adim**	$\boldsymbol{E}$	# of $\mathfrak{p}$
$(2,8,10)$	3	9	-1	3	$\mathbb{Q}(\sqrt{2},\sqrt{5})$	2
$(2,10,10)$	11	11	-1	1	$\mathbb{Q}(\sqrt{5})$	2
$(2,10,11)$	11	11	-1	$6\,(2)$	$\mathbb{Q}(\sqrt{5},\lambda_{11})$	2
$(2,12,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$	2
$(3,3,4)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(3,3,4)$	31	31	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(3,3,5)$	3	9	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(3,3,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(3,3,5)$	19	19	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(3,3,5)$	31	31	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(3,3,6)$	5	25	1	1	$\mathbb{Q}(\sqrt{12})$	1
$(3,3,7)$	2	8	1	1	$\mathbb{Q}(\lambda_7)$	1
$(3,3,7)$	13	13	1	1	$\mathbb{Q}(\lambda_7)$	3
$(3,3,9)$	19	19	1	1	$\mathbb{Q}(\lambda_9)$	3
$(3,3,15)$	2	16	1	1	$\mathbb{Q}(\lambda_{15})$	1
$(3,4,4)$	7	7	1	1	$\mathbb{Q}$	1
$(3,4,4)$	17	17	1	1	$\mathbb{Q}$	1
$(3,4,5)$	3	9	1	2	$\mathbb{Q}(\sqrt{5},\sqrt{8})$	2

$\vdots$

(a,b,c)	p	q	**PXL**	**adim**	E	# of $\mathfrak{p}$
$(3,4,6)$	5	5	-1	1	$\mathbb{Q}(\sqrt{24})$	2
$(3,4,7)$	7	7	1	2	$\mathbb{Q}(\sqrt{2},\lambda_7)$	2
$(3,4,12)$	13	13	-1	1	$\mathbb{Q}(\sqrt{3})$	2
$(3,5,5)$	2	4	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(3,5,5)$	5	5	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(3,5,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(3,6,6)$	13	13	1	1	$\mathbb{Q}$	1
$(3,6,8)$	7	7	-1	3	4.4.18432.1	4
$(3,7,7)$	7	7	1	2 (1)	$\mathbb{Q}(\lambda_7)$	1
$(3,7,7)$	2	8	1	2 (1)	$\mathbb{Q}(\lambda_7)$	1
$(4,4,4)$	17	17	1	1	$\mathbb{Q}(\sqrt{8})$	2
$(4,4,5)$	3	9	1	1	$\mathbb{Q}(\sqrt{5})$	1
$(4,4,6)$	13	13	-1	1	$\mathbb{Q}(\sqrt{12})$	2
$(4,5,6)$	5	5	-1	2	$\mathbb{Q}(\sqrt{5},\sqrt{24})$	2
$(4,6,6)$	7	7	-1	1	$\mathbb{Q}(\sqrt{8})$	2
$(4,8,8)$	3	9	-1	1	$\mathbb{Q}(\sqrt{2})$	1
$(5,5,5)$	11	11	1	1	$\mathbb{Q}(\sqrt{5})$	2
$(7,7,7)$	2	8	1	1	$\mathbb{Q}(\lambda_7)$	1

Appendix B

Equations

We provide the equations used in the computations of section 8.3.

We give coordinates $((x, y), (u, v))$ to $X \times X$. With this notation, the equations that define the divisor D_f are the following. The set of equations is presented in the following five pages.

$$
\begin{aligned}
D_f := [&x^5 - x^3y - xy - y^2 - x - y, \\
&u^5 - u^3v - uv - v^2 - u - v, \\
&1120x^{20}u^4 - 2068x^{20}u^3 + 8124x^{19}u^4 + 2407x^{20}u^2 - 16894x^{19}u^3 + \\
&35279x^{18}u^4 - 1641x^{20}u + 18092x^{19}u^2 - 67012x^{18}u^3 + 8178x^{19}u + \\
&102591x^{17}u^4 + 378x^{20} - 58447x^{18}u^2 - 173283x^{17}u^3 + \\
&216476x^{16}u^4 + 774x^{19} - 14247x^{18}u + 103331x^{17}u^2 \\
&- 297137x^{16}u^3 + 334741x^{15}u^4 + 1458x^{18} - 31130x^{17}u + \\
&180514x^{16}u^2 - 358567x^{15}u^3 + 360468x^{14}u^4 + 10605x^{17} + \cdots
\end{aligned}
\tag{B.0.1}
$$

$$\cdots - 90380x^{16}u + 290195x^{15}u^2 - 395289x^{14}u^3 + 240873x^{13}u^4 +$$

$$20415x^{16} - 159334x^{15}u + 394529x^{14}u^2 - 407100x^{13}u^3 + 44248x^{12}u^4 +$$

$$22701x^{15} - 112959x^{14}u + 418497x^{13}u^2 - 493887x^{12}u^3 - 105112x^{11}u^4 +$$

$$25606x^{14} - 115611x^{13}u + 111265x^{12}u^2 - 417580x^{11}u^3 - 92961x^{10}u^4 +$$

$$1092x^{13} - 103527x^{12}u + 145152x^{11}u^2 - 88490x^{10}u^3 - 92811x^9u^4 +$$

$$48856x^{12} + 186438x^{11}u + 267721x^{10}u^2 - 155622x^9u^3 - 45395x^8u^4 -$$

$$27776x^{11} - 191295x^{10}u - 178159x^9u^2 - 70489x^8u^3 + 16905x^7u^4 -$$

$$61956x^{10} - 74059x^9u + 378244x^8u^2 + 232801x^7u^3 + 15979x^6u^4 +$$

$$74366x^9 + 338472x^8u + 227589x^7u^2 - 74613x^6u^3 - 16012x^5u^4 -$$

$$87675x^8 - 182672x^7u - 189206x^6u^2 + 26802x^5u^3 + 25133x^4u^4 -$$

$$85989x^7 - 42976x^6u + 119160x^5u^2 + 38380x^4u^3 - 14569x^3u^4 +$$

$$57369x^6 + 50376x^5u - 22878x^4u^2 - 26236x^3u^3 + 5653x^2u^4 -$$

$$19638x^5 - 66959x^4u + 10199x^3u^2 + 7737x^2u^3 - 1185xu^4 - 18109x^4 +$$

$$33891x^3u - 10338x^2u^2 + 126xu^3 + 90u^4 + 8894x^3 - 13882x^2u +$$

$$3365xu^2 - 189u^3 - 1493x^2 + 903xu - 105u^2 - 176x + 18u + 4,$$

$$7605023584402176072496x^8u^2 + 2768486683241947883748x^8u +$$

$$2162467398048698636700x^7u^2 - 6272554892698832692599x^6yu^2 -$$

$$4626446567682633747828x^8v - 1168446771586826201673x^8 -$$

$$9165162915676858733619x^7u + 2241777840578137196064x^6yu -$$

$$8418141092008037071834x^6u^2 - 13292836185052144419762x^5yu^2 + \cdots$$

$$\cdots 754031123597981360894x^7v + 632890634371070363 4915x^6yv+$$

$$261519562851932525 2191x^7 + 183126279980146150 7208x^6y+$$

$$275607045825078494 8869x^6u + 154288573760108031 53841x^5yu-$$

$$117840515709020481 35703x^5u^2 - 723087253898449965 7093x^4yu^2+$$

$$169121563687819668 44899x^6v + 879413424446109769 7655x^5yv+$$

$$133822414691271501 96465x^6 + 408246958239092456 5047x^5y+$$

$$218525405985407980 87489x^5u + 132455195795541431 63167x^4yu-$$

$$229850669151600295 36074x^4u^2 - 232551287047907124 17887x^3yu^2+$$

$$136828221715604121 85605x^5v - 165783020433170604 550x^4yv-$$

$$693190230216616420 6278x^5 - 508345125902907242 0619x^4y-$$

$$118263504295692039 51840x^4u - 191996995153118114 52213x^3yu-$$

$$284844846987450460 75669x^3u^2 - 176900767152222656 02489x^2yu^2+$$

$$+ 178054734436963488 27856x^4v + 675202808346140479 378x^3yv+$$

$$667581488689260331 0402x^4 + 557716177775135174 0903x^3y+$$

$$199698786929799730 55652x^3u + 181201170634331357 35083x^2yu+$$

$$936713375105971953 531x^2u^2 + 114668534540373860 66020xyu^2+$$

$$105425239722421902 09720x^3v + 882442192180772032 8364x^2yv+$$

$$118771608066718536 72804x^3 + 133639132471749030 62953x^2y+$$

$$140594536526173404 71247x^2u + 102180578338932273 56605xyu-$$

$$308361787245220032 444xu^2 - 532277995611116580 5354yu^2 + \cdots$$

$\cdots + 5505912629321680476560x^2v - 4290695327689320279111xyv-$

$7612900075627672207215x^2 - 1431244666099995321496 96xy+$

$4434640084437900284987xu + 3704885128833955385271yu-$

$9937960689125203972 82u^2 + 5753504210077708198 3xv+$

$3829830430486931582408yv + 5885803647094172346013y+$

$9607901928515440165 07u + 2815067274380039139 80v+$

$1138251308293118019 17,$

$7901357140136684172 11x^8u^2 - 5219925169888931378 8x^8u+$

$4456263978221233809 60x^7u^2 - 4840651480726521393 93x^6yu^2-$

$3555897700178655696 39x^8v - 9783955480117807802 0x^8-$

$6783985660390369925 39x^7u + 1551985863932634878 18x^6yu-$

$1130522648181315434 79x^6u^2 - 8747651963076712124 24x^5yu^2+$

$5089323605089646824 3x^7v + 5498060684619324234 05x^6yv+$

$2458523737649488270 27x^7 + 2229736655780853767 66x^6y-$

$1860063919988596510 31x^6u + 9181350209001898414 69x^5yu-$

$5231507124342566705 61x^5u^2 - 3289278227725900677 29x^4yu^2+$

$1388867642711454788 442x^6v + 8826846130810806210 57x^5yv+$

$1142791546745352334 216x^6 + 5337320045492780220 10x^5y+$

$3944643531473448509 14x^5u + 8745865642708965232 36x^4yu-$

$1503623861758469781 638x^4u^2 - 1118256877330123036 794x^3yu^2 + \cdots$

$\cdots + 962253617070423872834x^5v + 260675420287904377496x^4yv-$

$731085570498024566668x^5 - 177841514864980758518x^4y-$

$135796587392191411610 6x^4u - 159533746801396364062 2x^3yu-$

$188255830384093788879 7x^3u^2 - 129392263402211967749 2x^2yu^2+$

$139075369269018976770 6x^4v + 246438908010171275168x^3yv+$

$793691222208583979104x^4 + 499223278514256382778x^3y+$

$645256167770372257021x^3u + 984786145000107598929x^2yu-$

$280718524673749556697x^2u^2 + 779933023636684223799xyu^2+$

$842189446494471065427x^3v + 558551444022004233780x^2yv+$

$913241896994237593431x^3 + 124496336355134294969 0x^2y+$

$727117765460043207926x^2u + 101244103092302818728 2xyu-$

$217533598677089394 58xu^2 - 344942106360625888966yu^2+$

$353025200232170583936x^2v - 211033121948623991455xyv-$

$163875785683850219832x^2 - 617198754625174179093xy+$

$597830134728356122829xu + 169901861802716830954yu-$

$822032246651072261 92u^2 + 823104554307996190 16xv+$

$191169787322405231086yv + 341475392487935405751x+$

$350318508927358217032y - 210287318910739415 84u-$

$95585144959427007 20v].$

Now we assume that u and v are elements of the function field of X satisfying $v^2 + (u^3 + u + 1) = u^5 - u$. The equation g_{P_0} is given by

$$
\begin{aligned}
g_{P_0} :=& 118016503u^{11} + 793929202u^{10} - 2478346563u^9 - 3325919630u^8 - \\
& 3561952636u^7 + 2886039937u^6 + 5879367604u^5 - 3830171961u^4 + \\
& 75101411u^3 + 2188669692u^2 - 697370245u + 85830184) \cdot \\
& (338078160u^{14} + 1369216548u^{13} + 2510230338u^{12} + 2713077234u^{11} + \\
& 1318504824u^{10} - 3414589416u^9 - 135231264u^8 - 236654712u^7 - \\
& 6668591706u^6 + 1850977926u^5 + 3220194474u^4 - 1293148962u^3 + \\
& 397241838u^2 - 8451954u)^{-1}v^{-1} + (375507055u^{14} + 718827791u^{13} - \\
& 1351825398u^{12} - 3390292268u^{11} - 6705483125u^{10} + 42915092u^9 - \\
& 3840900734u^8 - 10868247049u^7 + 12659952140u^6 + 12198614901u^5 - \\
& 5503860549u^4 - 1083606073u^3 + 1748789999u^2 - 686641472u + \\
& 85830184) \cdot (338078160u^{14} + 1369216548u^{13} + 2510230338u^{12} + \\
& 2713077234u^{11} + 1318504824u^{10} - 3414589416u^9 - 135231264u^8 - \\
& 236654712u^7 - 6668591706u^6 + 1850977926u^5 + 3220194474u^4 - \\
& 1293148962u^3 + 397241838u^2 - 8451954u)^{-1}.
\end{aligned}
\tag{B.0.2}
$$

Similarly, the equation g_{P_1} is given by

$$
\begin{aligned}
g_{P_1} :=&(9192u^{12} + 11490u^{11} + 10341u^{10} + 104559u^{9} + 116049u^{8}+\\
&189585u^{7} + 24129u^{6} - 659526u^{5} - 335508u^{4} + 291846u^{3}+\\
&135582u^{2} + 34470u + 1149) \cdot (17360u^{11} + 35588u^{10} + 40362u^{9}+\\
&23002u^{8} - 18662u^{7} - 161014u^{6} + 333746u^{5} - 518630u^{4} + 361088u^{3}-\\
&108500u^{2} + 21266u - 434)^{-1}v^{-1} + (-9192u^{14} - 2298u^{13} - 8043u^{12}-\\
&118347u^{11} - 181542u^{10} - 351594u^{9} - 2298u^{8} + 689400u^{7} - 13788u^{6}-\\
&476835u^{5} + 65493u^{4} + 167754u^{3} + 52854u^{2} - 13788u + 2298)\cdot\\
&(17360u^{11} + 35588u^{10} + 40362u^{9} + 23002u^{8} - 18662u^{7} - 161014u^{6}+\\
&333746u^{5} - 518630u^{4} + 361088u^{3} - 108500u^{2}+\\
&21266u - 434)^{-1}.
\end{aligned}
\tag{B.0.3}
$$

Bibliography

[1] Natália Archinard, *Hypergeometric abelian varieties*, Canad. J. Math. **55** (2003), no. 5, 897–932. MR 2005278 ↑6.

[2] J. S. Balakrishnan, A. J. Best, F. Bianchi, B. Lawrence, J. S. Müller, N. Triantafillou, and J. Vonk, *Two recent p-adic approaches towards the (effective) Mordell conjecture*, Arithmetic L-functions and differential geometric methods, Progr. Math., vol. 338, Birkhäuser/Springer, Cham, [2021] ©2021, pp. 31–74. MR 4311238 ↑9, 11, 135, 136, 137.

[3] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944. MR 3961086 ↑9, 126, 129.

[4] Jennifer Balakrishnan, Netan Dogra, Müller Steffen, Jan Tuitman, and Jan Vonk, *Magma code*, `https://github.com/steffenmueller/QCMod`, 2020. ↑140.

[5] Jennifer S. Balakrishnan, *Sage code*, `https://github.com/jbalakrishnan/AWS`, 2020. ↑141.

[6] Jennifer S. Balakrishnan and Amnon Besser, *Computing local p-adic height pairings on hyperelliptic curves*, Int. Math. Res. Not. IMRN **11** (2012), 2405–2444. ↑115, 117.

[7] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller, *Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves*, J. Reine Angew. Math. (2016), 51–79. ↑9.

[8] Jennifer S. Balakrishnan, Robert W. Bradshaw, and Kiran S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 16–31. MR 2721410 ↑129.

[9] Jennifer S. Balakrishnan and Netan Dogra, *An effective Chabauty-Kim theorem*, Compos. Math. **155** (2019), no. 6, 1057–1075. MR 3949926 ↑9, 10, 126, 129, 131.

[10] ———, *Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties*, Int. Math. Res. Not. IMRN (2021), no. 15, 11923–12008. MR 4294137 ↑9, 126.

[11] Jennifer S. Balakrishnan, Netan Dogra, Jan Steffen Müller, Jan Tuitman, and Jan Vonk, *Quadratic chabauty for modular curves: Algorithms and examples*, 2021. ↑9, 114, 126, 129, 130, 133.

[12] Amnon Besser, *p-adic heights and Vologodsky integration*, J. Number Theory **239** (2022), 273–297. MR 4434496 ↑94.

[13] Amnon Besser, J. Steffen Müller, and Padmavathi Srinivasan, *p-adic adelic metrics and quadratic chabauty i*, 2021. ↑9.

[14] L. Alexander Betts, *Weight filtrations on selmer schemes and the effective chabauty–kim method*, 2021. ↑126, 127.

[15] L. Alexander Betts and Netan Dogra, *The local theory of unipotent kummer maps and refined selmer schemes*, 2019. ↑11, 112, 126.

[16] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, second ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004. MR 2062673 ↑107.

[17] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478 ↑5, 11, 33, 70, 73, 77, 105, 135.

[18] Nicolas Bourbaki, *Commutative algebra. Chapters 1–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998, Translated from the French, Reprint of the 1989 English translation. MR 1727221 ↑113.

[19] David G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), no. 177, 95–101. MR 866101 ↑115, 117, 143.

[20] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885. MR 4484 ↑9, 85.

[21] Pete L. Clark and John Voight, *Algebraic curves uniformized by congruence subgroups of triangle groups*, Trans. Amer. Math. Soc. **371** (2019), no. 1, 33–82. MR 3885137 ↑4, 5, 8, 14, 15, 17, 19, 21, 23, 25, 28, 29, 32, 46, 55, 56, 78.

[22] Paula Cohen and Jürgen Wolfart, *Modular embeddings for some nonarithmetic Fuchsian groups*, Acta Arith. **56** (1990), no. 2, 93–110. MR 1075639 ↑6.

[23] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR 808103 ↑9, 11.

[24] ———, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR 808103 ↑10, 129.

[25] Robert F. Coleman and Benedict H. Gross, *p-adic heights on curves*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 73–81. MR 1097610 ↑11, 93.

[26] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comp. **88** (2019), no. 317, 1303–1339. MR 3904148 ↑106, 107, 139.

[27] David A. Cox and Walter R. Parry, *Genera of congruence subgroups in* **Q**-*quaternion algebras*, J. Reine Angew. Math. **351** (1984), 66–112. MR 749678 ↑7.

[28] C. J. Cummins and S. Pauli, *Congruence subgroups of* $\mathrm{PSL}(2,\mathbb{Z})$ *of genus less than or equal to 24*, Experiment. Math. **12** (2003), no. 2, 243–255. MR 2016709 ↑2.

[29] Henri Darmon, *A fourteenth lecture on Fermat's last theorem*, Number theory, CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, RI, 2004, pp. 103–115. MR 2076588 ↑6.

[30] Henri Darmon, Victor Rotger, and Ignacio Sols, *Iterated integrals, diagonal cycles and rational points on elliptic curves*, Publications mathématiques de Besançon. Algèbre et théorie des nombres, 2012/2, Publ. Math. Besançon Algèbre Théorie Nr., vol. 2012/, Presses Univ. Franche-Comté, Besançon, 2012, pp. 19–46. MR 3074917 ↑131.

[31] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR 2112196 ↑2.

[32] Juanita Duque-Rosero, Sachi Hashimoto, and Pim Spelier, *Geometric quadratic chabauty and p-adic heights*, `https://arxiv.org/abs/2207.10389`, 2022. ↑1, 84, 104, 123.

[33] ———, *Magma code*, `https://github.com/sachihashimoto/geo-quad-chab`, 2022. ↑11, 135.

[34] Juanita Duque-Rosero and John Voight, *Magma code*, `https://github.com/juanitaduquer/triangularModularCurves`, 2022. ↑5, 70, 74, 77, 150.

[35] ———, *Triangular modular curves of small genus*, Res. Number Theory **9** (2023), no. 1, Paper No. 3, 26. MR 4517324 ↑1, 14, 23, 36.

[36] Bas Edixhoven and Guido Lido, *Geometric quadratic chabauty*, Journal of the Institute of Mathematics of Jussieu (2021), 1–55. ↑ii, 8, 9, 86, 87, 91, 92, 93, 95, 96, 98, 100, 106, 108, 110, 112, 120, 121, 122, 125, 126, 136, 146, 147, 148, 149.

[37] Noam D. Elkies, *The Klein quartic in number theory*, The eightfold way, Math. Sci. Res. Inst. Publ., vol. 35, Cambridge Univ. Press, Cambridge, 1999, pp. 51–101. MR 1722413 ↑22.

[38] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR 718935 ↑8.

[39] Robert Fricke, *Die elliptischen Funktionen und ihre Anwendungen. Zweiter Teil. Die algebraischen Ausführungen*, Springer, Heidelberg, 2011. ↑2.

[40] A. Grothendieck, M. Raynaud, and D. S. Rim, *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin-New York, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. MR 0354656 ↑88.

[41] Sachi Hashimoto and Pim Spelier, *A geometric linear Chabauty comparison theorem*, Acta Arith. **202** (2022), no. 1, 67–88. MR 4378557 ↑10, 97, 126, 129, 138.

[42] Taira Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), no. 2, 213–246. ↑98.

[43] Kamal Khuri-Makdisi, *Linear algebra algorithms for divisors on an algebraic curve*, Math. Comp. **73** (2004), no. 245, 333–357. MR 2034126 ↑98.

[44] Minhyong Kim, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), no. 1, 89–133. MR 2512779 ↑9.

[45] Michael Klug, Michael Musty, Sam Schiavone, and John Voight, *Numerical calculation of three-point branched covers of the projective line*, LMS J. Comput. Math. **17** (2014), no. 1, 379–430. MR 3356040 ↑6.

[46] ———, *Numerical calculation of three-point branched covers of the projective line*, LMS J. Comput. Math. **17** (2014), no. 1, 379–430. MR 3356040 ↑15.

[47] Robert Kucharczyk and John Voight, *Hypergeometric functions and shimura varieties*, unpublished, 2022. ↑6.

[48] Franz-Viktor Kuhlmann, *Maps on ultrametric spaces, Hensel's lemma, and differential equations over valued fields*, Comm. Algebra **39** (2011), no. 5, 1730–1776. MR 2821504 ↑125.

[49] D. D. Long, C. Maclachlan, and A. W. Reid, *Arithmetic Fuchsian groups of genus zero*, Pure Appl. Math. Q. **2** (2006), no. 2, Special Issue: In honor of John H. Coates. Part 2, 569–599. MR 2251482 ↑3.

[50] A. M. Macbeath, *Generators of the linear fractional groups*, Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), Amer. Math. Soc., Providence, R.I., 1969, pp. 14–32. MR 0262379 ↑5.

[51] Colin Maclachlan and Alan W. Reid, *The arithmetic of hyperbolic 3-manifolds*, Graduate Texts in Mathematics, vol. 219, Springer-Verlag, New York, 2003. MR 1937957 ↑18.

[52] Nicolas Mascot, *Hensel-lifting torsion points on Jacobians and Galois representations*, Math. Comp. **89** (2020), no. 323, 1417–1455. MR 4063323 ↑98.

[53] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR 482230 ↑2.

[54] L. Moret-Bailly, *Pinceaux de variétés abéliennes*, Astérisque (1985), no. 129, 266. MR 797982 ↑88.

[55] Jan Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202. MR 1263527 ↑129.

[56] Steve Nugent and John Voight, *On the arithmetic dimension of triangle groups*, Math. Comp. **86** (2017), no. 306, 1979–2004. MR 3626545 ↑70, 150.

[57] A. P. Ogg, *Rational points on certain elliptic modular curves*, Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972), 1973, pp. 221–231. MR 0337974 ↑2.

[58] ______, *Diophantine equations and modular forms*, Bull. Amer. Math. Soc. **81** (1975), 14–27. MR 354675 ↑2.

[59] Andrew P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462. MR 364259 ↑2.

[60] Pierre Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier (Grenoble) **50** (2000), no. 3, 723–749. MR 1779891 ↑87.

[61] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-adic images of galois for elliptic curves over $\mathbb{Q}$*, 2021. ↑2.

[62] Benjamin Smith, *Explicit endomorphisms and correspondences*, PhD thesis, University of Sydney, 2005. ↑105, 107.

[63] Pim Spelier, *A geometric approach to linear Chabauty*, Master's thesis, Leiden University, 2020. ↑10, 97, 99, 100, 129.

[64] The Stacks Project Authors, *Stacks Project*, `https://stacks.math.columbia.edu`, 2018. ↑85.

[65] Giovanni Staglianò, *A Macaulay2 package for computations with rational maps*, J. Softw. Algebra Geom. **8** (2018), 61–70. MR 3857650 ↑109.

[66] Andrew V. Sutherland, *Fast Jacobian arithmetic for hyperelliptic curves of genus 3*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 2, Math. Sci. Publ., Berkeley, CA, 2019, pp. 425–442. MR 3952026 ↑116, 143.

[67] Kisao Takeuchi, *On some discrete subgroups of* $\mathrm{SL}_2(R)$, J. Fac. Sci. Univ. Tokyo Sect. I **16** (1969), 97–100. MR 262171 ↑18.

[68] ———, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), no. 1, 91–106. MR 429744 ↑4, 151.

[69] ———, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **24** (1977), no. 1, 201–212. MR 463116 ↑4, 17.

[70] J. G. Thompson, *A finiteness theorem for subgroups of* PSL(2, **R**) *which are commensurable with* PSL(2, **Z**), The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., Providence, R.I., 1980, pp. 533–555. MR 604632 ↑7.

[71] Raymond van Bommel, David Holmes, and J. Steffen Müller, *Explicit arithmetic intersection theory and computation of Néron-Tate heights*, Math. Comp. **89** (2020), no. 321, 395–410. MR 4011549 ↑119.

[72] John Voight, *Shimura curves of genus at most two*, Math. Comp. **78** (2009), no. 266, 1155–1172. MR 2476577 ↑2, 151.

[73] ———, *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, Quadratic and higher degree forms, Dev. Math., vol. 31, Springer, New York, 2013, pp. 255–298. MR 3156561 ↑60, 70.

[74] ———, *Quaternion algebras*, Graduate Texts in Mathematics, vol. 288, Springer, Cham, [2021] ©2021. MR 4279905 ↑15, 62, 77, 80, 81.