2022

Geometric and analytic methods for quadratic Chabauty

BOSTON UNIVERSITY

GRADUATE SCHOOL OF ARTS AND SCIENCES

Dissertation

GEOMETRIC AND ANALYTIC METHODS FOR QUADRATIC CHABAUTY

by

SACHI HASHIMOTO

B.A., University of Chicago, 2014

Submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

2022

Approved by

First Reader

Jennifer S. Balakrishnan, PhD
Clare Boothe Luce Associate Professor of Mathematics

Second Reader

Robert Pollack, PhD
Professor of Mathematics

Third Reader

J. Steffen Müller, PhD
Assistant Professor of Mathematics

Fourth Reader

David Rohrlich, PhD
Professor of Mathematics

To M and N
who grew up along with my thesis

Acknowledgments

It is a pleasure to thank my advisor, Jennifer Balakrishnan, for her support, encouragement, and guidance throughout my time at Boston University. This thesis would not have been possible without her invaluable mentorship.

This thesis also could not exist without the contributions of several other people. First, thank you to my collaborators Juanita Duque-Rosero and Pim Spelier for making the second half of this thesis a joy to work on.

I am thankful to the many people who have answered my questions and discussed math with me: including Alex Best, Edgar Costa, Stevan Gajović, Aash Jha, Borys Kadets, Angus McAndrew, Steffen Müller, Robert Pollack, David Rohrlich, Ari Shnidman, and John Voight. I also thank Yuval Wigderson for helping me solve numerous TeX problems while formatting this thesis.

I am very grateful to have had the opportunity to work with Bas Edixhoven during the Arizona Winter School in March 2020. Bas was always generous with his ideas and time, and I am grateful for his advice on the second part of this thesis.

Finally, thank you to all of my friends for being there and being you. Thank you for your generosity and understanding and for always cheering me on.

My work is supported by National Science Foundation grant DGE-1840990.

GEOMETRIC AND ANALYTIC METHODS FOR QUADRATIC CHABAUTY

SACHI HASHIMOTO

Boston University, Graduate School of Arts and Sciences, 2022

Major Professor: Jennifer S. Balakrishnan
Clare Boothe Luce Associate Professor of Mathematics

ABSTRACT

Let X be an Atkin–Lehner quotient of the modular curve $X_0(N)$ whose Jacobian J_f is a simple quotient of $J_0(N)^{\text{new}}$ over $\mathbf{Q}$. We give analytic methods for determining the rational points of X using quadratic Chabauty by explicitly computing two p-adic Gross–Zagier formulas for the newform f of level N and weight 2 associated with J_f when f has analytic rank 1. Combining results of Gross–Zagier and Waldspurger, one knows that for certain imaginary quadratic fields K, there exists a Heegner divisor in $J_0(N)(K)$ whose image is finite index in $J_f(\mathbf{Q})$ under the action of Hecke. We give an algorithm to compute the special value of the anticyclotomic p-adic L-function of f constructed by Bertolini, Darmon, and Prasanna, assuming some hypotheses on the prime p and on K. This value is proportional to the logarithm of the Heegner divisor on J_f with respect to the differential form fdq/q. We also compute the p-adic height of the Heegner divisor on J_f using a p-adic Gross–Zagier formula of Perrin-Riou.

Additionally, we give algorithms for the geometric quadratic Chabauty method of Edixhoven and Lido. Our algorithms describe how to translate their algebro-geometric method into calculations involving Coleman–Gross heights, logarithms, and divisor arithmetic. We achieve this by leveraging a map from the Poincaré biextension to the trivial biextension.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Let X be a nice (smooth projective geometrically integral) curve of genus $g > 1$ over a number field K. Faltings's theorem [Fal83] states that the set $X(K)$ of K-rational points of X is finite. However, there is no general method for determining this set explicitly. A major motivating question in the study of rational points is the following.

Motivating Question A. (How) can we provably determine $X(\mathbf{Q})$?

Since $X(\mathbf{Q})$ is simply a set, by embedding $X(\mathbf{Q})$ into something with more structure, we may be able to leverage that structure to gain information about $X(\mathbf{Q})$. This idea underlies several methods for finding rational points studied in this thesis. The methods we study fall under the umbrella of Chabauty's method, a p-adic method for finding rational points, where p is a prime of good reduction for X. The goal of effective Chabauty is to show that $X(\mathbf{Q})$ belongs to a finite and computable set; from there, we could hope to eliminate any extra points from the set and determine $X(\mathbf{Q})$ exactly. We obtain this finite and computable set by showing that $X(\mathbf{Q})$ lies in the zero set of nontrivial locally analytic functions from $X(\mathbf{Q}_p)$ to $\mathbf{Q}_p$. Since a locally analytic function has only finitely many zeros on each residue disk of $X(\mathbf{Q}_p)$, this exhibits $X(\mathbf{Q})$ inside a finite set. The difficult work of exhibiting $X(\mathbf{Q})$ inside this finite set lies in constructing these locally analytic functions and giving algorithms to explicitly compute them and their zeros on specific curves.

The simplest example of embedding $X(\mathbf{Q})$ inside an object with more structure comes from the Abel–Jacobi map. Assume that there is a rational point $b \in X(\mathbf{Q})$.

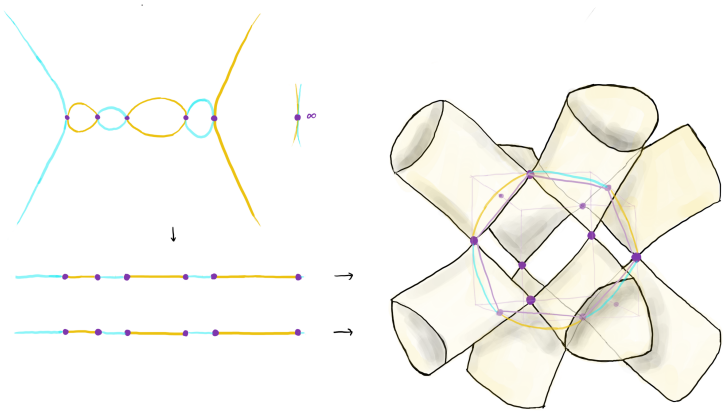

Figure 1.1: A genus 2 curve embedding in the quotient of its Jacobian by ± 1

The set $X(\mathbf{Q})$ embeds into the rational points of its Jacobian variety J by sending $P \in X(\mathbf{Q})$ to $[P - b] \in J(\mathbf{Q})$. The Mordell–Weil theorem states that $J(\mathbf{Q})$ has the structure of a finitely generated abelian group $J(\mathbf{Q}) \simeq \mathbf{Z}^r \oplus T$ for some $r \geq 0$ and finite abelian group T. Chabauty's method [Cha41] leverages the induced embedding $\iota : X(\mathbf{Q}_p) \to J(\mathbf{Q}_p)$ on p-adic points, where the objects $X(\mathbf{Q}_p)$ and $\overline{J(\mathbf{Q})}$, the p-adic closure of $J(\mathbf{Q})$ inside $J(\mathbf{Q}_p)$, gain the additional structure of p-adic manifolds of dimensions 1 and $r' \leq r$. Chabauty shows that when $r' < g$ the intersection

$$\iota(X(\mathbf{Q}_p)) \cap \overline{J(\mathbf{Q})} \subset J(\mathbf{Q}_p) \tag{$\star$}$$

of this 1-dimensional and r'-dimensional p-adic manifold inside of the g-dimensional p-adic manifold $J(\mathbf{Q}_p)$ is finite and contains $X(\mathbf{Q})$. Coleman [Col85a] made Chabauty's theoretical method effective by showing how to compute this intersection to find a finite set of p-adic points containing $X(\mathbf{Q})$ using p-adic (Coleman) integrals. The Coleman integrals of holomorphic differential forms are examples of locally analytic functions.

When $r' = g$, the intersection ($\star$) is no longer finite. Let $\rho(J)$ denote the Néron–Severi rank of J; we can think of this as the dimension of the space of trace 0

endomorphisms $f : J \to J$. When $r < g + \rho(J) - 1$, quadratic Chabauty [BD18, BD21] is a p-adic method that extends Chabauty's method by making effective M. Kim's program [Kim09] for an explicit Faltings's theorem via quotients of the unipotent fundamental group at depth 2. It replaces the role of the Jacobian with a non-abelian analogue carrying the structure of a "Selmer variety". In this case, the finite computable set containing $X(\mathbf{Q})$ is cut out by p-adic heights. The construction of this locally analytic function using p-adic heights plays a central role in Part I. We outline briefly how the function is constructed.

Nekovář [Nek93] constructs local and global p-adic heights of certain Galois representations of geometric origin. Using Kim's theory, Balakrishnan and Dogra assign a certain Galois representation to local and global points on X. Write $h_p(z)$ for the local height at p and $h(z)$ for the global height. Define the function $\rho(z) := h(z) - h_p(z)$ for $z \in X(\mathbf{Q}_p)$. We can show $h_p(z)$ and $h(z)$ are locally analytic functions on $X(\mathbf{Q}_p)$ away from b. First, by exhibiting $h_p(z)$ as the solution to a p-adic differential equation, we can write $h_p(z)$ as a locally analytic function. To write $h(z)$ as a locally analytic function, we need to write it in a locally analytic basis for $(H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \times H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee)^\vee$. This can be done by knowing "sufficiently many" rational points on X. Alternatively, if we do not know sufficiently many rational points, we can use an alternative construction of the height on the Jacobian due to Coleman and Gross, and write h in terms of a locally analytic basis of symmetric bilinear pairings for $J(\mathbf{Q}) \otimes \mathbf{Q}_p$. This second method requires knowing $r = g$ independent infinite order points on $J(\mathbf{Q})$. In Part I we develop a quadratic Chabauty method for certain quotients of modular curves that replaces this requirement for knowing rational points on X or J with computations of special values of p-adic L-value.

A special case of interest for Question A is when X is a modular curve or quotient of a modular curve. Modular curves parametrize geometric objects; finding the rational

points on a modular curve is equivalent to determining what geometric objects defined over $\mathbf{Q}$ have a certain property. We will study analytic techniques for applying the quadratic Chabauty method to modular curves in Part I. Our goal is to construct $\rho(z)$ without needing to know points on $J(\mathbf{Q})$ or $X(\mathbf{Q})$, other than the basepoint b. In particular, our methods apply to Atkin–Lehner quotients X of $X_0(N)$ whose Jacobians are simple quotients of $J_0(N)^{\text{new}}$ over $\mathbf{Q}$.

The Jacobians of modular curves have many endomorphisms coming from the action of Hecke correspondences, so this gives a natural source of elements of the Néron–Severi group. In particular, we will focus on the case when $r = g \geq 2$; then the simple quotients J_f of $J_0(N)^{\text{new}}$ have the special property that $r = g = \rho(J_f)$ and so satisfy the required inequality $r < g + \rho(J_f) - 1$.

The abelian variety $J_0(N)^{\text{new}}$ breaks up into simple isogeny factors whose L-functions can be written as the products of L-functions of newforms of weight 2 and level N. In this way we can rephrase our study of the Jacobians of these curves as a study of newforms and their L-functions. To be explicit, let X be an Atkin–Lehner quotient of $X_0(N)$ whose Jacobian J_f is a simple quotient of $J_0(N)^{\text{new}}$ over $\mathbf{Q}$. Since J_f is simple, there is some newform f of weight 2, level N, and coefficient field E_f such that

$$L(J_f, s) = \prod_{\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})} L(f^\sigma, s). \tag{$\dagger$}$$

Our main theorem is Theorem 5.2.2 where we give an analytic method for computing the quadratic Chabauty function $\rho(z)$ on these Atkin–Lehner quotients. The advantage of the analytic method that we provide is that unlike in the existing techniques in quadratic Chabauty for constructing these locally analytic functions $\rho(z)$, we do not need to know geometric data like infinite order points on the curve or its Jacobian. Amazingly f alone encodes enough information to get control over $X(\mathbf{Q})$.

Our method proceeds by studying Rankin–Selberg L-functions associated with f and imaginary quadratic field K. This analytic study of the L-functions of modular forms contains deep arithmetic information through the computation of special values of L-functions. For example, when f is an analytic rank 1 modular form attached to an elliptic curve $E/\mathbf{Q}$, Gross and Zagier [GZ86] prove a remarkable fact about the L-value $L'(f/K, 1)$, where K is an imaginary quadratic field satisfying a certain "Heegner hypothesis". This Heegner hypothesis for K guarantees the existence of a special divisor y_K, or Heegner divisor, on $J_0(N)$. The image of the Heegner divisor on the elliptic curve $\pi : J_0(N) \to E$ can be studied using the L-function of f. Gross and Zagier show that the Néron–Tate canonical height h_{NT} of the image of the Heegner divisor is proportional to the special value of the L-function

$$L'(f/K, 1) \doteq h_{\mathrm{NT}}(\pi(y_K)).$$

The symbol $\doteq$ denotes that there exists an explicit constant of proportionality C making the formula true.

In fact, the Gross–Zagier theorem more generally relates the derivative of the Rankin–Selberg L-function $L'(f, \chi, 1)$ of a weight 2 newform f to the canonical height of the f-isotypical component of y_K twisted by ring class characters χ. Under certain assumptions the image of y_K is finite index in $J(\mathbf{Q})$ under the action of Hecke. Using the Heegner divisor, and its relationship to $L'(f, \chi, 1)$ we replace the need for infinite order points in $J_f(\mathbf{Q})$ with computations of special values of Rankin–Selberg L-functions.

Now we assume that f is any newform of level N, weight 2, and analytic rank 1, and that the prime p is ordinary for f. Perrin-Riou [PR87] developed a p-adic version of Gross and Zagier's formula, replacing $L'(f/K, 1)$ with the derivative of a p-adic L-function $\mathcal{L}_p(f)$.

A p-adic L-function is an object that interpolates classical L-values; the special values of p-adic L-functions can similarly yield interesting arithmetic information. Let K_∞ denote the unique $\mathbf{Z}_p^2$ extension of K. Perrin-Riou's p-adic L-function interpolates central values of the Rankin L-function $L(f, \chi, 1)$ for finite order Hecke characters χ of $\mathrm{Gal}(K_\infty/K)$. She relates the derivative of this L-function in the "cyclotomic direction" at the trivial character $\mathcal{L}_p'(f, 1)$ to $h(y_{K,f})$ the cyclotomic p-adic height of the f-isotypical component of the Heegner divisor. This height was also studied in papers of Mazur–Tate [MT83], Schneider [Sch82], and Coleman–Gross [CG89]. Perrin-Riou shows

$$\mathcal{L}_p'(f, 1) \doteq h(y_{K,f}).$$

On the other hand, Bertolini, Darmon, and Prasanna [BDP13] constructed a different p-adic Rankin L-series L_p that also interpolates the central values of the Rankin L-function $L(f, \chi, 1)$ for a different set of Hecke characters of K. We call this the anticyclotomic p-adic L-function. In [BDP13] they shift the normalization of the p-adic L-function by the norm character $\mathbf{N}$, so that the special value is now at $\mathbf{N}$ instead of the trivial character: we write $L_p(f, 1) := L_p(f, \mathbf{N})$ to emphasize that both special values are occurring at the same place despite the apparent shift. While the functional equation forces $\mathcal{L}_p(f)$ to vanish at $\mathbf{N}$, the anticyclotomic p-adic L-function does not vanish at $\mathbf{N}$, and they obtain the special value formula

$$L_p(f, 1) \doteq (\log_{fdq/q} y_K)^2.$$

Here, $\log_{fdq/q}$ denotes the logarithm on $J_0(N)$ with respect to the differential form fdq/q. The character $\mathbf{N}$ lies outside of the range of interpolation for this L-function.

Edixhoven and Lido [EL21] translated the quadratic Chabauty method into algebro-geometric language to develop the geometric quadratic Chabauty method. Their method replaces the role of the Jacobian with a $\mathbf{G}_m^{\rho(J)-1}$-torsor T living over J that is

trivial when restricted to X. Their theory works with proper regular models over $\mathbf{Z}$; let $X_{\mathbf{Z}}$ be a proper regular model of X over $\mathbf{Z}$, then $X_{\mathbf{Z}}(\mathbf{Q}) = X_{\mathbf{Z}}(\mathbf{Z})$. The torsor T can be trivialized over an open covering of $X_{\mathbf{Z}}$. Let U be an open set in this cover. We can embed U via a section $\widetilde{j_b} : U(\mathbf{Z}_p) \to T(\mathbf{Z}_p)$. Then $U(\mathbf{Z}_p)$ is again a 1-dimensional p-adic manifold. Because $\mathbf{G}_m(\mathbf{Z}) = \{\pm 1\}$ is finite and $T(\mathbf{Z})$ lies over $J(\mathbf{Z})$, we can expect the closure of $T(\mathbf{Z})$ inside the $(g + \rho(J) - 1)$-dimensional p-adic manifold $T(\mathbf{Z}_p)$ to be of dimension at most r. Analogously to $(\star)$, when $r < g + \rho(J) - 1$ Edixhoven and Lido give an effective method to compute the intersection

$$\widetilde{j_b}(U(\mathbf{Z}_p)) \cap \overline{T(\mathbf{Z})} \subset T(\mathbf{Z}_p)$$

which is finite and contains $U(\mathbf{Z})$. In Part II we give algorithms for the geometric quadratic Chabauty method, and describe how to explicitly compute $\widetilde{j_b}(U(\mathbf{Z}_p)) \cap \overline{T(\mathbf{Z})}$ to finite p-adic precision.

1.1 Overview of the thesis

In Part I we give explicit methods to compute the p-adic height and logarithm of the Heegner divisor y_K from the modular form f. Chapter 3 features the computation of the special value of the anticyclotomic p-adic L-function $L_p(f, \mathbf{N})$. In Chapter 4 we discuss how to compute $\mathcal{L}_p'(f, 1)$ and the explicit constant of proportionality, in order to compute the height of y_K.

The special L-value computations from Chapters 3 and 4 are brought together in Chapter 5 where we give a formula for the locally analytic function that can be input into the quadratic Chabauty method to find a finite set containing $X(\mathbf{Q})$. The coefficients in this function are given by explicit constant multiples of the p-adic L-values $\mathcal{L}_p'(f, 1)$ and $L_p(f, 1)$ and the p-adic L-values associated with the Galois conjugates of f. The idea behind this construction is to replace the requirement to

know r independent infinite order points on $J(\mathbf{Q})$ with arithmetic information about the image of the divisor y_K on $J(\mathbf{Q})$. The special values of the p-adic L-functions capture the arithmetic information necessary to write $h(z)$ as a locally analytic function. This is done by comparing $h(y_K)$ to the values $(\log_{f^\sigma dq/q} y_K)^2$ as f^σ ranges over all Galois conjugates of f; this allows us to write $h(z)$ in terms of the locally analytic functions $(\log_{f^\sigma dq/q}(z))^2$.

Faltings's theorem also implies that the integer points on an affine genus 1 curve are finite. Quadratic Chabauty can be applied to the case of an affine rank 1 elliptic curve to determine a finite set of $\mathbf{Z}_p$ points containing the integer points. We give examples of this analytic method applied to the problem of determining integral points on several rank 1 elliptic curves, as well as the case of rational points on the genus 2 rank 2 curves $X_0(67)^+$, $X_0(73)^+$, $X_0^*(85)$, and $X_0(107)^+$. The rational points on these modular curves have already been determined using other methods [BBB+21, BDM+21, BGX21]; we provide a new way of computing these rational points.

We study algorithms for applying the geometric quadratic Chabauty method to curves in Part II in detail. Part II is joint work with Juanita Duque-Rosero and Pim Spelier. We show how to write the intersection of the $\mathbf{Z}_p$-points of an open set of the curve with the p-adic closure of the integer points of the torsor

$$\widetilde{j_b}(U(\mathbf{Z}_p)) \cap \overline{T(\mathbf{Z})}$$

only in terms of Coleman integrals and p-adic heights, which underscores the connection between the geometric method and the cohomological method.

The torsor T is a pullback of the universal $\mathbf{G}_m$-biextension, the Poincaré torsor $\mathcal{M}$, over $J \times J$ by a trace zero endomorphism $f : J \to J$. We introduce T, $\mathcal{M}$, and their various avatars in Chapter 7. Chapter 8 breaks down the geometric quadratic

Chabauty method into a series of algorithms that translate the method into the computation of Coleman integrals and p-adic heights as well as divisor arithmetic. Finally in Chapter 9 we provide a worked example of geometric quadratic Chabauty applied to the modular curve $X_0(67)^+$. The rational points of this curve have already been determined, but the example illustrates the practicality of the algorithms in the previous chapter.

1.2 Heights

The cyclotomic p-adic height pairings play an important role in both parts of this thesis. We introduce some background on these p-adic heights here following the perspective of Coleman and Gross. More details can be found in [MT83, CG89, BB12].

Let $\ell \neq p$ be a prime. We begin by discussing local heights h_ℓ. This depends on a choice of continuous character $\chi_\ell : \mathbf{Q}_\ell^\times \to \mathbf{Q}_p$. This is completely determined by the value of χ_ℓ on a uniformizer.

Definition 1.2.1. The local height h_ℓ is a function on pairs of $\mathbf{Q}_\ell$-rational divisors on X of degree zero with disjoint support such that

- h_ℓ is biadditive, continuous, and symmetric;
- $h_\ell(\operatorname{Div} f, D) = \chi_\ell(f(D))$ for f in the function field of X.

By [CG89, Proposition 1.2], there is a unique local height at primes $\ell \neq p$. This height can be extended compatibly to pairs of divisors with common support [BB15, Proposition 2.4], but we do not address this in detail here.

The local height at p is more subtle. We also fix χ_p a choice of continuous character $\chi_p : \mathbf{Q}_p^\times \to \mathbf{Q}_p$. Unlike χ_ℓ, this is not determined by a choice of χ_p on a uniformizer: the restriction to $\mathbf{Z}_p^\times$ factors through log, the p-adic logarithm, and by fixing a branch of the logarithm, we can write $\chi_p = t \circ \log$ for a $\mathbf{Q}_p$-linear map $t : \mathbf{Q}_p \to \mathbf{Q}_p$.

Let D_1 and D_2 be $\mathbf{Q}_p$-rational divisors on X of degree zero with disjoint support. Coleman and Gross define $h_p(D_1, D_2)$ as the Coleman integral of a third kind differential form $\int_{D_2} \omega_{D_1}$. We say that a differential form is of the third kind if it has at most simple poles at all points and integer residues; denote by $T(\mathbf{Q}_p)$ the set of third kind 1-forms of X defined over $\mathbf{Q}_p$.

The association $D_1 \mapsto \omega_{D_1}$ stems from the fact that the residue divisor of ω_{D_1} is D_1. That is, there is an exact sequence induced by applying the residue map to third kind differentials

$$0 \to H^0(X_{\mathbf{Q}_p}, \Omega^1) \to T(\mathbf{Q}_p) \xrightarrow{\text{res}} \mathrm{Div}^0(X_{\mathbf{Q}_p}) \to 0.$$

Giving a section of the residue map $D \mapsto \omega_D$ is equivalent to fixing a splitting of the Hodge filtration $H^1_{\mathrm{dR}}(X/\mathbf{Q}_p) \simeq H^0(X_{\mathbf{Q}_p}, \Omega^1) \oplus W$.

The local height at p is also continuous and bi-additive; when W is isotropic with respect to the cup product pairing on $H^1_{\mathrm{dR}}(X/\mathbf{Q}_p)$ the Coleman reciprocity law [CG89, Proposition 4.5] shows that h_p is also symmetric. We will always pick an isotropic subspace W and in Part I, since p will always be an ordinary prime for the Jacobian, the space W can always be taken to be the unit root subspace.

The local height at p can also be extended to pairs of divisors with common support, see [BB15] for more details. It depends on a choice of tangent vector at each point in the common support of the divisors. We do this compatibly for the local heights h_p and h_v when $v \neq p$ so that the global height $h := \sum_v h_v$ is independent of this choice. We write $h_p(x - b) := h_p(x - b, x - b)$ for the local height pairing at $x - b$ on $X_{\mathbf{Q}_p}$ assuming choices of tangent vectors t_b at b and t and x. In particular, when X is an elliptic curve, a dual vector to a Néron differential determines t_b and t (see [BBM16, Section 2] for more on tangent vectors).

Finally, we can define a global height h given a continuous idèle class character

$\chi : \mathbf{A}_{\mathbf{Q}}^{\times}/\mathbf{Q}^{\times} \to \mathbf{Q}_p$. The character χ specifies for each finite prime v a character $\chi_v : \mathbf{Q}_v^{\times} \to \mathbf{Q}_p$. Together with the choice W, this specifies a collection of local heights $(h_v)_{v \text{ prime}}$. The sum $h := \sum_v h_v$ defines a global height on $\mathrm{Div}^0_{\mathbf{Q}}(X)$ that is continuous, bilinear, and symmetric. The global height h is a pairing on the Jacobian $J(\mathbf{Q}) \times J(\mathbf{Q}) \to \mathbf{Q}_p$.

If $K/\mathbf{Q}$ is a number field, for any choice of continuous idèle class character $\chi_{\mathbf{Q}_p} : \mathbf{A}_K^{\times}/K^{\times} \to \mathbf{Q}_p$, we can analogously define height pairings h_v and h on $\mathrm{Div}^0_{K_v}(X)$ and $J(K)$ respectively. Over $\mathbf{Q}$, up to scaling, there is only one character $\chi : \mathbf{A}_{\mathbf{Q}}^{\times}/\mathbf{Q}^{\times} \to \mathbf{Q}_p$, the cyclotomic character. Over a number field $K/\mathbf{Q}$, there can be many different p-adic heights.

We use the notation $h(y)$ to mean the height pairing $h(y) := h(y, y)$ with respect to the cyclotomic character $\mathbf{A}_{\mathbf{Q}}^{\times}/\mathbf{Q}^{\times} \to \mathbf{Q}_p$. When the field of definition is not $\mathbf{Q}$ we will use other notation, as described in Chapter 4.

1.3 The logarithm

We recall some properties of the logarithm in this section. The Coleman integral on regular one-forms agrees with the logarithm on the residue disk $J(\mathbf{Q}_p)_0$ interpreted as a p-adic Lie group.

Definition 1.3.1. Let X be a scheme and R a local ring with residue field $\mathbf{F}_p$. For $x \in X(R)$ write $\bar{x}$ for the reduction map, $\bar{x} \in X(\mathbf{F}_p)$. Let $Q \in X(\mathbf{F}_p)$. We write $X(R)_Q$ for the residue disk $\{x \in X(R) : \bar{x} = Q\}$ over Q.

Recall that X is a nice curve over $\mathbf{Q}$ with Jacobian J.

Remark 1.3.2. Since in Part II, we work on the Néron model of J over $\mathbf{Z}$, we will be careful in stating our fields of definition.

For the remainder of this section, we will instead write J for the Néron model of the Jacobian of X over $\mathbf{Z}$, and J_R for $J \otimes R$.

Recall $H^0(J_{\mathbf{Z}_p}, \Omega^1_{J_{\mathbf{Z}_p}})$ is a free $\mathbf{Z}_p$-module of rank g. For any element $D \in J(\mathbf{Z}_p)$, we have an element

$$\log(D) := \int_0^D \in \mathrm{Hom}_{\mathbf{Z}_p}(H^0(J_{\mathbf{Z}_p}, \Omega^1_{J_{\mathbf{Z}_p}}), \mathbf{Q}_p), \tag{1.1}$$

sending a differential ω to the logarithm $\int_0^D \omega$. The resulting map $\log\colon D \mapsto \int_0^D$ is a homomorphism of abelian groups.

Proposition 1.3.3 ([Spe20, Lemma 3.7])**.** *Assume $p > 2$ is a prime number. Then the logarithm induces an isomorphism of abelian groups on the kernel of reduction $J(\mathbf{Z}_p)_0 \xrightarrow{\sim} H^0(J_{\mathbf{Z}_p}, \Omega^1_{J_{\mathbf{Z}_p}})^\vee$, where the dual is taken in the category of $\mathbf{Z}_p$-modules.*

Write $m := \mathrm{Ann}\, J(\mathbf{F}_p)$ to denote the smallest positive integer such that $m \cdot D = 0$ for all $D \in J(\mathbf{F}_p)$. In particular, the integral $\int_0^D := 1/m \cdot \int_0^{mD}$ lands in the submodule $\mathrm{Hom}_{\mathbf{Z}_p}(H^0(J_{\mathbf{Z}_p}, \Omega^1_{J_{\mathbf{Z}_p}}), (1/\mathrm{Ann}\, J(\mathbf{F}_p)) \cdot \mathbf{Z}_p)$.

As $\Omega^1_{J_{\mathbf{Z}_p}}$ is locally free,

$$\log : J_{\mathbf{Z}/p^n\mathbf{Z}}(\mathbf{Z}/p^n\mathbf{Z})_0 \to H^0(J_{\mathbf{Z}/p^n\mathbf{Z}}, \Omega^1_{J_{\mathbf{Z}/p^n\mathbf{Z}}})^\vee \otimes \mathbf{Z}/p^{n-1}\mathbf{Z},$$
$$D \mapsto \int_0^D$$

is an isomorphism given by lifting D to $\mathbf{Z}_p$, taking log, then reducing modulo p^{n-1}. If $|J(\mathbf{F}_p)|$ is invertible in $\mathbf{Z}_p$, this even extends to a morphism

$$J_{\mathbf{Z}/p^n\mathbf{Z}}(\mathbf{Z}/p^n\mathbf{Z}) \to H^0(J_{\mathbf{Z}/p^n\mathbf{Z}}, \Omega^1_{J_{\mathbf{Z}/p^n\mathbf{Z}}})^\vee \otimes \mathbf{Z}/p^{n-1}\mathbf{Z}. \tag{1.2}$$

Choosing a basis $(\omega_i)_{i=1}^g$ of $H^0(J_{\mathbf{Z}_p}, \Omega^1_{J_{\mathbf{Z}_p}})$ and dualizing, we get $\log : J(\mathbf{Z}_p)_0 \to \mathbf{Z}_p^g$, reducing to $\log : J(\mathbf{Z}/p^n\mathbf{Z})_0 \to (\mathbf{Z}/p^{n-1}\mathbf{Z})^g$.

Fix a point $R \in J(\mathbf{F}_p)$. For $D \in J(\mathbf{Z}_p)_R$, the logarithm $\log(D)$ has a convergent power series expansion [Spe20, Lemma 3.7]. Let $t_1, \ldots, t_g$ be local parameters of J at R and expand $\omega_i(t_1, \ldots, t_g) = \sum_{i=1}^g f_i(t_1, \ldots, t_g)dt_i$, with $f_i \in \mathbf{Z}_p[[t_1, \ldots, t_g]]$.

By formally integrating, ω_i has a unique local antiderivative g_i on $J(\mathbf{Z}_p)_R$ such that $dg_i = \omega_i$ and $g_i \in \mathbf{Q}_p[[t_1, \ldots, t_g]]$ with constant term 0. Let $\widetilde{R} \in J(\mathbf{Z}_p)_R$ be the

point where all t_i vanish. We may then evaluate the power series at D using the local parameters at R by

$$\log(D) := (g_1(t_1(D), \ldots, t_g(D)), \ldots, g_g(t_1(D), \ldots, t_g(D))) + \log(\widetilde{R}). \tag{1.3}$$

Remark 1.3.4. Let $X_{\mathbf{Z}_p}$ be a smooth model over $\mathbf{Z}_p$ for the curve $X/\mathbf{Q}$. Assume $X(\mathbf{Q}) \neq \emptyset$ and let $\iota : X_{\mathbf{Z}_p} \to J_{\mathbf{Z}_p}$ denote the Abel–Jacobi embedding sending $P \mapsto [P - b]$ for some $b \in X(\mathbf{Q})$.

For computational purposes, rather than evaluating in parameters on J, it is easier to exploit the isomorphism

$$\iota^* : H^0(X_{\mathbf{Z}_p}, \Omega^1_{X_{\mathbf{Z}_p}}) \simeq H^0(J_{\mathbf{Z}_p}, \Omega^1_{J_{\mathbf{Z}_p}}).$$

Suppose we can express $D = \sum_i n_i P_i$ as a sum of points on $X_{\mathbf{Z}_p}$, where $P_i \in X(L)$ for some finite extension $L/\mathbf{Z}_p$. Then we may evaluate $\log(D)$ using linearity of the logarithm and expanding in a local parameter on $X_{\mathbf{Z}_p}$ at each point. As $X_{\mathbf{Z}_p}$ is one-dimensional over $\mathbf{Z}_p$, we only need one parameter, see [Bal15b] for example, or the discussion in the following section.

In Part I we typically choose a distinguished element $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1_{X_{\mathbf{Q}_p}})$ and evaluate log on $D \in J(\mathbf{Q}_p)$ with respect to ω. We write this as

$$\log_\omega(D).$$

In Part II we rely on the fact that, by choosing a basis of $H^0(J_{\mathbf{Z}_p}, \Omega^1_{J_{\mathbf{Z}_p}})$, the logarithm gives an isomorphism $\log : J(\mathbf{Z}_p)_0 \simeq p\mathbf{Z}_p^g$.

1.4 Coleman integration

Let X^{an} denote the rigid analytic space over $\mathbf{Q}_p$ which is the generic fiber of $X_{\mathbf{Z}_p}$. Coleman gives a definition of the integral $\int_P^Q \eta$ on the rigid analytic space X^{an}. To do so, we work over a wide open space $V \subset X^{\mathrm{an}}$ constructed by deleting a finite number of closed disks from X^{an} of radius less than 1. He defines an integral for $P, Q \in V$

and η any differential ω of the second kind on V [Col85b] (a differential ω is of the second kind if it is everywhere meromorphic and the residue at every pole is zero).

We begin by recalling some facts about rigid analysis, following [Bes12, Section 1.3].

Definition 1.4.1. The Tate algebra T_n is

$$T_n := \mathbf{Q}_p\langle t_1, \ldots, t_n\rangle$$

is the subring of formal power series in n variables that consists of sums $\sum_I a_I x^I$ such that $\lim_{I\to\infty} |a_I| \to 0$.

The Tate algebra is the subring of $\mathbf{Q}_p[[t_1, \ldots, t_n]]$ that consists of convergent power series on $\mathbf{Z}_p^n$.

The Tate algebra plays a similar role in rigid geometry as polynomial rings over fields in algebraic geometry. In particular, T_n has many nice ring theoretic properties.

Proposition 1.4.2 (Noether normalization)**.** *Let $\mathfrak{a}$ be an ideal of T_n and $A \simeq T_n/\mathfrak{a}$. There exists a finite injective morphism $T_d \to A$ for some d. Furthermore, the Krull dimension of A is equal to d.*

Definition 1.4.3. An affinoid algebra is a $\mathbf{Q}_p$-algebra that is isomorphic to $T_n/\mathfrak{a}$ for some n and some ideal $\mathfrak{a}$ of T_n.

Let A be an affinoid algebra and write $\mathrm{MaxSpec}(A)$ for the set of maximal ideals of A. These are associated to each other in the same way that an affine scheme $\mathrm{MaxSpec}(k[x_1, \ldots, x_n]/I)$ is associated to $k[x_1, \ldots, x_n]/I$.

Rigid geometry describes a Grothendieck topology on $\mathrm{MaxSpec}(A)$, and this allows us to the define sheaves and gluing of affinoids, leading to the notion of a rigid analytic space. Rigid analytic spaces are locally isomorphic to $\mathrm{MaxSpec}(A)$ for A an affinoid algebra. We will not describe this construction in detail, and instead refer the reader to [FvdP04].

The Frobenius morphism on the special fiber of $X_{\mathbf{Z}_p}$ lifts to $\phi : X^{\mathrm{an}} \to X^{\mathrm{an}}$, that is, a morphism of rigid analytic varieties which reduces to (relative) Frobenius on $X_{\mathbf{F}_p}$. We fix a choice of lift ϕ. Fix also an embedding of $\mathbf{Q}_p$ into $\mathbf{C}_p$.

Theorem 1.4.4 ([Col85b, Theorem 2.1])**.** *Suppose there is a polynomial $\mathcal{P}(T) \in \mathbf{C}_p[T]$ which does not vanish on any root of unity, and that*

$$\mathcal{P}(\phi^*)\omega \text{ is exact.}$$

Then there is a function f_ω on $X(\mathbf{C}_p)$ which is analytic on each residue disc such that $df_\omega = \omega$ and $\mathcal{P}(\phi^*)(f_\omega)$ is analytic. The function f_ω is unique up to a constant and is independent of ϕ and $\mathcal{P}$.

In this way, Coleman provides a way to compute a locally analytic antiderivative of ω. Coleman also shows his definition agrees with the one induced by the p-adic Lie group structure of $J_{\mathbf{Q}_p}$ when $\eta \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$.

Coleman proves, in several corollaries, properties of the antiderivative, which we collect here in one theorem. Fix an algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$. For all points $P, Q, R \in V(\overline{\mathbf{Q}}_p)$ and one-forms ω, η of the second kind on $X_{\mathbf{Q}_p}$, the Coleman integral enjoys the following properties:

Theorem 1.4.5. *(Coleman)*

1. *Linearity:* $\int_P^Q (\alpha\omega + \beta\eta) = \alpha \int_P^Q \omega + \beta \int_P^Q \eta$, *for all* $\alpha, \beta \in \mathfrak{q}_p$.
2. *Additivity:* $\int_P^Q \omega = \int_P^R \omega + \int_R^Q \omega$.
3. *Fundamental theorem of calculus:* $\int_P^Q df = f(Q) - f(P)$ *for f a rigid analytic function on V.*
4. *Change of variables: if $V' \subset X'$ is another wide open subspace of a rigid analytic space X', for any rigid analytic map $\phi\colon V \to V'$, we have* $\int_{\phi(P)}^{\phi(Q)} \omega = \int_P^Q \phi^*(\omega)$.
5. *For any divisor $D := \sum_i Q_i - P_i$ of degree zero on X defined over $\overline{\mathbf{Q}}_p$, and for ω a regular one-form, then $\int_D \omega := \sum_i \int_{P_i}^{Q_i} \omega$ is well-defined, and $\int_D \omega = 0$ when D is principal.*
6. *Galois equivariance: if $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, then* $\left(\int_P^Q \omega\right)^\sigma = \int_{\sigma(P)}^{\sigma(Q)} \omega^\sigma$.

Remark 1.4.6. Let $Q_i, P_i \in \overline{\mathbf{Q}}_p$ such that $D := \sum_i Q_i - P_i$ is a divisor of degree zero on X defined over $\mathbf{Q}_p$. Let $\omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1)$. By (5) and (6) of Theorem 1.4.5, the

integral

$$\int_D \omega = \sum_i \int_{P_i}^{Q_i} \omega$$

is well-defined, only depends on the class $[D]$, and belongs to $\mathbf{Q}_p$, even though the individual integrals in the sum $\int_{P_i}^{Q_i} \omega$ may not belong to $\mathbf{Q}_p$.

When the rank r of $J(\mathbf{Q})$ is less than the genus g of X, the space of vanishing differentials

$$\mathrm{Van}(X(\mathbf{Q})) := \left\{ \omega \in H^0(X_{\mathbf{Q}_p}, \Omega^1) \colon \int_D \omega = 0 \text{ for all } D \in J(\mathbf{Q}) \right\}$$

is at least $(g-r)$-dimensional, and thus nonzero.

Coleman [Col85a] proves a bound on the number of rational points $\#X(\mathbf{Q}) \leq \#X(\mathbf{F}_p) + 2g - 2$ by bounding the number of zeros of a nonzero differential in $\mathrm{Van}(X(\mathbf{Q}))$, assuming $p > 2g$ and $r < g$. Coleman's proof suggests an algorithm for bounding $X(\mathbf{Q})$ by computing the set

$$X(\mathbf{Q}_p)_1 := \left\{ Q \in X(\mathbf{Q}_p) : \int_D^{\deg(D)Q} \omega = 0 \text{ for all } \omega \in \mathrm{Van}(X(\mathbf{Q})) \right\}.$$

Since the Coleman integral is locally analytic, it can be expressed as the integral of a convergent p-adic power series on each residue disk. Computing $X(\mathbf{Q}_p)_1$ yields finitely many solutions in each disk, and so finitely many in total. Therefore $X(\mathbf{Q}) \subseteq X(\mathbf{Q}_p)_1$ is finite.

The Coleman integral can be explicitly computed on hyperelliptic curves [BBK10, Bal15a] and more general curves (subject to some assumptions) [BT20]. We now outline the basic principle behind these algorithms.

To evaluate Coleman integrals, we work locally in each residue disc, where the Coleman integral can be expressed as a convergent power series in a parameter, called a local coordinate. If $K(X)$ denotes the function field of X, then our local coordinate is simply a uniformizing parameter t for $K(X)_P$, that is, an element $t \in K(X)_P$ such

that the valuation of t is one.

Suppose P and Q are in the same residue disc, and that this disc does not contain a pole of ω. Then it is straightforward to compute a Coleman integral between P and Q. This kind of integral is called a tiny integral. We simply write P, Q, and ω in the local coordinate t, as $t(P)$, $t(Q)$, and $\omega(t)$, and integrate formally:

$$\int_P^Q \omega = \int_{t(P)}^{t(Q)} \omega(t)dt. \tag{1.4}$$

The residue discs of $X(\mathbf{Q}_p)$ are disjoint, so we now face the problem of "analytic continuation" in the p-adics. Coleman's idea is to analytically continue along the Frobenius map, $x \mapsto x^p$. This gives a canonical path between two discs, along which we can integrate differential forms.

The rigid cohomology $H^1_{\mathrm{rig}}(X_{\mathbf{Q}_p})$ is a $2g$-dimensional $\mathbf{Q}_p$-vector space equipped with an action of the Frobenius map ϕ^*. Let $\omega_1, \ldots, \omega_{2g}$ be a basis for $H^1_{\mathrm{rig}}(X)$. For each ω_i, suppose we can compute the action of ϕ^* on ω_i. Then, by also computing reductions in $H^1_{\mathrm{rig}}(X_{\mathbf{Q}_p})$ we can write

$$\phi^*\omega_i = df_i + \sum_{j=1}^{2g} M_{ij}\omega_j \tag{1.5}$$

for some $M_{ij} \in \mathbf{Q}_p$, and f_i an overconvergent function on X^{an} (see [Bal15b, Section 2] for more details). Then $M = (M_{ij})_{1 \le i,j \le 2g}$ is a $2g \times 2g$ matrix that describes the action of Frobenius on cohomology. To compute M we can use Kedlaya's algorithm for hyperelliptic curves [Ked01, Ked03] and Tuitman's algorithm for general curves [Tui16, Tui17].

We can now compute $\int_P^Q \omega$ for P and Q in different residue disks. By linearity of the Coleman integral, it suffices to compute $\int_P^Q \omega_i$ for each i. First suppose P and Q

are points where f_i converges. Then by change of variables and (1.5)

$$\int_{\phi(P)}^{\phi(Q)} \omega_i = \int_P^Q \phi^* \omega_i = \int_P^Q (df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j) = f_i(Q) - f_i(P) + \sum_{j=1}^{2g} M_{ij} \int_P^Q \omega_j.$$

Therefore

$$\sum_{j=1}^{2g} (M - I)_{ij} \int_P^Q \omega_i = f_i(P) - f_i(Q) - \int_P^{\phi(P)} \omega_i - \int_{\phi(Q)}^Q \omega_i.$$

Since the matrix M representing the action of ϕ^* on $H^1_{\mathrm{rig}}(X_{\mathbf{Q}_p})$ has eigenvalues that are algebraic integers of norm $p^{1/2}$, we know that $M - I$ is invertible.

The function f_i might not converge at P, but since f_i is overconvergent, near the boundary of the residue disk of P it will converge. We compute the integral $\int_P^Q \omega$ by taking $S \in X(\mathbf{Q}_p(p^{1/e}))$ on the boundary for e large enough and breaking up the integral as $\int_P^S \omega + \int_S^Q \omega$.

Coleman also defined a theory of iterated Coleman integrals [Col82, Bes02]

$$\int_P^Q \eta_n \dots \eta_1.$$

Formally, iterated integrals are like path integrals

$$\int_P^Q \eta_n \dots \eta_1 = \int_0^1 \int_0^{R_1} \cdots \int_0^{R_{n-1}} \eta_n(R_n) \dots \eta_1(R_1).$$

The local height $h_p(z - b)$ can be expressed as a double Coleman integral [BBM16, Theorem 2.2].

Part I

p-adic Gross–Zagier and Quadratic Chabauty

Chapter 2

Introduction and Background I

2.1 Introduction I

In a way, the first part of this thesis is about the special values of Rankin L-functions attached to weight 2 newforms f and characters χ associated with an imaginary quadratic field K. While these Rankin L-functions do not make many explicit appearances, they play a crucial role in the analytic side of the theory.

Our story begins with the Gross–Zagier formula [GZ86]. Assume that every prime dividing the level N of f splits in K; this is the Heegner hypothesis, and it guarantees the existence of a Heegner divisor $y \in J_0(N)(H)$ defined over the Hilbert class field H/K. The Gross–Zagier formula relates the canonical height of y to the derivative of an L-function $L'(f, \chi, 1)$ attached to a character $\chi \in \mathrm{Gal}(H/K)$. The complex vector space $J_0(N)(H) \otimes \mathbf{C}$ decomposes into eigenspaces $V^{\chi,f}$ indexed by characters $\chi \in \mathrm{Gal}(H/K)$ and newforms f. Let $y_{\chi,f}$ denote the projection of y into the subspace $V^{\chi,f}$ such that the Hecke operator T_m acts via $T_m y_{\chi,f} = a_m(f) y_{\chi,f}$ and $\sigma \in \mathrm{Gal}(H/K)$ acts by $\sigma y_{\chi,f} = \chi(\sigma) y_{\chi,f}$. The Gross–Zagier formula says

$$L'(f, \chi, 1) \doteq h_{\mathrm{NT}}(y_{\chi,f}).$$

The L-function $L'(f, \chi, 1)$ is the L-function of the tensor product representation of f and a weight 1 modular form Θ_χ attached to χ called its theta series. In the case treated here, where K has class number 1, then χ is simply the trivial character $\mathbf{1}$.

We have the equality

$$L(f, \mathbf{1}, s) = L'(f, s)L(f^\varepsilon, s)$$

where ε is the quadratic character associated with K. Combining this with the Gross–Zagier formula leads to a formula for the height of $y_f := y_{\mathbf{1},f}$.

The Heegner hypothesis forces the sign of $L(f, \chi, s)$ to be -1. In particular, we consider the case when f has analytic rank 1, so $\operatorname{ord}_{s=1} L(f, s) = 1$ and $\operatorname{ord}_{s=1} L(f^\varepsilon, s)$ is even. A theorem of Waldspurger shows there exists infinitely many choices of K such that $L(f^\varepsilon, 1) \neq 0$, in which case y_f has non-zero height. Let X be a quotient of $X_0(N)$ by a group of Atkin–Lehner involutions with Jacobian J_f a simple quotient of $J_0(N)^{\text{new}}$ over $\mathbf{Q}$. Then J_f corresponds to some newform f as in (†). Write $\pi : J_0(N) \to J_f$ for the quotient map. In other words, $\pi(y) \in J_f(K)$ is non-torsion. In fact, $\pi(y)$ generates the Mordell–Weil group of J_f over $\mathbf{Q}$ in the following sense.

Since the sign of the Fricke involution is the negative of the sign of the functional equation of $L(f, s)$ in weight 2, the condition $\operatorname{ord}_{s=1} L(f, s) = 1$ forces the Fricke sign of f to be $+1$. Furthermore complex conjugation on $\pi(y)$ acts by the Fricke involution, so $\pi(y) \in J_f(\mathbf{Q})$ is a rational point. The Hecke action on J_f can be identified with an order $\mathcal{O}_f$ in K. Then $\mathcal{O}_f\pi(y)$ is a finite index subgroup of $J_f(\mathbf{Q})$.

Part I is a study of the p-adic properties of y_f and therefore a study of $J_f(\mathbf{Q}) \subset J_f(\mathbf{Q}_p)$ via the study of p-adic interpolations of the Rankin L-series $L(f, \chi, 1)$ for certain characters χ associated to K.

2.2 Modular forms, modular curves, Heegner points

This section will provide background on modular curves, modular forms, and Heegner points. For background on modular curves, we loosely follow [BGJGP05] but take the perspective of Katz [BDP13, Section 1.1] on viewing modular forms as functions on marked elliptic curves with level structure.

2.2.1 Algebraic modular forms and modular curves

Let $\mathcal{H} := \{z \in \mathbf{C} | \mathrm{Im}(z) > 0\}$ denote the upper half plane. Throughout we will use the convention that $z := x + iy$, so $\mathrm{Im}(z) = y$.

The group $\mathrm{SL}_2(\mathbf{R})$ acts by fractional linear transformation on $\mathcal{H}$. It has the discrete subgroup $\mathrm{SL}_2(\mathbf{Z})$, of 2×2 matrices with integer entries that have determinant 1. The congruence subgroup $\Gamma_0(N)$ is defined by

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \middle| c \equiv 0 \mod N \right\}.$$

Throughout, we want to consider modular forms in the sense of Katz, as functions on isomorphism classes of triples (E, C_N, ω_E) where $(E, C_N) \in X_0(N)$ is an elliptic curve with a cyclic subgroup of order N, and ω_E is a regular differential on E. We describe now how to formalize this notion, following the exposition in [BDP13, Section 1.1].

Definition 2.2.1. Let R be a ring. An elliptic curve E with $\Gamma_0(N)$-level structure over R is a pair (E, C_N) where $E \to \mathrm{Spec}\, R$ is an elliptic curve over $\mathrm{Spec}\, R$ and C_N is a sub-group scheme of E such that there exists an isomorphism $t : \mathbf{Z}/N\mathbf{Z} \to C_N$ over R.

A marked elliptic curve E with $\Gamma_0(N)$-level structure over R is a triple (E, C_N, ω) such that ω is a global section of Ω^1_E over $\mathrm{Spec}\, R$ and (E, C_N) is an elliptic curve with $\Gamma_0(N)$-level structure.

Definition 2.2.2. Let F be a field and R an F-algebra. A weakly holomorphic algebraic modular form f of weight k for $\Gamma_0(N)$ defined over F is a rule that assigns to every isomorphism class of marked elliptic curves with $\Gamma_0(N)$-level structure (E, C_N, ω) over R an element $f(E, C_N, \omega) \in R$ such that

1. for every homomorphism of F-algebras $j : R \to R'$, $f((E, C_N, \omega) \otimes_j R') = j(f(E, C_N, \omega))$;
2. for all $\lambda \in R^\times$, $f(E, C_N, \lambda\omega) = \lambda^{-k}(E, C_N, \omega)$.

Let us denote by $(\mathrm{Tate}(q), T_N, du/u)$ the Tate curve $\mathbf{G}_m/q^{\mathbf{Z}}$ along with $\Gamma_0(N)$ structure T_N and canonical differential du/u where u is the usual parameter in $\mathbf{G}_m$. The Tate curve is defined over $F((q^{1/d}))$ for some $d|N$.

Definition 2.2.3. An algebraic modular form f of weight k for $\Gamma_0(N)$ defined over F is a weakly holomorphic one such that $f(\mathrm{Tate}(q), T_N, du/u) \in F[[q^{1/d}]]$.

We can view algebraic modular forms as sections of line bundles in the following way. If $N \geq 3$, the modular curve $Y_0(N)$ is a moduli space: for any $\mathbf{Z}[1/N]$-algebra R, the points $Y_0(N)(R)$ can be identified with the set of isomorphism classes of elliptic curves with $\Gamma_0(N)$-level structure over R. Let $\mathcal{E}$ be the universal elliptic curve with $\Gamma_0(N)$-level structure and $\pi : \mathcal{E} \to Y_0(N)$. Let $\underline{\omega} := \pi_* \Omega^1_{\mathcal{E}/Y_0(N)}$ be the sheaf of relative differentials. Then if g is a weakly holomorphic modular form of weight k for $\Gamma_0(N)$, we can view g as a global section of $\underline{\omega}$ by $g(E, C_N) = g(E, C_N, \omega)\omega^k$ where ω is chosen to be a generator of $\Omega^1_{E/R}$. Furthermore, $\underline{\omega}$ admits an extension to a line bundle on $X_0(N)$, which we will also denote by $\underline{\omega}$, and this line bundle is characterized by the property that the global sections $H^0(X_0(N), \underline{\omega}^k)$ are exactly the space of weight k modular forms for $\Gamma_0(N)$.

We now specialize to modular curves over the complex numbers. Working over $\mathbf{C}$, $X_0(N)(\mathbf{C})$ is a compact Riemann surface and the map $\mathcal{H} \to \Gamma_0(N)\backslash\mathcal{H}$ sending

$$\tau \mapsto (\mathbf{C}/(\mathbf{Z} + \tau\mathbf{Z}), 1/N) \tag{2.1}$$

identifies $Y_0(N)(\mathbf{C})$ with $\Gamma_0(N)\backslash\mathcal{H}$, where we identify $1/N$ with the cyclic subgroup it generates by abuse of notation.

Definition 2.2.4. If g is a weakly holomorphic modular form of weight k it gives a holomorphic section of the sheaf $\underline{\omega}^k$ (viewed now as an analytic sheaf on the Riemann surface $X_0(N)(\mathbf{C})$) and gives rise to a holomorphic function on $\mathcal{H}$ by the definition

$$g(\tau) := g(\mathbf{C}/(\mathbf{Z} + \tau\mathbf{Z}), 1/N, 2\pi i z) \tag{2.2}$$

where z is the usual coordinate on $\mathbf{C}/(\mathbf{Z}+\tau\mathbf{Z})$.

This satisfies the familiar property

$$g\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k g(\tau) \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \tag{2.3}$$

Let $S_2(\Gamma_0(N))$ denote the weight 2 modular forms for $\Gamma_0(N)$. For $g \in S_2(\Gamma_0(N))$, and $\gamma \in \Gamma_0(N)$ by (2.3) a simple calculation shows

$$f(\gamma(z))d(\gamma(z)) = f(z)dz.$$

Write $q = e^{2\pi i z}$. Since $d\log q = dq/q$, we can identify differential forms on $\mathcal{H}/\Gamma_0(N)$ with $S_2(\Gamma_0(N))dq/q$. Under pullback by $\mathcal{H}/\Gamma_0(N) \to Y_1(N) \hookrightarrow X_0(N)$ the differential forms $H^0(X_0(N), \Omega^1)$ can be identified with $S_2(\Gamma_0(N))dq/q$.

Recall that $X_0(N)$ is a smooth projective curve that is the compactification of $Y_0(N)$ by finitely many cusps. In particular, we call ∞ the rational cusp on $X_0(N)$ given by the limit as $t \to +\infty$ of it. Let $J_0(N)$ be the Jacobian $\mathrm{Pic}^0(X_0(N))$. We embed $X_0(N) \to J_0(N)$ sending $P \mapsto [P-\infty]$. Under pullback, we may identify $H^0(J_0(N), \Omega^1)$ with $H^0(X_0(N), \Omega^1)$.

We now define degeneracy maps and their corresponding sub- and quotient varieties. For every triple (d, M, N) such that $d|(N/M)$. Then $d \mapsto d \cdot z$ induces a degeneracy operator $X_0(M) \to X_0(N)$. This operator therefore induces maps $S_2(M) \to S_2(N)$ and $J_0(M) \to J_0(N)$. We can interpret this operator on pairs (E, C_N) of elliptic curves with cyclic subgroup C_N in the following way. Let $C_d \subset C_N$ be the unique cyclic subgroup of order d. Then $(E/C_d, C_N/C_d)$ is the image on $X_0(M)$ of (E, C_N) under the degeneracy operator given by (d, M, N).

Definition 2.2.5. Denote by $J_0(N)_{\text{old}}$ of $J_0(N)$ to be the abelian subvariety (defined over $\mathbf{Q}$) that is generated by the images of the morphisms $J_0(M) \to J_0(N)$ as we range over all triples (d, M, N) such that $M|N$, $M \neq N$, and $d|(N/M)$.

We define $J_0(N)^{\text{new}}$ to be the quotient $J_0(N)/J_0(N)_{\text{old}}$.

Definition 2.2.6. Similarly we define $S(\Gamma_0(N))_{\text{old}}$ to be the images of all the degeneracy maps $S(\Gamma_0(M)) \to S(\Gamma_0(N))$ as we range over all triples (d, M, N) such that $M|N$, $M \neq N$, and $d|(N/M)$.

We denote $S(\Gamma_0(N))_{\text{new}}$ to be the orthogonal complement of $S(\Gamma_0(N))_{\text{old}}$ under the Petersson inner product.

Let T_m denote the Hecke operators on $J_0(N)$ for $m \geq 1$. The Hecke algebra $\mathbf{T}$ is the ring of endomorphisms of $J_0(N)$ generated by the T_n. There is a unique basis of $S(\Gamma_0(N))_{\text{new}}$ that is a normalized eigenform for all the Hecke operators T_m [Li75, p.294].

Definition 2.2.7. We define New_N to consist of this basis

$$\text{New}_N := \left\{ g(q) = \sum_{n \geq 1} a_n(g) q^n \in S(\Gamma_0(N))_{\text{new}} : a_1 = 1 \text{ and } T_m g = a_m g \right\}.$$

A newform of level N is an element of New_N.

The field of definition of the Fourier coefficients of a newform g is a number field $E_g := \mathbf{Q}(a_2, a_3, \dots)$. Shimura [Shi73, Theorem 1] associated to every newform $g \in \text{New}_N$ an abelian variety quotient A_g of $J_0(N)$ of dimension $[E_g : \mathbf{Q}]$ defined over $\mathbf{Q}$ in the following way. Let I_g be the kernel of the homomorphism $\mathbf{T} \to \mathbf{Z}[a_1, a_2, \dots]$ sending $T_n \mapsto a_n$. Then

$$A_g := J_0(N)/I_g J_0(N).$$

Ribet showed that A_g is $\mathbf{Q}$-simple [Rib80].

Then $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on New_N by acting on the Fourier coefficients of the newforms. The groups the newforms into Galois orbits of newforms, which we refer to as newform orbits. Shimura's association $g \mapsto A_g$ is injective on these newform orbits.

Theorem 2.2.8 ([BGJGP05, Proposition 3.2]). *Let $g \in \mathrm{New}_N$ and $g' \in \mathrm{New}_{N'}$. Then A_g is isogenous to $A_{g'}$ over $\mathbf{Q}$ if and only if $N = N'$ and $g = g^\sigma$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.*

Combining the two previous results, we have an isogeny decomposition over $\mathbf{Q}$

$$J_0(N)^{\mathrm{new}} \sim_{\mathbf{Q}} \bigoplus_{g \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\backslash \mathrm{New}_N} A_g. \tag{2.4}$$

Let $g \in \mathrm{New}_N$. Then we have an equality of L-functions

$$L(A_g, s) = \prod_{i=1}^{[E_g:\mathbf{Q}]} L(g^\sigma, s) \text{ for } \sigma \in \mathrm{Gal}(E_g/\mathbf{Q}).$$

The Gross–Zagier–Kolyvagin–Logachev Theorem (see [DLF21, Appendix] for a proof) gives a result about the rank of a modular abelian variety given the analytic rank.

Theorem 2.2.9 (Gross–Zagier–Kolyvagin–Logachev). *Let $g \in \mathrm{New}_N$.*

If $\mathrm{ord}_{s=1}(L(g^\sigma, s)) = 0$ for some $\sigma \in \mathrm{Gal}(E_g/\mathbf{Q})$, then $\mathrm{ord}_{s=1}(L(g^\sigma, s)) = 0$ for all σ, and $\mathrm{rank}\, A_g(\mathbf{Q}) = 0$.

If $\mathrm{ord}_{s=1}(L(g^\sigma, s)) = 1$ for some $\sigma \in \mathrm{Gal}(E_g/\mathbf{Q})$, then $\mathrm{ord}_{s=1}(L(g^\sigma, s)) = 1$ for all σ and $\mathrm{rank}\, A_g(\mathbf{Q}) = [E_g : \mathbf{Q}] = \dim(A_g)$.

Since it can be difficult to verify $\mathrm{rank}\, A_g(\mathbf{Q})$ but easier to compute the order of vanishing of the L-function, we rely on this result throughout to compute the rank of the abelian varieties we consider.

Let g be a newform and write $\pi : J_0(N) \to A_g$. Then by [DLF21, (42)] there is an isomorphism $[\cdot] : E_g \to \mathrm{End}^0(A_g)$ such that for all primes ℓ coprime to N, $[a_\ell(g)] \in \mathrm{End}^0(A_g)$ and $[a_\ell(g)] \circ \pi = \pi \circ T_\ell$. We can therefore consider $\mathrm{End}^0(A_g)$ as an order inside E_g; we denote this order by $\mathcal{O}_g$. Then A_g has the structure of an $\mathcal{O}_g$-module.

In practice, aside from the special case of elliptic curves, we will work with Jacobians J_g of Atkin–Lehner quotients of $X_0(N)$ that arise as simple quotients of $J_0(N)^{\mathrm{new}}$

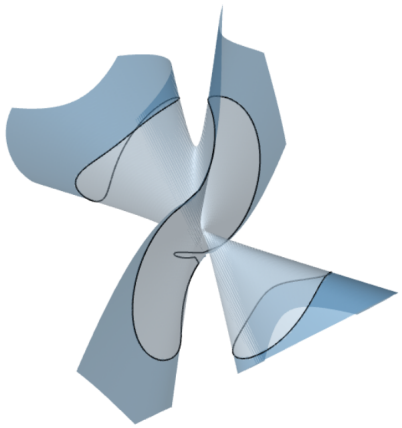

Figure 2.1: The real points of the regular model $y^2 + (x^3 + x + 1)y = (x^5 - x)$ of $X_0(67)^+$

instead of A_g. The variety J_g is isogenous to A_g, but the quotient map $\pi : J_0(N) \to J_g$ is easier to describe (in particular, we are able to compute heights on the quotient J_g, see Proposition 4.0.4). We define the Atkin–Lehner involutions of $S_2(\Gamma_0(N))$.

Definition 2.2.10. Let $Q|N$ be a positive divisor of N. There exist integers $x, y, z, t \in \mathbf{Z}$ such that the matrix

$$\begin{pmatrix} Qx & y \\ Nz & Qt \end{pmatrix}$$

has determinant Q. Then W_Q normalizes $\Gamma_0(N)$ and induces an operator w_Q on $S_2(\Gamma_0(N))$, called the Atkin–Lehner operator, that commutes with all the Hecke operators T_p for $p \nmid N$. Furthermore, $w_Q^2 = 1$. The Atkin–Lehner involution w_N is called the Fricke involution.

If $f \in S_2(\Gamma_0(N))$ is an eigenform for all T_p for $p \nmid N$, then it is an eigenform for w_Q, and so we can discuss its Atkin–Lehner sign or Fricke sign to be this eigenvalue.

Suppose $X = X_0(N)/\langle w_{n_1}, \ldots, w_{n_m} \rangle$ is the quotient of $X_0(N)$ by a group of Atkin–Lehner involutions $w_{n_1}, \ldots, w_{n_m}$, and let J_f be the Jacobian of X. Then

$$H^0(J_f, \Omega^1) = \{g \in S_2(\Gamma_0(N)) : g|_{w_{n_i}} = g, i = 1, \ldots, m\}.$$

If $\phi : X_0(N) \to X$ induces a map on differential forms that satisfies the inclusion

$$\phi^* H^0(J_f, \Omega^1) \subseteq S_2(\Gamma_0(N))_{\text{new}}$$

then J_f is a quotient of $J_0(N)^{\text{new}}$, isogenous to A_f for some newform f, and satisfies (†). This explains the label f on J_f. We denote by $\pi : J_0(N) \to J_f$ the map induced by the pushforward ϕ_* of the quotient map on $X_0(N)$.

We denote the Atkin–Lehner quotient $X_0(N)/\langle w_N \rangle$ by $X_0(N)^+$ and the quotient $X_0(N)$ modulo the full group of Atkin–Lehner involutions by $X_0^*(N)$.

2.2.2 Heegner points

We now introduce definitions and notation for Heegner points and discuss relevant background. More details on Heegner points and references for this section can be found in [Gro84, GZ86, GKZ87].

Let K be an imaginary quadratic field of class number one. Let N be a positive integer.

Definition 2.2.11. The Heegner hypothesis for K and N is the assumption that every prime $q|N$ splits in K

If N satisfies the Heegner hypothesis then we can write $(N) = \mathfrak{n}\overline{\mathfrak{n}}$ in $\mathcal{O}_K$. Write $\mathfrak{n} = \mathbf{Z}N + \mathbf{Z}\frac{b+\sqrt{D}}{2}$ for some $b \in \mathbf{Z}$. Then under the map (2.1), the point

$$\tau_{\mathfrak{n}} := \frac{b + \sqrt{D}}{2N} \tag{2.5}$$

corresponds to the elliptic curve with $\Gamma_0(N)$-level structure $(\mathbf{C}/\overline{\mathfrak{n}}^{-1}, 1/N)$. Then since $\mathfrak{n}$ is a fractional ideal of $\mathcal{O}_K$, we can see that $\mathbf{C}/\overline{\mathfrak{n}}^{-1}$ is an elliptic curve with CM by $\mathcal{O}_K$ and hence has a model A defined over $\mathcal{O}_K$. (The cyclic subgroup generated by $1/N$, corresponding to $A[\mathfrak{n}]$, will also be defined over $\mathcal{O}_K$, while the generator $1/N$ is only defined over the ray class field of conductor $\mathfrak{n}$.)

Definition 2.2.12. We define the Heegner point to be the point $P_K := (A, A[\mathfrak{n}]) \in X_0(N)(K)$.

We now discuss the choice of a differential form for A in order to evaluate modular forms at the Heegner point. Let A be an elliptic curve defined over $\mathcal{O}_K$ with complex lattice $\mathbf{C}/\overline{\mathfrak{n}}^{-1}$, and choose ω_A a Néron differential on A. Then the period lattice of ω_A is $\Omega_K \cdot \mathcal{O}_K \subset \mathbf{C}$. Then for any modular form g of weight k for $\Gamma_0(N)$ we have

$$g(A, A[\mathfrak{n}], \omega_A) = g(\mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau_{\mathfrak{n}}), 1/N, \Omega_K \overline{\alpha} dz) = \frac{g(\tau_{\mathfrak{n}})}{(\overline{\alpha}\Omega_K)^k} \tag{2.6}$$

where $\overline{\alpha}$ is a generator of $\overline{\mathfrak{n}}$. Let Ω_A be $1/(2\pi i)$ times the real period of A. By [BDP17, p.25] these are related by $\Omega_K = \Omega_A/\sqrt{D}$.

Example 2.2.13. Let $N = 89$ and $K = \mathbf{Q}(\sqrt{-11})$. Then $\tau_{\mathfrak{n}} = \frac{-73+\sqrt{-11}}{178}$ the point which, under (2.1), maps to an elliptic curve $(\mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau_{\mathfrak{n}}), 1/N)$ with $\Gamma_0(N)$-level structure on $X_0(N)$. Write $\Lambda := (\mathbf{Z} + \mathbf{Z}\tau)$. The complex curve associated to $\tau_{\mathfrak{n}}$ has the Weierstrass equation

$$y^2 = 4x^3 - g_2(\Lambda) - g_3(\Lambda).$$

We will re-scale, following [Sta96, Section 2], to find a model A defined over $\mathbf{Q}$ (with the N-isogeny defined over $\mathcal{O}_K$). It will be convenient to first move $\tau_{\mathfrak{n}}$ by an element of $\Gamma_0(N)$. Let

$$G_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then $\tau' := G_0(\tau) = \frac{105+\sqrt{-11}}{178}$. Consider the equation

$$y^2 = 4x^3 - (-11)\frac{E_4(\tau')}{12\eta(\tau')^8} + (-11)\sqrt{-11}\frac{E_6(\tau')}{216\eta(\tau')^{12}}. \tag{2.7}$$

This is a re-scaling of the above Weierstrass equation for $\mathbf{C}/\Lambda$ so has CM by $\mathcal{O}_K$, but is defined over $\mathbf{Q}$ (and the N-isogeny is defined over $\mathcal{O}_K$). In fact it is the curve

$$y^2 = x^3 - \frac{22}{3}x - \frac{847}{108},$$

which is isomorphic to

$$A : y^2 = x^3 + x^2 - 117x - 541.$$

Then $\Omega_A = 0.72399225501256909123536415 \cdot \frac{1}{2\pi i}$.

Remark 2.2.14. Note that Ω_A does not depend on the choice of N, only on the discriminant D of K. Define the Chowla–Selberg period

$$\Omega_{\mathrm{CS},D} := \left(\sqrt{\pi} \prod_{a=1}^{|D|-1} \Gamma\left(\frac{a}{|D|}\right)^{\varepsilon(a)} \right)^{1/2}. \tag{2.8}$$

Gross [Gro78] shows that the real period $\Omega_A \cdot (2\pi i)$ is equal to $\Omega_{\mathrm{CS},D}$ up to an algebraic integer.

Example 2.2.15. In the example above, where $D = -11$ we have

$$\Omega_{\mathrm{CS},D} = 6.184341053563215130336290612 79$$

and we see numerically that

$$\Omega_{\mathrm{CS},D}/(\Omega_A \cdot 2\pi i) = \sqrt[4]{2^2 \cdot 11^3}.$$

Definition 2.2.16. The point P_K gives rise to a divisor class $y_K := [P_K - \infty] \in J_0(N)(K)$ which we refer to as the Heegner cycle.

Remark 2.2.17. This terminology is not standard, and does not agree with the terminology of [BDP13], where they use cycle to mean the point on $X_0(N)$. However, in this thesis we would like to distinguish between $P_K \in X_0(N)(K)$ and $y_K \in J_0(N)(K)$.

Consider the vector space $V = J_0(N)(K) \otimes \overline{\mathbf{Q}}$. The height pairing gives an inner product on V for which the Hecke operators are self-adjoint: the adjoint of an endomorphism of an abelian variety with respect to the height pairing is the Rosati involution by [MT83, (3.4.3)] c.f. Proposition 4.0.3. Since the Hecke algebra on $X_0(N)$ is a product of totally real fields, the Rosati involution (which is totally positive) is forced to be the identity.

By the spectral theorem, the fact that the Hecke operators are self-adjoint for the height pairing yields a decomposition

$$V = \bigoplus_f V^f \tag{2.9}$$

into eigenspaces, summing over all Hecke eigenforms f of weight 2 and level N (not up to Galois conjugacy).

Definition 2.2.18. Let $f \in \mathrm{New}_N$ and $\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})$. We denote by y_{K,f^σ} the f^σ-isotypical component of y_K, with $y_{K,f^\sigma} \in V^{f^\sigma} \subset J_0(N)(K) \otimes E_f$.

Then by breaking y_K into its components, we can write

$$y_K = \sum_{f \in \mathrm{New}_N} \sum_{\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})} y_{K,f^\sigma}.$$

Because distinct eigenvectors are orthogonal

$$\langle y_{K,f^\sigma}, y_{K,f^\tau} \rangle = 0$$

whenever $\sigma \neq \tau$.

Let $f \in \mathrm{New}_N$. The Gross–Zagier formula [GZ86, Theorem I.6.3] says

$$L'(f,1)L(f^\varepsilon,1) = h_{\mathrm{NT}}(y_{K,f})$$

where h_{NT} denotes the real valued canonical height on $J_0(N)$.

A theorem of Waldspurger then guarantees infinitely many K such that $L(f^\varepsilon,1) \neq 0$ by relating the value $L(f^\varepsilon,1)$ to the $|D|$th Fourier coefficient of another modular form of weight $3/2$ obtained via the Shimura correspondence. We do not know an explicit way to construct a suitable K a priori (or equivalently compute the Shimura correspondence); instead we choose some K, and if $y_{K,f}$ is torsion, we can try again with another choice of K.

The Fricke involution w_N on $X_0(N)$ induces an involution on $S_2(\Gamma_0(N))$. In weight 2, the sign of the functional equation of $L(f,s)$ is the opposite of the sign of the Fricke involution. Since f has analytic rank 1, $L'(f,1) \neq 0$ only if the Fricke sign is 1. Thus we restrict our attention to the case of Fricke sign 1.

The action of complex conjugation on $\pi(y_K)$ is given by

$$\pi(w_N(P_K) - \infty)$$

therefore $\pi(y_K) \in J_f(\mathbf{Q})$ [Gro84, (5.2)]. Finally, the action of the Hecke algebra on the Heegner cycle $\mathcal{O}_f\pi(y_K)$ generates a finite index subgroup of $J_f(\mathbf{Q})$ [DLF21, 7 Appendix].

2.2.3 Labels for modular forms

We will often denote (Galois orbits of) newforms by labels. These labels are LMFDB labels [LMF22]. For example, there is a 2-dimensional space of newforms of level 67 and weight 2 with Atkin–Lehner sign +1 that has LMFDB label `67.2.a.b`. The label comprises (in order) the level, weight, and then the letter a to indicate trivial character. The final letter gives a unique label to the newform orbit itself; this is given according to lexicographical order based on the trace form.

Where appropriate, we will also reference curves with LMFDB labels. All of the labels in this thesis are LMFDB labels.

2.3 $\mathbf{Z}_p^d$-extensions

Let $p > 2$ be a prime number. For any field, and $d \geq 1$, we can consider its $\mathbf{Z}_p^d$-extensions. For example, $\mathbf{Q}$ has one $\mathbf{Z}_p$-extension, the cyclotomic extension, which we briefly describe now. Let p be a prime number and let ζ_{p^n} be a primitive p^nth root of

unity. Then $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \simeq (\mathbf{Z}/p\mathbf{Z})^\times$ and

$$\mathbf{Q}(\zeta_\infty) := \bigcup_{n=0}^{\infty} \mathbf{Q}(\zeta_{p^n})$$

has Galois group

$$\begin{aligned}\mathrm{Gal}(\mathbf{Q}(\zeta_\infty)/\mathbf{Q}) =& \varprojlim \mathrm{Gal}(\mathbf{Q}(\zeta_p^n)/\mathbf{Q}) \simeq \varprojlim (\mathbf{Z}/p^n\mathbf{Z})^\times \\ =& \mathbf{Z}_p^\times \simeq \mu_{p-1} \times (1 + p\mathbf{Z}_p),\end{aligned}$$

where μ_{p-1} is a cyclic group of order $p-1$. Then the cyclotomic $\mathbf{Z}_p$-extension is $\mathbf{Q}_\infty := \mathbf{Q}(\zeta_\infty)^{\mu_{p-1}}$, and we write $\Gamma_{\mathbf{Q}} := \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$.

When K is an imaginary quadratic field and $d = 1$ there are two $\mathbf{Z}_p$-extensions, the cyclotomic extension K_∞^{cyc} and the anticyclotomic extension K_∞^{ac}. The extension K_∞^{cyc} is the compositum of K and $\mathbf{Q}_\infty$. There is a unique $\mathbf{Z}_p^2$-extension K_∞/K. Each of these extensions $K_\infty/K, K_\infty^{\mathrm{cyc}}/K$, and K_∞^{ac}/K is a pro-finite extension and we denote the respective Galois groups as Γ_K, Γ_K^+ and Γ_K^-. Then we can decompose $\Gamma_K = \Gamma_K^+ \times \Gamma_K^-$ by studying the action of complex conjugation $c \in \Gamma_K$, i.e. $c^{-1}gc = g^{\pm 1}$ for all $g \in \Gamma_K^\pm$.

Let $\Gamma = \Gamma_K, \Gamma_K^+$ or Γ_K^-. The Iwasawa module attached to the extension is the completed group ring $\Lambda = \mathbf{Z}_p[[\Gamma]]$, this is a $(d+1)$-dimensional regular complete local ring. By choosing topological generators $\gamma_1, \ldots, \gamma_d$ for Γ, we can write

$$\mathbf{Z}_p[[\Gamma]] \simeq \mathbf{Z}_p[[T_1, \ldots, T_d]].$$

When the field K is understood, we omit the subscript K.

2.4 Hecke characters

We explain Hecke characters and their varied appearances in this section. For this section we fix embeddings $\iota_p : \overline{\mathbf{Q}} \hookrightarrow \mathbf{C}_p$ and $\iota_\infty : \overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$. Recall that K is still an

imaginary quadratic field.

Let $\mathfrak{c}$ be an integral ideal of K. Let $I_{\mathfrak{c}}$ denote the group of fractional ideals of K prime to $\mathfrak{c}$. Let $J_{\mathfrak{c}}$ be the set of ideals in K satisfying

$$J_{\mathfrak{c}} = \{(\alpha) : \text{ for all prime ideals } \mathfrak{q}|\mathfrak{c}, v_{\mathfrak{q}}(\alpha - 1) \geq \mathrm{ord}_{\mathfrak{q}}(\mathfrak{c})\} \subset I_{\mathfrak{c}}.$$

Definition 2.4.1. Let $(n_1, n_2) \in \mathbf{Z}^2$. An algebraic Hecke character of infinity type (n_1, n_2) and conductor dividing $\mathfrak{c}$ is a homomorphism

$$\chi : I_{\mathfrak{c}} \to \mathbf{C}^{\times}$$

such that

$$\chi((\alpha)) = \alpha^{n_1}\overline{\alpha}^{n_2}, \quad \text{for all } \alpha \in J_{\mathfrak{c}}.$$

It is possible that χ can be extended to some Hecke character of conductor dividing $\mathfrak{c}'$; the smallest such integral ideal $\mathfrak{c}'$ is the conductor of χ.

Example 2.4.2. Let $\mathfrak{q}$ be an $\mathcal{O}_K$-ideal. The norm character $\mathbf{N}_K$ sending $\mathfrak{q} \mapsto \#(\mathcal{O}_K/\mathfrak{q})$ has infinity type $(1, 1)$ and conductor $\mathcal{O}_K$.

We can associate to a Hecke character an idèle class character $\chi : \mathbf{A}_K^{\times}/K^{\times} \to \mathbf{C}^{\times}$ such that $\chi_{\infty}(z) = z^{-n_1}\bar{z}^{-n_2}$, where χ_{∞} denotes the component of χ at $(K \otimes \mathbf{R})^{\times}$. The map $(K \otimes \mathbf{R})^{\times} \to \mathbf{C}^{\times}$ is constructed using the embedding ι_{∞}.

Remark 2.4.3. The reader is warned that the sign convention used here for the infinity type is the negative of the convention in many other papers. This is the sign convention that agrees with [BDP13].

Algebraic Hecke characters are in bijection with algebraic p-adic Hecke characters, as we now describe. Let $p = \mathfrak{p}\overline{\mathfrak{p}}$ be a prime that splits in K. A p-adic Hecke character is a continuous homomorphism $\chi_{\mathbf{Q}_p} : \mathbf{A}_K^{\times}/K^{\times} \to \overline{\mathbf{Q}}_p^{\times}$. It is algebraic if there are integers n_1 and n_2 such that the local factors $\chi_{\mathfrak{p}}$ on $K_{\mathfrak{p}}^{\times} \simeq \mathbf{Q}_p^{\times}$ and $\chi_{\bar{\mathfrak{p}}}$ on $K_{\bar{\mathfrak{p}}}^{\times}$ on $\mathbf{Q}_p^{\times}$ are of the form $\chi_{\mathfrak{p}}(z) = z^{-n_1}$ and $\chi_{\bar{\mathfrak{p}}}(z) = z^{-n_2}$. Then $\chi_{\mathbf{C}}$ an algebraic Hecke character of

infinity type (n_1, n_2) corresponds to the p-adic Hecke character $\chi_{\mathbf{Q}_p}$ via the formula

$$\chi_{\mathbf{Q}_p}(z) = \iota_p \circ \iota_\infty^{-1}(\chi_{\mathbf{C}}(z) z_\infty^{n_1} \bar{z}_\infty^{n_2}) z_{\mathfrak{p}}^{-n_1} z_{\bar{\mathfrak{p}}}^{-n_2}$$

for an idèle $z = (z_v)$.

Now $\overline{\mathbf{Q}}_p^\times$ is a totally disconnected topological group, so the kernel of χ contains the connected component of the identity. The global Artin map $\mathbf{A}_K^\times / K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is surjective and its kernel is the connected component of the identity: therefore if $\chi_{\mathbf{Q}_p}$ is algebraic, then $\chi_{\mathbf{Q}_p}$ factors through $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. We call this the associated p-adic Galois representation

$$\chi_G : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \overline{\mathbf{Q}}_p^\times.$$

It relates to the original Hecke character by the equation

$$\chi_G(\mathrm{Frob}_{\mathfrak{q}}) = \chi(\mathfrak{q})$$

for any prime ideal $\mathfrak{q}$ of K not dividing $\mathfrak{c}'p$. Conversely, given any v-adic Galois representation $\mathrm{Gal}(K^{\mathrm{ab}}/K) \to \overline{\mathbf{Q}}_p^\times$ we can obtain an idèle class character $\mathbf{A}_K^\times / K^\times \to \overline{\mathbf{Q}}_p^\times$ by precomposing with the Artin map.

Chapter 3

The special value of the anticyclotomic p-adic L-function

In this chapter, we explain how to compute the special value of the p-adic Rankin L-series $L_p(f,1)$ introduced by Bertolini, Darmon, and Prasanna [BDP13] attached to the newform $f \in S_2(\Gamma_0(N))$ and the imaginary quadratic field K satisfying the hypotheses below. This value occurs at norm the character $\mathbf{N}$ with infinity type $(1,1)$. Since the norm character $\mathbf{N}$ lies outside of the range of interpolation for L_p, this value is not readily accessible. We follow a method of Rubin [Rub81] for evaluating the Katz 2-variable p-adic L-function outside the range of interpolation. Our method requires us to first evaluate the p-adic L-function at certain characters in the range of interpolation. In the case of the p-adic Rankin L-series of Bertolini, Darmon, and Prasanna, if χ is a character in the range of interpolation, then the value $L_p(f)$ at χ is shown to be an explicit multiple of the central value of the Rankin L-series $L(f,\chi,1)$ as in (3.2). An explicit Waldspurger's formula (Theorem 3.1.7) relates the central L-values $L(f,\chi,1)$ to the square of the Shimura–Maass derivative of f at the Heegner point. By considering p-adic characters in the "anticyclotomic" direction, Bertolini, Darmon, and Prasanna obtain the special value formula, relating the square of the logarithm of the Heegner cycle to $L_p(f,1)$. We will refer to $L_p(f,1)$ as the anticyclotomic p-adic L-function.

The chapter is divided into two sections. The first section is devoted to explaining how to compute the values of $L_p(f)$ in the range of interpolation. The strategy here

is to compute the Shimura–Maass derivatives at f evaluated at the Heegner point. The second section develops the computation of the special value $L_p(f,1)$ following Rubin's method. The key proposition is Proposition 3.2.1, which relates the value $L_p(f,1)$ to values inside the range of interpolation.

Let f be a newform in $S_2(\Gamma_0(N))$ with coefficient field E_f. We start by collecting some running assumptions that will be used for the remainder of the chapter. Let $p > 2$ be a prime, and assume that

$$p \text{ splits in } E_f \tag{H1}$$

and fix an embedding $e : E_f \to \mathbf{Q}_p$. This is a simplifying assumption to avoid working in extensions of $\mathbf{Q}_p$ for our computations. Assume also

$$f \text{ is of analytic rank 1;} \tag{H2}$$

$$K = \mathbf{Q}(\sqrt{D}) \text{ is an imaginary quadratic field of class number 1 with odd discriminant } D < -3; \tag{H3}$$

The class number 1 and $D < -3$ assumptions are simplifying assumptions. Assume also the Heegner hypothesis, that

$$\text{every prime } q \text{ dividing } N \text{ splits in } K. \tag{H4}$$

This ensures the existence of the Heegner cycle $y_K := [P_K - \infty] \in J_0(N)(K)$. Furthermore, we require

$$(p) = \mathfrak{p}\overline{\mathfrak{p}} \text{ splits in } K. \tag{H5}$$

This is required for the construction of the p-adic L-function.

Now, we are ready to state the main theorem of [BDP13, Main Theorem]: they show that

$$L_p(f,1) = \left(\frac{1 - a_p(f) + p}{p}\right)^2 \log_{fdq/q}(y_K)^2, \tag{3.1}$$

where $\log_{fdq/q}$ denotes the logarithm on $J_0(N)$ and $L_p(f,1)$ denotes the value of $L_p(f)$ at the character $\mathbf{N}$ (see Remark 3.1.2 for an explanation regarding this notation). Our goal in this chapter is to provide a method for computing $L_p(f,1)$.

Remark 3.0.1. The logarithm on a quotient A of $J_0(N)$ can be compared to the logarithm on $J_0(N)$ via the quotient map $\pi : J_0(N) \to A$, which induces an inclusion $\pi^* : H^0(A,\Omega^1) \hookrightarrow H^0(J_0(N),\Omega^1)$.

When $\pi_E : X_0(N) \to E$ is the modular parametrization of E, then $\pi : J_0(N) \to E$ is induced by pushforward of π_E. Then there exists $\omega \in H^0(E,\Omega^1)$ such that $\pi^*\omega = f(q)dq/q$. Then by change of variables (see Theorem 1.4.5), for any $D \in J_0(N)(\overline{\mathbf{Q}}_p)$, we have $\log_\omega \pi(D) = \log_{\pi^*\omega} D = \log_{fdq/q}(D)$.

In the case where J_f is the Jacobian of the quotient of $X_0(N)$ by a group of Atkin–Lehner involutions $w_{n_1},\dots,w_{n_m}$ and $\pi : J_0(N) \to J_f$ is induced by the pushforward of the quotient map $X_0(N) \to X_0(N)/\langle w_{n_1},\dots,w_{n_m}\rangle$ then $H^0(J_f,\Omega^1) = \{g \in S_2(\Gamma_0(N)) : g|_{w_{n_i}} = g, i = 1,\dots,m\}$ and $\pi^* g = g$. Then for any $D \in J_0(N)(\overline{\mathbf{Q}}_p)$ we have $\log_{fdq/q} \pi(D) = \log_{\pi^* fdq/q} D$.

Finally, the following slightly more general case is important, but we do not study it in detail in this thesis. Let I_f be the kernel of the homomorphism $\mathbf{T} \to \mathbf{Z}[a_1,a_2,\dots]$ sending $T_n \mapsto a_n$. Let A_f be the optimal quotient attached to f by Shimura [Shi73, Theorem 1] with quotient map $\pi : J_0(N) \to A_f$. Then $H^0(A_f,\Omega^1) \simeq H^0(J_0(N),\Omega^1)[I_f]$ and this space of differentials also corresponds to the submodule of $S_2(\Gamma_0(N))_{\mathbf{Q}}[I_f]$ of weight 2 cuspforms with rational Fourier coefficients that is annihilated by I_f. Then $f \in S_2(\Gamma_0(N))_{\mathbf{Q}}[I_f]$ and so we could consider the logarithm $\log_{fdq/q}$ as a logarithm on A_f.

We start by recalling the interpolation property of the p-adic L-function L_p in [BDP13] associated to f. The interpolation property will provide enough information to work with the p-adic L-function for our purposes; for more details on the construction of the anticyclotomic p-adic L-function see the main reference [BDP13] or [BCD+14] for an expository article. Recall that K_∞^{ac}/K is the anticyclotomic $\mathbf{Z}_p$-extension of K, and $\Gamma^- := \mathrm{Gal}(K_\infty^{\mathrm{ac}}/K)$ denotes its Galois group. Write $\hat{\mathcal{O}}$ for the completion of the ring of integers of the maximal unramified extension of $\mathbf{Q}_p$ and define $\Lambda^{\mathrm{ac}} := \mathbf{Z}_p[[\Gamma^-]]\hat{\otimes}_{\mathbf{Z}_p}\hat{\mathcal{O}}$.

Let $S \subset \mathrm{Hom}_{\mathrm{cts}}(\Gamma^-,\overline{\mathbf{Q}}_p^\times)$ be the subset of Galois characters associated to Hecke

characters of K with infinity type $(1+r, 1-r)$ for some integer $r \geq 1$. Bertolini, Darmon, and Prasanna prove that there exists $L_p(f) \in \Lambda^{\mathrm{ac}}$ interpolating an algebraic L-value $L_{\mathrm{alg}}(f, \chi^{-1}, 0)$ for $\chi \in S$. Each $\chi \in S$ determines a map $\Lambda^{\mathrm{ac}} \to \widehat{\overline{\mathbf{Q}}}_p$ by $\hat{\mathcal{O}}$-linear extension. The interpolation property [BDP13, (5.2.3)] for $L_p(f)$ says that for all $\chi \in S$ and Ω_p a p-adic period associated to the Heegner cycle defined in [BDP13, (5.2.2)], we have

$$\chi(L_p(f))/\Omega_p^{2(2+2r)} = (1 - \chi^{-1}(\overline{\mathfrak{p}})a_p + \chi^{-2}(\overline{\mathfrak{p}})p)^2 L_{\mathrm{alg}}(f, \chi^{-1}, 0). \tag{3.2}$$

The left hand side of (3.2) is our notation for evaluating the p-adic L-function $L_p(f)$ at χ for χ in the range of interpolation. The norm character $\mathbf{N}$ (with infinity type $(1,1)$) is not in S, so we cannot use (3.2) to evaluate "$\mathbf{N}(L_p(f))$". However, for $\chi \in S$, we can evaluate $\chi(L_p(f))$, which we will now explain.

3.1 Evaluating inside the range of interpolation

We first say a few words about the definition of the L-series $L(f, \chi^{-1}, s)$ as a Rankin product; this definition will not be used in the rest of the chapter but is provided to show the parallels with the Gross–Zagier story and with Perrin-Riou's p-adic L-function as well as to orient the reader. The L-series $L(f, \chi^{-1}, s)$ can be written explicitly (in some right half plane of $\mathbf{C}$) as

$$L(f, \chi^{-1}, s) = \sum_{n \geq 1} \left(\sum_{\mathbf{N}(\mathfrak{a}) = n} \chi^{-1}(\mathfrak{a}) \right) n^{-s} \tag{3.3}$$

where the sum is taken over ideals $\mathfrak{a}$ of norm N in K. We use χ^{-1} rather than χ in this chapter to agree with the convention used in [BDP13]. This can be expressed as

an Euler product, over prime ideals $\mathfrak{q}$ of K,

$$L(f,\chi^{-1},s)=\prod_{\mathfrak{q}}[(1-\alpha_{\mathbf{N}\mathfrak{q}}(f)\chi^{-1}(\mathfrak{q})\mathbf{N}\mathfrak{q}^{-s})(1-\beta_{\mathbf{N}\mathfrak{q}}(f)\chi^{-1}(\mathfrak{q})\mathbf{N}\mathfrak{q}^{-s})]^{-1} \tag{3.4}$$

where $\alpha_q(f)$ and $\beta_q(f)$ are the roots of the Hecke polynomial $x^2-a_q(f)x+q$ and if $\mathbf{N}\mathfrak{q}=q^t$ then we set $\alpha_{\mathbf{N}\mathfrak{q}}:=\alpha_q(f)^t$ and $\beta_{\mathbf{N}\mathfrak{q}}:=\beta_q(f)^t$. Using Rankin's method, one can show that $L(f,\chi^{-1},s)$ has an analytic continuation on the entire complex plane.

Remark 3.1.1. Note that if χ has infinity type (ℓ_1,ℓ_2) then $\chi^{-1}\mathbf{N}^{\ell_1}$ has infinity type $(0,\ell_1-\ell_2)$ and the modular form associated to this Hecke character has weight $\ell_1-\ell_2+1$. The Rankin L-series $L(f,\chi^{-1},s)$ is a shift of $L(f,\chi^{-1}\mathbf{N}^{\ell_1},s)$ given by

$$L(f,\chi^{-1},s)=L(f,\chi^{-1}\mathbf{N}^{\ell_1}\mathbf{N}^{-\ell_1},s)=L(f,\chi^{-1}\mathbf{N}^{\ell_1},s+\ell_1).$$

Remark 3.1.2. The L-values $L_{\mathrm{alg}}(f,\chi^{-1},0)$ are defined to be an explicit constant multiple of the Rankin L-series evaluated at zero, $L(f,\chi^{-1},0)$. In particular, in this chapter, we will carefully study a subset of the characters χ_r of infinity type $(1+r,1-r)$ where $r=j(p-1)$ for some positive integer j. We can rewrite the Rankin L-value as

$$L(f,\chi_r^{-1}\mathbf{N}^{-1},0)=L(f,\chi_r^{-1},1).$$

In Chapter 4, we will see a complementary p-adic L-function constructed by Perrin-Riou that interpolates the values $L(f,\chi,1)$ for finite order Hecke characters χ. Because the Rankin L-values that the anticyclotomic p-adic L-function interpolates are shifted by $\mathbf{N}^{-1}$, the special value in this chapter occurs at $\mathbf{N}$, while the special value of Perrin-Riou's p-adic L-function occurs at the trivial character $\mathbf{1}$. To emphasize the fact that these p-adic L-functions are interpolating the same Rankin L-values with different normalizations, we use the notation $L_p(f,1)$ for the special value of the anticyclotomic p-adic L-function and $\mathcal{L}_p'(f,1)$ for the special value of Perrin-Riou's p-adic L-function.

In order to p-adically interpolate the values $L(f,\chi^{-1},0)$ and evaluate the anticyclotomic p-adic L-function, we interpret $L_{\mathrm{alg}}(f,\chi^{-1},0)$ as values of a p-adic modular form. This is done using an explicit form of Waldspurger's formula [BDP13, Theorem 5.4]. Throughout the chapter, we rely on the description of $L_{\mathrm{alg}}(f,\chi^{-1},0)$ as a value of a

p-adic modular form, rather than as proportional to the Rankin L-value $L(f, \chi^{-1}, 0)$. We precede the statement of this formula with a discussion of the Shimura–Maass operator.

Recall that we view modular forms as algebraic modular forms, i.e. global sections $H^0(X_0(N), \overline{\omega}^k)$ as in Section 2.2.1 and in particular Definition 2.2.4. We also rely heavily on the background and notation surrounding Heegner points in Section 2.2.2. In particular, recall that the marked elliptic curve with $\Gamma_0(N)$-torsion corresponding to the Heegner point in $P_K \in X_0(N)(K)$ is denoted by

$$(A, A[\mathfrak{n}], \omega_A) = (\mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau_{\mathfrak{n}}), 1/N, \Omega_K \mathfrak{n} dz).$$

Let $M_k(\Gamma_0(N))$ denote the space of modular forms of weight k and $g \in M_k(\Gamma_0(N))$.

Definition 3.1.3. The Shimura–Maass derivative δ_k is defined as

$$\delta_k(g) = \frac{1}{2\pi i}\left(\frac{\partial}{\partial z} + \frac{k}{2iy}\right) g(z).$$

Definition 3.1.4. We say g is a nearly holomorphic modular form of weight k and order less than or equal to P if g is C^∞ on $\mathcal{H}$ and we can express g as a sum

$$g(z) = \sum_{j=0}^{P} g_j(z) y^{-j}$$

where $g_j(z)$ are holomorphic functions on $\mathcal{H}$, the function g transforms like a modular form of weight k for $\Gamma_0(N)$, and g has finite limit at the cusps. We denote the space of such forms $N_k^P(\Gamma_0(N))$.

The following lemmas can be proved with simple calculations.

Lemma 3.1.5 ([Urb14, Lemma 2.1.3])**.** *Let $g \in N_k^P(\Gamma_0(N))$ Assume $P > 2k$. There exist $g_0, \ldots, g_P$ with $g_i \in M_{k-2i}(\Gamma_0(N))$ such that*

$$g = g_0 + \delta_{k-2} g_1 + \cdots + \delta_{k-2P}^P g_P.$$

Lemma 3.1.6 ([Zag08, (52)]). *If $g \in M_k(\Gamma_0(N))$ and $\gamma \in \Gamma_0(N)$ such that $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $\delta_k(\gamma g) = (c+d)^{k+2}\delta_k(g)$.*

Thus, Lemma 3.1.5 and Proposition 3.1.6 imply that the Shimura–Maass derivative is an operator $\delta_k : N_k^P(\Gamma_0(N)) \to N_{k+2}^P(\Gamma_0(N))$.

We denote by δ^r the r-fold composition $\delta_{k+2r-2} \circ \cdots \circ \delta_k$. Let d be the Atkin–Serre derivative that acts on q-expansions by qd/dq.

Shimura [Shi75] showed that the values of $\delta^r f$ and $d^r f$ agree and are algebraic on CM points. In particular, we have the following:

$$d^r f(A, A[\mathfrak{n}], \Omega_A) = \delta^r f(A, A[\mathfrak{n}], \omega_A) \in E_f K. \tag{3.5}$$

We now come to the statement of Waldspurger's formula [BDP13, Theorem 5.4].

Theorem 3.1.7 (Waldspurger's formula)**.**

$$(\delta^{r-1} f(A, A[\mathfrak{n}], \omega_A))^2 = 1/2(2\pi/\sqrt{D})^{2r-1}(r-1)!r!\frac{L(f, \chi_r, 0)}{(2\pi i \overline{\alpha}\Omega_K)^{4r}}.$$

To interpolate $L(f, \chi_r, 0)$ and therefore

$$(\delta^{r-1} f(A, A[\mathfrak{n}], \omega_A))^2 = (d^{r-1} f(A, A[\mathfrak{n}], \omega_A))^2$$

p-adically, we take the p-depletion

$$d^{r-1} f^{[p]}(q) = \sum_{(n,p)=1} n^{r-1} a_n(f) q^n.$$

The set $\{d^{r-1} f^{[p]}\}$ is a p-adic family of modular forms, and there exists a p-adic period $\Omega_p \in \mathbf{C}_p^\times$ such that

$$L_p(f, K, \chi_r) := \Omega_p^{4r}(d^{r-1} f^{[p]}(A, A[\mathfrak{n}], \omega_A))^2$$

extends to a p-adic analytic function of $r \in (\mathbf{Z}/(p-1)\mathbf{Z}) \times \mathbf{Z}_p$ [BDP13, Theorem 5.9].

Remark 3.1.8. The period pair (Ω_K, Ω_p) is only well-defined as a pair: both periods depend linearly on the choice of ω_A, but their ratio is independent of this choice of scalar multiple. For convenience, we used the period Ω_A instead of Ω_K in our computations (see Section 2.2.2 for the discussion of the complex period).

We now describe how to compute the anticyclotomic p-adic L-function explicitly in the range of interpolation by computing the Shimura–Maass derivative $\delta^{r-1} f(\tau_{\mathfrak{n}})$. Let $\chi_r \in S$ be the Galois character associated to the Hecke character of K of infinity type $(1+r, 1-r)$ with $r \geq 1$. Then the algebraic L-function in the interpolation formula (3.2) can be written as

$$L_{\mathrm{alg}}(f, \chi_r^{-1}, 0) = \delta^{r-1} f(A, A[\mathfrak{n}], \omega_A)^2 = \frac{(\delta^{r-1} f(\tau_{\mathfrak{n}}))^2}{(\bar{\alpha}\Omega_K)^{4r}}. \tag{3.6}$$

We would like to evaluate the right hand side of (3.6). As r gets large in the usual absolute value, this value also gets large, and a naive strategy like applying the equality (3.5) and evaluating a truncated q-expansion of $d^{r-1} f(\tau_{\mathfrak{n}})$ does not approximate the true algebraic value well.

However, [Zag08, Section 6.3] and [VZ93] explain that the values of the Shimura–Maass derivative of a modular form evaluated at any CM point satisfy a recurrence relation due to a large amount of algebraic structure on the ring of modular forms $M_*(\Gamma_0(N))$. We recall briefly some of the essential ideas involved in the proof.

In addition to the Shimura–Maass and Atkin–Serre differential operators, we introduce the ϑ differential operator that acts on a weight k modular form g by

$$\vartheta g = dg - \frac{k}{12} E_2 g$$

where E_2 is the weight 2 Eisenstein series. Table 3.1 shows some properties of these differential operators; by "preserves modularity", we mean that modular forms of weight k map to modular forms of weight $k+2$.

	d	δ	ϑ
modularity	not preserved	preserved	preserved
holomorphicity	preserved	not preserved	preserved
Fourier expansions	simple action	simple action	complicated

Table 3.1: Properties of the differential operators

We also define modified version of the ϑ operator by $\vartheta^{[0]}g = g$ and

$$\vartheta^{[r+1]}g = \vartheta(\vartheta^{[r]}g) - r(k+r-1)(E_4/144)\vartheta^{[r-1]}g \text{ for } r \geq 1. \tag{3.7}$$

The Cohen–Kuznetsov series are formal generating series attached to the differential operators that have nice transformation properties under $\Gamma_0(N)$. We provide the details necessary for our calculations here; the interested reader can see [Zag08, Section 5.2] or [Zag94] for more details, as well as [VZ93, Section 7] for some example calculations. The goal of studying these series is to understand that the relationships between the Cohen–Kuznetsov series show that the set of values $\{\delta^r(\tau_{\mathfrak{n}})\}_{r\geq 0}$ inherits a recursive relation coming from the recursive definition of $\vartheta^{[i]}$. We can define a Cohen–Kuznetsov series associated to each operator by

$$\tilde{g}_\vartheta(z,X) = \sum_{n=0}^{\infty} \frac{\vartheta^{[n]}g(z)}{n!(k)_n}X^n,\ \tilde{g}_d(z,X) = \sum_{n=0}^{\infty} \frac{d^n g(z)}{n!(k)_n}X^n,\ \tilde{g}_\delta(z,X) = \sum_{n=0}^{\infty} \frac{\delta^n g(z)}{n!(k)_n}X^n.$$

These power series satisfy

$$\tilde{g}_\vartheta(z,X) = e^{-XE_2(z)/12}\tilde{g}_d(z,X) = e^{-XE_2^*(z)/12}\tilde{g}_\delta(z,X) \tag{3.8}$$

where $E_2^*(z) := E_2(z) - 3/(\pi y)$.

The key idea is that if $E_2^*(z_0) = 0$, then (3.8) implies that $\vartheta^{[i]}g(z_0) = \delta^i g(z_0)$ for all $i \geq 0$. Then, because $\vartheta^{[i]}g(z_0)$ is defined recursively, we can compute $\delta^i g(z_0)$ recursively. This method requires two pieces of input.

1. Since in general $E_2^*(\tau_{\mathfrak{n}}) \neq 0$, we need to modify the operator $\vartheta^{[i]}$ for the CM point $\tau_{\mathfrak{n}}$ with an appropriate holomorphic function $\phi(z)$ such that $\phi^*(z) := \phi(z) - 1/(4\pi y)$ transforms like a modular form of weight 2 on $\Gamma_0(N)$. Define $\vartheta_\phi g := dg - k\phi g$. The resulting relationship (3.8) becomes $\tilde{g}_{\vartheta_\phi}(z, X) = e^{-X\phi^*(z)}\tilde{g}_\delta(z, X)$ on $\mathcal{H}$, and we require $\phi^*(\tau_{\mathfrak{n}}) = 0$.

2. We need generators $g_1, \ldots, g_n$ for $M_*(\Gamma_0(N))$ so that we can compute ϑ_ϕ of each generator as well as the values $g_i(\tau_{\mathfrak{n}})$ and $(\vartheta_\phi g_i)(\tau_{\mathfrak{n}})$ for each generator to determine the recurrence relation.

We can always take $\phi = (1/12)E_2 + A$ for some weight 2 holomorphic or meromorphic function A on $\Gamma_0(N)$ [Zag08, Section 5.2]. Therefore to compute ϕ we evaluate E_2 on $\tau_{\mathfrak{n}}$, and we evaluate a basis of weight 2 level N forms on $\tau_{\mathfrak{n}}$. Then we solve for ϕ by finding a linear combination of the weight 2 level N forms that when evaluated at $\tau_{\mathfrak{n}}$ equal to E_2 evaluated at $\tau_{\mathfrak{n}}$.

Define the modular form $\Phi := d\phi - \phi^2$. We also obtain operators $\vartheta_\phi^{[n]}$ satisfying the recurrence relation

$$\vartheta_\phi^{[0]} g = g, \vartheta_\phi^{[r+1]} g = \vartheta_\phi(\vartheta_\phi^{[r]} g) + r(k + r - 1)\Phi(\vartheta_\phi^{[r-1]} g). \tag{3.9}$$

To rigorously evaluate $g_i(\tau_{\mathfrak{n}})$ and $(\vartheta_\phi g_i)(\tau_{\mathfrak{n}})$ as algebraic numbers we need to bound the denominators of these values that, a priori, lie in K by (3.5). (Note that although f has coefficients in $\mathcal{O}_{E_f}$, the coefficients of g_i lie in $\mathbf{Z}[1/(6N)]$. By scaling, we can ensure the modular forms we evaluate have coefficients in $\mathbf{Z}$.) With work, one can explicitly bound these denominators. For example, when $N = p$, Deligne and Rapoport [DR73, VII, 3.19-3.20] show that the denominators are at most $p^{\lceil kp/(p-1)\rceil}$.

Remark 3.1.9. The recursive methods explained here combined with the rigorous methods in the appendix to [BDP17] resolve the issue described in [BDP17, Remark 5.1.4] of how to compute rigorous tables of values of Shimura–Maass derivatives at CM points for a fixed modular form.

We give some intuition following the discussion in [BDP17, Appendix B]. Consider the $\mathcal{O}_K$-module $M_k(\Gamma_0(N), \mathcal{O}_K)$ consisting of weight k modular forms g for $\Gamma_0(N)$ whose q-expansions have coefficients in $\mathcal{O}_K$. The problem is that for $g \in M_k(\Gamma_0(N), \mathcal{O}_K)$, the evaluation of $g(A, A[\mathfrak{n}], \omega_A)$ is not necessarily $\mathcal{O}_K$-integral, but belongs to $\mathcal{O}_K[1/N]$. One can construct a finite index $\mathcal{O}_K$-module $M_{k,\mathcal{O}_K}$ of the module $M_k(\Gamma_0(N), \mathcal{O}_K)$ such that for every $g \in M_{k,\mathcal{O}_K}$, the evaluation of $g(A, A[\mathfrak{n}], \omega_A)$ is $\mathcal{O}_K$-integral. This is tensor-compatible with the corresponding $\mathbf{Z}$-modules:

$$\mathcal{O}_K \otimes_{\mathbf{Z}} M_{k,\mathbf{Z}} = M_{k,\mathcal{O}_K} \otimes_{\mathbf{Z}} M_k(\Gamma_0(N), \mathbf{Z}) = M_k(\Gamma_0(N), \mathcal{O}_K)$$

so the exponent of the finite abelian group $M_k(\Gamma, \mathbf{Z})/M_{k,\mathbf{Z}}$ multiplies $M_k(\Gamma_0(N), \mathcal{O}_K)$ into $M_{k,\mathcal{O}_K}$ and is an explicit bound on the denominator. (In fact, it gives a much stronger result: this gives a bound on all denominators for all number fields.)

Example 3.1.10. Let f be the modular form 37.2.a.a with weight 2 and level 37. We have a basis of weight 2 forms on $\Gamma_0(37)$ given by

$$\begin{aligned} f_1 &= 1 - 2q^3 + 10q^4 + 2q^5 + 14q^6 + 6q^7 + 10q^8 + 18q^9 + O(q^{10}) \\ f_2 &= q + q^3 - 2q^4 - q^7 - 2q^9 + O(q^{10}) \\ f_3 &= q^2 + 2q^3 - 2q^4 + q^5 - 3q^6 - 4q^9 + O(q^{10}). \end{aligned}$$

Let $\tau_{\mathfrak{n}} = \frac{-27+\sqrt{-11}}{2 \cdot 37}$. Let $p = 5$. By the discussion above, we can bound the denominators of $f_i(\tau_{\mathfrak{n}})$ and $E_2^*(\tau_{\mathfrak{n}})$ by $37^{\lceil 2p/(p-1) \rceil} = 37^3$. We can compute $E_2^*(\tau_{\mathfrak{n}})/(\Omega_A)^2 = 4400 - 3696\sqrt{-11}$. We also compute $f_i(\tau_{\mathfrak{n}})$:

$$\begin{aligned} f_1(\tau_{\mathfrak{n}})/\Omega_A^2 &= 2420 + 572\sqrt{-11} \\ f_2(\tau_{\mathfrak{n}})/\Omega_A^2 &= -726 + 154\sqrt{-11} \\ f_3(\tau_{\mathfrak{n}})/\Omega_A^2 &= -1210 - 286\sqrt{-11}. \end{aligned}$$

Therefore $\phi = 1/12 E_2 - 1/12(-28/11 f_1 - 160/11 f_2)$.

Given an expression $M_*(\Gamma) = \mathbf{Q}[g_1, \ldots, g_n]/I$, we can use the iterative relation

$$\vartheta_\phi^{[r+1]} f = \vartheta_\phi(\vartheta_\phi^{[r]} f) + r(r+1)\Phi(\vartheta_\phi^{[r-1]} f) \text{ for } r \geq 1 \tag{3.10}$$

and apply the Leibniz rule to the monomials in $\vartheta_\phi^{[r]} f$ to apply ϑ_ϕ iteratively. For example, to compute $\vartheta_\phi^{[2]} f$ given $\vartheta_\phi^{[1]} f$ as a sum of monomials in the generators, we need to apply ϑ_ϕ to each monomial of weight 4. Either the monomial is one variable and we look up the precomputed $\vartheta_\phi(g_i)$ or it is of the form $\vartheta_\phi(g_i g_j) = \vartheta_\phi(g_i) g_j + g_i \vartheta_\phi(g_j)$ where we look up the $\vartheta_\phi(g_i)$ in a table. We simply need to pre-compute $\vartheta_\phi(g_i)/\Omega_A^{\mathrm{wt}(g_i)+2}$ and $g_i(\tau_\mathfrak{n})/\Omega_A^{\mathrm{wt}(g_i)}$.

Remark 3.1.11. The slowest part of the computation is expressing $\vartheta_\phi^{[r+1]} f$ in the basis of monomials for the graded weight $2(r+1)+2$ piece. We use $\mathbf{Q}$-linear algebra: we evaluate $\vartheta_\phi^{[r+1]} f$ and the monomial generators as q-expansions, using precision equal to the Sturm bound, then solve for $\vartheta_\phi^{[r+1]} f$ in terms of the generators.

To obtain the generators and relations for

$$M_*(\Gamma_0(N)) = \mathbf{Q}[g_1, \ldots, g_n]/I$$

we use the Magma code for computing canonical rings by [ABB+]. By [VZB19] we need generators up to degree 6 and relations up to degree 12.

Example 3.1.12. Continuing Example 3.1.10, we can use these methods to compute

$$f(\tau_\mathfrak{n})/\Omega_A^2 = 1694 + 726\sqrt{-11} \text{ and } \delta f(\tau_\mathfrak{n})/\Omega_A^4 = 532400 - 447216\sqrt{-11}.$$

To evaluate the anticyclotomic p-adic L-function at $\mathbf{N}$, we will need to turn the algebraic values into p-adic values. Note we have fixed an embedding $K \to \mathbf{Q}_p$ given by the splitting $p = \mathfrak{p}\overline{\mathfrak{p}}$. We define $\mathfrak{p}$ to be the prime with valuation 1 and use the isomorphism $K_\mathfrak{p} \simeq \mathbf{Q}_p$ to obtain a p-adic value from the algebraic value.

Remark 3.1.13. When $[E_f : \mathbf{Q}] > 1$, then $\delta^{r-1} f(\tau_\mathfrak{n})/\Omega_A^{2r}$ belong to the compositum of K and E_f and we use the embedding $e : E_f \to \mathbf{Q}_p$ to make the value p-adic. Changing

the embedding e is equivalent to picking a Galois conjugate f^σ for $\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})$. Furthermore, since the operator d is Galois-equivariant, and we have the equality (3.5), it follows

$$\delta^{r-1} f^\sigma(\tau_n) = \sigma(\delta^{r-1} f(\tau_n)).$$

In this way, we can obtain all $[E_f : \mathbf{Q}]$ p-adic values of $\delta^{r-1} f^\sigma(\tau_n)$ for $\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})$ from knowing a single value $\delta^{r-1} f(\tau_n)$.

Example 3.1.14. Let f be a newform in the newform orbit 85.2.a.b given by

$$f(q) := q + (\sqrt{2}-1)q^2 + (-\sqrt{2}-2)q^3 + (-2\sqrt{2}+1)q^4 - q^5 - \sqrt{2}q^6 + O(q^7).$$

The coefficient field of f is $E_f = \mathbf{Q}(\sqrt{2})$. Let $K = \mathbf{Q}(\sqrt{-19})$. Then the compositum of K and E_f can be written as $\mathbf{Q}(\mu)$ where μ has minimal polynomial $z^4 + 34z^2 + 441$. Then

$$\delta^5(f(\tau_{\mathfrak{n}}))/\Omega_A^{12} =$$
$$14261866508824\mu^3 + 57409577045856\mu^2 + 562228325968312\mu + 246810650617152.$$

We have two choices of embedding $E_f \to \mathbf{Q}_p$. We can send $\sqrt{2} \mapsto 4+5\cdot 7+4\cdot 7^2+O(7^4)$, in which case

$$\delta^5(f(\tau_{\mathfrak{n}}))/\Omega_A^{12} = 57202333 + O(7^{10}). \tag{3.11}$$

Otherwise, if we send $\sqrt{2} \mapsto 3 + 7 + 2\cdot 7^2 + 6\cdot 7^3 + O(7^4)$, then

$$\delta^5(f(\tau_{\mathfrak{n}}))/\Omega_A^{12} = -133321896 + O(7^{10}). \tag{3.12}$$

Now fix the choice of embedding $E_f \to \mathbf{Q}_p$. Then by Remark 3.1.13, (3.11) and (3.12) are the two p-adic values of $\delta^5(f(\tau_{\mathfrak{n}}))/\Omega_A^{12}$ and $\delta^5(f^\sigma(\tau_{\mathfrak{n}}))/\Omega_A^{12}$ for $\sigma \in \mathrm{Gal}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$.

3.2 Evaluating outside of the range of interpolation

We now discuss an application of Rubin's method to compute the value $L_p(f, 1)$ outside of the range of interpolation.

Let $r \in \mathbf{N}$. Let $\chi_r \in S$ be the Galois character associated to the Hecke character

with infinity type $(1+r, 1-r)$. Define

$$\ell(r) := L_p(f, \chi_r)\Omega_p^{-4r}. \tag{3.13}$$

We want to compute $\ell(0)$. Since this is not in the range of interpolation, we compute auxiliary values $\ell((p-1)), \ell(2(p-1)), \ldots, \ell(B(p-1))$ in the range of interpolation and recover $\ell(0)$ modulo $\mathfrak{p}^B$ from a version of [Rub94, Theorem 9, Proposition 7] for the anticyclotomic p-adic L-function of Bertolini, Darmon, and Prasanna.

The main result of this section is the following proposition.

Proposition 3.2.1. *Let $\ell(r)$ be defined as above. Then for any $B \in \mathbf{N}$, we have*

$$\ell(0)^{(p-1)/2} \equiv \sum_{j=1}^{B} \left(\sum_{i=j}^{B} (-1)^{j-1} \binom{i-1}{j-1} \right) \ell(j(p-1))^{(p-1)/2} \mod \mathfrak{p}^B. \tag{3.14}$$

Furthermore, $\ell(0) \equiv \ell((p-1)^2/2) \mod \mathfrak{p}$.

Assuming $\ell(0) \not\equiv 0 \mod \mathfrak{p}$, Proposition 3.2.1 allows us to uniquely recover $\ell(0)$ from the auxiliary values $\ell(j(p-1))$. We now prove Proposition 3.2.1.

Following Rubin, we introduce a ring $\mathcal{I}$ of generalized Iwasawa functions. A function g on $\mathbf{Z}_p$ is in $\mathcal{I}$ if there exist units $u_1, \ldots, u_m \in 1 + \mathfrak{p}\hat{\mathcal{O}}$ and a power series $H \in \hat{\mathcal{O}}[[X_1, \ldots, X_m]]$ such that $g(s) = H(u_1^s - 1, \ldots, u_m^s - 1)$ for all $s \in \mathbf{Z}_p$.

Recall $\chi_{i(p-1)} \in S$ is a Galois character associated to a Hecke character of K with infinity type $(1 + i(p-1), 1 - i(p-1))$. By composing with a projection arising from $\mathbf{Z}_p^\times \simeq (\mathbf{Z}/p\mathbf{Z})^\times \times (1 + p\mathbf{Z}_p)$, we have

$$\langle \chi_{i(p-1)} \rangle : \Gamma^- \to \mathbf{Z}_p^\times \to 1 + p\mathbf{Z}_p \tag{3.15}$$

since $\chi_{i(p-1)}$ already takes values in $1 + p\mathbf{Z}_p$ [dS87, §II.4.17]. For $F \in \Lambda^{\mathrm{ac}}$, we have $\langle \chi_{i(p-1)} \rangle(F) \in \widehat{\overline{\mathbf{Q}}}_p$, and furthermore for $s \in \mathbf{Z}_p$ we can define $\chi_{s(p-1)} := \langle \chi_{(p-1)} \rangle^s$ and evaluate $\chi_{s(p-1)}(F) \in \widehat{\overline{\mathbf{Q}}}_p$ by continuity.

Define

$$H(s) := (\Omega_p^{(p-1)^2})^{-2s} L_p(f, \chi_{s(p-1)})^{(p-1)/2}. \tag{3.16}$$

By [dS87, §II.4.3(10)], we have

$$\Omega_p^{(p-1)^2} \in 1 + \mathfrak{p}\hat{\mathcal{O}} \tag{3.17}$$

so H is well-defined. For $i \in \mathbf{Z}$, note that

$$H(i) = \ell((p-1)i)^{(p-1)/2}. \tag{3.18}$$

Analogously to [Rub94, Proposition 7], we have the following proposition.

Proposition 3.2.2. *Let $\ell(r)$ and H be defined as in (3.13) and (3.16). Then*

1. *$H \in \mathcal{I}$.*
2. *$\ell(0) \equiv \ell((p-1)^2/2) \mod \mathfrak{p}$.*

Proof. We define functions f_1 and f_2 by

$$\begin{aligned} f_1(s) &:= L_p(f, \chi_{s(p-1)}) \\ f_2(s) &:= (\Omega_p^{(p-1)^2})^{-2s}. \end{aligned} \tag{3.19}$$

Then $H = f_1^{(p-1)/2} f_2$. We know $f_1 \in \mathcal{I}$ since $\chi_{i(p-1)}$ is a character into $1 + p\mathbf{Z}_p$ for all $i \in \mathbf{N}$ (see (3.15)) and by (3.17) we know $f_2 \in \mathcal{I}$, so $H \in \mathcal{I}$.

Finally, since $f_1(s) \equiv f_1(s') \mod \mathfrak{p}$ for all $s, s' \in \mathbf{Z}_p$ we have

$$\ell(0) = f_1(0) \equiv \Omega_p^{-2(p-1)^2} f_1((p-1)/2) = \ell((p-1)^2/2) \mod \mathfrak{p}. \tag{3.20}$$

□

Remark 3.2.3. Proposition 3.2.2 (2) is only helpful if $\ell((p-1)^2/2) \not\equiv 0 \mod \mathfrak{p}$. More generally, one can see that by (3.17), for $n \geq 1$ we have

$$\ell(0) = f_1(0) \equiv \Omega_p^{-2(p-1)^2 p^{n-1}} f_1((p-1)p^{n-1}/2) = \ell((p-1)^2 p^{n-1}/2) \mod \mathfrak{p}^n. \tag{3.21}$$

The main difficulty in applying this congruence is computing $\ell((p-1)^2 p^{n-1}/2)$.

From here it is straightforward to follow Rubin's proof to obtain a proof of Proposition 3.2.1: we recapitulate it briefly. He defines a difference operator Δ on $\mathcal{I}$ by $\Delta(g)(s) := g(s+1) - g(s)$. If $g \in \mathcal{I}$ then $\Delta(g) \in \mathfrak{p}\mathcal{I}$ [Rub94, Lemma 8].

By inverting $(1+\Delta)^{-1} = \sum_{i=0}^{\infty}(-1)^i \Delta^i$ and applying the congruence, we obtain the desired formula [Rub94, Theorem 9]

$$g(0) = \sum_{j=1}^{B} \left(\sum_{i=j}^{B} (-1)^{j-1} \binom{i-1}{j-1} \right) g(j) \mod \mathfrak{p}^B. \tag{3.22}$$

By applying this to $H \in \mathcal{I}$ we can compute the special values.

f	p	D	time	Sturm Bound
37.2.a.a	5	−11	34.400	7
43.2.a.a	5	−19	44.080	8
61.2.a.a	5	−19	75.710	11
83.2.a.a	5	−19	160.310	14
89.2.a.a	3	−11	197.880	15
58.2.a.a	11	−7	2162.400	15
77.2.a.a	5	−19	703.310	16
101.2.a.a	5	−19	887.750	17
131.2.a.a	5	−19	22818.670	22

Table 3.2: Timings for fixed $B = 5$ and varying N for modular forms with rational Fourier coefficients

f	p	D	time	Sturm Bound
67.2.a.b	11	−7	36542.740	12
73.2.a.b	11	−19	51209.140	13
107.2.a.a	11	−7	285919.670	18
85.2.a.b	7	−19	8436.150	18

Table 3.3: Timings for fixed $B = 5$ and varying N with $[E_f : \mathbf{Q}] = 2$

Remark 3.2.4. We have written code to compute $\ell(0)$ and $L_p(f, 1)$ in Magma V2.26-10. The biggest impediment to considering large levels N is the time it takes to compute

B	time
5	34.400
6	46.600
7	54.590
8	67.310
9	90.890
10	119.230
11	168.080
12	234.080

Table 3.4: Timings for 37.2.a.a, $p = 5$, $D = -19$, as B varies

generators and relations for the ring $M_*(\Gamma_0(N))$; this computation takes a very long time when $N \geq 100$. The timing scales with the Sturm bound [Ste07, Corollary 9.20]

$$\left\lfloor \frac{k \cdot [\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(N)]}{12} \right\rfloor = \left\lfloor \frac{k \cdot N \prod_{p|N} \left(1 + \frac{1}{p}\right)}{12} \right\rfloor$$

which gives the precision needed to determine a modular from its truncated q-expansion.

For a fixed B, the timing also scales in p, because $B(p-1)$ gets larger as p gets larger, so when p is large more values of the Shimura–Mass derivative of f need to be computed to reach the same level of precision. See Tables 3.2, 3.3, and 3.4 for timings. These timings were done on a 2017 Macbook Pro with a 2.3 GHz Dual-Core Intel Core i5 processor and 8 GB of RAM. All times are given in seconds.

Example 3.2.5. Let f be the newform with LMFDB label 37.2.a.a, $D = -11$, and $p = 5$. We compute the values of $\ell(r)$ in Table 3.5. So Proposition 3.2.1 implies that

$$H(0) = L_p(f, 1)^2 \equiv 2502536 \mod \mathfrak{p}^{10}$$

and

$$L_p(f, 1) \equiv \ell(8) \equiv 830906 \mod \mathfrak{p}$$

so

$$L_p(f, 1) \equiv 4635631 \mod \mathfrak{p}^{10}.$$

r	$\ell(r) \mod \mathfrak{p}^{10}$
4	-2341944
8	830906
12	-3933069
16	-35494
20	1760756
24	1706556
28	1972781
32	-3662194
36	3734381
40	4015256

Table 3.5: $\ell(r)$ for 37.2.a.a

Remark 3.2.6. The values in Table 3.5 are computed and stored as algebraic numbers in K, then embedded in $K_{\mathfrak{p}} \simeq \mathbf{Q}_p$ in order to evaluate the p-adic L-function. For example, when f is the newform with LMFDB label 37.2.a.a, we compute

$$\begin{aligned}
\delta^3 f(\tau_{\mathfrak{n}})/\Omega_A^8 =& 606067123200\sqrt{-11} + 2439275869184,\\
\delta^7 f(\tau_{\mathfrak{n}})/\Omega_A^{16} =& 42017607447247025950398873600\sqrt{-11}+\\
& 271366721229196042648325980 16,\\
\delta^{11} f(\tau_{\mathfrak{n}})/\Omega_A^{24} =& -444448834547949937451654180963580819957350400\sqrt{-11}+\\
& 799395222080018537470761730767912422692880384.
\end{aligned}$$

Using (3.2) we can see that these relate to the values in Table 3.5 by

$$\ell(r) = (1 - a_p(f)\beta^{r-1}\overline{\beta}^{-k-(r-1)} + \beta^{k+2(r-1)-1}\overline{\beta}^{-k-2(r-1)-1})^2(\delta^{r-1}f(\tau_{\mathfrak{n}}))^2/\Omega_A^{4r}$$

where β is a generator for $\mathfrak{p}$ and $\overline{\beta}$ for $\overline{\mathfrak{p}}$. These values get extremely large in absolute value as r gets large.

For 77.2.a.a, $D = -19$, and $p = 5$, we can similarly compute $\ell(0) \mod B = 7$:

$$L_p(f,1) \equiv 4 + 2\cdot 5 + 4\cdot 5^2 + 3\cdot 5^3 + 5^4 + 3\cdot 5^6 \mod \mathfrak{p}^7.$$

This agrees with the computed value of $\left(\frac{1-a_p(f)+p}{p}\right)^2 \log(\pi(y_K))^2$ on the associated

elliptic curve E. In this case the Heegner cycle has index 2 in $E(\mathbf{Q})$.

Example 3.2.7. Let f be a newform in the orbit 85.2.a.b. Then f has coefficient field $\mathbf{Q}(\sqrt{2})$, and we denote

$$f(q) := q + (\sqrt{2}-1)q^2 + (-\sqrt{2}-2)q^3 + (-2\sqrt{2}+1)q^4 - q^5 - \sqrt{2}q^6 + O(q^7)$$
$$f^\sigma(q) := q + (-\sqrt{2}-1)q^2 + (\sqrt{2}-2)q^3 + (2\sqrt{2}+1)q^4 - q^5 + \sqrt{2}q^6 + O(q^7)$$

where $\sigma \in \mathrm{Gal}(\mathbf{Q}(\sqrt{2})/\mathbf{Q})$ is the nontrivial automorphism. Let $D = -19$, and $p = 7$ and fix the embedding $\sqrt{2} \mapsto 4 + 5 \cdot 7 + 4 \cdot 7^2 + O(7^4)$. We compute the values of $\ell(r)$ in Table 3.6.

r	$\ell(r) \mod \mathfrak{p}^{10}$
6	19467645
12	27057027
18	−443168
24	72608418
30	−32171562
36	−95344303
42	−68492493
48	−129070518
54	−81233717
60	24574313

Table 3.6: $\ell(r)$ for f in 85.2.a.b

So Proposition 3.2.1 implies that

$$L_p(f, 1) \equiv -25026440 \cdot 7^2 \mod \mathfrak{p}^{10}.$$

Per Remark 3.1.13, for f^σ, we use the same algebraic values that give the values in Table 3.6 under the other embedding to obtain the values in Table 3.7. So Proposition 3.2.1 implies that

$$L_p(f^\sigma, 1) \equiv -107584760 \cdot 7^{-2} \mod \mathfrak{p}^{10}.$$

In other words, we have determined $(\log_{fdq/q} \pi(y_K))^2$ and $(\log_{f^\sigma dq/q} \pi(y_K))^2$, the values of the square of the logarithm of the Heegner cycle on the Jacobian of $X_0^*(85)$ with respect to the basis $fdq/q, f^\sigma dq/q$ of $H^0(X_0^*(85), \Omega^1)$.

r	$\ell(r) \mod \mathfrak{p}^{10}$
6	43423556
12	−73857066
18	−23385339
24	−3074238
30	−124792286
36	−117649341
42	−70665601
48	99453799
54	−97983002
60	2301594

Table 3.7: $\ell(r)$ for f^σ in 85.2.a.b

Chapter 4

Perrin-Riou's p-adic Gross–Zagier formula

Recall that $f \in S_2(\Gamma_0(N))$ is a weight 2 newform for $\Gamma_0(N)$. In this chapter we discuss the computation of the cyclotomic p-adic height of the f-isotypical component of the Heegner cycle $h(y_{K,f})$ using the p-adic Gross–Zagier formula of Perrin-Riou [PR87]. Like the anticyclotomic L-function of the previous chapter, Perrin-Riou's p-adic L-function $\mathcal{L}_p(f)$ also interpolates the central value of the Rankin L-series $L(f, \chi, 1)$ for certain Hecke characters χ, and she also provides a p-adic Gross–Zagier formula with a special value at $\mathbf{1}$. The nature of Perrin-Riou's construction of the p-adic Rankin L-series associated to f and K leads $\mathbf{1}(\mathcal{L}_p(f))$ to vanish, and instead she considers the derivative in the cyclotomic direction (4.3), which she shows is proportional to the p-adic height of the Heegner cycle.

Our goal is to outline how to compute the derivative $\mathcal{L}_p(f)$ at $\mathbf{1}$ in the cyclotomic direction, as well as the other constants appearing in the p-adic Gross–Zagier formula, and therefore the height of the Heegner cycle. In order to do this, we will use the relationship between Perrin-Riou's p-adic L-function and the p-adic L-function of Amice-Vélu and Vishik. We then use the theory of overconvergent modular symbols [PS11] to compute values of the latter p-adic L-function.

For this chapter we assume the following hypotheses.

Assume $p > 2$ is a prime number that does not divide N. (H6)

Let $E_f/\mathbf{Q}$ be the coefficient field of f.

Assume p splits in E_f; (H7)

we do this to avoid working in extensions of $\mathbf{Q}_p$ in our computations. Fix an embedding $e : E_f \to \mathbf{Q}_p$ arising from completing at a prime above p. Assume

f^σ is ordinary in e, that is, $e(a_p(f^\sigma))$ is a unit for all $\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})$. (H8)

We continue to assume that

f has analytic rank 1; (H9)

$K = \mathbf{Q}(\sqrt{D})$ is an imaginary quadratic field of class number 1 with odd discriminant $D < -3$; (H10)

and the Heegner hypothesis

every prime q dividing N splits in K. (H11)

Let K_∞/K be the (unique) $\mathbf{Z}_p^2$-extension of K with Galois group $\Gamma := \mathrm{Gal}(K_\infty/K)$. Write $\mathcal{O}$ for the ring of integers in $\overline{\mathbf{Q}}_p$. Let $\psi : \Gamma \to \mathcal{O}^\times$ be a finite order character. The theta series

$$\Theta_\psi := \sum_{\mathfrak{a} \subset \mathcal{O}_K} \psi(\mathfrak{a}) q^{\mathrm{Nm}(\mathfrak{a})} \tag{4.1}$$

is a weight 1 modular form. We denote the Rankin–Selberg convolution by $L(f, \psi, s) := L(f, \Theta_\psi, s)$. Perrin-Riou constructs a p-adic L-function $\mathcal{L}_p(f) \in \mathbf{Z}_p[[\Gamma]]$ characterized by the interpolation property that for any finite order character $\psi : \Gamma \to \mathcal{O}^\times$, the values

$$\psi(L_p(f)) \doteq L(f, \psi, 1) \tag{4.2}$$

are proportional. (As in (3.2), the left hand side is our notation for evaluation $L_p(f)$ at ψ in the range of interpolation.) Using the functional equation for $\mathcal{L}_p(f)$ we can show that that $\mathcal{L}_p(f)$ vanishes at the trivial character $\mathbf{1}$.

Perrin-Riou relates the derivative of this p-adic L-function at $\mathbf{1}$ to a p-adic height pairing defined by Schneider and Mazur–Tate [Sch82, MT83] on abelian varieties. This coincides also with the height pairing of Coleman–Gross [CG89] in the case of Jacobians, when the required splitting of the Hodge filtration is given by the unit root subspace of $H^1(X_{\mathbf{Q}_p}, \Omega^1)$ [Col91]. This height pairing for divisors is discussed in Section 1.2, where we used the notation $h(\cdot,\cdot)$ for the global height. To avoid confusion while working over multiple base fields, and save space, we will use $\langle \cdot, \cdot \rangle$ notation for the (global) height with a subscript denoting the choice of idèle class character. We will later use the notation $h(y)$ to mean the height pairing $h(y) = h(y, y)$ with respect to the cyclotomic character $\mathbf{A}_{\mathbf{Q}}^{\times}/\mathbf{Q}^{\times} \to \mathbf{Q}_p$. When the field of definition is not $\mathbf{Q}$ we will always use the notation $\langle \cdot, \cdot \rangle$ with a subscript to denote the choice of idèle class character.

This height pairing $\langle \cdot, \cdot \rangle_v$ depends on a choice of idèle class character:

$$\ell_K : \mathbf{A}_K^{\times}/K^{\times} \to \mathbf{Q}_p$$

equivalently, a homomorphism into the additive group $\ell_K : \Gamma \to \mathbf{Q}_p$, which we will take to be the cyclotomic character. We can decompose ℓ_K as the composition $\ell_K = \log_p \circ \lambda$ where $\lambda : \Gamma \to 1 + p\mathbf{Z}_p$ is the cyclotomic character.

The derivative of $\mathcal{L}_p(f)$ in the direction of ℓ_K at the trivial character $\mathbf{1}$ is defined as

$$\mathcal{L}'_{p,\ell_K}(f, 1) := \left(\frac{d}{ds} \lambda^s(\mathcal{L}_p(f)) \right) \Big|_{s=0}. \tag{4.3}$$

Our notation $\mathcal{L}'_{p,\ell_K}(f, 1)$ for the special value is used to emphasize the similarity with

the anticyclotomic p-adic L-function; see Remark 3.1.2. Let v be the cyclotomic character of $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$ (this is the restriction of λ to $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$).

Recall that $y_K \in J_0(N)(K)$ denotes the Heegner cycle associated to K, and for $\sigma \in \mathrm{Gal}(E_f/K)$, we write y_{K,f^σ} for the f^σ-isotypical part of y_K, which belongs to $J_0(N)(K) \otimes E_f$.

By (H8), f is ordinary in e; let $\alpha_p(f)$ denote the unit root of the Frobenius polynomial $x^2 - e(a_p)x + p$ in $\mathbf{Q}_p$.

Theorem 4.0.1 ([PR87, Theorem 1.3])**.** *The function $\mathcal{L}_p(f)$ vanishes at $\mathbf{1}$ and the derivative at $\mathbf{1}$ in the direction ℓ_K is*

$$\mathcal{L}'_{p,\ell_K}(f,1) = \left(1 - \frac{1}{\alpha_p(f)}\right)^4 \langle y_{K,f}, y_{K,f}\rangle_v. \tag{4.4}$$

Remark 4.0.2. As discussed in Section 2.3, the Galois group Γ is non-canonically isomorphic to $\mathbf{Z}_p[[T_1,T_2]]$ and so the space of finite order characters $\Gamma \to \mathcal{O}^\times$ has $\mathbf{Z}_p$-rank 2. However, the height $\langle y_{K,f}, y_{K,f}\rangle_v$ and the derivative of $\mathcal{L}_p(f)$ in the direction of ℓ_K are zero when ℓ_K is associated to a dihedral character of Γ (a character belonging to Γ^-).

We now discuss how to modify Theorem 4.0.1 to obtain the heights of the images of Heegner cycles on Atkin–Lehner quotients J_f of $J_0(N)$. These formulas lay the groundwork for doing quadratic Chabauty on quotients of $X_0(N)$.

Proposition 4.0.3 ([MT83, (3.4.3)])**.** *Let $g : A \to B$ be a homomorphism of principally polarized abelian varieties over $\mathbf{Q}$, $a \in A(K)$, and $b \in B(K)$. Let $g^\vee$ denote the dual map $g^\vee : B^\vee \to A^\vee$, while $\lambda_A : A \to A^\vee$ and $\lambda_B : B \to B^\vee$ denote the principal polarizations. Then*

$$\langle a, (\lambda_A^{-1} \circ g^\vee \circ \lambda_B)(b)\rangle_v = \langle g(a), b\rangle_v.$$

We deduce the following proposition from Mazur and Tate's formula.

Proposition 4.0.4. *Let $\phi : X_0(N) \to X$ be an Atkin–Lehner quotient, such that the Jacobian J_f of X is a $\mathbf{Q}$-simple quotient of $J_0(N)^{\mathrm{new}}$ associated to f via (†). Let $\pi : J_0(N) \to J_f$ be induced by the pushforward. We continue to suppose p is ordinary*

for J_f (H8). Then

$$\mathcal{L}'_{p,\ell_K}(f,1) = \left(1 - \frac{1}{\alpha_p(f)}\right)^4 \frac{\langle \pi(y_{K,f}), \pi(y_{K,f})\rangle_v}{(\deg \phi)}. \tag{4.5}$$

Proof. Let $\pi^\vee : J_f^\vee \to J_0(N)^\vee$ be the dual map on the dual abelian varieties and $\theta_J : J_0(N)^\vee \to J_0(N)$ be the principal polarization on $J_0(N)$. Consider the polarization $\theta_f = \pi \circ \theta_J \circ \pi^\vee : J_f^\vee \to J_f$. This is not the principal polarization on J_f as the Jacobian of X (for instance, it is not generally an isomorphism). Let $\lambda : J_f^\vee \to J_f$ be the principal polarization of J_f. In particular, by identifying $\phi_* = \pi$ and $\phi^* = \theta_J \circ \pi^\vee \circ \lambda^{-1}$ we see that $(\deg \phi)\lambda = \theta_f$. In other words $\phi_*\phi^* = \mathrm{id}_{J_f} \deg \phi$, so letting

$$e := \left(\frac{1}{\deg \phi}\right) \theta_J \circ \pi^\vee \circ \lambda^{-1} \circ \pi$$

we see that e is an idempotent in $\mathrm{End}^0(J_0(N))$ which gives projection onto the component $\mathrm{End}^0(J_f)$.

Proposition 4.0.3 gives

$$\langle y_{K,f}, (\theta_J \circ \pi^\vee \circ \lambda^{-1})\pi(y_{K,f})\rangle_v = \langle \pi(y_{K,f}), \pi(y_{K,f})\rangle_v.$$

But the left hand side is also equal to $(\deg \phi)\langle y_{K,f}, e y_{K,f}\rangle_v = (\deg \phi)\langle y_{K,f}, y_{K,f}\rangle_v$, since $y_{K,f} = e y_{K,f}$ and e is idempotent.

So $\langle y_{K,f}, y_{K,f}\rangle_v = \langle \pi(y_{K,f}), \pi(y_{K,f})\rangle_v/(\deg \phi)$, as claimed. □

Note that the height on the right hand side of Lemma 4.0.4 is equal to the Mazur–Tate height, or Coleman–Gross height (when we choose the required splitting of the Hodge filtration to be given by the unit root subspace of $H^1(X_{\mathbf{Q}_p}, \Omega^1)$).

The following corollary follows from the formula for taking the trace [MT83, (1.10.5)].

Corollary 4.0.5. *Let $\phi : X_0(N) \to X$ be an Atkin–Lehner quotient, such that the Jacobian J_f of X is a $\mathbf{Q}$-simple quotient of $J_0(N)^{\mathrm{new}}$ associated to f via (†). Let $\pi : J_0(N) \to J_f$ be induced by the pushforward. Make an identification $\mathrm{End}^0(J_0(N)) \simeq$*

E_f. We have

$$\langle \pi(y_K), \pi(y_K) \rangle_{v_{\mathbf{Q}}} = \frac{1}{2} \sum_{\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})} \langle \pi(y_{K,f^\sigma}), \pi(y_{K,f^\sigma}) \rangle_v,$$

where on the left hand side we are considering $\pi(y_K)$ as a point in $J_f(\mathbf{Q})$.

Proof. We have that $y_K = \sum_{f \in \mathrm{New}_N} \sum_{\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})} y_{K,f^\sigma}$. For $g \neq f$ the g-isotypical subspace of $J_0(N)$ is in the kernel of π, so

$$\langle \pi(y_K), \pi(y_K) \rangle_v = \sum_{\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})} \langle \pi(y_{K,f^\sigma}), \pi(y_{K,f^\sigma}) \rangle_v.$$

Then by [MT83, (1.10.5)]

$$[K : \mathbf{Q}] \langle \pi(y_K), \pi(y_K) \rangle_v = \langle 2\pi(y_K), 2\pi(y_K) \rangle_{v_{\mathbf{Q}}}$$

where $2\pi(y_K)$ is the trace of $\pi(y_K)$ from $K/\mathbf{Q}$. □

Perrin-Riou provides a comparison of the p-adic L-function described here to the p-adic L-function $L_{p,\mathrm{MTT}}(f)$ of Amice-Vélu and Vishik [PR87, (1.1)] discussed in the paper of Mazur, Tate, and Teitelbaum [MTT86]. This comparison will be important computationally, since the latter L-function can be computed in Sage. We first give a brief description of the interpolation property of the p-adic L-function $L_{p,\mathrm{MTT}}(f)$; more details can be found in [MTT86]. Let γ be a topological generator for $\Gamma_{\mathbf{Q}}$ (defined in Section 2.3). Let ζ be a primitive p^rth root of unity. We write ψ_ζ for the associated character of $\Gamma_{\mathbf{Q}}$ sending $\gamma \mapsto \zeta$. We can also think of this as a Dirichlet character by considering it as a character of $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^r})/\mathbf{Q}) \simeq (\mathbf{Z}/p^r\mathbf{Z})^\times$. Write $\tau(\psi_\zeta)$ for the Gauss sum. Then there exists an element

$$\psi_\zeta(L_{p,\mathrm{MTT}}(f)) = e_p(\zeta) \frac{L(f, \psi_\zeta^{-1}, 1)}{\Omega_f^{\mathrm{sgn}(\psi_\zeta)}} \tag{4.6}$$

where $\Omega_f^\pm$ are certain periods associated to f, which we will elaborate on later (see

(4.6) and Algorithm 4.0.9), and

$$e_p(\zeta) = \begin{cases} \alpha_p^{-r-1} \frac{p^{r+1}}{\tau(\psi_\zeta^{-1})} & \text{if } \zeta \neq 1 \\ \alpha_p(f)^{-1} \left(1 - \frac{1}{\alpha_p(f)}\right)^2 & \text{if } \zeta = 1. \end{cases} \tag{4.7}$$

Let $v_{\mathbf{Q}}$ be the cyclotomic character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Let $\Omega_f := 8\pi^2\|f\|$ be the period of the modular form f [PR87, p.458]. Let ε denote the quadratic character associated to K with conductor $|D|$. Then

$$v(\mathcal{L}_p(f, \mathbf{1})) = v_{\mathbf{Q}}(L_{p,\mathrm{MTT}}(f))v_{\mathbf{Q}}(L_{p,\mathrm{MTT}}(f^\varepsilon)) \left(\frac{\sqrt{|D|}}{\Omega_f}\right). \tag{4.8}$$

Sage has an implementation of the p-adic L-function of Amice-Vélu and Vishik, so in practice, we use (4.8) and the fact that $L(f, 1) = 0$ to translate Theorem 4.0.1 from a statement about the derivative of $\mathcal{L}_p(f, 1)$ in the direction of ℓ_K into a statement about this p-adic L-function to compute the cyclotomic p-adic height of $y_{K,f}$:

$$\mathcal{L}'_{p,\ell_K}(f, 1) = L'_{p,\mathrm{MTT}}(f, 1)L_{p,\mathrm{MTT}}(f^\varepsilon, 1) \left(\frac{\Omega_f^+\Omega_{f\varepsilon}^+\sqrt{|D|}}{\Omega_f}\right). \tag{4.9}$$

Remark 4.0.6. There is an apparent discrepancy between (4.8) and our equation for the comparison between the p-adic L-function of Perrin-Riou and Mazur: the factor $\Omega_f^+\Omega_{f\varepsilon}^+$. This comes about because the notation for the interpolation formula for the p-adic L-function in [SW13] and other modern papers is different from that originally used in [MTT86] and [PR87]. In [MTT86, Section 14] they write the interpolation formula without the period.

To compute $L_{p,\mathrm{MTT}}(f^\varepsilon, 1)$ we use the interpolation property of the p-adic L-function (4.6):

$$L_{p,\mathrm{MTT}}(f^\varepsilon, 1) = (1 - 1/\alpha_p(f^\varepsilon))^2 L(f^\varepsilon, 1)/\Omega_{f^\varepsilon}^+. \tag{4.10}$$

Since we chose K to be a field where p splits, $a_p(f^\varepsilon) = \varepsilon(p)a_p(f) = a_p(f)$ and therefore $\alpha_p(f^\varepsilon) = \alpha_p(f)$. We use the equality $(1 - 1/\alpha_p(f^\varepsilon))^2 = (1 - 1/\alpha_p(f))^2$ to cancel some

factors.

When we combine (4.10) with (4.9), we have

$$\langle y_{K,f}, y_{K,f}\rangle_v = \tag{4.11}$$
$$\left(\frac{\Omega_f^+\Omega_{f^\varepsilon}^+\sqrt{|D|}}{\Omega_f}\right)\left(1-\frac{1}{\alpha_p(f)}\right)^{-2}\frac{L(f^\varepsilon,1)}{\Omega_{f^\varepsilon}^+}\frac{d}{dT}L_{p,\mathrm{MTT}}(f,T)\Big|_{T=0}\log_p(1+p).$$

The conversion from $L_{p,\mathrm{MTT}}(f,s)$ to the series expansion $L_{p,\mathrm{MTT}}(f,T)$ requires a choice of topological generator $1+p$ for the Galois group of the cyclotomic $\mathbf{Z}_p$-extension $\mathrm{Gal}(K_\infty^{\mathrm{cyc}}/K)$. (See [SW13, Section 3] for more details on the definition of $L'_{p,\mathrm{MTT}}(f,s)$, the series expansion, and the derivative in the case where f has rational Fourier coefficients.)

Let $\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})$. By plugging in f^σ on the right hand side of (4.11), we obtain $\langle y_{K,f^\sigma}, y_{K,f^\sigma}\rangle_v$.

Algorithm 4.0.7 (The cyclotomic p-adic height over K of the f-isotypical component of the Heegner cycle $y_{K,f}$).
Input:

- $f \in S_2(\Gamma_0(N))$ newform with coefficients in E_f;
- K imaginary quadratic field of class number 1 and discriminant $D < -3$ satisfying (H4) for N;
- p a prime split in K; and
- an embedding $e : E_f \to \mathbf{Q}_p$ such that f is ordinary in e.

Output: The cyclotomic p-adic height $\langle y_{K,f}, y_{K,f}\rangle_v$ over K of $y_{K,f} \in J_0(N)(K)\otimes E_f$.

1. Compute $\frac{d}{dT}L_{p,\mathrm{MTT}}(f,T)\big|_{T=0}$ using overconvergent modular symbols [PS11].
2. Compute $L(f^\varepsilon,1)$ using Dokchitser's algorithms [Dok04].
3. Compute Ω_f^+ using Algorithm 4.0.9 (normalized according to Sage).
4. Compute $\|f\|$, for example, using [Col18].
5. Return $\frac{\Omega_f^+\sqrt{|D|}}{8\pi^2\|f\|}\cdot\left(1-\frac{1}{\alpha_p(f)}\right)^{-2}\cdot L(f^\varepsilon,1)\cdot\frac{d}{dT}L_{p,\mathrm{MTT}}(f,T)\big|_{T=0}\log(1+p)$.

Remark 4.0.8. It appears that the convention of the sign of the height in Perrin-Riou differs from the convention chosen in Mazur–Tate–Teitelbaum and Pollack–Stevens. To achieve the correct normalization for p-adic BSD we negate the sign of the height returned by Algorithm 4.0.7.

To compute the quantity Ω_f^+ we exploit the relationship [MTT86, I §8 (8.6)] between f and quadratic twists of f by fundamental discriminants $D' > 0$. Let $\tau(\chi)$ denote the Gauss sum

$$\tau(\chi) := \sum_{a \mod D'} \chi(a) e^{2\pi i a/D'}. \tag{4.12}$$

Since D' is a fundamental discriminant, $\tau(\chi) = \sqrt{D'}$.

Before we state the formula we need, we establish some background on modular symbols, following [PS11, Pol14]. Write $\Delta_0 := \mathrm{Div}^0(\mathbf{P}^1(\mathbf{Q}))$. We can act on Δ_0 by elements of $\Gamma_0(N)$ via fractional linear transformation. Via this action, we can act on the the set of additive homomorphisms $\mathrm{Hom}(\Delta_0, \mathbf{C})$ has an action

$$\varphi|\gamma := \varphi(\gamma E)$$

where $\varphi \in \mathrm{Hom}(\Delta_0, \mathbf{C})$, $E \in \Delta_0$, and $\gamma \in \Gamma_0(N)$. The **C-valued modular symbols** are those symbols that are invariant under the action of all $\gamma \in \Gamma_0(N)$, i.e. $\varphi|\gamma = \varphi$. We denote the space of these symbols as $\mathrm{Symb}_\Gamma(\mathbf{C})$.

For example, for any weight 2 newform g there exists a $\mathbf{C}$-valued modular symbol $\psi_g \in \mathrm{Symb}_\Gamma(\mathbf{C})$ given by

$$\{s\} - \{r\} \mapsto 2\pi i \int_r^s g(z)dz.$$

In this context, $\{s\} - \{r\}$ denotes the divisor with support $+1$ on $s \in \mathbf{Q}$ and -1 on $r \in \mathbf{Q}$. This symbol encodes information about the twisted L-values of g.

To determine the symbol ψ_g inside $\mathrm{Symb}_\Gamma(\mathbf{C})$ we use the action of the Hecke

operators. There is a 2-dimensional subspace of $\mathrm{Symb}_\Gamma(\mathbf{C})$ where the action of Hecke is equal to the eigenvalues of g. The set $\mathrm{Hom}(\Delta_0, \mathbf{C})$ has an involution given by

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

and so ψ_g can be decomposed as a sum of modular symbols $\psi_g = \psi_g^+ + \psi_g^-$. There exist complex numbers Ω_g^+ and Ω_g^+ such that $\varphi_g^+ := \psi_g^+/\Omega_g^+$ and $\varphi_g^- := \psi_g^-/\Omega_g^-$ take values in E_g (see [Shi77, Theorem 2.1] or [BMS16, Theorem 2.2]).

The period Ω_g^+ is only well-defined up to an element of $\overline{\mathbf{Q}}$ that is a unit in $\mathbf{Q}_p$. In practice, to evaluate the symbol $\psi_g^\pm$ and therefore the p-adic L-values of g, Sage makes a random choice of generator in the Hecke-eigenspace of $\mathrm{Hom}(\Delta_0, \mathbf{C})^\pm$ corresponding to g [Ste00, Section 3.5.3]. However, when the characteristic polynomial of T_2 acting on the plus modular symbols space associated to g is irreducible, the algorithm is deterministic.

By [MTT86, I §8 (8.6)] we can write the following relationship between modular forms and modular symbols

$$\frac{L(f^\chi, 1)}{\Omega_f^+} = \frac{\tau(\chi)}{D'} \sum_{\substack{a=1 \\ \gcd(a,D')=1}}^{\lfloor D'/2 \rfloor} \chi(a)(\varphi_f^+(\{a\} - \{D'\}) + \varphi_f^+(\{-a\} - \{D'\})). \tag{4.13}$$

We then evaluate the modular symbols φ_f^+ in Sage. If f^χ is rank 0, the sum will be non-zero. This leads to the following algorithm for extracting the choice of Ω_f^+ that Sage uses to evaluate φ_f^+.

Algorithm 4.0.9 (The plus period, as normalized in Sage).

Input:

- p a prime
- $f \in S_2(\Gamma_0(N))$ newform with coefficients in E_f and an embedding $e : E_f \to \mathbf{Q}_p$ such that f is ordinary in e

Output: The period Ω_f^+ (as normalized in Sage)

1. Set $D' := 5$.
2. Compute the right hand side of (4.13) by evaluating the modular symbols and set R equal to this value.
3. If R is equal to 0, set D' to the next largest fundamental discriminant, and go back to Step (2).
4. Compute $L(f^\chi, 1)$ using Dokchitser's algorithms [Dok04].
5. Return $R/L(f^\chi, 1)$.

Remark 4.0.10. When f is the modular form associated to an elliptic curve, we can take Ω_f^+ to be the real period of the elliptic curve Ω_E^+. This can be approximated using [Coh93, Algorithm 7.4.7]

Example 4.0.11. Let f be the modular form associated to the elliptic curve with LMFDB label `61.a1` and $p = 5$ a prime of good ordinary reduction. Let $\pi_E : X_0(61) \to E$ denote the modular parametrization. Choose $D = -19$ a Heegner discriminant for E. Then the p-adic L-series expansion for $E/\mathbf{Q}$ can be computed using [PS11]

$$\begin{aligned} &L_{p,\mathrm{MTT}}(f, T) = \\ &O(5^{10}) + (1 + 2 \cdot 5^2 + 5^3 + 5^4 + 3 \cdot 5^5 + 2 \cdot 5^7 + O(5^8)) \cdot T \\ &+ (1 + 4 \cdot 5 + 3 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + 5^5 + O(5^6)) \cdot T^2 + O(T^3). \end{aligned}$$

We also compute:

$$\log_p(1 + p) = 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 5^6 + 4 \cdot 5^7 + O(5^8).$$

Using the interpolation property, we have $v_{\mathbf{Q}}(L_{p,\mathrm{MTT}}(f^\varepsilon)) = \left(1 - \frac{1}{\alpha_p}\right)^2 L(f^\varepsilon, 1)/\Omega_{f^\varepsilon}^+$ and we can evaluate

$$L(f^\varepsilon, 1)/\Omega_{f^\varepsilon}^+ = 2 \tag{4.14}$$

while

$$\left(1 - \frac{1}{\alpha_p}\right)^2 = 4 + 2 \cdot 5 + 4 \cdot 5^3 + 2 \cdot 5^4 + 5^5 + 5^6 + 2 \cdot 5^7 + 3 \cdot 5^8 + 2 \cdot 5^9 + O(5^{10}).$$

Finally, by [Cre95, Proposition 1], we have $\Omega_f = 2 \deg \pi_E \cdot \operatorname{Vol} E$, so

$$\left(\frac{\Omega_f^+ \Omega_{f^\varepsilon}^+ \sqrt{|D|} \deg \pi_E}{\Omega_f} \right) = \left(\frac{\Omega_f^+ \Omega_{f^\varepsilon}^+ \sqrt{|D|}}{2 \operatorname{Vol} E} \right) = 1.$$

Altogether, we evaluate the following formula for the (global) p-adic height of $\pi_E(y_{K,f})$:

$$\begin{aligned}
&\frac{1}{2}\langle \pi_E(y_{K,f}), \pi_E(y_{K,f}) \rangle_v = \langle \pi_E(y_{K,f}), \pi_E(y_{K,f}) \rangle_{v_{\mathbf{Q}}} = h(\pi_E(y_{K,f})) \\
&= \left(\frac{\Omega_f^+ \Omega_{f^\varepsilon}^+ \sqrt{|D|}}{2 \operatorname{Vol} E} \right) \left(1 - \frac{1}{\alpha_p} \right)^{-2} \frac{L(f^\varepsilon, 1)}{\Omega_{f^\varepsilon}^+} \frac{d}{dT} L_{p,\mathrm{MTT}}(f, T) \Big|_{T=0} \log_p(1+p) \\
&= 4 \cdot 5 + 4 \cdot 5^2 + 2 \cdot 5^3 + 5^4 + 4 \cdot 5^5 + 5^6 + 2 \cdot 5^7 + 4 \cdot 5^8 + O(5^9).
\end{aligned}$$

Since f has analytic rank 1, by Gross–Zagier–Kolyvagin the rank of $E(\mathbf{Q})$ is one and the trace of the f-isotypical component of the Heegner cycle found here generates $E(\mathbf{Q})$ up to finite index.

Example 4.0.12. Let $p = 11$ and $D = -19$. Let f and f^σ be the modular forms in the newform orbit `73.2.a.b` given by

$$\begin{aligned}
f &= q + (-\nu - 1)q^2 + (\nu - 2)q^3 + 3\nu q^4 + (-\nu - 1)q^5 + q^6 - 3q^7 + O(q^8) \\
f^\sigma &= q + (\nu - 2)q^2 + (-\nu - 1)q^3 + (-3\nu + 3)q^4 + (\nu - 2)q^5 + q^6 - 3q^7 + O(q^8).
\end{aligned}$$

This has coefficient field $E_f = \mathbf{Q}(\nu)$ where ν has minimal polynomial $\nu^2 - \nu - 1$. Then $\{f dq/q, f^\sigma dq/q\}$ is a basis for the holomorphic differential forms of the modular curve $X_0(73)^+$. Fix the embedding

$$\begin{aligned}
e : E_f &\to \mathbf{Q}_p \\
\nu &\mapsto 8 + 7 \cdot 11 + 10 \cdot 11^2 + 7 \cdot 11^3 + 5 \cdot 11^4 + 4 \cdot 11^5 + O(11^6).
\end{aligned} \tag{4.15}$$

By computing the derivatives of the p-adic L-functions in Sage, we get the values

$$\begin{aligned}
&\frac{d}{dT} L_{p,\mathrm{MTT}}(f, T) \Big|_{T=0} = \\
&7 + 7 \cdot 11 + 2 \cdot 11^2 + 9 \cdot 11^3 + 4 \cdot 11^4 + 6 \cdot 11^5 + 3 \cdot 11^6 + 10 \cdot 11^8 + O(11^9)
\end{aligned} \tag{4.16}$$

and

$$\frac{d}{dT}L_{p,\mathrm{MTT}}(f^\sigma,T)\Big|_{T=0} = \tag{4.17}$$
$$2+5\cdot 11+6\cdot 11^2+3\cdot 11^3+8\cdot 11^4+7\cdot 11^5+5\cdot 11^6+O(11^9).$$

We have that $a_p(f)=\nu-2$ and $a_p(f^\sigma)=-\nu-1$. Using the embedding above, we have

$$\alpha_p(f)=6+5\cdot 11+10\cdot 11^2+5\cdot 11^3+7\cdot 11^4+10\cdot 11^5+O(11^6) \tag{4.18}$$

and

$$\alpha_p(f^\sigma)=2+8\cdot 11+7\cdot 11^2+10\cdot 11^3+5\cdot 11^4+9\cdot 11^5+O(11^6). \tag{4.19}$$

It is easy to compute $\log_p(1+p)$. It remains to compute the twisted L-value and the periods. We fix a complex embedding given by

$$\begin{aligned} e_c : E_f &\to \mathbf{C} \\ \nu &\mapsto 1.618033988749894848204586834 4. \end{aligned} \tag{4.20}$$

We can compute the Petersson norm of f and f^σ using (4.20). We get

$$\|f\| = 0.986763670300520172786668613591471383226644464936 98$$

and

$$\|f^\sigma\| = 0.368434065439145662313004808733615200728772025804 07.$$

Changing the complex embedding would swap the values of the norms.

Using Dokchitser's package for computing values of L-functions we now compute $L(f^\varepsilon,1)$ where ε is the quadratic character twisting by $D=-19$ (of conductor 19). Then f^ε is a modular form of level $\gcd(N,19^2)=73\cdot 19^2$. In Magma, we can create an L-series by specifying the gamma factors, weight, and level, as well as around 8000 of the local factors. The gamma parameters are $[0,1]$, weight is 2, dimension is 2, and $N=73\cdot 19^2$. This yields

$$L(f^\epsilon,1) = 4.771908418763801343640052622 88$$

where we have fixed the embedding e_c.

Finally, we compute Ω_f^+. For $D' = 5$ we find that the right hand side of (4.13) is $-4/\sqrt{5}$. We compute

$$L(f^\chi, 1) = 6.346830432177527464345151973 23.$$

Therefore

$$\Omega_f^+ = 3.547986072003329999229678641 2.$$

Combining the complex terms, we find

$$\frac{\Omega_f^+ L(f^\varepsilon, 1)\sqrt{|D|}}{\Omega_f} = 0.947213595499957939281834733 75.$$

This appears to have minimal polynomial $20x^2 - 20x + 1$, and so belong to E_f. In fact, it seems to be $e_c(r_1)$ where $r_1 := 2/5\nu + 3/10$.

For f^σ we get

$$L(f^{\sigma\varepsilon}, 1) = 0.207510534959807400659573747986$$

and

$$\Omega_{f^\sigma}^+ = (3.036893980578977101558866855 15)/(-4/\sqrt{5}).$$

So in total we have

$$\frac{\Omega_{f^\sigma}^+ L(f^{\sigma\varepsilon}, 1)\sqrt{|D|}}{\Omega_{f^\sigma}} = 0.052786404500042060718165266254.$$

This also appears to have minimal polynomial equal to $20x^2 - 20x + 1$ and is $e_c(r_2)$ where $r_2 := -2/5\nu + 7/10$.

Then

$$e(r_1) = 9 + 10 \cdot 11 + 2 \cdot 11^3 + 11^4 + 5 \cdot 11^5 + 4 \cdot 11^6 + 9 \cdot 11^7 + O(11^9).$$

Then we use the values $e(r_1)$, (4.16), and (4.18) in the equation (4.11) to obtain the height of $y_{K,f} \in J_0(N)(K)$. To project $\pi : J_0(73) \to J_0(73)^+$, we multiply by the degree of the quotient map $X_0(73) \to X_0(73)^+$ which is 2.

$$\langle \pi(y_{K,f}), \pi(y_{K,f}) \rangle_v = \tag{4.21}$$

$$3 \cdot 11 + 8 \cdot 11^2 + 11^3 + 4 \cdot 11^5 + 9 \cdot 11^6 + 7 \cdot 11^7 + 3 \cdot 11^8 + O(11^{10})$$

Recall that $v \in \mathrm{Gal}(K/\mathbf{Q})$ and we would like to compute the height over $\mathbf{Q}$ of $\pi(y_{K,f})$ in $J_0(N)^+(\mathbf{Q})$ as in Corollary 4.0.5. Let $\sigma \in \mathrm{Gal}(\mathbf{Q}(\nu)/\mathbf{Q})$ be the nontrivial automorphism. We can compute $\langle \pi(y_{K,f^\sigma}), \pi(y_{K,f^\sigma}) \rangle_v$ by plugging the terms $e(r_2)$, (4.17), and (4.19) for f^σ into (4.11). We have

$$\langle \pi(y_{K,f^\sigma}), \pi(y_{K,f^\sigma}) \rangle_v = \tag{4.22}$$
$$9 \cdot 11 + 9 \cdot 11^2 + 10 \cdot 11^3 + 11^5 + 7 \cdot 11^6 + 4 \cdot 11^7 + 4 \cdot 11^8 + 4 \cdot 11^9 + O(11^{10}).$$

Summing (4.21) and (4.22) and dividing by 2 (which cancels with $\deg(\phi)$), we obtain the height over $\mathbf{Q}$:

$$\langle \pi(y_{K,f}), \pi(y_{K,f}) \rangle_{v_{\mathbf{Q}}} = \tag{4.23}$$
$$11 + 7 \cdot 11^2 + 11^3 + 11^4 + 5 \cdot 11^5 + 5 \cdot 11^6 + 11^7 + 8 \cdot 11^8 + 4 \cdot 11^9 + O(11^{10}).$$

Chapter 5

Quadratic Chabauty

Quadratic Chabauty [BD18, BD21] is a recent advance in the study of rational points; it allows us to compute a finite set of p-adic points containing $X(\mathbf{Q})$ in some cases when the rank of J is greater than or equal to the genus of X.

For this chapter we assume the following hypotheses. Assume:

$$X \text{ is a smooth projective geometrically integral curve defined over } \mathbf{Q} \text{ of genus } g > 0; \tag{H12}$$

$$X(\mathbf{Q}) \neq \emptyset \text{ and fix a basepoint } b \in X(\mathbf{Q}); \tag{H13}$$

$$J(\mathbf{Q}) \text{ has rank } r = g \text{ and, if } g > 1 \text{ then } J \text{ has Néron–Severi rank } \rho(J) > 1; \tag{H14}$$

$$\text{and } p \text{ is a prime of good reduction for } X \text{ such that } \log\colon J(\mathbf{Q}) \otimes \mathbf{Q}_p \to H^0(J_{\mathbf{Q}_p}\Omega^1)^\vee \text{ is an isomorphism.} \tag{H15}$$

So that we can explicitly relate the height on $J_0(N)$ to the height on the quotient:

$$\text{either } f \text{ is a newform with rational Fourier coefficients, in which case } A_f \text{ is an elliptic curve; otherwise we assume that } X_0(N) \to X \text{ is an Atkin–Lehner quotient, such that the Jacobian } J_f \text{ of } X \text{ is a } \mathbf{Q}\text{-simple quotient of } J_0(N)^{\mathrm{new}} \text{ associated to } f \text{ via } (\dagger). \tag{H16}$$

The Chabauty–Coleman method considers the case where $r' := \dim \overline{J(\mathbf{Q})}$ is less than g and so (H15) fails (usually we simply check $r < g$, which suffices since $r' \leq r$). If

the logarithm is not an isomorphism then by fixing a basis $\omega_1, \ldots, \omega_g$ for $H^0(X_{\mathbf{Q}_p}, \Omega^1)$, there is a nontrivial linear relation between the functionals $\lambda_i : D \mapsto \log_{\omega_i}(D)$ on $J(\mathbf{Q})$. Write $\sum_i \alpha_i \lambda_i = 0$ for the linear relation. Consider $\lambda_i : x \mapsto \log_{\omega_i}(x - b)$ as a functional on $X(\mathbf{Q}_p)$. Since the map $\lambda = (\lambda_1, \ldots, \lambda_g) : X(\mathbf{Q}_p) \to \mathbf{Q}_p^g$ has Zariski dense image in each residue disk [Kim09, Theorem 1], the linear relation on $X(\mathbf{Q})$ does not extend to all $X(\mathbf{Q}_p)$. Furthermore λ is given by convergent power series in each residue disk, and so $X(\mathbf{Q})$ is contained in the finite set $\{z \in X(\mathbf{Q}_p) : \sum_i \alpha_i \lambda_i(z - b) = 0\}$.

Quadratic Chabauty uses local and global p-adic height functions to construct a quadratic Chabauty function, which plays the same role that the linear relations $\sum_i \alpha_i \lambda_i(z - b)$ play in the Chabauty–Coleman method. We will denote the cyclotomic global height on $y \in J(\mathbf{Q})$ by $h(y) := \langle y, y \rangle_{v_{\mathbf{Q}}}$ when the field of definition and choice of idèle class character is clear. Otherwise we will use the notation in Chapter 4.

First, we describe the strategy of quadratic Chabauty for integral points on affine elliptic and hyperelliptic curves of odd degree $X/\mathbf{Q}$ [BBM16]. Let b be the point at infinity. Recall that the local height h_p depends on a choice of tangent vectors for points in the common support; to construct $\rho(z)$ one makes a specific choice of tangent vector [BBM16, p.5]. Consider the function $\rho(z) := h(z - b) - h_p(z - b)$ on $X(\mathbf{Q})$. The global p-adic height decomposes into a sum of local heights $h = \sum_v h_v$ over finite primes v, so $\rho(z)$ has the same value as the sum $\sum_{v \neq p} h_v(z - b)$ on $X(\mathbf{Q})$. Then we can write $\rho(z)$ as a locally analytic function on $X(\mathbf{Q}_p) - \{b\}$ [BBM16] which we will explain in the next paragraph. Furthermore, $\rho(z - b)$ takes on only finitely many values in $\mathbf{Q}_p$. These local heights $h_v(z - b)$ for $v \neq p$ can be defined in terms of intersection theory on a regular model $\mathcal{X}_{\mathbf{Z}_v}$ of $X_{\mathbf{Q}_v}$. In particular h_v factors through the reduction map to the special fiber of $\mathcal{X}_{\mathbf{Z}_v}$ and the image of h_v in $\mathbf{Q}_p$ is a finite set of values $S \subset \mathbf{Q}_p$ which is simply $\{0\}$ when v is a prime of good reduction [BBM16,

Lemma 2.4]. Then, we can solve for

$$\rho(z) = s$$

for each $s \in S$ by expanding ρ as a power series in each residue disk of X. This equation $\rho(z) = s$ has only finitely many zeros.

We now explain how to write $\rho(z)$ as a locally analytic function. First, we can realize $h_p(z-b)$ as a double Coleman integral from a tangential basepoint at b [BBM16, Theorem 2.2], which shows that $h_p(z-b)$ is locally analytic. The key technical input is Besser's p-adic Arakelov theory [Bes05]. Then, since the height pairing $h(D,E)$ is a bilinear form on $J(\mathbf{Q}) \otimes \mathbf{Q}_p$, we can write it in terms of a basis of bilinear forms on $J(\mathbf{Q}) \otimes \mathbf{Q}_p$. We fix a basis $\{\omega_1, \ldots, \omega_g\}$ for $H^0(X_{\mathbf{Q}_p}, \Omega^1)$. The bilinear forms

$$g_{ij}(D,E) := \frac{1}{2}(\log_{\omega_i}(D)\log_{\omega_j}(E) + \log_{\omega_j}(D)\log_{\omega_i}(E)) \tag{5.1}$$

are locally analytic. The key idea for writing $h(z-b)$ as a locally analytic function is to express

$$h = \sum_{ij} \alpha_{ij} g_{ij} \tag{5.2}$$

for some $\alpha_{ij} \in \mathbf{Q}_p$. We can compute α_{ij} by evaluating h and the g_{ij} on r independent points of $J(\mathbf{Q})$. This expression (5.2) holds when restricted to the pullback $h(z-b) = h(z-b, z-b)$ on $X(\mathbf{Q}) \otimes \mathbf{Q}_p$. Therefore $\rho(z)$ is locally analytic when $z \neq b$.

In Section 5.1 we discuss how to adapt this in the case of a rank 1 elliptic curve E and decompose the height as in (5.2) without knowing any infinite order point of $E(\mathbf{Q})$. Together with the computation of the Kodaira symbols, which determine the values of h_v at primes v of bad reduction, this yields a finite computable set containing the integral points of E.

Remark 5.0.1. Generally, quadratic Chabauty is not the most efficient method for

finding integral points on a given rank 1 elliptic curve. For example, given an infinite order point on E, one can use linear forms in logarithms [Sma94]. We view this case as a sandbox for our methods for higher genus curves.

In Section 5.2 we give the construction of the quadratic Chabauty function $\rho(z)$ on Atkin–Lehner quotients X of $X_0(N)$ with simple Jacobians J_f arising as quotients of $J_0(N)^{\text{new}}$. The local height functions h_v do not immediately extend to functions on $X(\mathbf{Q}_v)$; more sophisticated heights machinery is needed to deal with this case. By associating points on X with Galois representations, we can define $\rho(z) = h(z) - h_p(z)$ on $X(\mathbf{Q}_p)$ through Nekovář's theory of p-adic heights as discussed in [Nek93, BD18]. Here, and henceforth we will suppress the basepoint b in our notation. The basepoint b is implicitly used in the association of $z \in X(\mathbf{Q}_p)$ to the Galois representation input into h and h_v. By exhibiting $h_p(z)$ as the solution to a p-adic differential equation, one can see that $h_p(z)$ is locally analytic.

Similar to the case for integral points, to write $h(z)$ as a locally analytic function $X(\mathbf{Q}_p) \to \mathbf{Q}_p$, we need to write it in a locally analytic basis for $(H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \times H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee)^\vee$. This can again be done by knowing "sufficiently many" rational points [BDM+21, Section 3.2]. If we do not know sufficiently many rational points, we can use the relationship between h and the Coleman–Gross height on J [Bes04]. Then we use the basis of symmetric bilinear pairings (5.1) for $J(\mathbf{Q}) \otimes \mathbf{Q}_p$. This requires knowing $r = g$ independent infinite order points.

In Theorem 5.2.2, we show that it is possible to explicitly compute $\rho(z)$ as a locally analytic function without knowing any infinite order points in the case of Atkin–Lehner quotients with simple Jacobians. This uses the special value formulas from Chapters 3 and 4. Finally, we provide several examples of how to apply Theorem 5.2.2 in practice. We compute a finite set of p-adic points containing the rational points on $X_0(67)^+$ and $X_0(107)^+$ by computing $\rho(z)$ and solving for its zeros. We compute $\rho(z)$ for $X_0^*(85)$ but do not compute the local heights away from p. We also discuss the computation

of $\rho(z)$ for $X_0(73)^+$ and the difficulties with computing one of its associated p-adic L-values.

5.1 Integral points on rank one elliptic curves

In this section we study the case of determining integral points on a rank 1 genus 1 (elliptic) curve E. A consequence of Faltings's theorem is that the affine curve obtained by removing a point $\mathcal{X} := E - \mathcal{O}$ has finitely many integral points $\mathcal{X}(\mathbf{Z})$. Quadratic Chabauty for integral points on rank 1 elliptic curves requires an infinite order point in $E(\mathbf{Q})$. We replace this requirement with the computation of special values of two p-adic L-functions constructed by Perrin-Riou (see Chapter 4) and Bertolini, Darmon, and Prasanna (see Chapter 3) that determine the height and logarithm of a Heegner cycle for E, respectively. This allows us to determine $\mathcal{X}(\mathbf{Z})$ without knowing a rational point of infinite order.

Let E be a rank one elliptic curve over $\mathbf{Q}$ with conductor N given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Fix a prime $p > 2$ of good ordinary reduction. Let $\mathcal{E}/\mathbf{Z}$ denote the minimal regular model of E and $\mathcal{X} = \mathcal{E} - \mathcal{O}$ the complement of the zero section in $\mathcal{E}$. Fix also differentials $\omega_0 = \frac{dx}{2y+a_1x+a_3}$ and $\omega_1 = x\omega_0$.

Let b be a tangential basepoint at the point at infinity or an integral 2-torsion point (see [Bes12, Section 1.5.4] for more on tangential basepoints). Consider the two functions, the double Coleman integral

$$D_2(z) := \int_b^z \omega_0\omega_1 \tag{5.3}$$

as well as the logarithm, which can be expressed as the Coleman integral

$$\log(z) := \int_b^z \omega_0. \tag{5.4}$$

Theorem 5.1.1 ([Kim10, BKK11]). *Suppose E has analytic rank 1 over $\mathbf{Q}$ and Tamagawa product 1. Then $D_2(z)/(\log(z))^2$ is constant on non-torsion integral points of $\mathcal{X}$.*

We sketch a proof of this fact. Since E is rank 1 over $\mathbf{Q}$, the $\mathbf{Z}_p$-module $\mathbf{Z}_p \otimes E(\mathbf{Q})$ is 1-dimensional, and has only a 1-dimensional space of quadratic forms. Both $\log^2$ and h (the global p-adic height) are quadratic forms on this space, therefore there is a constant $\gamma \in \mathbf{Q}_p$ such that $\gamma \log(z)^2 = h(z)$ for all $z \in E(\mathbf{Q})$. The global height decomposes into a sum of local heights $h = \sum_v h_v$. In particular, because E has Tamagawa product one, the local height contributions $h_v(z)$ for $v \neq p$ are 0 on integral points of $\mathcal{X}$. The local height at p on $z \in \mathcal{X}(\mathbf{Z})$ is given by $h_p(z) = 2D_2(z) + c\log(z)^2$, for a specific constant c (see (5.5)). Dividing by $\log(z)^2$, we see $D_2(z)/\log(z)^2$ is constant on $\mathcal{X}(\mathbf{Z})$.

Since D_2 and log are computable [BBK10, Bal13], this gives a viable (if inefficient) method of computing integral points on $\mathcal{X}$.

In quadratic Chabauty for integral points on elliptic curves, Balakrishnan, Besser, and Müller [BB15, BBM17] remove the Tamagawa number 1 hypothesis in Theorem 5.1.1 and give algorithms to compute a finite set of p-adic points containing the integral points. We recall a related theorem.

Suppose that $p > 3$ and let E_2 be the Katz p-adic weight 2 Eisenstein series [Kat76, MST06]. Define the constant

$$c := \frac{a_1^2 + 4a_2 - E_2(E, \omega_0)}{12}. \tag{5.5}$$

Furthermore, let $h : E(\mathbf{Q}) \to \mathbf{Q}_p$ be $2p$ times the (global) p-adic height of [MST06].

The factor of $2p$ is needed to make the BSD conjecture as stated in [MTT86] hold, see [BM, Remark 2.6]. For any non-torsion point $P \in E(\mathbf{Q})$ define γ by

$$\gamma := \frac{h(P)}{\log(P)^2}. \tag{5.6}$$

Remark 5.1.2. The quantity γ does not depend on P. As noted above, the $\mathbf{Z}_p$-module $\mathbf{Z}_p \otimes E(\mathbf{Q})$ is 1-dimensional, and has only a 1-dimensional space of quadratic forms, and $\log(P) \neq 0$ when P is non-torsion.

Theorem 5.1.3 ([Bia20, Theorem 1.7])**.** *Let E be a rank 1 elliptic curve over $\mathbf{Q}$ with good ordinary reduction at p and bad reduction at the primes in a finite set S. There is a computable finite set $W \subset \mathbf{Q}_p$, $W = \prod_{q \in S} W_q$ such that W_q is the possible local height contributions for an integral point at bad places, and W_q is determined by the Kodaira type of the reduction of E at q. For $w \in W$ define $\|w\|$ to be the sum of its elements.*

If E has good reduction at $q = 2$ or $q = 3$, and $\overline{E}(\mathbf{F}_q) = \{\mathcal{O}\}$, or if E has split multiplicative reduction of Kodaira type I_1 at 2, then

$$\mathcal{X}(\mathbf{Z}) = \emptyset.$$

Otherwise,

$$\mathcal{X}(\mathbf{Z}) \subseteq \bigcup_{w \in W} \psi(w),$$

where

$$\psi(w) := \{z \in \mathcal{X}(\mathbf{Z}_p) : 2D_2(z) + c\log(z)^2 + \|w\| = \gamma \log(z)^2\}. \tag{5.7}$$

We describe γ in terms of two different special values of p-adic L-functions associated to $f \in S_2(\Gamma_0(N))$ the cusp form related to E by modularity. This allows us to obtain new input into quadratic Chabauty as described in Theorem 5.1.3, by replacing the γ in (5.7) with one determined by special values of L-functions.

Theorem 5.1.4. *The quantities*

$$\gamma = \frac{\frac{1}{2}\deg \pi_E \left(1 - \frac{1}{\alpha_p}\right)^{-4} \mathcal{L}'_{p,\ell_K}(f,1)}{\left(\frac{1-a_p(f)+p}{p}\right)^{-2} L_p(f,1)} \tag{5.8}$$

are equal whenever $L(f^\varepsilon, 1) \neq 0$. *Furthermore,* γ *is computable.*

In other words $\rho(z) = h_p(z) - \gamma \log(z)^2$ *is a computable locally analytic function from* $\mathcal{X}(\mathbf{Z}_p)$ *to* $\mathbf{Q}_p$ *that takes values on a finite computable set when evaluated on* $\mathcal{X}(\mathbf{Z})$.

Theorem 5.1.4 allows us to determine a finite set of p-adic points of $\mathcal{X}$ containing $\mathcal{X}(\mathbf{Z})$ without knowing an infinite order point of $E(\mathbf{Q})$. The theorem relies on the previous hypotheses on p, f, and N which are collected at the start of Chapters 3 and 4.

Proof. Corollary 4.0.4 shows that

$$\langle \pi_E(y_{K,f}), \pi(y_{K,f}) \rangle_v = \deg \pi_E \mathcal{L}'_{p,\ell_K}(f,1) \left(1 - \frac{1}{(\alpha_p(f))}\right)^{-4}$$

while (3.1) shows $L_p(f,1)\left(\frac{1-a_p(f)+p}{p}\right)^{-2}$ is equal to $(\log_{fdq/q} \pi_E(y_K))^2$. Corollary 4.0.5 implies that

$$\frac{1}{2}\langle \pi_E(y_{K,f}), \pi(y_{K,f}) \rangle_v = h(\pi_E(y_K)).$$

□

Remark 5.1.5. We can also apply these methods to compute a finite set of p-adic points containing the rational points of a genus 2 bielliptic curve $X/\mathbf{Q}$ without knowing any infinite order points on the Jacobian. Let X have Jacobian isogenous to $E_1 \times E_2$. Then we can apply the formula in [BD18, Theorem 1.4] using the γ_1 and γ_2 in Theorem 5.1.4 associated with each E_i as input.

Example 5.1.6. Let E be the elliptic curve with LMFDB label `43.a1` and consider $p = 11$ a prime of good ordinary reduction. We choose $D = -7$ a Heegner discriminant for E in which p and $N = 43$ split. Fix a model for E

$$\mathcal{X} : y^2 + y = x^3 + x^2.$$

As in Examples 4.0.11 and 3.2.5, we compute the constant γ:

$$\gamma = \frac{h(\pi_E(y_{K,f}))}{\log(\pi_E(y_{K,f}))^2}$$

$$
\begin{aligned}
&= \frac{\mathcal{L}'_{p,\ell_K}(f,1)\left(\frac{1}{2}\right)\left(1-\frac{1}{\alpha_p}\right)^{-4}\deg\pi_E}{L_p(f,1)\left(\frac{1-a_p(f)+p}{p}\right)^{-2}} \\
&= \frac{9\cdot 11+5\cdot 11^2+5\cdot 11^3+3\cdot 11^4+7\cdot 11^6+4\cdot 11^7+4\cdot 11^8+O(11^9)}{11^2+8\cdot 11^3+9\cdot 11^4+6\cdot 11^5+8\cdot 11^6+6\cdot 11^7+4\cdot 11^8+4\cdot 11^9+O(11^{10})} \\
&= 9\cdot 11^{-1}+10+2\cdot 11+4\cdot 11^2+5\cdot 11^4+8\cdot 11^5+10\cdot 11^6+O(11^7).
\end{aligned}
$$

We proceed to solve the equations described by (5.7). The only prime of bad reduction for E is 43, and the Kodaira type of E over 43 is I_1 so $W=\{0\}$, and so $\mathcal{X}(\mathbf{Z})\subset\{h_p(z)=\gamma\log(z)^2\}$. Using a modified version of the code associated to [Bia20], we obtain the finite set:

$$
\begin{aligned}
&\{(-1,-1),(-1,0),(0,-1),(0,0),(1,-2),(1,1),(2,-4),(2,3),(21,-99),(21,98),\\
&(10\cdot 11+7\cdot 11^2+O(11^3),10+10\cdot 11+9\cdot 11^2+5\cdot 11^3+O(11^4)),\\
&(10\cdot 11+7\cdot 11^2+O(11^3),11^2+5\cdot 11^3+O(11^4)),\\
&(1+6\cdot 11+2\cdot 11^2+O(11^3),9+3\cdot 11^2+O(11^3)),\\
&(1+6\cdot 11+2\cdot 11^2+O(11^3),1+10\cdot 11+7\cdot 11^2+O(11^3)),\\
&(2+9\cdot 11+7\cdot 11^2+O(11^3),3+8\cdot 11+11^2+O(11^3)),\\
&(2+9\cdot 11+7\cdot 11^2+O(11^3),7+2\cdot 11+9\cdot 11^2+O(11^3))\}.
\end{aligned}
$$

This contains the 10 integral points on $\mathcal{X}$ as well as 3 pairs of $\mathbf{Z}_{11}$-points conjugate under the hyperelliptic involution.

Example 5.1.7. Let E be the elliptic curve with LMFDB label 83.a1 and $p=11$ a prime of good ordinary reduction. We choose $D=-19$ a Heegner discriminant for E in which p and $N=83$ split. Fix a model for E

$$\mathcal{X}: y^2+xy+y=x^3+x^2+x.$$

Using the methods described in previous sections, we compute the constant γ:

$$
\begin{aligned}
\gamma &= \frac{h(\pi_E(y_{K,f}))}{\log(\pi_E(y_{K,f}))^2} \\
&= \frac{\mathcal{L}'_{p,\ell_K}(f,1)\left(1-\frac{1}{\alpha_p}\right)^{-4}\frac{1}{2}\deg\pi_E}{L_p(f,1)\left(\frac{1-a_p(f)+p}{p}\right)^{-2}}
\end{aligned}
$$

$$= \frac{9 \cdot 11 + 10 \cdot 11^2 + 7 \cdot 11^3 + 3 \cdot 11^4 + 8 \cdot 11^5 + 4 \cdot 11^6 + 4 \cdot 11^7 + 7 \cdot 11^8 + O(11^9)}{9 \cdot 11^2 + 3 \cdot 11^4 + 6 \cdot 11^5 + 11^6 + 9 \cdot 11^7 + 6 \cdot 11^8 + 6 \cdot 11^9 + 11^{10} + O(11^{11})}$$
$$= 11^{-1} + 6 + 5 \cdot 11^2 + 11^3 + 4 \cdot 11^4 + 9 \cdot 11^5 + 4 \cdot 11^6 + O(11^7).$$

We proceed to solve the equations described by (5.7). The only prime of bad reduction for E is 83, and the Kodaira type of E over 83 is I_1 so $W = \{0\}$, and so $\mathcal{X}(\mathbf{Z}) \subset \{h_p(z) = \gamma \log(z)^2\}$. Using a modified version of the code associated to [Bia20], we obtain the finite set:

$$\{(0,-1),(0,0),(1,-3),(1,1),(4,-12),(4,7)$$
$$(6 + 9 \cdot 11 + 6 \cdot 11^2 + O(11^3), 10 + 10 \cdot 11 + 5 \cdot 11^2 + O(11^3)),$$
$$(6 + 9 \cdot 11 + 6 \cdot 11^2 + O(11^3), 5 + 11 + 9 \cdot 11^2 + O(11^3)),$$
$$(6 + 10 \cdot 11 + 6 \cdot 11^2 + O(11^3), 10 + 8 \cdot 11 + 8 \cdot 11^2 + O(11^3)),$$
$$(6 + 10 \cdot 11 + 6 \cdot 11^2 + O(11^3), 5 + 2 \cdot 11 + 6 \cdot 11^2 + O(11^3)),$$
$$(5 \cdot 11 + 2 \cdot 11^2 + O(11^3), 5 \cdot 11 + 10 \cdot 11^2 + O(11^3))),$$
$$(5 \cdot 11 + 2 \cdot 11^2 + O(11^3), 10 + 9 \cdot 11^2 + O(11^3)),$$
$$(4 + 4 \cdot 11 + 7 \cdot 11^2 + O(11^3), 10 + 2 \cdot 11 + 3 \cdot 11^2 + O(11^3)),$$
$$(4 + 4 \cdot 11 + 7 \cdot 11^2 + O(11^3), 7 + 3 \cdot 11 + O(11^3)),$$
$$(1 + 5 \cdot 11 + 7 \cdot 11^2 + O(11^3), 1 + 9 \cdot 11 + 2 \cdot 11^2 + O(11^3)),$$
$$(1 + 5 \cdot 11 + 7 \cdot 11^2 + O(11^3), 8 + 7 \cdot 11 + O(11^3))\}.$$

This contains the 6 integral points on $\mathcal{X}$ as well as 5 pairs of $\mathbf{Z}_{11}$-points conjugate under the hyperelliptic involution.

Example 5.1.8. Let E be the elliptic curve with LMFDB label `131.a1` and $p = 7$ a prime of good ordinary reduction. This is a model for $X_0^+(131)$. We choose $D = -19$ a Heegner discriminant for E in which p and $N = 131$ split. Fix a model for E

$$\mathcal{X} : y^2 + y = x^3 - x^2 + x.$$

Using the methods described in previous sections, we compute the constant γ:

$$\gamma = \frac{h(\pi_E(y_{K,f}))}{\log(\pi_E(y_{K,f}))^2}$$

$$
\begin{aligned}
&= \frac{\mathcal{L}'_{p,\ell_K}(f,1)\left(\frac{1}{2}\right)\left(1-\frac{1}{\alpha_p}\right)^{-4}\deg\pi_E}{L_p(f,1)\left(\frac{1-a_p(f)+p}{p}\right)^{-2}} \\
&= \frac{4\cdot 7+5\cdot 7^2+7^3+3\cdot 7^5+3\cdot 7^6+2\cdot 7^7+3\cdot 7^8+7^9+2\cdot 7^{10}+O(7^{11})}{2\cdot 7^2+2\cdot 7^3+2\cdot 7^4+4\cdot 7^6+6\cdot 7^7+7^9+4\cdot 7^{10}+5\cdot 7^{11}+4\cdot 7^{12}+O(7^{13})} \\
&= 2\cdot 7^{-1}+4+7+7^2+5\cdot 7^3+7^4+6\cdot 7^5+2\cdot 7^6+6\cdot 7^7+3\cdot 7^8+O(7^{10}).
\end{aligned}
$$

We proceed to solve the equations described by (5.7). The only prime of bad reduction for E is 131, and the Kodaira type of E over 131 is I_1 so $W=\{0\}$, and so $\mathcal{X}(\mathbf{Z})\subset\{h_p(z)=\gamma\log(z)^2\}$. Using a modified version of the code associated to [Bia20], we obtain the finite set:

$$
\begin{aligned}
&\{(0,-1),(0,0),(2,-3),(2,2),\\
&(5+6\cdot 7+4\cdot 7^2+3\cdot 7^4+7^5+O(7^6),6+7+3\cdot 7^2+2\cdot 7^5+O(7^6)),\\
&(5+6\cdot 7+4\cdot 7^2+3\cdot 7^4+7^5+O(7^6),5\cdot 7+3\cdot 7^2+6\cdot 7^3+6\cdot 7^4+4\cdot 7^5+O(7^6)),\\
&(5+4\cdot 7+6\cdot 7^2+7^3+5\cdot 7^5+O(7^6),6\cdot 7+2\cdot 7^3+6\cdot 7^4+6\cdot 7^5+O(7^6)),\\
&(5+4\cdot 7+6\cdot 7^2+7^3+O(7^6),6+6\cdot 7^2+4\cdot 7^3+O(7^6)),\\
&(4\cdot 7+6\cdot 7^2+2\cdot 7^3+2\cdot 7^4+O(7^5),4\cdot 7+2\cdot 7^2+5\cdot 7^3+4\cdot 7^4+O(7^5)),\\
&(4\cdot 7+6\cdot 7^2+2\cdot 7^3+2\cdot 7^4+O(7^5),6+2\cdot 7+4\cdot 7^2+7^3+2\cdot 7^4+O(7^5)),\\
&(2+2\cdot 7^3+O(7^4),2+5\cdot 7^3+O(7^4)),\\
&(2+2\cdot 7^3+O(7^4),4+6\cdot 7+6\cdot 7^2+7^3+O(7^4))\}.
\end{aligned}
$$

This contains the 4 integral points on $\mathcal{X}$ as well as 4 pairs of $\mathbf{Z}_7$-points conjugate under the hyperelliptic involution.

5.2 Rational points on higher genus curves

We now discuss how to extend the results of the previous section to construct functions that pick out rational points on higher genus curves.

Nekovář's theory of p-adic heights allows us to compute p-adic heights of Galois representations of geometric origin, giving a more general setting for p-adic heights. This enables us extend the height h to a height on $X(\mathbf{Q}_p)$ such that the height on $X(\mathbf{Q})$

decomposes as a sum of local heights h_v. Since we will not rely on any technical details used to construct or compute Nekovář heights, we refer the reader to [BD18, BD21] for more details, as well as the overview in [BDM+21]. This global height h can be written in terms of a basis of bilinear pairings

$$H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \otimes H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \to \mathbf{Q}_p.$$

The following theorem is the analog of Theorem 5.1.3.

Theorem 5.2.1 ([BD18, Proposition 5.5])**.** *Let $\psi_1, \dots, \psi_M$ be a basis for $(H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \otimes H^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee)^\vee$. There are finite computable constants $\alpha_1, \dots, \alpha_M \in \mathbf{Q}_p$ such that the function $X(\mathbf{Q}_p) \to \mathbf{Q}_p$ given by*

$$\rho(z) := \sum_{i=1}^{M} \alpha_i \psi_i(z) - h_p(z)$$

is a locally analytic function. Furthermore, there exists a finite set $S \subset \mathbf{Q}_p$ such that $\{\rho(x) \in S : x \in X(\mathbf{Q}_p)\}$ contains $X(\mathbf{Q})$.

The set S is given by computing local heights away from p at primes v of bad reduction. For each v, the local height $h_v : X(\mathbf{Q}_v) \to \mathbf{Q}_p$ has finite image [KT08], $h_v(X(\mathbf{Q}_v)) \subset S_v$ where S_v is finite. We can take $S := \{\sum_v s_v : s_v \in S_v\}$. When X has a semistable regular model with irreducible special fibers, then $S = \{0\}$ [BDM+21, Theorem 3.2].

In order to compute the α_i in Theorem 5.2.1, we need to know sufficiently many rational points on X or r independent points on $J(\mathbf{Q})$. We now present a construction of ρ for certain curves with modular Jacobians that does not require knowing rational points on X or J, other than the basepoint b. The theorem relies on the previous hypotheses on p, f, and N which are collected at the start of Chapters 3 and 4. This is the main result of this chapter.

Theorem 5.2.2. *Let $X/\mathbf{Q}$ be an Atkin–Lehner quotient of $X_0(N)$ with $\mathbf{Q}$-simple*

Jacobian J_f, associated to f via (†) for some newform $f \in S_2(\Gamma_0(N))$ of analytic rank 1. Write $\phi : X_0(N) \to X$ for the quotient map.

Let p be a good prime that is ordinary for all f^σ, for $\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})$. Assume p splits in E_f and let e be a choice of embedding $e : E_f \to \mathbf{Q}_p$. Recall that ε is the quadratic character associated with the imaginary quadratic field K.

Define constants

$$\alpha_\sigma := \frac{\frac{1}{2}(\deg(\phi)\mathcal{L}'_{p,\ell_K}(f^\sigma, 1)\left(1 - \frac{1}{e(\alpha_p(f^\sigma))}\right)^{-4}}{L_p(f^\sigma, 1)e(\left(\frac{1-a_p(f^\sigma)+p}{p}\right)^{-2})}$$

for $\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})$. Assume $L(f^\varepsilon, 1) \neq 0$.

The α_σ are computable and for $z \in X(\mathbf{Q})$ we have

$$\sum_{\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})} \alpha_\sigma (\log_{f^\sigma dq/q}(z))^2 = h(z).$$

Hence

$$\rho(z) = \sum_{\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})} \alpha_\sigma (\log_{f^\sigma dq/q}(z))^2 - h_p(z)$$

is a locally analytic function on $X(\mathbf{Q}_p)$ away from b. Furthermore, there exists a finite set $S \subset \mathbf{Q}_p$ such that $\{\rho(x) \in S : x \in X(\mathbf{Q}_p)\}$ contains $X(\mathbf{Q})$.

We give algorithms to compute the numerator and denominator of the constants α_σ appearing in Theorem 5.2.2 in Chapters 4 and 3 respectively.

Proof. Since

$$\{f^\sigma dq/q \text{ for } \sigma \in \mathrm{Gal}(E_f/\mathbf{Q})\}$$

is a basis for $H^0(X_{\mathbf{Q}_p}, \Omega^1)$ the functions

$$\frac{1}{2}(\log_{f^\sigma dq/q}(D)\log_{f^\tau dq/q}(E) + \log_{f^\sigma dq/q}(E)\log_{f^\tau dq/q}(D)) \text{ for } \sigma, \tau \in \mathrm{Gal}(E_f/\mathbf{Q})$$

form a basis for the symmetric bilinear pairings on $J_f(\mathbf{Q}) \otimes \mathbf{Q}_p$ by (H15).

We will show that for $z \in X(\mathbf{Q})$, we have the equality $\rho(z) = h(z) - h_p(z)$, and in

particular

$$\sum_{\sigma\in \mathrm{Gal}(E_f/\mathbf{Q})} \alpha_\sigma (\log_{f^\sigma dq/q}(z))^2 = h(z). \tag{5.9}$$

Let $\pi : J_0(N) \to J_f$ be induced by the pushforward of ϕ. Corollary 4.0.4 shows that

$$\langle \pi(y_{K,f^\sigma}), \pi(y_{K,f^\sigma})\rangle_v = \deg(\phi)\mathcal{L}'_{p,\ell_K}(f^\sigma, 1)\left(1 - \frac{1}{e(\alpha_p(f^\sigma))}\right)^{-4}$$

while (3.1) shows $L_p(f^\sigma, 1)e(\left(\frac{1-a_p(f^\sigma)+p}{p}\right)^{-2})$ is equal to $(\log_{f^\sigma dq/q}\pi(y_K))^2$.

Corollary 4.0.5 implies that

$$\sum_{\sigma\in \mathrm{Gal}(E_f/\mathbf{Q})} \alpha_\sigma (\log_{f^\sigma dq/q}\pi(y_K))^2 = h(\pi(y_K))$$

where $h : J(\mathbf{Q}) \to \mathbf{Q}_p$ is the global p-adic height.

Recall from Section 2.2.2 that $\mathcal{O}_f y_K$ generates a finite index subgroup of $J_f(\mathbf{Q})$. Consider the action of $\mathcal{O}_f$ as through the embedding $e : \mathcal{O}_f \to \mathbf{Q}_p$ so that $\mathcal{O}_f\pi(y_K) \subseteq J_f(\mathbf{Q}) \otimes \mathbf{Q}_p$. The bilinearity of the height implies that for all $C_1, C_2 \in \mathbf{Q}_p$,

$$\langle C_1\pi(y_K), C_2\pi(y_K)\rangle_{v_\mathbf{Q}} = C_1C_2\langle \pi(y_K), \pi(y_K)\rangle_{v_\mathbf{Q}}.$$

Every $D \in J_f(\mathbf{Q})$ can be written as $C\pi(y_K)$ for some $C \in \mathbf{Q}_p$. Therefore, since the logarithm is linear

$$\langle \pi(y_K), \pi(y_K)\rangle_{v_\mathbf{Q}} = \sum_{\sigma\in \mathrm{Gal}(E_f/\mathbf{Q})} \alpha_\sigma \log_{f^\sigma dq/q}(\pi(y_K)) \log_{f^\sigma dq/q}(\pi(y_K))$$

implies that

$$\langle D, E\rangle_{v_\mathbf{Q}} = \sum_{\sigma\in \mathrm{Gal}(E_f/\mathbf{Q})} \alpha_\sigma \log_{f^\sigma dq/q}(D) \log_{f^\sigma dq/q}(E)$$

for all $D, E \in J_f(\mathbf{Q})$. □

Then $\log_{f^\sigma dq/q}(z)$ has a power series expansion in each residue disk, and is locally analytic on $X(\mathbf{Q})$. We can then extend $h(z)$ to a locally analytic function on $x \in X(\mathbf{Q}_p)$ away from b, see for example [BDM+21, Section 3.3.1]). Finally, $h_p(z)$ is the solution to a p-adic differential equation and therefore also locally analytic [BDM+19, Lemma 3.7].

Example 5.2.3. We consider the case of $X_0(67)^+$, a genus 2 rank 2 hyperelliptic curve. Let f and f^σ be the newforms in the orbit 67.2.a.b. Then $E_f = \mathbf{Q}(\nu)$ where ν has minimal polynomial $z^2 - z - 1$. Let f be the newform with the q-expansion

$$f(q) = q + (-\nu - 1)q^2 + (\nu - 2)q^3 + 3\nu q^4 - 3q^5 + q^6 + O(q^7).$$

Let $p = 11$ and $D = -7$. We fix the embedding $e : E_f \to \mathbf{Q}_p$ sending $\nu \mapsto 4 + 3 \cdot 11 + 3 \cdot 11^3 + O(11^4)$.

Using the methods of Chapter 3 we find that

$$\log_{fdq/q}(\pi(y_K))^2 = 3 \cdot 11^2 + 9 \cdot 11^3 + 10 \cdot 11^4 + 4 \cdot 11^5 + 8 \cdot 11^6 + O(11^7),$$
$$\log_{f^\sigma dq/q}(\pi(y_K))^2 = 11^2 + 11^4 + 11^5 + 9 \cdot 11^6 + 6 \cdot 11^7 + O(11^8).$$

There is a Magma implementation of quadratic Chabauty [BMTV]. To specify the function ρ in terms of a basis of symmetric bilinear forms on $J(\mathbf{Q}) \otimes \mathbf{Q}_p$ in Magma, we need to relate the basis of symmetric bilinear forms on $J(\mathbf{Q}) \otimes \mathbf{Q}_p$ back to the coordinates of X. This requires some linear algebra, as we now explain.

Let g_1 and g_2 be a basis of modular forms for $S_2(67)^+_{\text{new}}$ given by

$$g_1(q) := q - 3q^3 - 3q^4 - 3q^5 + q^6 + 4q^7 + 3q^8 + 5q^9 - 3q^{11} + 6q^{12} - 8q^{13} + \cdots$$
$$g_2(q) := q^2 - q^3 - 3q^4 + 3q^7 + 4q^8 + 3q^9 - 3q^{10} - 2q^{11} + 3q^{12} - 3q^{13} + \cdots .$$

We can construct a model X of $X_0(67)^+$ over $\mathbf{Q}$ where under the identification $H^0(X, \Omega^1) \simeq S_2(67)^+_{\text{new}}$, the differential dx/y is g_1 and xdx/y is g_2. This is achieved by letting $x = g_2/g_1$ and $y = qdx/g_1$ and solving for the linear dependence in the monomials $1, x, x^2, \ldots, x^6, y^2$. The resulting model is

$$X : y^2 = h(x) = 9x^6 - 14x^5 + 9x^4 - 6x^3 + 6x^2 - 4x + 1. \tag{5.10}$$

To find fdq/q on this model, we solve for f in terms of g_1 and g_2. We have $f = g_1 - (\nu + 1)g_2$. Therefore

$$fdq/q = \frac{dx}{y} - (\nu + 1)\frac{xdx}{y}. \tag{5.11}$$

Write $A := 1$ and $B := -\nu - 1$.

Using the techniques in Chapter 4 we get that

$$\langle \pi(y_{K,f}), \pi(y_{K,f}) \rangle_v = 2 \cdot 11 + 7 \cdot 11^2 + 4 \cdot 11^3 + 6 \cdot 11^5 + 11^6 + 11^7 + O(11^9)$$
$$\langle \pi(y_{K,f^\sigma}), \pi(y_{K,f^\sigma}) \rangle_v =$$
$$5 \cdot 11 + 10 \cdot 11^3 + 9 \cdot 11^4 + 10 \cdot 11^5 + 3 \cdot 11^6 + 10 \cdot 11^7 + O(11^8)$$

Let

$$\alpha_1 := \frac{\langle \pi(y_{K,f}), \pi(y_{K,f}) \rangle_v}{(\log_{fdq/q} \pi(y_K))^2}$$

and let

$$\alpha_2 := \frac{\langle \pi(y_{K,f^\sigma}), \pi(y_{K,f^\sigma}) \rangle_v}{(\log_{f^\sigma dq/q} \pi(y_K))^2}.$$

Then using linearity of the logarithm and (5.11), by setting $\alpha_{00} = \alpha_1 A^2 + \alpha_2 A^{\sigma 2}$, $\alpha_{01} = 2(\alpha_1 AB + \alpha_2 A^\sigma B^\sigma)$ and $\alpha_{11} = \alpha_1 B^2 + \alpha_2 B^{\sigma 2}$ we obtain the relation

$$h = \alpha_{00} g_{00} + \alpha_{01} g_{01} + \alpha_{11} g_{11} \tag{5.12}$$

where the g_{ij} are defined in (5.1) with respect to the basis $dx/y, xdx/y$. Instead of the g_{ij}, we could use the symmetric bilinear forms $\log^2_{f^\sigma dq/q}$ for $\sigma \in \mathrm{Gal}(E_f/\mathbf{Q})$ with the coefficients α_σ as in Theorem 5.2.2, and we write $f^\sigma dq/q$ in coordinates using (5.11). We use the g_{ij} basis mainly for convenience: the code [BMTV] defaults to this basis when writing h as a linear combination of symmetric bilinear forms.

Let $\rho = h - h_p$. Solving for $\rho = 0$ gives the points found in [BBB+21, Table 1].

The canonical embedding (for non-hyperelliptic curves) gives a map $\tau \mapsto \mathbf{P}^n$ with image $X_0(N)$. Composing with the quotient to the Atkin–Lehner involution, we can actually find where the image of a CM point is on this model. Using this, Galbraith [Gal96] constructs a model for $X_0(67)^+$ and then determines the Heegner points for various discriminants.

For $X_0(67)^+$ with the model

$$y^2 = x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1$$

the Heegner point for $D = -7$ is $[0 : 1 : 1]$.

Then by writing down a change of model, we find that the Heegner point maps to $[1 : -1 : 1]$ on the model (5.10). Galbraith does not write down which point at infinity the cusp ∞ maps to; we can try both $[1 : \pm 1 : 0]$ (on the weighted projective plane

model associated to (5.10)) to see which gives the correct height. We find that the point $[1:-1:0]$ on Galbraith's model which maps to $[0:1:1]$ on (5.10) will have the correct height. Let $\pi(y_K) := [1:-1:1] - [0:1:1]$ on (5.10).

Sage has an implementation of Coleman integrals; using this and (5.11) it is straightforward to verify the logarithm computation. Using Gajović's forthcoming work on local heights for even degree hyperelliptic curves we can compute $h_p(\pi(y_K))$. Gajović's implementation requires two disjoint representations for $\pi(y_K)$. We consider the following points on (5.10): $P := [1:-1:1]$, $Q := [0:1:1]$, $R := [1:1:2]$, $\infty_- := [1:-3:0]$, and $\infty_+ := [1:3:0]$. Let ι denote the hyperelliptic involution. Then $D := P - Q$ is a representing divisor for $\pi(y_K)$ and $2D \sim R - \infty_-$ is a linear equivalence. Gajović's code works with antisymmetric representations of divisors, i.e. representations of the form $E - \iota E$ (see [BB12, Section 5] for more details). Therefore we rewrite the class of $2D$ as

$$\begin{aligned}(R-\infty_-) - (\iota R - \infty_+) + \frac{1}{2}(R + \iota R - \infty_- - \infty_+) = \\ (R-\infty_-) - (\iota R - \infty_+) + \frac{1}{2}\operatorname{Div}(x - x(R)).\end{aligned}$$

Then the local height $h_p(\pi(y_K))$ can be written only in terms of pairings with antisymmetric representations of divisors

$$\begin{aligned}&h_p(D, R-\infty_-) = \\ &h_p(R - \iota R, P - Q) - h_p(\infty_- - \infty_+, P - Q) + \frac{1}{2}\log\left(\frac{x(P)-x(R)}{x(Q)-x(R)}\right).\end{aligned}$$

To obtain the global height, we use work of [vBHM20] to compute that there are no local height contributions away from p, and so the height pairing factors through the Jacobian, and we can write

$$\begin{aligned}&h(\pi(y_K)) = \\ &\frac{1}{2}\left(h_p(R - \iota R, P - Q) - h_p(\infty_- - \infty_+, P - Q) + \frac{1}{2}\log\left(\frac{x(P)-x(R)}{x(Q)-x(R)}\right)\right) \\ &= 7\cdot 11 + 7\cdot 11^2 + 3\cdot 11^3 + 10\cdot 11^4 + 5\cdot 11^5 + 5\cdot 11^6 + 10\cdot 11^8 + 8\cdot 11^9 + O(11^{10}).\end{aligned}$$

The map $X_0(67) \to X_0(67)^+$ is degree 2 so $h(\pi(y_K))$ is simply equal to the sum of $\langle \pi(y_{K,f}), \pi(y_{K,f})\rangle_v$ and $\langle \pi(y_{K,f^\sigma}), \pi(y_{K,f^\sigma})\rangle_v$ by Corollary 4.0.5.

Example 5.2.4. Let f and f^σ be the modular forms in the newform orbit 73.2.a.b, $p = 11$, and $D = -19$.

In Example 4.0.12 we computed the heights of $\pi(y_{K,f})$ and $\pi(y_{K,f^\sigma})$. We continue to fix the embedding (4.15) from $E_f \to \mathbf{Q}_p$ used in Example 4.0.12. Under this embedding, using the approach described in Chapter 3 we find

$$(\log_{fdq/q} \pi(y_K))^2 = 5 \cdot 11^2 + 4 \cdot 11^3 + 11^4 + 5 \cdot 11^5 + O(11^7). \tag{5.13}$$

Considering f^σ, we find the values of Table 5.1. If we try to apply Proposition 3.2.1,

r	$\ell(r) \mod \mathfrak{p}^8$
10	$-58247856 \cdot 11^2$
20	$2039940 \cdot 11^2$
30	$-81550875 \cdot 11^2$
40	$17026861 \cdot 11^2$
50	$80617080 \cdot 11^2$
60	$-85405924 \cdot 11^2$
70	$25100640 \cdot 11^2$
80	$-17022609 \cdot 11^2$

Table 5.1: $\ell(r)$ for f^σ in 73.2.a.b

we find that $\ell(0)^5 \equiv 0 \mod \mathfrak{p}^8$ so we need more precision to determine any information about $(\log_{f^\sigma dq/q} \pi(y_K))^2$.

Galbraith computes the model

$$y^2 = x^6 + 2x^5 + x^4 + 6x^3 + 2x^2 - 4x + 1.$$

for $X_0(73)^+$ and shows that the Heegner point for D on this model is $[0 : 1 : 1]$; it turns out the image of the Heegner cycle can be represented by $[0 : 1 : 1] - [1 : 1 : 0]$ on Galbraith's model.

We use the model

$$y^2 = x^6 + 10x^5 - 15x^4 + 2x^3 + 6x^2 - 4x + 1,$$

which is constructed so that $fdq/q = dx/y - (\nu+1)xdx/y$. By creating an isomorphism with Galbraith's model, we can compute that the Heegner cycle is the class of $\pi(y_K) = [1 : -1 : 1] - [0 : -1 : 1]$. We can use this to verify the logarithm computation

above in Sage, and figure out the missing logarithm.

The height computations can be done using Balakrishnan's Sage code [Bal] for local heights at p and the local heights away from p can be found in [BMS16, Table 4.3]. They use the model

$$y^2 = x^6 - 2x^5 + x^4 - 6x^3 + 2x^2 + 4x + 1$$

where the Heegner cycle is sent to the class of $[0 : -1 : 1] - [1 : 1 : 0]$.

Using this computation in Sage of $(\log_{f^\sigma dq/q} \pi(y_K))^2$ that did not come directly from the p-adic L-function, we constructed $\rho(z)$ and used the quadratic Chabauty code [BMTV] to solve for a finite set of p-adic points containing $X_0(73)^+$.

Example 5.2.5. Let f and f^σ be the newforms in the newform orbit `107.2.a.a` defined over $E_f = \mathbf{Q}(\nu)$ where ν satisfies the polynomial $z^2 - z - 1$. Let

$$f = q - \nu q^2 + (\nu - 2)q^3 + (\nu - 1)q^4 + (\nu - 2)q^5 + (\nu - 1)q^6 + O(q^7). \tag{5.14}$$

Let $p = 11$ and K be the imaginary quadratic field with discriminant $D = -7$. Let $e : E_f \to \mathbf{Q}_p$ sending $\nu \mapsto 4 + 3 \cdot 11 + 3 \cdot 11^3 + O(11^4)$.

By picking a basis of newforms j_1, j_2 with rational coefficients for the weight 2 and level 107 space of newforms with Atkin–Lehner sign $+1$, we can construct a rational model for $X_0(107)^+$ with $j_1 dq/q = dx/y$ and $j_2 = xdx/y$.

$$\begin{aligned} j_1(q) &= q - 2q^3 - q^4 - 2q^5 - q^6 - q^7 - q^8 + 2q^9 + O(q^{10}), \\ j_2(q) &= q^2 - q^3 - q^4 - q^5 - q^6 + 2q^7 - 2q^8 + 3q^9 + O(q^{10}). \end{aligned}$$

Then our model is

$$y^2 = x^6 - 10x^5 + 17x^4 - 18x^3 + 10x^2 - 4x + 1.$$

By solving for f in terms of j_1 and j_2 we find that $dx/y - \nu x dx/y = f dq/q$. We can find a finite index subgroup of the Mordell–Weil group generated by the classes of $Q_1 := [0 : 1 : 1] - [0 : -1 : 1]$ and $Q_2 = [1/2 : -1/8 : 1] - [0 : -1 : 1]$. The logarithms $L_{Q_i} := \log_{fdq/q} Q_i$ (under the embedding e) are

$$\begin{aligned} L_{Q_1} &= 3 \cdot 11 + 4 \cdot 11^2 + 2 \cdot 11^3 + 9 \cdot 11^4 + 11^5 + 10 \cdot 11^7 + 7 \cdot 11^8 + 4 \cdot 11^9 + O(11^{10}) \\ L_{Q_2} &= 2 \cdot 11 + 8 \cdot 11^2 + 7 \cdot 11^4 + 4 \cdot 11^5 + 6 \cdot 11^6 + 3 \cdot 11^7 + 3 \cdot 11^8 + O(11^{10}). \end{aligned}$$

We also can compute the logarithm of the Heegner point using the techniques described in Chapter 3. The values of $\ell(r)$ are given in Table 5.2. Then we compute $L_p(f,1) =$

r	$\ell(r)$ mod $\mathfrak{p}^5$
10	-22250
20	-17899
30	-70252
40	28890
50	56376

Table 5.2: $\ell(r)$ for f in 107.2.a.a

$-50731 + O(11^5)$ and the logarithm of the Heegner cycle is

$$(\log_{fdq/q} \pi(y_K))^2 = 4 \cdot 11^2 + 8 \cdot 11^4 + 2 \cdot 11^6 + O(11^7).$$

For the conjugate modular form $f^\sigma dq/q$ in the newspace we have the values given in Table 5.3 and so

r	$\ell(r)$ mod $\mathfrak{p}^5$
10	39142
20	70280
30	39031
40	-40900
50	49703

Table 5.3: $\ell(r)$ for f^σ in 107.2.a.a

$$L_p(f,1) = 37471 + O(11^5)$$

and therefore

$$(\log_{fdq/q} \pi(y_K))^2 = 3 \cdot 11^2 + 4 \cdot 11^3 + 2 \cdot 11^5 + 10 \cdot 11^6 + O(11^7).$$

Then we can check that when $A = \pm 2$ and $B = \pm 1$ we have the relation

$$A^2(L_{Q_1}/2)^2 + 2AB(L_{Q_1}/2)(L_{Q_2}/2) + B^2(L_{Q_2}/2)^2 = (\log_{fdq/q} \pi(y_K))^2.$$

The division by two occurs because the Q_i are not 2-saturated in the Mordell–Weil

group.

We finish the example by computing the heights of $\pi(y_{K,f})$. To do this we fix the complex embedding

$$\begin{aligned} e_c : E_f &\to \mathbf{C} \\ \nu &\mapsto 1.6180339887498948482045868344. \end{aligned}$$

First, using Collins's Sage code [Col18] we can compute

$$\begin{aligned} \Omega_f &= 42.114698727536408694805394869 \\ \Omega_{f^\sigma} &= 51.071742506523227798145108077. \end{aligned}$$

In Sage, we can also compute

$$\begin{aligned} &\frac{d}{dT} L_{p,MTT}(f,T)\Big|_{T=0} = \\ &4 + 7\cdot 11 + 7\cdot 11^2 + 7\cdot 11^3 + 8\cdot 11^4 + 11^5 + 3\cdot 11^6 + 4\cdot 11^7 + 7\cdot 11^8 + O(11^9) \\ &\frac{d}{dT} L_{p,MTT}(f^\sigma,T)\Big|_{T=0} = \\ &6 + 11 + 6\cdot 11^2 + 9\cdot 11^3 + 7\cdot 11^5 + 7\cdot 11^6 + 2\cdot 11^7 + 5\cdot 11^8 + O(11^9). \end{aligned}$$

Let χ be the quadratic character with $D' = 5$ and recall that ε denotes the quadratic character associated with K. Following Algorithm 4.0.9 we find that the periods are $\Omega_f^+ = L(f^\chi, 1)/(-4/\sqrt{5})$ and $\Omega_{f^\sigma}^+ = L(f^{\sigma\chi}, 1)/((-4)/\sqrt{5})$. We compute

$$\begin{aligned} L(f^\chi, 1) &= 3.948128129878725068182473057 93 \\ L(f^{\sigma\chi}, 1) &= 2.407825595820719138901798594 30 \\ L(f^\varepsilon, 1) &= 0.996703058180421475347204490138 \\ L(f^{\sigma\varepsilon}, 1) &= 5.188648615277820825148086683 41. \end{aligned}$$

Combining the complex values, we find

$$\begin{aligned} \frac{\Omega_f^+ L(f^\varepsilon, 1)\sqrt{|D|}}{\Omega_f} &= -0.138196601125010515179541316 6 \\ \frac{\Omega_{f^\sigma}^+ L(f^{\sigma\varepsilon}, 1)\sqrt{|D|}}{\Omega_{f^\sigma}} &= -0.361803398874989484820458683 4. \end{aligned}$$

Let $r_1 := 1/10\nu - 3/10$ and $r_2 := -1/10\nu - 1/5$ be the roots of the polynomial $20x^2 + 10x + 1$. The complex values $-0.13819660112501051517954131 66$ and $-0.36180339887498948482045868 34$ are within 10^{-28} of the algebraic numbers $e_c(r_1)$ and $e_c(r_2)$. Under the assumption that $-0.13819660112501051517954131 66 = e_c(r_1)$ and $-0.36180339887498948482045868 34 = e_c(r_2)$, we have

$$\begin{aligned}&\langle \pi(y_{K,f}), \pi(y_{K,f})\rangle_v = \\ &7 \cdot 11 + 8 \cdot 11^2 + 5 \cdot 11^3 + 11^4 + 3 \cdot 11^5 + 11^6 + 10 \cdot 11^7 + 8 \cdot 11^8 + O(11^9).\\ &\langle \pi(y_{K,f^\sigma}), \pi(y_{K,f^\sigma})\rangle_v = \\ &5 \cdot 11 + 9 \cdot 11^2 + 8 \cdot 11^3 + 10 \cdot 11^4 + 8 \cdot 11^5 + 8 \cdot 11^6 + 6 \cdot 11^7 + O(11^9).\end{aligned}$$

We ran the quadratic Chabauty code [BMTV] using the resulting $\rho(z)$ from Theorem 5.2.2 and recovered a finite superset of the rational points on $X_0(107)^+$.

Example 5.2.6. Let f and f^σ be the newforms in the orbit 85.2.a.b defined over $E_f = \mathbf{Q}(\sqrt{2})$. Let

$$f = q + (\sqrt{2} - 1)q^2 + (-\sqrt{2} - 2)q^3 + (-2\sqrt{2} + 1)q^4 - q^5 - \sqrt{2}q^6 + O(q^7).$$

We finish Example 3.2.7 by computing the heights. Let $p = 7$ and $D = -19$. Recall we have fixed a p-adic embedding $e : E_f \to \mathbf{Q}_p$ by $\sqrt{2} \mapsto 3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + O(7^4)$. Using the methods described in Chapter 4 and already exhibited in the previous examples, we find

$$\begin{aligned}&\langle \pi(y_{K,f}), \pi(y_{K,f})\rangle_v = 6 \cdot 7^{-3} + 3 \cdot 7^{-2} + 3 \cdot 7^{-1} + 6 \cdot 7 + 2 \cdot 7^3 + 3 \cdot 7^5 + 2 \cdot 7^7 + O(7^9)\\ &\langle \pi(y_{K,f^\sigma}), \pi(y_{K,f^\sigma})\rangle_v = 3 \cdot 7 + 6 \cdot 7^2 + 4 \cdot 7^4 + 3 \cdot 7^5 + 7^6 + 3 \cdot 7^7 + 7^8 + O(7^9).\end{aligned}$$

Note that in this case the degree of the quotient $X_0(85) \to X_0^*(85)$ is 4 so the sum of the heights must be multiplied by 2 to obtain $h(\pi(y_K))$.

Picking a basis of newforms g_1, g_2 with rational coefficients for the weight 2 and level 85 space of newforms with both Atkin–Lehner signs equal to $+1$, we can construct a rational model for $X_0^*(85)$ with $g_1 dq/q = dx/y$ and $g_2 = xdx/y$.

$$\begin{aligned}g_1(q) &= q^2 - q^3 - 2q^4 - q^6 + q^7 + q^8 + 4q^9 + O(q^{10}),\\ g_2(q) &= q - 3q^3 - q^4 - q^5 - q^6 - q^7 - 2q^8 + 7q^9 + O(q^{10}).\end{aligned}$$

The model is

$$y^2 = x^6 - 4x^5 + 12x^4 - 22x^3 + 32x^2 - 40x + 25.$$

Furthermore we have the relationship $(\sqrt{2}-1)dx/y + xdx/y = fdq/q$. On this model, $(\log_{fdq/q}([1:-1:0]-[1:1:0]))^2$ agrees with $(\log_{fdq/q}\pi(y_K))^2$. Furthermore, since $[2:5:1]-[2:-5:1]$ is linearly equivalent to twice $[1:-1:0]-[1:1:0]$, we can compute the global height of this divisor using Gajović's code:

$$\begin{aligned} h([1:-1:0]-[1:1:0]) &= \frac{1}{2}h_p([1:-1:0]-[1:1:0],[2:5:1]-[2:-5:1]) \\ &= 5\cdot 7^{-3} + 1 + 4\cdot 7 + 6\cdot 7^3 + 7^4 + 6\cdot 7^5 + 3\cdot 7^6 + 3\cdot 7^7 + 3\cdot 7^8 + 5\cdot 7^9 + O(7^{10}). \end{aligned}$$

In addition to calculating the function $\rho(z)$, to do quadratic Chabauty we have to compute the finite set of values $\rho(z)$ can take on. For the previous examples the set was simply $\{0\}$, but for $X_0^*(85)$ there are nontrivial local height contributions away from p that must be accounted for. We did not compute these values, and so we did not compute $X_0^*(85)(\mathbf{Q})$.

The rational points on the curves $X_0(67)^+$, $X_0(73)^+$, $X_0(107)^+$, and $X_0^*(85)$ are already known [BBB+21, BDM+21, BGX21], but Theorem 5.2.2 and the examples discussed give a new way of constructing the function ρ.

Part II

Geometric Quadratic Chabauty

Chapter 6

Introduction and Background II

6.1 Introduction II

In Part II we present algorithms for the geometric quadratic Chabauty method of Edixhoven and Lido [EL21]. This part is joint work with Juanita Duque-Rosero and Pim Spelier. Let $X_{\mathbf{Q}}$ be a smooth, projective, geometrically irreducible curve of genus $g > 1$ over $\mathbf{Q}$. Let $J_{\mathbf{Q}}$ be the Jacobian of $X_{\mathbf{Q}}$, with Mordell–Weil rank r and Néron–Severi rank $\rho > 1$. Let $p > 2$ be a prime of good reduction for $X_{\mathbf{Q}}$. Geometric quadratic Chabauty is an effective p-adic method for producing a finite set of p-adic points containing the rational points of $X_{\mathbf{Q}}$, when $r < g + \rho - 1$.

In contrast to quadratic Chabauty [BD18, BD21], which works in certain Selmer varieties, the geometric method can be described algebro-geometrically, and the computations take place in $\mathbf{G}_m$-torsors over $J_{\mathbf{Q}}$. By pulling back the Poincaré torsor on $J_{\mathbf{Q}} \times J_{\mathbf{Q}}$ by a nontrivial trace zero morphism $f : J_{\mathbf{Q}} \to J_{\mathbf{Q}}$, we can construct a nontrivial torsor T over $J_{\mathbf{Q}}$ whose restriction to $X_{\mathbf{Q}}$ is trivial. This allows us to embed $X_{\mathbf{Q}}$ 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 $X_{\mathbf{Q}}$ with the p-adic closure of the integer points $\overline{T(\mathbf{Z})}$. This intersection contains $X(\mathbf{Q})$.

We describe new explicit methods for geometric quadratic Chabauty that work mainly in the trivial biextension $\mathbf{Q}_p^g \times \mathbf{Q}_p^g \times \mathbf{Q}_p$. Working on the trivial biextension translates the geometric quadratic Chabauty method into the language of Coleman–Gross heights and Coleman integrals. We explicitly give this translation into the

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

There has been recent interest in geometric methods [Fly97, Spe20, EL21] to compute $X_{\mathbf{Q}}(\mathbf{Q})$. For example, Flynn [Fly97] studies equations representing the formal group of the Jacobian and determines $X_{\mathbf{Q}}(\mathbf{Q})$ for many genus 2 rank 1 curves. In our algorithms, we depart from this strategy of computing equations for the formal group using parameters on the Jacobian; we show that using the local Coleman–Gross height and Coleman integrals we can obtain a homeomorphism from residue disks of the torsor to residue disks of the trivial biextension, where the group law is simply addition. This is the basis of the algorithms provided here.

We provide an example of our new method applied to the 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 [BBB+21], this provides a new way of analyzing the set of rational points.

6.2 Overview and Set-up

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

Let $X_{\mathbf{Q}}$ be any smooth, projective, geometrically irreducible curve over $\mathbf{Q}$ with a proper regular model X of $X_{\mathbf{Q}}$ over the integers and a fixed base point $b \in X_{\mathbf{Q}}(\mathbf{Q}) = X(\mathbf{Z})$. Let X^{sm} denote the open subscheme of X consisting of points at which X is smooth over $\mathbf{Z}$; then $X^{\mathrm{sm}}(\mathbf{Z}) = X(\mathbf{Z})$. Let $J_{\mathbf{Q}}$ denote the Jacobian of $X_{\mathbf{Q}}$ and J

denote the Néron model of $J_{\mathbf{Q}}$ over the integers. Suppose $J_{\mathbf{Q}}$ has Mordell–Weil rank r and Néron–Severi rank $\rho = \rho(J_{\mathbf{Q}})$.

The goal in geometric quadratic Chabauty is to lift X into a nontrivial $\mathbf{G}_m^{\rho-1}$-torsor T over J through a section $\widetilde{j_b}$ lying over the Abel–Jacobi embedding $j_b : X^{\mathrm{sm}} \to J$. Over $\mathbf{Q}$ we find this $\widetilde{j_b}$ by giving a trivializing section of the $\mathbf{G}_m^{\rho-1}$-torsor $j_b^* T_{\mathbf{Q}}$ over $X_{\mathbf{Q}}$. If we want to spread this out over $\mathbf{Z}$, there is an obstruction coming from the multidegree. The map $\mathrm{Pic}(X) \to \mathrm{Pic}(X_{\mathbf{Q}})$ is not in general an isomorphism, and $j_b^* T$ is not in general trivial over X since its multidegree over the fibers $X_{\mathbf{F}_\ell}$ of X might be non-zero. This is the only obstruction: the torsor can be trivialized over an open U constructed by picking one irreducible component in each fiber $X_{\mathbf{F}_\ell}$ and removing the singular points. There is a finite number of these open sets that cover X^{sm}. We

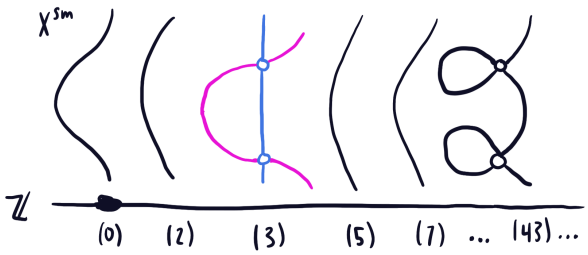

Figure 6.1: The fiber over (3) has two components, so X^{sm} can be covered by two open sets

fix such an open U, and the trivialization $\widetilde{j_b} : U \to T$ lying over j_b.

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

Theorem 6.2.1. *[EL21, Section 9.2] When $r < g + \rho - 1$, the intersection*

$$\widetilde{j_b}(U(\mathbf{Z}_p)) \cap \overline{T(\mathbf{Z})} \subset T(\mathbf{Z}_p)$$

is finite.

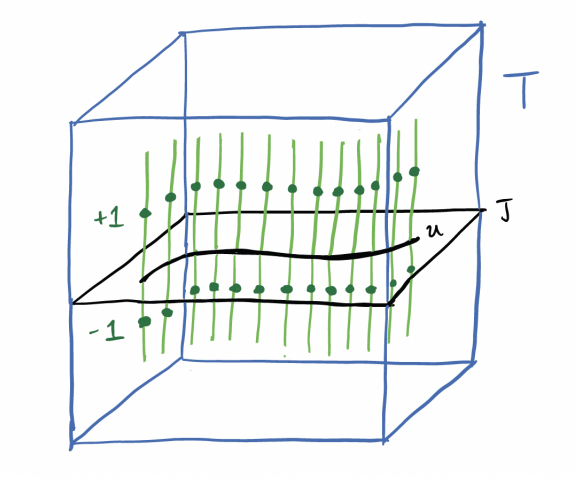

Figure 6.2: The embedding of $U(\mathbf{Z}_p)$ into $T(\mathbf{Z}_p)$ when $r = g = \rho = 2$

The geometric quadratic Chabauty method computes this finite set $\widetilde{j_b}(U(\mathbf{Z}_p)) \cap \overline{T(\mathbf{Z})}$, working in one residue disk of $U(\mathbf{Z}_p)$ at a time. In Algorithm 8.4.2 we give an algorithm to determine $\widetilde{j_b}(U(\mathbf{Z}_p)) \cap \overline{T(\mathbf{Z})}$ to finite precision.

To construct the $\mathbf{G}_m^{\rho-1}$-torsor T over J we start with the universal $\mathbf{G}_m$-torsor. In our calculations this takes the form of the Poincaré torsor $\mathcal{M}^\times$ over $J \times J^0$ (this is actually a pullback of the Poincaré torsor over $J \times J^{\vee 0}$; for more details see Chapter 7). Here $J^{\vee 0}$ is the fiberwise connected component of $J^\vee$ containing 0.

Remark 6.2.2. Since p is a prime of good reduction for $J^{\vee 0}$, then $J^0_{\mathbf{Z}_{(p)}} = J_{\mathbf{Z}_{(p)}}$ and $J^{\vee 0}_{\mathbf{Z}_{(p)}} = J^\vee_{\mathbf{Z}_{(p)}}$.

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

$$m := \mathrm{lcm}\{\#(J/J^0)(\overline{\mathbf{F}}_q) : q \text{ prime}\} \tag{6.1}$$

and note $m\cdot : J \to J^0$ is then 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 $\alpha_i : J \to J^0$ to be of the form $m \cdot \circ \operatorname{tr}_{c_i} \circ f_i$ with $c_i \in J(\mathbf{Z})$.

The torsor T is the product $T = \prod_{i=1}^{\rho-1} (\mathrm{id}, \alpha_i)^* \mathcal{M}^\times$. In order to embed U through a section $\widetilde{j_b} : U \to T$, the torsor T pulled back to U must be trivial: that is $j_b^* (\mathrm{id}, \alpha_i)^* \mathcal{M}^\times$ must be trivial. 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.

$$\begin{array}{ccccc} & & T & \longrightarrow & \mathcal{M}^{\times,\rho-1} \\ & \overset{\widetilde{j_b}}{\nearrow} & \downarrow & & \downarrow \\ U & \xrightarrow{j_b} & J & \xrightarrow{(\mathrm{id}, m \cdot \circ \operatorname{tr}_{c_i} \circ f_i)_i} & J \times (J^{\vee 0})^{\rho-1} \end{array} \tag{6.2}$$

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

Definition 6.2.3. For Y a scheme, S a ring with residue field $\operatorname{Spec} \mathbf{F}_p \to \operatorname{Spec} S$ and $Q \in Y(\mathbf{F}_p)$, we define the residue disk over Q, denoted by $Y(S)_Q := \{y \in Y(S) : \overline{y} = Q\}$, to be the set of all S-points specializing to Q.

The geometric quadratic Chabauty method is an effective method for finding the intersection $\widetilde{j_b}(U(\mathbf{Z}_p)) \cap \overline{T(\mathbf{Z})}$, residue disk by residue disk. Let $\overline{P} \in U(\mathbf{F}_p)$. The residue disk $U(\mathbf{Z}_p)_{\overline{P}}$ embeds into the residue disk $T(\mathbf{Z}_p)_{\widetilde{j_b}(\overline{P})}$ 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 $T(\mathbf{Z})_{\widetilde{j_b}(\overline{P})} \to J(\mathbf{Z})_{j_b(\overline{P})}$ is a bijection. By [Par00, Proposition 2.3] and again the fact that $p > 2$ the residue disk $J(\mathbf{Z})_{j_b(\overline{P})}$ is up to a translation isomorphic to $\mathbf{Z}_p^r$. In [EL21, Theorem 4.10] this bijection $T(\mathbf{Z})_{\widetilde{j_b}(\overline{P})} \to J(\mathbf{Z})_{j_b(\overline{P})}$ is upgraded to a morphism $\kappa : \mathbf{Z}_p^r \to T(\mathbf{Z}_p)_{\widetilde{j_b}(\overline{P})}$ with image exactly $\overline{T(\mathbf{Z})}_{\widetilde{j_b}(\overline{P})}$.

We make the geometric quadratic Chabauty method explicit by giving algorithms to compute $\widetilde{j_b}$ and κ in a residue disk as polynomials in parameters up to finite preci-

sion. This 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.

6.2.1 Structure

In Chapter 7 we provide background on the Poincaré torsor and its other realizations. We solve the problem of how to efficiently represent elements of a residue disk of T. We show how to represent elements of the Poincaré torsor $\mathcal{M}^\times$ using the following statement that appears in [EL21, Section 9.3].

Proposition 6.2.4. *There is a morphism of biextensions over $J(\mathbf{Q}_p) \times J(\mathbf{Q}_p)$*

$$\Psi : \mathcal{M}^\times(\mathbf{Q}_p) \to J(\mathbf{Q}_p) \times J(\mathbf{Q}_p) \times \mathbf{Q}_p, \tag{6.3}$$

with the trivial $\mathbf{Q}_p$-biextension structure on the latter product.

Note that by Remark 6.2.2, $J^0(\mathbf{Q}_p) = J(\mathbf{Q}_p)$. This proposition allows us to record elements of $\mathcal{M}^\times(\mathbf{Q}_p)$ up to p-adic finite precision. In Proposition 7.3.3 we describe the image of integer points of T in the trivial biextension $\mathcal{N} := J(\mathbf{Q}_p) \times J(\mathbf{Q}_p) \times \mathbf{Q}_p$.

Since we can construct a bijection from residue disks of $J(\mathbf{Z}_p)$ to $\mathbf{Z}_p^g$ using Coleman integrals, we can explicitly write down a homeomorphism from the residue disk $T(\mathbf{Z}_p)_{\widetilde{j_b}(\overline{P})}$ to $\mathbf{Z}_p^{g+\rho-1}$ factoring through Ψ; this is done in Corollary 7.3.12. Crucially, we prove that this homeomorphism is given by convergent power series on $\mathbf{Z}_p^{g+\rho-1}$, i.e. power series that modulo every power of p are given by polynomials.

Then in Section 8.1 we give an algorithm to construct the unique line bundle associated to the endomorphism f from a divisor in $U \times X$ satisfying certain properties described in Lemma 8.1.4. Using this line bundle we write down a theoretical formula for the trivializing section $\widetilde{j_b} : U \to T$. 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 8.2. In Section 8.3 we give formulas for computing

integer points in the biextension $\mathcal{N}$ that are the image of generating sections of certain residue disks of $\mathcal{M}$.

Finally, in Section 8.4 we tie everything together with the algorithm for geometric quadratic Chabauty in a residue disk $U(\mathbf{Z})_{\overline{P}}$. In this section, we also describe how to compute a finite set of p-adic points to precision 2 containing the integer points in a single residue disk $U(\mathbf{Z})_{\overline{P}}$. We do this by reducing our computations to $T(\mathbf{Z}/p^2\mathbf{Z})_{\widetilde{j_b}(\overline{P})}$ and using a Hensel-like lemma [EL21, Theorem 4.12]. Chapter 9 shows a worked example of the algorithms applied to the case of $X_0(67)^+$. The rational points on this curve have been determined previously [BBB+21], but the computations here demonstrate the practicality of the geometric quadratic Chabauty algorithms presented here for hyperelliptic modular curves.

Chapter 7

Understanding the biextension and T

A crucial object of study is the Poincaré torsor. This has a few incarnations, which we introduce in this chapter.

7.1 The Poincaré torsor $\mathcal{P}$

First we introduce the Poincaré torsor $\mathcal{P}^\times_{\mathbf{Q}}$ over $J_{\mathbf{Q}} \times J^\vee_{\mathbf{Q}}$, its biextension structure, and the torsor $\mathcal{P}^\times$ over the integers. For more details on the Poincaré torsor and biextensions, see [MB85, §I.2.5] or Grothendieck's Exposés VII and VIII [GRR72]. The abelian variety $J^\vee_{\mathbf{Q}}$ is a moduli space for line bundles algebraically equivalent to zero on $J_{\mathbf{Q}}$; every $[c] \in J^\vee_{\mathbf{Q}}$ corresponds to a line bundle $\mathcal{L}_c$ on $J_{\mathbf{Q}}$. The universal line bundle over $J_{\mathbf{Q}} \times J^\vee_{\mathbf{Q}}$ is the Poincaré bundle $\mathcal{P}_{\mathbf{Q}}$. It satisfies the property that $\mathcal{P}_{\mathbf{Q}}|_{J_{\mathbf{Q}} \times [c]} \simeq \mathcal{L}_c$ and it is rigidified at 0, i.e. $\mathcal{P}_{\mathbf{Q}}|_{0 \times J^\vee}$ is trivial. Furthermore, under the natural identification $(J^\vee_{\mathbf{Q}})^\vee = J_{\mathbf{Q}}$, this line bundle is also the universal line bundle over $J_{\mathbf{Q}} \times J^\vee_{\mathbf{Q}}$ parametrizing line bundles on $J^\vee_{\mathbf{Q}}$.

Given a line bundle $\mathcal{L}$ over a scheme S, there is an associated $\mathbf{G}_m$-torsor $\mathcal{L}^\times$ defined by taking the sheaf of non-vanishing sections, and similarly given a $\mathbf{G}_m$-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 $\mathbf{G}_m$-torsor $\mathcal{P}^\times_{\mathbf{Q}}$ over $J_{\mathbf{Q}} \times J^\vee_{\mathbf{Q}}$, called the Poincaré torsor. Alternatively,

$$\mathcal{P}^\times_{\mathbf{Q}} = \mathrm{Isom}_{J_{\mathbf{Q}} \times J^\vee_{\mathbf{Q}}}(\mathcal{O}_{J_{\mathbf{Q}} \times J^\vee_{\mathbf{Q}}}, \mathcal{P}_{\mathbf{Q}}),$$

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

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

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

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

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

called $\otimes_1$. These two partial group laws are compatible. Let $x_1, x_2 \in J_{\mathbf{Q}}(S)$, $y_1, y_2 \in J_{\mathbf{Q}}^\vee(S)$, and $z_{ij} \in (x_i, y_j)^* \mathcal{P}_{\mathbf{Q}}^\times(S)$, 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. The structure of these two partial group laws over the product $J_{\mathbf{Q}} \times J_{\mathbf{Q}}^\vee$, together with this compatibility, makes $\mathcal{P}_{\mathbf{Q}}^\times$ a $\mathbf{G}_m$-biextension over $J_{\mathbf{Q}} \times J_{\mathbf{Q}}^\vee$.

For our applications, we need to work over the integers. Let J^0 be the fiberwise connected component of J containing 0, representing line bundles of multidegree 0, 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 $(x, y) \in (J \times J^{\vee 0})(\mathbf{Z})$ form a $\mathbf{G}_m(\mathbf{Z})$-torsor, i.e. a $\{\pm 1\}$-torsor. So there is exactly one integer point lying over (x, y), up to sign.

7.2 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 $J \times J^0$, $\mathcal{M}^\times$ and $\mathcal{N}$ the trivial biextension.

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

$$\mathcal{M}^\times := (\mathrm{id}, j_b^{*,-1})^* \mathcal{P}^\times. \tag{7.1}$$

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 $(x, y) \in (J \times J)(S)$ by $\mathcal{M}^\times(x, y)$. This fiber $\mathcal{M}^\times(x, y)$ is the $\mathbf{G}_m$-torsor

$$E^* \mathcal{L}^\times := \mathrm{Norm}_{E^+/S} \left(\mathcal{L}^\times \mid_{E^+} \right) \otimes \mathrm{Norm}_{E^-/S} \left(\mathcal{L}^\times \mid_{E^-} \right)^{-1}, \tag{7.2}$$

which we also denote by $\mathrm{Norm}_{E/S} \mathcal{L}^\times$. This fiber can be thought of as the aggregate of how $\mathcal{L}$ looks around E.

This description of the fiber is proven in [EL21, Proposition 6.8.7] and more general facts about these norms can be found in [EL21, Section 6]. Because equation (7.2) may seem a bit opaque, we provide some examples of how to apply the formula in practice.

Example 7.2.1. 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. Then the $\mathbf{G}_m$-torsor $E^*\mathcal{O}_X(D)^\times$ is generated by E^*1, where $1 \in \mathcal{O}_X(D)^\times$.

Definition 7.2.2. Let D and E be two divisors on X defined over a scheme S. We say D and E are disjoint over S if their support is disjoint as closed subschemes of S. In particular, it is not enough to have disjoint S-points if D or E does not split completely over S.

Example 7.2.3. Suppose the fiber of $X^{\mathrm{sm}}/\mathbf{Z}$ over 2 is irreducible. Let $[D] \in J(\mathbf{Z})$ and $[E] \in J^0(\mathbf{Z})$ with representing divisors D and E. Assume D and E are disjoint over $\mathbf{Z}[\frac{1}{2}]$ and meet with multiplicity 1 over 2. Then $E^*\mathcal{O}_X(D)^\times$ is generated by $2^{-1}E^*1$.

Remark 7.2.4. Let S be a scheme. If $D = \operatorname{Div} g \in \operatorname{Div}^0(X)$ is the principal divisor of a rational function g and is disjoint from $E \in \operatorname{Div}^0(X)$, 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 $g(E) \in \mathbf{G}_m(S)$.

Remark 7.2.5. In general, if $[D] \in J(\mathbf{Z})$, $[E] \in J(\mathbf{Z})$, and we have a choice of representing divisors D and E that are disjoint over $\mathbf{Q}$, using intersection theory we can determine $n \in \mathbf{Q}^\times$ 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 [EL21, Section 6.9].

The partial group laws on $\mathcal{M}^\times$ are also very explicit: they are given by the morphisms

$$E_1^*\mathcal{L}^\times \otimes E_2^*\mathcal{L}^\times \to (E_1 + E_2)^*\mathcal{L}^\times \tag{7.3}$$

corresponding to $\otimes_2$ and

$$E^*\mathcal{L}_1^\times \otimes E^*\mathcal{L}_2^\times \to E^*(\mathcal{L}_1 \otimes \mathcal{L}_2)^\times \tag{7.4}$$

corresponding to $\otimes_1$.

Example 7.2.6. Let $x_1, x_2 \in J(\mathbf{Z})$ and $y_1, y_2 \in J^0(\mathbf{Z})$. Let $z_{ij} \in \mathcal{M}^\times(\mathbf{Z})$ be points above (x_i, y_j). Then for $n_1, n_2, m_1, m_2 \in \mathbf{Z}$ 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 generating points that lie over generators of the Jacobian and then applying the partial group laws. In Section 8.3 we will use this idea to determine the integer points of the torsor T landing in a specific residue disk of T.

7.3 The trivial biextension $\mathcal{N}$

In practice, we will often translate between $\mathcal{M}$ and the trivial biextension $\mathcal{N}$ where we do our computations. We explain how to make this translation following [EL21, Section 9.3].

Let $[D] \in J(\mathbf{Q}_p)$ and $[E] \in J^0(\mathbf{Q}_p)$ be divisor classes with a choice of representing divisors D and E that are disjoint over $\mathbf{Q}_p$. Then $E^*\mathcal{O}_X(D)^\times$ is a $\mathbf{Q}_p^\times$-torsor, trivial with generator E^*1 by Example 7.2.1. Let h_p be the cyclotomic Coleman–Gross local height at p [CG89, Section 5]. Choose a branch of the logarithm with $\log p = 0$ so that it is compatible with h_p. We define a map

$$\begin{aligned} \psi : \mathcal{M}^\times(\mathbf{Q}_p) &\to \mathbf{Q}_p \\ E^*\lambda \in E^*\mathcal{O}_X(D)^\times &\mapsto \log \lambda + h_p(D, E). \end{aligned} \tag{7.5}$$

We define $\mathcal{N}$ to be the trivial $\mathbf{Q}_p$-biextension $J(\mathbf{Q}_p) \times J(\mathbf{Q}_p) \times \mathbf{Q}_p$ over $J(\mathbf{Q}_p) \times J(\mathbf{Q}_p)$, and we define a morphism

$$\Psi : \mathcal{M}^\times(\mathbf{Q}_p) \to \mathcal{N}$$

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

Remark 7.3.1. Since $\log(-1) = 0$, Ψ sends the two integer points of $\mathcal{M}^\times(\mathbf{Z})$ above a fixed integer point of $J \times J^0$ to the same point.

The partial group laws in $\mathcal{N}$ are just addition. Let $[D_i] \in J(\mathbf{Q}_p)$ and $[E_i], \in J(\mathbf{Q}_p)$ and $v_i \in \mathbf{Q}_p$ for $i = 1, 2$. The first group law is

$$([D_1], [E_1], v_1) +_1 ([D_2], [E_1], v_2) = ([D_1] + [D_2], [E_1], v_1 + v_2).$$

The second group law is

$$([D_1], [E_1], v_1) +_2 ([D_1], [E_2], v_2) = ([D_1], [E_1] + [E_2], v_1 + v_2).$$

The following proposition appears in [EL21, Section 9.3] but is not proven.

Proposition 7.3.2. *The map $\Psi : \mathcal{M}^\times(\mathbf{Z}_p) \to \mathcal{N}$ is a morphism of biextensions.*

Proof. First we show that Ψ is well defined. For divisor classes $[D] \in J(\mathbf{Q}_p)$ and $[E] \in J(\mathbf{Q}_p)$ we can always choose representing divisors D and E with disjoint support over $\mathbf{Q}_p$; 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 7.2.4. 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 matter. By symmetry of the norm [EL21, 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 (7.3) and (7.4). Let $[D_1], [D_2] \in J(\mathbf{Q}_p)$, and $[E] \in J^0(\mathbf{Q}_p)$ 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 7.3.3. *Let $[D] \in J(\mathbf{Z})$ and $[E] \in J(\mathbf{Z})$ with representing divisors D and E that have disjoint support over $\mathbf{Z}_{(p)}$. Let F be the unique vertical divisor such that $F + E$ has multidegree 0 on all fibers $X_{\mathbf{F}_q}$. Let $z \in \mathcal{M}^\times([D], [E + F])(\mathbf{Z})$. 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 $F = \sum_q F_{\mathbf{F}_q}$ where q ranges over the primes of bad reduction for X and $F_{\mathbf{F}_q}$ has support in $X_{\mathbf{F}_q}$. Then by [EL21, Proposition 6.9.3] we have the equation

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

where q ranges over the bad primes.

Recall that $\operatorname{Norm}_E(\mathcal{L}^\times)$ is by definition $\operatorname{Norm}_{E/\operatorname{Spec}\mathbf{Z}}(\mathcal{L}^\times|_E)$; this torsor is canonically identified with $\mathcal{O}_{\operatorname{Spec}\mathbf{Z}}(\prod_q q^{-(E \cdot D)_q})^\times$ 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 $\mathbf{Z}_{(q)}$ taking values in $\mathbf{Z}$.

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

$$\begin{aligned} \psi(z) &= \log \prod_q q^{-((E+F) \cdot D)_q} + h_p(D, E) \\ &= \sum_{q \neq p} h_q(D, E) + h_p(D, E) \\ &= h([D], [E]) \end{aligned}$$

as we wanted. □

7.3.1 The torsor T_f

We set up some notation. Recall from Section 6.2 that we have fixed an open set $U \subset X^{\mathrm{sm}}$ that contains the smooth points of one irreducible component of each fiber. Let f be a trace 0 endomorphism of J. Recall the integer m from (6.1). The map

$m \cdot \circ f$ is a morphism $J \to J^0$. Let $c \in J(\mathbf{Z})$ denote the unique element such that $j_b^*(\mathrm{id}, m \cdot \circ \mathrm{tr}_c \circ f)^* \mathcal{M}^\times$ is trivial over U. Let $\alpha_f := m \cdot (\mathrm{tr}_c \circ f)$. Let $\xi_f : T_f \to J$ denote the $\mathbf{G}_m$-torsor $(\mathrm{id}, \alpha)^* \mathcal{M}^\times$ over J. The trivialization of $j_b^*(\mathrm{id}, m \cdot \circ \mathrm{tr}_c \circ f)^* \mathcal{M}^\times$ then gives us a morphism $\widetilde{j_{b,f}} : U \to T_f$ of schemes over J.

Remark 7.3.4. If f is identically zero, then T_f is isomorphic to the trivial $\mathbf{G}_m$-torsor over J. If $r < g$ this reduces to the geometric linear Chabauty case, see [Spe20, HS22] 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 7.3.10. Throughout the rest of this section, fix a $\bar{t} \in T_f(\mathbf{F}_p)$. Then we want to work inside the residue disk $T_f(\mathbf{Z}_p)_{\bar{t}}$. Since T_f is trivial on fibers, the residue disk $T_f(\mathbf{Z}_p)_{\bar{t}}$ is isomorphic to $J(\mathbf{Z}_p)_{\xi_f(\bar{t})} \times \mathbf{G}_m(\mathbf{Z}_p)_u$ for some unit $u \in \mathbf{F}_p$. We would like to parametrize this residue disk.

Definition 7.3.5. Let Y be a smooth scheme over $\mathbf{Z}_p$ of relative dimension d, and let $y \in Y(\mathbf{F}_p)$. 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 $t' \colon Y(\mathbf{Z}_p)_Q \to \mathbf{Z}_p^d$. We call t' a parametrization given by parameters t_i.

Example 7.3.6. Take $Y = \mathbf{G}_m = \operatorname{Spec} \mathbf{Z}_p[x, x^{-1}]$ over $\mathbf{Z}_p$; this is of relative dimension 1. Let $y = 1 \in \mathbf{G}_m(\mathbf{F}_p)$. Then $x - 1$ is a parameter at y; it induces a parametrization $\theta : \mathbf{G}_m(\mathbf{Z}_p)_y \to \mathbf{Z}_p$ 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 $\varphi = \log/p : \mathbf{G}_m(\mathbf{Z}_p)_y \to \mathbf{Z}_p$, 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 $\frac{1}{p}\big(xp - \frac{(xp)^2}{2} + \cdots\big) \in \mathbf{Z}_p[[x]]$.

In [EL21, Lemma 6.6.8] the residue disk $T_f(\mathbf{Z}_p)_{\bar{t}}$ 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 [Mas20], where the Khuri-Makdisi representation [KM04] 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 $T_f(\mathbf{Z}_p)_{\bar{t}}$ and $\mathbf{Z}_p^{g+1}$ that is not a parametrization in the sense of Definition 7.3.5. To describe the relationship between this bijection and the parametrization of this residue disk we need the framework of convergent power series.

Definition 7.3.7. Let $n \in \mathbf{N}$. The ring of convergent power series in n variables is defined as

$$\mathbf{Z}_p\langle x_1, \ldots, x_n\rangle := \{g \in \mathbf{Z}_p[[x_1, \ldots, x_n]] : \forall M, g \bmod p^M \text{ is a polynomial}\}.$$

It consists of those power series converging on all of $\mathbf{Z}_p^n$. Unlike normal power series, one can always compose two converging power series, as by definition the resulting infinite sum inside $\mathbf{Z}_p\langle x_1, \ldots, x_n\rangle$ converges.

Remark 7.3.8. Let Y be a smooth scheme over $\mathbf{Z}_p$ of relative dimension d, let $y \in Y(\mathbf{F}_p)$, and let $\theta, \theta' : Y(\mathbf{Z}_p)_y \to \mathbf{Z}_p^d$ be two parametrizations. Then the composite $\theta' \circ \theta^{-1} : \mathbf{Z}_p^d \to \mathbf{Z}_p^d$ is given by (multivariate) convergent power series that are linear modulo p, and in fact are of degree at most M modulo p^M.

As discussed above, we can find a bijection between residue disks of T_f and $\mathbf{Z}_p^{g+1}$ using the logarithm of the Jacobian, which gives an isomorphism $\log : J(\mathbf{Z}_p)_0 \to p\mathbf{Z}_p^g$ by choosing a basis of $H^0(J_{\mathbf{Z}_p}, \Omega^1)$.

Definition 7.3.9. Recall that we fixed a $\bar{t} \in T_f(\mathbf{F}_p)$. Choose $\widetilde{t} \in T_f(\mathbf{Z}_p)_{\bar{t}}$ to be a lift of $\bar{t}$. Let $\varphi_f : T_f(\mathbf{Z}_p)_{\bar{t}} \to \mathbf{Z}_p^{g+1}$ be defined by

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

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

Similarly to Example 7.3.6, this is not a parametrization; it shares some of the

properties of a parametrization, notably the property in Remark 7.3.8, as the following lemma shows.

Lemma 7.3.10. *The pseudoparametrization φ_f is a bijection, and for any parametrization $\theta : T_f(\mathbf{Z}_p)_{\bar{t}} \to \mathbf{Z}_p^{g+1}$ the resulting map $\varphi_f \circ \theta^{-1} : \mathbf{Z}_p^{g+1} \to \mathbf{Z}_p^{g+1}$ is given by convergent power series that are linear modulo p.*

Proof. Recall that the $\mathbf{G}_m(\mathbf{Z}_p)$-torsor $T_f(\mathbf{Z}_p)_{\bar{t}}$ over $J(\mathbf{Z}_p)_{\xi_f(\bar{t})}$ is trivial. In fact, we can say something stronger: for $Y/\mathbf{Z}_p$ a scheme, and $y \in Y(\mathbf{F}_p)$, as in [EL21, Section 3] write $\widetilde{Y}_y^p$ for the scheme representing points reducing to y, i.e. such that we have $\widetilde{Y}_y^p(S) = Y(S)_y$ for S a ring over $\mathbf{Z}_p$. Then the trivialization gives us an isomorphism

$$\widetilde{T}_{\bar{t}}^p \cong \widetilde{J}^p_{\xi_f(\bar{t})} \times \widetilde{\mathbf{G}_{mu}}^p$$

for some unit $u \in \mathbf{F}_p$. By Remark 7.3.8 we can take any choice of parameters, so we choose our parameters at $\bar{t}$ to come from parameters at J and $\mathbf{G}_m$. Now we can use general results on formal logarithms of group schemes over $\mathbf{Z}_p$ when $p > 2$. By [Spe20, Lemma 3.7] formal logarithms are always given by convergent power series that are linear mod p, and the desired result follows immediately. □

7.3.2 The torsor T

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

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

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

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

Again we can pseudoparametrize residue disks of T.

Definition 7.3.11. Recall that we fixed a $\bar{t} \in T_f(\mathbf{F}_p)$. We also fix $\widetilde{t} \in T_f(\mathbf{Z}_p)_{\bar{t}}$ a lift of $\bar{t}$. Let ζ_i denote the projection $T \to T_i$ for $i = 1, \ldots, \rho - 1$. Let $\varphi : T(\mathbf{Z}_p)_{\bar{t}} \to \mathbf{Z}_p^{g+\rho-1}$

be defined by

$$\varphi(t) = ((\log \xi(t) - \log \xi(\widetilde{t}))/p, \pi_{g+1} \circ \varphi_{f_1} \circ \zeta_1(t), \ldots, \pi_{g+1} \circ \varphi_{f_{\rho-1}} \circ \zeta_{\rho-1}(t)).$$

We call φ a *pseudoparametrization* of the residue disk $T(\mathbf{Z}_p)_{\overline{t}}$.

Corollary 7.3.12. *The pseudoparametrization map φ is a bijection, and for any parametrization $\theta : T(\mathbf{Z}_p)_{\overline{t}} \to \mathbf{Z}_p^{g+\rho-1}$ the resulting map $\varphi \circ \theta^{-1} : \mathbf{Z}_p^{g+\rho-1} \to \mathbf{Z}_p^{g+\rho-1}$ is given by convergent power series that are linear modulo p.*

Corollary 7.3.13. *For any parametrization $\theta : T(\mathbf{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbf{Z}_p^{g+\rho-1}$, the map $\overline{\varphi \circ \theta^{-1}} : \mathbf{F}_p^{g+\rho-1} \to \mathbf{F}_p^{g+\rho-1}$ obtained by reducing θ and φ modulo p is an affine linear isomorphism.*

Remark 7.3.14. The main advantage of this method is that for φ_f we need only to compute the map ψ defined in (7.5); it is this fact that allows to us to mainly work in $\mathcal{N}$ and only translate back to image of the residue disk under φ when needed.

Chapter 8

Algorithms for geometric quadratic Chabauty

8.1 The line bundle

In this section we describe how to explicitly construct the nontrivial $\mathbf{G}_m$-torsor T and give a formula for the section $\widetilde{j_b} : U \to T$. For this, we want to work with endomorphisms of J. We make this explicit by considering correspondences on $X_{\mathbf{Q}} \times X_{\mathbf{Q}}$ and extensions on $U \times X$.

Remark 8.1.1. 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, you can construct a regular model by repeatedly blowing up the projective closure of its generic fiber and this model is therefore projective over $\mathbf{Z}$. 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 implemented in Magma, for example. 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.

As explained in Section 7.3.2, to construct the torsor T, we need $\rho - 1$ independent trace zero endomorphisms $(f_i)_{i=1}^{\rho-1} : J \to J$. (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 $X(\mathbf{Z})$ for higher n. In fact,

if we use n nontrivial independent endomorphisms such that $r < g + n - 1$, then we expect to cut out $X(\mathbf{Z})$ exactly unless there is some geometric reason for extra points.) To work with any endomorphism $f : J \to J$ explicitly, we recall some facts about correspondences, as can be found in [Smi05]. 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 $\pi_1^{D_i} : D_i \to X$ 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 8.1.2. Take the negation $-1\cdot : J \to J$ 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 $\widetilde{j_b} : U \to T$. For this latter goal, we partially follow [EL21, Section 7]. In the case where $X_{\mathbf{Q}}$ is a classical modular curve we can construct many trace zero endomorphisms using the Hecke algebra. See for example the computation leading to (9.4) in Chapter 9.

We now focus on the computations for a single trace zero endomorphism $f : J \to J$. We can compute equations for a correspondence $D_{f,\mathbf{Q}} \subset X_{\mathbf{Q}} \times X_{\mathbf{Q}}$ inducing f using the code of Costa, Mascot, Sijsling, and Voight [CMSV19]. The input of that algorithm is the 2×2 matrix giving the representation of the morphism f on a basis of differential forms $H^0(X_{\mathbf{Q}}, \Omega^1)$.

Algorithm 8.1.3 (Compute A_α).
Input: $D_f \subset X_{\mathbf{Q}} \times X_{\mathbf{Q}}$ a divisor.
Output: a divisor A_α on $U \times X$.

1. Spread out $D_{f,\mathbf{Q}}$ to D'_f over $U \times X$ by clearing denominators of the generators of the Groebner basis.

2. Set $B := D'_f|_{U\times b}$ and $C := D'_f|_{\Delta_U}$.
3. Set $A_\alpha := m\left(D'_f - B\times X + U\times B - U\times C\right)$ (where m is defined in (6.1)).
4. Return A_α, as a Groebner basis over $\mathbf{Z}$.

Lemma 8.1.4. *The divisor A_α on $U\times X$ given by Algorithm 8.1.3 has the following properties:*

(a) the endomorphism of J induced by the correspondence A_α is still f;

(b) $\mathcal{O}_U(A_\alpha|_{U\times b})$ is rigidified with trivializing section 1;

(c) $\mathcal{O}_U(A_\alpha|_\Delta)$ is rigidified, compatible with the previous rigidification;

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

Proof. Since the endomorphism induced by a divisor does not change under the addition of horizontal or vertical divisors [Smi05, Theorem 3.4.7], then (a) holds. A quick computation of restricting A_α to $U\times b$ and Δ shows that A_α is constructed so that (b) and (c) are true. Finally, by [BL04, 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 8.1.5. Conditions (d) and (b) are the other way from the order chosen in Edixhoven–Lido, in order to agree with the convention in [CMSV19]. (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 $\mathcal{L}_\alpha = \mathcal{O}_{U\times X}(A_\alpha)$ on $U\times X$, rigidified on $U\times b$, of degree 0 on the fibers of the first projection, and such that $\Delta^*\mathcal{L}_\alpha$ is trivial. This induces the endomorphism f by

$$[x-y] \mapsto (\mathcal{L}_\alpha)_{x\times X}\otimes(\mathcal{L}_\alpha)^{-1}_{y\times X}. \tag{8.1}$$

Corollary 8.1.6. *Let $c := [(\mathcal{L}_{\alpha,\mathbf{Q}})_{b\times X}] \in J(\mathbf{Q}) = J(\mathbf{Z})$. Let $\alpha = m\cdot\circ\,\mathrm{tr}_c\circ f$ be the morphism $\alpha : J\to J^0$. Then $j_b^*(id,\alpha)^*\mathcal{M}^\times$ is trivial over U.*

Proof. This follows directly from [EL21, 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 8.1.7 (Compute c).
Input: equations for a correspondence A_α inducing the morphism $f : J \to J$.
Output: a divisor representing $c = [(\mathcal{L}_\alpha)_{b\times X}] \in J(\mathbf{Q}) = J(\mathbf{Z})$.

1. Compute the generic fiber $A_{\alpha,\mathbf{Q}}$ of A_α.
2. Compute equations for the divisor $A_{\alpha,\mathbf{Q}}|_{b\times X}$ by specializing the equations of $A_{\alpha,\mathbf{Q}}$ to b in the first two coordinates.
3. Return a Groebner basis for $A_{\alpha,\mathbf{Q}}|_{b\times X}$ over $\mathbf{Q}$.

Algorithm 8.1.8 (Compute f_*).
Input: a morphism of projective schemes $f : X \to Y$ given as a graded ring morphism $f^* : S \to R$, 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 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 to be the ideal $(b - f^*(b) \mid b \in B)$.
3. Compute a Groebner basis for I.
4. Compute the degree $d := \deg f|_Z \to \operatorname{Proj} S/I$.
5. Return a Groebner basis for I^d.

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

Remark 8.1.9. In Step 4, 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 [Sta18] for a discussion on an implementation in Macaulay2.

Algorithm 8.1.10 (Apply f).
Input: a ring S and two effective divisors D_+ and D_- on U of the same degree; the correspondence A_α from Algorithm 8.1.3 inducing the morphism $f : J \to J$.
Output: the Jacobian point $f([D_+ - D_-]) \in J(S)$.

1. For $D \in \{D_+, D_-\}$ do:
   (a) Compute a Groebner basis for $A_\alpha|_{D\times X}$ as a divisor on $D \times X$.

(b) Write $D = \sum_i n_i D_i$ as a sum of prime divisors using primary decomposition.

(c) Compute the Groebner basis for the pushforward $E(D_i) := n_i f_*(D_i)$ on X using Algorithm 8.1.8 for every D_i.

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

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

Remark 8.1.11. 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 $\widetilde{j_b} : U \to T$ lying above the Abel–Jacobi map $j_b : U \to J$ with basepoint b. Let $\bar{z} \in X(\mathbf{F}_p)$. Since the pullback $j_b^* T$ is trivial, there is a morphism $\widetilde{j_b} : U \to T$ embedding each residue disk $U(\mathbf{Z}_p)_{\bar{z}}$ into the $(g + \rho - 1)$-dimensional residue disk $T(\mathbf{Z}_p)_{\widetilde{j_b}(\bar{z})}$, where $z \in U(\mathbf{Z}_p)$. To compute this map, we follow [EL21, 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 [EL21, 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 8.1.4 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 $U_{\mathbf{F}_q}$. In our case, these are always 0. It remains to compute the 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. We define V to be the unique vertical divisor on $U \times X$ such that $\mathcal{L}_\alpha(V)$ has multidegree 0 on all fibers of the projection having support disjoint from $U \times b$. Then $V_{\mathbf{F}_q}$ is a sum of irreducible components of $U_{\mathbf{F}_q} \times X_{\mathbf{F}_q}$ and hence splits as a linear combination of $U_{\mathbf{F}_q} \times Y_{\mathbf{F}_q}$ where $Y_{\mathbf{F}_q}$ is an irreducible component of $X_{\mathbf{F}_q}$. Then for $q \mid n$ we let $V_q \in \mathbf{Z}$ be the coefficient of the component $(U_{\mathbf{F}_q} \times U_{\mathbf{F}_q})$ in $V_{\mathbf{F}_q}$. (Note that $V_{\mathbf{F}_q}$ is not V_q.) To compute these numbers, we give the following algorithm.

Remark 8.1.12. By our choice of A_α, the section ℓ trivializing $\Delta^*(\mathcal{L}_\alpha)$ is canonically 1 over all of $\mathbf{Z}$ and hence the W_q are always 0 in our case.

Algorithm 8.1.13 (Calculate V_q).
Input: the curve X, a bad prime q dividing n, the open set U such that $U(\mathbf{F}_q) \neq \emptyset$, and the divisor A_α on $X \times X$.
Output: the integer V_q.

1. Pick a point $\overline{Q} \in U(\mathbf{F}_q)$.
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 $X_{\mathbf{F}_q}$.
5. Compute the unique linear combination $D \subset X_{\mathbf{F}_q}$ 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 p.
6. Set V_q to be the coefficient of the irreducible component containing $U_{\mathbf{F}_q}$ in D.
7. Return V_q.

Remark 8.1.14. If $U(\mathbf{F}_q)$ is empty for some prime q, we can discard U. Integer points reduce to smooth points, so $U(\mathbf{Z}) = \emptyset$ in this case.

By [EL21, Proposition 7.5] we have

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

We apply [EL21, Proposition 7.8] to give a formula for $\widetilde{j_b}(z)$.

$$\widetilde{j_b}(z) = \prod_{q|n} q^{-V_q}(z^*1) \otimes (b^*1)^{-1} = (z-b)^* \prod_{q|n} q^{-V_q} \in (z-b)^*\mathcal{O}_X(A_\alpha|_{z\times X}) \tag{8.2}$$

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

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

Remark 8.1.15. If the open U contains a $\mathbf{Z}$-point $Q \in U(\mathbf{Z})$, then it is not necessary to compute the V_q. In this case, we can instead use the fact that $\psi(\widetilde{j_b}(Q))$ is $\psi(t)$ where t

is the $\mathbf{Z}$-point (unique up to sign) of T lying above $Q-b$. Then using Proposition 7.3.3 we can compute $\psi(t)$, find the height $h_p(Q-b, A_\alpha|_{Q\times X})$ and read off the difference $\sum_{q|n} V_q \log q$.

8.2 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 $\overline{P} \in U(\mathbf{F}_p)$.

Recall the pseudoparametrization $\varphi : T(\mathbf{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbf{Z}_p^{g+\rho-1}$ from Definition 7.3.11. Let $\mathbf{Z}_p \to U(\mathbf{Z}_p)_{\overline{P}}$ be a parametrization of the residue disk. Define the map $\lambda : \mathbf{Z}_p \to T(\mathbf{Z}_p)_{\widetilde{j_b}(\overline{P})}$ to be the composite of this parametrization $\mathbf{Z}_p \to U(\mathbf{Z}_p)_{\overline{P}}$ and $\widetilde{j_b}$. In this section show how to apply the following proposition.

Proposition 8.2.1. *The map $\varphi \circ \lambda$ is given by convergent power series that are linear modulo p and its image is cut out by equations $f_1 = \cdots = f_{g+\rho-2} = 0$ with $f_1, \ldots, f_{g+\rho-2} \in \mathbf{Z}_p\langle x_1, \ldots, x_{g+\rho-1}\rangle$ convergent power series that are linear modulo p.*

Proof. This follows from Corollary 7.3.12. □

We first present a general algorithm to compute the trivializing section $\varphi \circ \lambda$. Let ν be a local parameter in the residue disk of the curve above $\overline{P}$. We can parametrize this residue disk up to finite precision by

$$\mathbf{F}_p \to U(\mathbf{Z}/p^2\mathbf{Z})_{\overline{P}}, \quad \nu \mapsto P_\nu.$$

To compute $\widetilde{j_b}(P_\nu)$ in $\mathcal{N}$, 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 $U(\mathbf{Z}/p^2\mathbf{Z})_{\overline{P}}$, we can interpolate between these values to determine the map. Therefore it is enough to determine the map on $\mathbf{Z}/p^2\mathbf{Z}$ points. We give an algorithm to compute $\widetilde{j_b}(P)$ when P is a $\mathbf{Z}/p^2\mathbf{Z}$ point.

Algorithm 8.2.2 (The trivializing section).

Input: A point $P_\nu \in U(\mathbf{Z}/p^2\mathbf{Z})_{\overline{P}}$.
Output: the value $\varphi \circ \lambda(P_\nu)$.

1. Calculate the Coleman integral $\log(P_\nu - b)$.
2. Compute $A_{\alpha_i}|_{P_\nu \times X}$ for each $i = 1, \ldots, (g + \rho - 1)$ using Algorithm 8.1.10.
3. Calculate all $h_p(P_\nu - b, A_{\alpha_i})$.
4. Set

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

5. Return $(\varphi \circ \lambda)(P_\nu)$.

We will describe a practical algorithm to do Step (3) of Algorithm 8.2.2 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 divisors [BB12, Algorithm 5.7]. Forthcoming work of Gajović extends this algorithm to even degree models. Furthermore, divisors and their arithmetic can be made explicit through Mumford representations, as we now explain.

Definition 8.2.3. Let $Y : y^2 = H(x)$ be a hyperelliptic curve over k of genus g such that $H(x)$ has degree $2g + 1$. Let $D = \sum_i n_i P_i$ be an effective divisor in $\mathrm{Div}(Y)$. Let ι denote the hyperelliptic involution. If $P_i \neq \iota(P_j)$ for all $i \neq j$ and D is disjoint from ∞ we say D is in general position.

Definition 8.2.4. Let $D \in \mathrm{Div}(Y)$ be a divisor in general position and write $D = \sum_i n_i P_i$ with $P_i = (x_i, y_i)$. The Mumford representation of is the pair of polynomials (u, v) defined by

$$u(x) := \prod_i (x - x_i)^{n_i}$$

and v is the unique polynomial such that $\deg v < \deg u$ and u divides $H - v^2$. We write $\mathrm{Div}(u, v) = D$.

It is reduced if $\deg u \leq g$.

The following composition and reduction algorithms can be found in [Sut19, Section 3]. We apply these algorithms and associated code to carry out the related computations. In Algorithm 8.2.7 we emphasize the explicit nature of Cantor's algorithm to obtain the linear equivalence as well as the reduced divisor.

Algorithm 8.2.5 (Compose).
Input: (u_1, v_1) and (u_2, v_2) Mumford representations for D and E in $\mathrm{Div}(Y)$ such that $D + E$ is also in general position.
Output: (w, z) the Mumford representation for $D + E$.

1. Compute $c_1, c_2, c_3 \in k[x]$ such that $1 = c_1u_1 + c_2u_2 + c_3(v_1 + v_3)$.
2. Set $w := u_1u_2$.
3. Set $z := ((c_1u_1v_1 + c_2u_2v_1 + c_3(v_1v_2 + H))/w) \mod u_3$.
4. Return (w, z).

Remark 8.2.6. If $D + E$ is not in general position, Algorithm 8.2.5 can be modified to return the Mumford representation for a divisor that is linearly equivalent to $D + E$, obtained by removing any pairs z and $\iota(z)$ in the support of $D + E$. Instead of Step (1), define $d := \gcd(u_1, u_2, v_1 + v_2)$ and compute $c_1, c_2, c_3 \in k[x]$ such that $d = c_1u_1 + c_2u_2 + c_3(v_1 + v_3)$, and then set $w := u_1u_2/d^2$ in Step (2).

Algorithm 8.2.7 (Reduce).
Input: (u, v) the Mumford representation for a divisor $D \in \mathrm{Div}(Y)$ with $\deg u > g+1$.
Output: (w, z) a reduced Mumford representation and s a rational function such that $\mathrm{Div}(w, z) + \mathrm{Div}\, s = D$ and $\deg w \leq g + 1$.

1. Set $s := 1$.
2. Write $\lambda u' := H - v^2/u$ for $\lambda \in k$ and $u' \in k[x]$ monic.
3. Set $s := s \cdot (y - v)/u'$.
4. Set $v' := -v \mod u'$.
5. If $\deg u' > g + 1$, set $u := u'$ and $v := v'$ and go to back Step (2). Otherwise set $w := u'$ and $z := v'$ and return (w, z) and s.

We can now give a practical algorithm to compute the local heights in Step (3) of Algorithm 8.2.2. When X is a hyperelliptic curve of the form $y^2 = H(x)$, given

$P_\nu \in U(\mathbf{Z}/p^2\mathbf{Z})$ we can apply Algorithm 8.1.10 to obtain $A_{\alpha_i}|_{P_\nu \times X}$ as a divisor on $X_{\mathbf{Q}_p}$.

Remark 8.2.8. When describing a divisor on a hyperelliptic curve over a field, it is often easier to work with the Mumford representation of a representing divisor. We can translate from a Groebner basis to a Mumford representation in the following way. Let X be a hyperelliptic curve over a field k given by $y^2 = H(x)$. Let $\pi : X \to \mathbf{P}^1$ 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 X, 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 $\mathbf{P}^1$ such that $D - \pi^* E$ is disjoint from $\iota(D - \pi^* E)$, and hence find a Mumford representation for $D - \pi^* E$.

Algorithm 8.2.9 (Local heights for the trivializing section on a hyperelliptic curve).
Input: A point $P_\nu \in U(\mathbf{Z}/p^2\mathbf{Z})_{\overline{P}}$ on a hyperelliptic curve $X : y^2 = H(x)$ and the Mumford representation of $A_{\alpha_i}|_{P_\nu \times X}$ as a divisor on X.
Output: the value $h_p(P_\nu - b, A_{\alpha_i}|_{P_\nu \times X})$.

1. Set $n := 1$.
2. Use Algorithm 8.2.5 and Algorithm 8.2.7 to compute a Mumford representation (u_n, v_n) and a rational function s_n such that $\mathrm{Div}(u_n, v_n) + \mathrm{Div}\, s_n = nA_{\alpha_i}|_{P_\nu \times X}$.
3. Check if u_n factors completely over $\mathbf{Q}_p$ 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 $Q_i := (x_i, y_i) \in X(\mathbf{Q}_p)$.
7. Compute $h_p(P_\nu - b, \sum_{i=1}^{\deg(u_n)} Q_i - \deg(u_n)\infty)$ using [BB12, 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 8.2.9 does not always terminate; we cannot guarantee that eventually $nA_{\alpha_i}|_{P_\nu \times X}$ splits completely into a sum of points over $\mathbf{Q}_p$.

8.3 Integer points of the torsor

Next we discuss the integer points of the torsor T. We give an algorithm to construct a map $\kappa : \mathbf{Z}_p^{g+\rho-1} \to T(\mathbf{Z}/p^2\mathbf{Z})_{\widetilde{j_b(\overline{P})}}$ with image exactly $\overline{T(\mathbf{Z})}_{\widetilde{j_b(\overline{P})}}$. In practice, to give an upper bound on $\#U(\mathbf{Z})_{\overline{P}}$, we only need to compute the image of the map κ in $T(\mathbf{Z}/p^2\mathbf{Z})_{\widetilde{j_b(\overline{P})}}$, because after composing with the pseudoparametrization φ from Definition 7.3.11 the map κ is given by convergent power series.

Note that if the residue disk $T(\mathbf{Z})_{\widetilde{j_b(\overline{P})}}$ 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 $\widetilde{t} \in T(\mathbf{Z})_{\widetilde{j_b(\overline{P})}}$ by arithmetic in the Jacobian. It is enough to consider if the corresponding residue disk $J(\mathbf{Z})_{\widetilde{j_b(\overline{P})}}$ 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 of generating sections on certain fibers of $\mathcal{M}^\times$.

We construct integer points on $\mathcal{N}$ that are the image of generating sections of residue disks of $\mathcal{M}^\times$ following the method in Example 7.2.6. Let $G_1, \ldots, G_{r'}$ be a generating set for the full Mordell–Weil group, with $r' \geq r$.

Algorithm 8.3.1 (Compute the Q_{ij}).
Input: Representing divisors $G_1, \ldots, G_{r'}$ for a generating set of the Mordell–Weil group of J, a trace zero endomorphism $f : J \to J$, an $\mathbf{F}_p$-point $\overline{P} \in U(\mathbf{Z}_p)_{\overline{P}}$.
Output: Integer points Q_{ij} on $\mathcal{N}$ that are the image of the generating section of $\mathcal{M}^\times(G_i, f(G_j))(\mathbf{Z})$ and Q_{i0} that are the image of the generating section of $\mathcal{M}^\times(G_i, c)(\mathbf{Z})$ for $1 \leq i, j \leq r'$.

1. For each G_i, use Algorithm 8.1.10 to compute representing divisors $D_1, \ldots, D_{r'}$ of $f(G_i)$.
2. Use Algorithm 8.1.7 to compute a divisor D_0 whose class is the point $c \in J$.
3. Compute the local height $h_p(G_i, D_j)$ and $h_p(G_i, D_0)$ for $1 \leq i, j \leq r'$.
4. Using [vBHM20, Section 2], compute the height $h_\ell(G_i, D_j)$ at $\ell \neq p$ and $h_\ell(G_i, D_0)$ at $\ell \neq p$ for $1 \leq i, j \leq r'$.

5. Return $Q_{ij} := (G_i, f(G_j), \sum_{\ell \text{ prime}} h_\ell(G_i, D_j))$ and
   $Q_{0i} := (G_i, c, \sum_{\ell \text{ prime}} h_\ell(G_i, D_0))$ for $1 \le i, j \le r'$.

Let $\widetilde{G_i}$ be a basis for the kernel of reduction $J(\mathbf{Z}) \to J(\mathbf{F}_p)$ for $i = 1, \ldots, r$. (Note that the reduction map is injective when restricted to the torsion of $J(\mathbf{Z})$, so the kernel of reduction is a free $\mathbf{Z}$-module of rank r.) Write

$$\widetilde{G_i} = \sum_{j=1}^{r'} e_{ij} G_j$$

for some $e_{ij} \in \mathbf{Z}$. Let $\widetilde{G_t}$ denote the projection of $\tilde{t} \in T(\mathbf{Z})_{\widetilde{j_b(\overline{P})}}$ to $J_{j_b(\overline{P})}$. Write

$$\widetilde{G_t} = \sum_{i=1}^{r'} e_{0i} G_i$$

for some $e_{0i} \in \mathbf{Z}$. Using the biextension group laws and the points Q_{ij} we construct a series of points in $\mathcal{M}^\times$ living over certain points in $J \times J$ that are the image of generating sections of the corresponding residue disks in $\mathcal{M}^\times(\mathbf{Z})$.

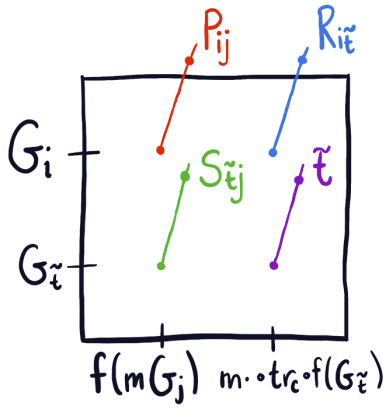

Figure 8.1: A schematic of the constructed integer points above $J \times J$

A formula for the points P_{ij} over $(\widetilde{G_i}, f(m\widetilde{G_j}))$ is

$$P_{ij} := \sum_{k=1}^{r'}{}_1 \, e_{ik} \cdot_1 \left(\sum_{\ell=1}^{r'}{}_2 \, m \cdot_2 e_{j\ell} \cdot_2 Q_{k\ell} \right). \tag{8.3}$$

Here, $\cdot_i$ and $\sum_i$ for $i = 1, 2$ denote the biextension group laws (7.4) and (7.3).

Now we construct $\tilde{t}$, a $\mathbf{Z}$-point living over $(\widetilde{G_t}, m\alpha(\widetilde{G_t}))$.

$$\tilde{t} := \sum_{k=1}^{r'}{}_1 \, e_{0k} \cdot_1 \left(m \cdot_2 Q_{k0} +_2 \sum_{\ell=1}^{r'}{}_2 \, m \cdot_2 e_{0\ell} \cdot_2 Q_{k\ell} \right). \tag{8.4}$$

Next $R_{i\tilde{t}}$ live over $(\widetilde{G_i}, m\alpha(\widetilde{G_t}))$ and hence

$$R_{i\tilde{t}} := \sum_{k=1}^{r'}{}_1 \, e_{ik} \cdot_1 \left(m \cdot_2 Q_{k0} +_2 \sum_{\ell=1}^{r'}{}_2 \, m \cdot_2 e_{0\ell} \cdot_2 Q_{k\ell} \right). \tag{8.5}$$

Finally, $S_{\tilde{t}j}$ live over $(\widetilde{G_t}, f(m\widetilde{G_j}))$ and so

$$S_{\tilde{t}j} := \sum_{k=1}^{r'}{}_1 \, e_{0k} \cdot_1 \left(\sum_{\ell=1}^{r'}{}_2 \, m \cdot_2 e_{j\ell} \cdot_2 Q_{k\ell} \right). \tag{8.6}$$

Remark 8.3.2. In $\mathcal{M}^\times$, these points are all unique up to sign. Since we are recording the image in $\mathcal{N}$, this sign does not matter.

For $n = (n_1, \ldots, n_r) \in \mathbf{Z}^r$ we can now construct the points $A_{\tilde{t}}(n)$, $B_{\tilde{t}}(n)$, $C_{\tilde{t}}(n)$, and $D_{\tilde{t}}(n)$ in $T(\mathbf{Z})$ given by [EL21, (4.2)-(4.4)]. The key property of this construction is that $D_{\tilde{t}}(n)$ lies above the point $\widetilde{j_b}(\overline{P}) \in J(\mathbf{F}_p)$. Furthermore, by [EL21, (4.6)-(4.9)], we have that $D_{\tilde{t}}((p-1)n)$ is in the residue disk $T(\mathbf{Z})_{\widetilde{j_b}(\overline{P})}$, allowing us to explicitly construct the map

$$\kappa_{\mathbf{Z}} : \mathbf{Z}^r \to T(\mathbf{Z})_{\widetilde{j_b}(\overline{P})}, \qquad (n_1, n_2) \mapsto D_{\tilde{t}}((p-1)n_1, \ldots, (p-1)n_r), \tag{8.7}$$

Finally, by [EL21, Theorem 4.10], the map $\kappa_{\mathbf{Z}}$ extends to a bijection

$$\kappa : \mathbf{Z}_p^{g+\rho-1} \to T(\mathbf{Z}_p)_{\widetilde{j_b}(\overline{P})} \tag{8.8}$$

with image $\overline{T(\mathbf{Z})}_{\widetilde{j_b}(\overline{P})}$.

8.4 The upper bound for a single residue disk

In this section, we present the main algorithm for doing geometric quadratic Chabauty. This algorithm ties together the results of the previous sections.

Before we present this, we give the theorem for the upper bound on a single residue disk from [EL21, Theorem 4.12] phrased in terms of our set up.

Theorem 8.4.1 ([EL21, Theorem 4.12])**.** *Consider $X(\mathbf{Z})_{\overline{P}}$ a residue disk of X and recall κ as in 8.8. Recall also the bijection φ given in Definition 7.3.11.*

Let $f_1, f_2, \dots, f_{g+\rho-2} \in \mathbf{Z}_p\langle z_1, \dots, z_{g+\rho-1}\rangle$ be the convergent power series cutting out the image of $\varphi \circ \widetilde{j_b}$ given by Proposition 8.2.1. Let $g_i := (\varphi \circ \kappa)^* f_i \in \mathbf{Z}_p\langle n_1, \dots, n_r\rangle$ for $i = 1, \dots, (g+\rho-2)$.

Denote by $\overline{g_i}$ the image of these power series in $\mathbf{F}_p[n_1, \dots, n_r]$. They are at most quadratic. Furthermore, if $\bar{A} := \mathbf{F}_p[n_1, \dots, n_r]/(\overline{g_1}, \dots, \overline{g_{g+\rho-2}})$ is finite, then the size of the common zero set $S := Z(\overline{g_1}, \dots, \overline{g_{g+\rho-2}})$ in $\mathbf{F}_p^r$ is an upper bound on $\#X(\mathbf{Z})_{\overline{P}}$, with each element in $\overline{\kappa}(S) \in T(\mathbf{Z}/p^2\mathbf{Z})_{\widetilde{j_b}(\overline{P})}$ lifting to at most one point in $\widetilde{j_b}(U(\mathbf{Z}_p)_{\overline{P}}) \cap \operatorname{im} \kappa$.

Using Theorem 8.4.1 we can compute the intersection of the curve and the integer points of the torsor, when this is finite.

Algorithm 8.4.2 (Geometric quadratic Chabauty).
Input:

- $X_{\mathbf{Q}}/\mathbf{Q}$ a smooth, projective, geometrically irreducible curve over $\mathbf{Q}$ such that $X_{\mathbf{Q}}(\mathbf{Q}) \neq \varnothing$ 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;
- an open set $U \subset X^{\mathrm{sm}}$ containing the smooth points of one irreducible component of $X_{\mathbf{F}_q}$ for all primes q;
- a prime $p > 2$ of good reduction for X;
- a basepoint $b \in X(\mathbf{Z})$;
- a point $\overline{P} \in U(\mathbf{F}_p)$;

- a generating set $G_1, \dots, G_{r'}$ of the Mordell–Weil group of J.

Output: a finite subset of $U(\mathbf{Z}/p^2\mathbf{Z})_{\overline{P}}$ containing $U(\mathbf{Z})_{\overline{P}}$, or FAIL.

1. Compute the correspondence A_α that induces the endomorphism $f : J \to J$ as given in Lemma 8.1.4.
2. Find the divisor representing $c = [(\mathcal{L}_\alpha)_{b\times X}] \in J$ using Algorithm 8.1.7.
3. Calculate the values $\varphi \circ \lambda(P_0)$ and $\varphi \circ \lambda(P_1)$ obtained from applying Algorithm 8.2.2. Interpolate these two results to find equations for the linear map $\varphi \circ \lambda$.
4. With the generating set $G_1, \dots, G_{r'}$, use Algorithm 8.3.1 to compute integer points $Q_{i0}, Q_{ij} \in \mathcal{N}$ that are the images of the generating sections of $\mathcal{M}^\times(G_i, f(G_j))(\mathbf{Z})$ and $\mathcal{M}^\times(G_i, c)(\mathbf{Z})$ for $1 \le i, j \le r'$.
5. Using the elements Q_{ij}, find the map $\kappa_{\mathbf{Z}} : \mathbf{Z}^r \to T(\mathbf{Z}_p)_{\tilde{j}_b(\bar{P})}$ as in (8.7) and extend it to the map $\kappa : \mathbf{Z}_p^r \to T(\mathbf{Z}_p)_{\tilde{j}_b(\bar{P})}$.
6. Compute the intersection of $\varphi \circ \lambda$ and $\varphi \circ \kappa$: define $f_1, \dots, f_{g+\rho-1}$ by Proposition 8.2.1 and let $g_i := (\varphi \circ \kappa)^* f_i$. Compute $\bar{A} := \mathbf{F}_p[n_1, \dots, n_r]/(\overline{g_1}, \dots, \overline{g_{g+\rho-2}})$ from Theorem 8.4.1 and check if it is finite. If it is finite, return the intersection of $\varphi \circ \lambda$ and $\varphi \circ \kappa$ by computing the common zeros S of $\overline{g_i}$. Otherwise, return FAIL.

To compute a finite set of p-adic points containing $X(\mathbf{Z})$, we construct an open covering $\{U_i\}_{i\in I}$ of X^{sm} such that each U_i contains the smooth points of one irreducible component of $X_{\mathbf{F}_q}$ for all primes q. We iterate Algorithm 8.4.2 over all U_i and all residue disks of U_i.

Remark 8.4.3. If Algorithm 8.4.2 returns FAIL, not all hope is lost. In fact, [EL21, Section 9.2] proves that $\widetilde{j_b}(U(\mathbf{Z}_p)) \cap \overline{T(\mathbf{Z})}$ is always finite. If calculations modulo p^2 do not yield a finite upper bound, one can look at a higher precision by considering the residue disks $U(\mathbf{Z}_p)_{\overline{P}}$, where $\overline{P} \in U(\mathbf{Z}/p^k\mathbf{Z})$ for some integer k. An example of the geometric Chabauty method with precision p^3 is given in Remark 9.0.11.

Remark 8.4.4. In practice, to run Algorithm 8.4.2 we need to be able to compute local Coleman–Gross heights on the curve X. Currently, this has only been made algorithmic for hyperelliptic curves.

Chapter 9

An example of the geometric quadratic Chabauty method

We give an example of the implementation on the modular curve $X_0(67)^+$ of the algorithms presented in Chapter 8. The rational points on this curve have already been determined [BBB+21] using quadratic Chabauty and a Mordell–Weil sieve, but we can also use the methods presented here to show the following theorem about the rational points of the curve. 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 $\mathbf{P}^2_{(1,3,1)}$. Then $X(\mathbf{Q}) = X(\mathbf{Z})$ and we show the following.

Theorem 9.0.1. *The integer points of $X(\mathbf{Z})$ that do not reduce to $(1, 4) \in X(\mathbf{F}_7)$ are contained in the set*

$$\begin{aligned}
&\{[0 : -1 : 1], [4 \cdot 7 + O(7^2) : 6 + 6 \cdot 7 + O(7^2) : 1],\\
&[0 : 0 : 1], [(4 \cdot 7 + O(7^2) : 3 \cdot 7 + O(7^2) : 1)],\\
&[1 : 0 : 1], [1 + 2 \cdot 7 + O(7^2) : 5 \cdot 7 + O(7^2) : 1],\\
&[1 : -3 : 1], [1 + 2 \cdot 7 + O(7^2) : 4 + O(7^2) : 1],\\
&[1 : -1 : 0], [1 : 6 + 3 \cdot 7 + O(7^2) : 3 \cdot 7 + O(7^2)],\\
&[1 : 0 : 0], [1, 4 \cdot 7 + O(7^2), 4 \cdot 7 + O(7^2)]\}.
\end{aligned}$$

Remark 9.0.2. The residue disk above $(1, 4) \in X(\mathbf{F}_7)$ 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, using the notation of Theorem 8.4.1, the ring $\mathbf{F}_p[n_1, n_2]/(\overline{g_1}, \overline{g_2}) \simeq \mathbf{F}_p[n_2]$ is not finite.

In theory, by increasing the precision one should be able to find a finite list of p-adic points lying above this residue disk. However, we ran into issues computing the required heights in Sage and Magma. The Sage code [Bal] has difficulty computing a required p-adic field extension and the Magma implementation of p-adic heights in [BMTV] does not currently implement p-adic heights at infinity, which are necessary when computing the map $\widetilde{j_b}$ using Algorithm 8.2.9. We are working on implementing local heights at infinity in Magma to resolve this technical issue.

Remark 9.0.3. In [HS22], together with Spelier, we give the following comparison between the geometric linear Chabauty method and the Chabauty–Coleman methods, showing that the geometric linear Chabauty method refines the Chabauty–Coleman method.

Let $\mathcal{X}/\mathbf{Z}_{(p)}$ be a smooth model for the curve X over the local ring. Let $\mathcal{J}/\mathbf{Z}_{(p)}$ be the Jacobian of $\mathcal{X}$.

Theorem 9.0.4 ([HS22, Theorem 4.1]). *Let $\mathcal{X}(\mathbf{Z}_p)_{\mathrm{GLC}}$ and $\mathcal{X}(\mathbf{Z}_p)_1$ be the finite subsets of $\mathcal{X}(\mathbf{Z}_p)$ produced by the geometric linear Chabauty and Chabauty–Coleman methods respectively. We have the inclusions*

$$\mathcal{X}(\mathbf{Z}_{(p)}) \subseteq \mathcal{X}(\mathbf{Z}_p)_{\mathrm{GLC}} \subseteq \mathcal{X}(\mathbf{Z}_p)_1.$$

Furthermore, for any point $R \in \mathcal{X}(\mathbf{Z}_p)_1 \setminus \mathcal{X}(\mathbf{Z}_p)_{\mathrm{GLC}}$, one of the following two conditions holds:

1. *the point $\overline{R}$ fails the Mordell–Weil sieve at p, i.e. the image of $R - b$ in $\mathcal{J}(\mathbf{F}_p)$ is not contained in the image of $\overline{\mathcal{J}(\mathbf{Z}_{(p)})}$ in $\mathcal{J}(\mathbf{F}_p)$;*
2. *or for $T \in \mathcal{J}(\mathbf{Z}_{(p)})_{\overline{R-b}}$, the element $\log(R - b - T)$ is not in the $\mathbf{Z}_p$-submodule $\log \overline{\mathcal{J}(\mathbf{Z}_{(p)})}_0$ of $H^0(\mathcal{J}_{\mathbf{Z}_p}, \Omega^1_{\mathcal{J}_{\mathbf{Z}_p}})^\vee$, only in its p-saturation $\log N_0$.*

It would be interesting to compare the corresponding sets for the (cohomological) quadratic Chabauty [BD18, BD21] and geometric quadratic Chabauty methods [EL21] and understand if a similar theorem holds. The algorithms described in the preceding chapters lay the groundwork for such a comparison, since Algorithm 8.4.2 describes the geometric quadratic Chabauty method using the same heights that appear in the cohomological method.

We present the computations in a single residue disk over $\overline{P} = (0, -1) \in X(\mathbf{F}_7)$ where we show the following.

Proposition 9.0.5. *The integer points of* $X(\mathbf{Z})$ *reducing to* $(0,-1) \in X(\mathbf{F}_7)$ *are contained in the set*

$$\{(0,-1),(4\cdot 7+O(7^2),6+O(7^2))\}.$$

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 [BBB+21, Section 6]. The Jacobian J has Mordell–Weil rank 2 and $J_{\mathbf{Q}}$ 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. Hence, there are only irreducible fibers over every prime.

Remark 9.0.6. For this example curve, all of the fibers are 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 $J/J^0(\overline{\mathbf{F}}_p)$, 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 $\mathbf{Z}$. Above, we consider the lists of open subschemes U of X^{sm} obtained by removing, for each bad prime q, all but one irreducible components of X^{sm}. In this example, there is only one subscheme to consider: the scheme X^{sm} obtained by removing the $\mathbf{F}_{67}$-point given by the two Galois conjugate nodes in the fiber over 67. Since X is regular, $X^{\mathrm{sm}}(\mathbf{Z}) = X(\mathbf{Z})$.

Let ι be the hyperelliptic involution of X. We list some rational points on the curve that will be used in our computations:

$$\begin{aligned}
P &:= [0:-1:1], & \iota P &:= [0:0:1],\\
Q &:= [-1:0:1], & \iota Q &:= [-1:1:1],\\
b &:= [1:0:1], & \iota b &:= [1:-3:1],\\
R &:= [1:-3:2], & \iota R &:= [1:-10:2],\\
\infty_+ &:= [1:0:0], & \infty_- &:= [1:-1:0].
\end{aligned} \tag{9.1}$$

These points turn out to be the only rational points on X, as proven in [BBB+21, Theorem 6.3] by a combination of quadratic Chabauty and the Mordell–Weil sieve.

Let $p = 7$. We perform some local computations. There are 9 points on $X(\mathbf{F}_p)$. For each $\mathbf{F}_p$-point x of X^{sm}, we need an element in $T(\mathbf{Z})_{\widetilde{j_b(x)}}$, or equivalently an element in $J(\mathbf{Z})_{j_b(x)}$. Every residue disk of $X(\mathbf{Z}_p)$ contains an integer point; only R and ιR reduce to the same point. Therefore, none of the residue disks $J(\mathbf{Z})_{j_b(x)}$ 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 [HS22, Section 3.4] for more details.

This example presents the specific case of the residue disk corresponding to $X(\mathbf{Z})_{\overline{P}}$, where P is the point defined in (9.1). 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 $j_b : X^{\mathrm{sm}} \to J$ denote the Abel–Jacobi map with basepoint b defined in (9.1). We also have a set of generators for the Mordell–Weil group $J(\mathbf{Z})$ from the LMFDB,

$$\begin{aligned} G_1 &:= [P - \iota P], \\ G_2 &:= [P + Q - 2 \cdot \iota P]. \end{aligned} \tag{9.2}$$

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 $H^0(X_{\mathbf{Q}}, \Omega^1_{X_{\mathbf{Q}}})$:

$$\left\{ \frac{dx}{2y - x^3 - x - 1}, \ \frac{x dx}{2y - x^3 - x - 1} \right\}. \tag{9.3}$$

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 $H^0(X_{\mathbf{Q}}, \Omega^1_{X_{\mathbf{Q}}})$ and $S_2(67)^+$. We choose a basis for $S_2(67)^+$ that is given by q-expansions with rational

coefficients, as follows:

$$g_1 := q - 3q^3 - 3q^4 - 3q^5 + q^6 + 4q^7 + 3q^8 + O(q^9),$$
$$g_2 := q^2 - q^3 - 3q^4 + 3q^7 + 4q^8 + O(q^9).$$

Then we choose the model for X where $\frac{du}{v}$ corresponds to $g_1\frac{dq}{q}$ and $x\frac{du}{v}$ corresponds to $g_2\frac{dq}{q}$, by setting $u = \frac{g_2}{g_1}$ and $v = q\frac{du}{g_1}$. 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 (9.3) 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 (9.3). The trace of this matrix is non-zero, so we let $f := 2T_2 + 3\,\mathrm{id} : J \to J$. The endomorphism f has trace zero and matrix representation

$$\begin{pmatrix} 1 & -2 \\ -2 & -1 \end{pmatrix} \tag{9.4}$$

with respect to the basis presented in (9.3). Using the work of [CMSV19], we can compute a divisor $D_f \subset X \times X$ inducing f. Then Algorithm 8.1.3 produces the divisor A_α that satisfies the properties of Lemma 8.1.4. The equations cutting out D_f are long and complicated and can be found at (9.11).

We now use Algorithm 8.1.10 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 (9.2).

Since $J(\mathbf{Z}) = J(\mathbf{Q})$, the divisor $f(G_i)$ only needs to be computed over the rationals for $i = 1, 2$. For example, applying (8.1) 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

$$f(G_1) = -G_1 + 2G_2 = [-(P - \iota P) + 2(P + Q - 2\iota P)] = [P + 2Q - 3\iota P], \quad (9.5)$$
$$f(G_2) = 2G_1 + G_2 = [2(P - \iota P) + 1(P + Q - 2\iota P)] = [3P + Q - 4\iota P].$$

Furthermore, we compute $c = [-11G_1 - 8G_2]$ using Algorithm 8.1.7.

We can parametrize the residue disk over $\overline{P}$ up to finite precision by

$$\mathbf{F}_p \to X(\mathbf{Z}/p^2\mathbf{Z})_{\overline{P}}, \quad \nu \mapsto P_\nu \text{ such that } x(P_\nu)/p = \nu.$$

We now find the trivializing section $\varphi \circ \lambda$. As described in Section 8.2, we will directly compute $\widetilde{j_b}(P_0)$ and $\widetilde{j_b}(P_1)$ following Algorithm 8.2.2 and interpolate to determine the map. What the following computations show is that

$$\varphi \circ \lambda(\nu) = (2\nu, 0, 6 - \nu). \quad (9.6)$$

By Proposition 8.2.1, this map is given by convergent power series and is linear modulo p. Giving $\mathbf{Z}_p^3$ the coordinates (x_1, x_2, x_3), the image of $\varphi \circ \lambda$ is cut out by the equations $f_1 = x_2 = 0$, $f_2 = 2x_3 + x_1 + 2 = 0$.

Algorithm 8.2.2 relies on being able to compute Coleman–Gross local heights. Balakrishnan [Bal] has implemented Coleman–Gross local heights $h_p(D, E)$ for disjoint divisors of degree 0 on a curve Y with a few requirements:

1. the hyperelliptic curve $Y : y^2 = H(x)$ is given by a monic odd degree model;
2. 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 $P_i, Q_j \in Y(\mathbf{Q}_p)$.

Remark 9.0.7. Suppose that $D = \sum_i n_i P_i$ and $E = \operatorname{Div} r + E'$ where $E' = \sum_j m_j Q_j$

with $P_i, Q_j \in Y(\mathbf{Q}_p)$. 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 given by

$$y^2 = g(x) := x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1$$

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 $\mathbf{Q}_p$ given by the coordinate transformation from the even degree model

$$(x,y) \mapsto (c_0 \cdot x/(x-\beta), \beta^3 y/(x-\beta)^3). \tag{9.7}$$

Remark 9.0.8. 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 $\psi(\widetilde{j_b}(P)) = h_p(P - b, A_\alpha|_{P\times X})$. Since $B \cap P_\nu$ is empty over $\mathbf{Z}/p^2\mathbf{Z}$ for all $\nu \in \mathbf{F}_p$, 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 (9.12). By Remark 9.0.7, 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 described in Algorithms 8.2.5 and 8.2.7, 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 Algorithm 8.2.5 we can compute (u_2, v_2), the Mumford representation for $2D_{P_1}$. Applying Algorithm 8.2.7 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

$$2D_{P_1} = \operatorname{Div}(u_1, v_1) = \operatorname{Div}((y - v_2(x))/u_3(x)) + \operatorname{Div}(u_3, v_3). \tag{9.8}$$

Remark 9.0.9. 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 $\mathbf{Q}_p$. Using the equations (9.7) 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

$$\{Q_1, Q_2\} :=$$
$$\{(469610\cdot 7 + O(7^9), -15018865 + O(7^9)),\ (499647 + O(7^9), -14480684 + O(7^9))\}.$$

By (9.8) we have

$$2D_{P_1} = Q_1 + Q_2 + \mathrm{Div}((y - v_2(x))/u_3(x)) + 2\infty,$$

where

$$\begin{aligned} v_2(x) := &- (462222 + O(7^8))x^3 + (73804 + O(7^8))x^2 + (1999391 + O(7^8))x \\ &- 1649234 + O(7^8) \end{aligned}$$

and

$$u_3(x) := (1 + O(7^8))x^2 + (1977884 + O(7^8))x + 297368 \cdot 7 + O(7^8).$$

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 (9.13). 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

$$\log g_{P_1}(P_1 - b) = 6 \cdot 7 + 3 \cdot 7^2 + 2 \cdot 7^3 + 2 \cdot 7^4 + O(7^5)$$

$$\log(y - v_2)(P_1 - b)/u_3(P_1 - b)) = 7^2 + 3 \cdot 7^3 + 2 \cdot 7^4 + O(7^5))$$

$$h_p(P_1 - b, Q_1 + Q_2 + 2\infty + 2(4\infty_- - \iota b - 5\iota Q)) = 5 \cdot 7 + 7^2 + 4 \cdot 7^3 + O(7^4)$$

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 $\varphi : T(\mathbf{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbf{Z}_p^3$ given in Definition 7.3.11. We can compute this using the logarithm, normalized by the logarithm at P:

$$\log(P_0 - b) - \log(P_0 - b) = (0, 0),$$
$$\log(P_1 - b) - \log(P_0 - b) = (2 \cdot 7 + O(7^2), O(7^2)).$$

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 (9.6).

We now discuss the map κ using formulas in Section 8.3. We will show that the map $\varphi \circ \kappa : \mathbf{Z}_p^2 \to \mathbf{Z}_p^3$ which is given by convergent power series, modulo p is

$$(n_1, n_2) \mapsto (n_1, -n_1 - 2n_2, -3n_1^2 - n_1 n_2 - n_1 + n_2 - 1). \tag{9.9}$$

Following Algorithm 8.3.1 we construct the points of $\mathcal{M}^\times(G_i, f(G_j))(\mathbf{Z})$ and $\mathcal{M}^\times(G_i, c)(\mathbf{Z})$ for $i, j = 1, 2$ as in [EL21, Section 8.3].

We work out the example $\mathcal{M}^\times(G_1, f(G_2))(\mathbf{Z})$ here in detail. Recall from (9.5) that we have $G_1 = [P - \iota P]$ and $f(G_2) = [3P + Q - 4\iota P]$. By (7.2), the $\mathbf{G}_m$-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 $\mathbf{Q}$, 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 $\mathbf{Z}$ because $-\iota Q$ and ιb intersect over $\mathbf{Z}/2\mathbf{Z}$ so

$$h(P - \iota P, 3(P - \iota P) + (P - \iota Q)) = h_p(P - \iota P, 3(P - \iota P) + (P - \iota Q)) + \log(2).$$

We can compute

$$\begin{aligned} Q_{12} &= ([P-\iota P],[3(P-\iota P)+(P-\iota Q)],h(P-\iota P,3(P-\iota P)+(P-\iota Q)) \\ &= (G_1, f(G_1), 7+O(7^4)). \end{aligned}$$

The remaining Q_{ij} are:

$$\begin{aligned} Q_{11} &= (G_1, f(G_1), 2\cdot 7 + 5\cdot 7^3 + O(7^4)) \\ Q_{21} &= (G_2, f(G_1), 4\cdot 7 + 3\cdot 7^2 + 2\cdot 7^3 + O(7^4)) \\ Q_{22} &= (G_2, f(G_2), 3\cdot 7^2 + 4\cdot 7^3 + O(7^4)) \\ Q_{10} &= (G_1, c, 3\cdot 7 + 4\cdot 7^2 + 5\cdot 7^3 + O(7^4)) \\ Q_{20} &= (G_2, c, 3\cdot 2\cdot 7 + 2\cdot 7^3 + O(7^4)). \end{aligned}$$

Remark 9.0.10. In practice, since we will need to add Q_{ij} in $\mathcal{N} \simeq J(\mathbf{Q}_p)\times J(\mathbf{Q}_p)\times \mathbf{Q}_p$ we use the map $\log : J(\mathbf{Q}_p) \to \mathbf{Q}_p^g$ 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 $\mathbf{Q}_p^g$ instead of $J(\mathbf{Q}_p)$.

We proceed to compute the bijection $\kappa : \mathbf{Z}_p^2 \to T(\mathbf{Z}_p)_{\widetilde{j_b(\overline{P})}}$ of the integral points of T modulo p^2, as in [EL21, Section 8.5]. The divisor $j_b(\overline{P}) \in J(\mathbf{F}_p)$ is equal to the image of

$$\widetilde{G_t} := G_1 + 3G_2$$

in $J(\mathbf{F}_p)$ 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 $J(\mathbf{Z}) \to J(\mathbf{F}_p)$. 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 $\kappa_{\mathbf{Z}}$ is given in coordinates in $\mathcal{N}$ by sending (n_1, n_2) to

$$
\begin{aligned}
&((7+7^2+7^3+O(7^4))\cdot n_1+(4\cdot 7^3+O(7^4))\cdot n_2+5\cdot 7+5\cdot 7^2+7^3+O(7^4),\\
&(6\cdot 7+4\cdot 7^2+3\cdot 7^3+O(7^4))\cdot n_1+(5\cdot 7+O(7^4))\cdot n_2+5\cdot 7^2+3\cdot 7^3+O(7^4)),\\
&((6\cdot 7+5\cdot 7^2+6\cdot 7^3+O(7^4))\cdot n_1+(2\cdot 7+2\cdot 7^2+6\cdot 7^3+O(7^4),\\
&(4\cdot 7+3\cdot 7^2+3\cdot 7^3+O(7^4))\cdot n_1+(3\cdot 7+3\cdot 7^2+O(7^4))\cdot n_2\\
&+4\cdot 7+2\cdot 7^3+O(7^4)),\\
&(4\cdot 7+6\cdot 7^2+3\cdot 7^3+O(7^4))\cdot n_1^2+(6\cdot 7+7^2+4\cdot 7^3+O(7^4))\cdot n_2^2+\\
&(6\cdot 7+3\cdot 7^2+2\cdot 7^3+O(7^4))\cdot n_1+(7+7^3+O(7^4))\cdot n_2+6\cdot 7\\
&+6\cdot 7^2+3\cdot 7^3+O(7^4))
\end{aligned}
$$

where we apply the logarithm to the first two coordinates as in Remark 9.0.10.

Finally, by [EL21, Theorem 4.10], the map $\kappa_{\mathbf{Z}}$ extends to a bijection

$$\kappa : \mathbf{Z}_p^2 \to T(\mathbf{Z}_p)_{\widetilde{j_b}(\overline{P})} \tag{9.10}$$

with image $\overline{T(\mathbf{Z})}_{\widetilde{j_b}(\overline{P})}$. This map κ is given by convergent power series $(\kappa_1, \kappa_2, \kappa_3) \in \mathbf{Z}_p\langle x_1, x_2\rangle^3$, with κ_1, κ_2 linear modulo p and κ_3 at worst quadratic modulo p. Applying Corollary 7.3.12, we obtain the formula for $\varphi \circ \kappa$ given in (9.9).

We now have the tools to prove the upper bound on the number of points in the residue disk $\#X(\mathbf{Z})_{\overline{P}}$. We use Theorem 8.4.1. We define

$$\overline{g_1} := \kappa^* \overline{f_1} = -n_1 - 2n_2, \quad \overline{g_2} := \kappa^* \overline{f_2} = n_1^2 - 2n_1 n_2 - n_1 + 2n_2,$$

and $\overline{A} := \mathbf{F}_p[n_1, n_2]/(\overline{g_1}, \overline{g_2})$. The ring $\overline{A}$ is isomorphic to $\mathbf{F}_p[n_2]/(n_2^2 - 3n_2) \cong \mathbf{F}_p \times \mathbf{F}_p$, so by Theorem 8.4.1 we have an upper bound of 2 on $\#X(\mathbf{Z})_{\overline{P}}$. 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 $X(\mathbf{Z}/p^2\mathbf{Z})_{\overline{P}}$; the other P_ν have no rational points lying over them.

By iterating over all residue disks, and observing that Algorithm 8.4.2 always returns fail for the Weierstrass residue disk R, we obtain Theorem 9.0.1.

Remark 9.0.11. 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" $X(\mathbf{Z}_p)_{P_4}$ and $T(\mathbf{Z}_p)_{\widetilde{j_b}(P_4)}$, consisting of points that reduce to a specified $\mathbf{Z}/p^2\mathbf{Z}$-point. We can parametrize $X(\mathbf{Z}_p)_{P_4}$ with the map $\mathbf{Z}_p \to X(\mathbf{Z}_p)_{P_4}$ sending μ to $P_{4+p\mu}$. With respect to our usual bijection $\varphi : T(\mathbf{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbf{Z}_p^3$, we get a bijection of the higher residue disk of the torsor $T(\mathbf{Z}_p)_{\widetilde{j_b}(P_4)} \to (1,0,2) + p\mathbf{Z}_p^3$. Given these identifications, the inclusion $\widetilde{j_b} : X^{\mathrm{sm}}(\mathbf{Z}_p)_{P_4} \to T(\mathbf{Z}_p)_{\widetilde{j_b}(P_4)}$ is given by power series that are linear modulo p. Like in Section 8.2, these can be found by interpolation. Similarly, κ restricted to $(1 + p\mathbf{Z}_p) \times (3 + p\mathbf{Z}_p)$ gives the inclusion $\kappa : \overline{T(\mathbf{Z})}_{\widetilde{j_b}(P_4)} \to T(\mathbf{Z}_p)_{\widetilde{j_b}(P_4)}$. 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 $T(\mathbf{Z}/p^3\mathbf{Z})_{\widetilde{j_b}(P_4)} \cong \mathbf{F}_p^3$ is $(5,1,5)$, corresponding to $P_{4+p\mu}$ with $\mu = 4$. This is the point $P_{32} \in X(\mathbf{Z}/p^3\mathbf{Z})_{P_4}$.

In total, we can strengthen Proposition 9.0.5 to say the residue disk $X(\mathbf{Z})_{\overline{P}}$ is contained in the set

$$\{P, (4 \cdot 7 + 4 \cdot 7^2 + O(7^3), 6 + 6 \cdot 7 + 6 \cdot 7^2 + O(7^3))\}.$$

9.1 Supplementary equations

$$\begin{aligned} D_f := [&x^5 - x^3y - xy - y^2 - x - y, \\ &u^5 - u^3v - uv - v^2 - u - v, \\ &1120x^{20}u^4 - 2068x^{20}u^3 + 8124x^{19}u^4 + 2407x^{20}u^2 - 16894x^{19}u^3 + 35279x^{18}u^4 - \\ &1641x^{20}u + 18092x^{19}u^2 - 67012x^{18}u^3 + 102591x^{17}u^4 + 378x^{20} - 8178x^{19}u + \\ &58447x^{18}u^2 - 173283x^{17}u^3 + 216476x^{16}u^4 + 774x^{19} - 14247x^{18}u + 103331x^{17}u^2 - \\ &297137x^{16}u^3 + 334741x^{15}u^4 + 1458x^{18} - 31130x^{17}u + 180514x^{16}u^2 - 358567x^{15}u^3 + \\ &360468x^{14}u^4 + 10605x^{17} - 90380x^{16}u + 290195x^{15}u^2 - 395289x^{14}u^3 + 240873x^{13}u^4 + \\ &20415x^{16} - 159334x^{15}u + 394529x^{14}u^2 - 407100x^{13}u^3 + 44248x^{12}u^4 + 22701x^{15} - \\ &112959x^{14}u + 418497x^{13}u^2 - 493887x^{12}u^3 - 105112x^{11}u^4 + 25606x^{14} - 115611x^{13}u + \end{aligned} \tag{9.11}$$

$$111265x^{12}u^2 - 417580x^{11}u^3 - 92961x^{10}u^4 + 1092x^{13} - 103527x^{12}u + 145152x^{11}u^2 -$$
$$88490x^{10}u^3 - 92811x^9u^4 + 48856x^{12} + 186438x^{11}u + 267721x^{10}u^2 - 155622x^9u^3 -$$
$$45395x^8u^4 - 27776x^{11} - 191295x^{10}u - 178159x^9u^2 - 70489x^8u^3 + 16905x^7u^4 -$$
$$61956x^{10} - 74059x^9u + 378244x^8u^2 + 15979x^6u^4 + 74366x^9 + 338472x^8u +$$
$$227589x^7u^2 - 232801x^7u^3 + 74613x^6u^3 - 16012x^5u^4 - 87675x^8 - 182672x^7u -$$
$$189206x^6u^2 + 26802x^5u^3 + 25133x^4u^4 - 85989x^7 - 42976x^6u + 119160x^5u^2 +$$
$$38380x^4u^3 - 14569x^3u^4 + 57369x^6 + 50376x^5u - 22878x^4u^2 - 26236x^3u^3 + 5653x^2u^4 -$$
$$19638x^5 - 66959x^4u + 10199x^3u^2 + 7737x^2u^3 - 1185xu^4 - 18109x^4 + 33891x^3u -$$
$$10338x^2u^2 + 126xu^3 + 90u^4 + 8894x^3 - 13882x^2u + 3365xu^2 - 189u^3 - 1493x^2 +$$
$$903xu - 105u^2 - 176x + 18u + 4,$$
$$7605023584402176072496x^8u^2 + 2768486683241947883 74x^8u +$$
$$2162467398048698636700x^7u^2 - 6272554892698832692599x^6yu^2 -$$
$$4626446567682633747828x^8v - 1168446771586826201673x^8 -$$
$$9165162915676858733619x^7u + 22417778405781371960 64x^6yu -$$
$$8418141092008037071834x^6u^2 - 1329283618505214441 9762x^5yu^2 +$$
$$7540311235979813608 94x^7v + 6328906343710703634915x^6yv +$$
$$2615195628519325252191x^7 + 1831262799801461507208x^6y +$$
$$2756070458250784948869x^6u + 1542885737601080315 3841x^5yu -$$
$$1178405157090204813570 3x^5u^2 - 7230872538984499657093x^4yu^2 +$$
$$1691215636878196684489 9x^6v + 8794134244461097697655x^5yv +$$
$$1338224146912715019646 5x^6 + 4082469582390924565047x^5y +$$
$$2185254059854079808748 9x^5u + 1324551957955414316 3167x^4yu -$$
$$2298506691516002953607 4x^4u^2 - 2325512870479071241 7887x^3yu^2 +$$
$$1368282217156041218560 5x^5v - 1657830204331706045 50x^4yv -$$
$$6931902302166164206278x^5 - 5083451259029072420619x^4y -$$
$$1182635042956920395184 0x^4u - 1919969951531181145221 3x^3yu -$$
$$2848448469874504607566 9x^3u^2 - 1769007671522226560248 9x^2yu^2 +$$
$$1780547344369634882785 6x^4v + 6752028083461404793 78x^3yv +$$
$$6675814886892603310402x^4 + 5577161777751351740903x^3y +$$
$$1996987869297997305565 2x^3u + 1812011706343313573508 3x^2yu +$$
$$9367133751059719535 31x^2u^2 + 1146685345403738606602 0xyu^2 +$$
$$1054252397224219020 9720x^3v + 8824421921807203283 64x^2yv +$$
$$1187716080667185367280 4x^3 + 1336391324717490306295 3x^2y +$$
$$1405945365261734047124 7x^2u + 1021805783389322735660 5xyu -$$
$$3083617872452200324 44xu^2 - 5322779956111165805354yu^2 +$$

$$55059126293216804765 60x^2v - 42906953276893202791 11xyv -$$
$$76129000756276722072 15x^2 - 14312446660999532149696xy +$$
$$44346400844378002849 87xu + 37048851288339553852 71yu -$$
$$99379606891252039728 2u^2 + 57535042100777081983xv +$$
$$38298304304869315824 08yv + 5885803647094172346013y +$$
$$960790192851544016507u + 281506727438003913980v +$$
$$113825130829311801917,$$
$$79013571401366841721 1x^8u^2 - 52199251698889313788x^8u +$$
$$44562639782212338096 0x^7u^2 - 48406514807265213939 3x^6yu^2 -$$
$$35558977001786556963 9x^8v - 97839554801178078020x^8 -$$
$$67839856603903699253 9x^7u + 15519858639326348781 8x^6yu -$$
$$11305226481813154347 9x^6u^2 - 87476519630767121242 4x^5yu^2 +$$
$$50893236050896468243x^7v + 5498060684619324234 05x^6yv +$$
$$24585237376494882702 7x^7 + 22297366557808537676 6x^6y -$$
$$18600639199885965103 1x^6u + 91813502090018984146 9x^5yu -$$
$$52315071243425667056 1x^5u^2 - 32892782272590067729x^4yu^2 +$$
$$13888676427114547884 42x^6v + 88268461308108062105 7x^5yv +$$
$$11427915467453523342 16x^6 + 53373200454927802201 0x^5y +$$
$$39446435314734485091 4x^5u + 87458656427089652323 6x^4yu -$$
$$15036238617584697816 38x^4u^2 - 11182568773301230367 94x^3yu^2 +$$
$$96225361707042387283 4x^5v + 26067542028790437749 6x^4yv -$$
$$73108557049802456668x^5 - 17784151486498075851 8x^4y -$$
$$13579658739219141161 06x^4u - 15953374680139636406 22x^3yu -$$
$$18825583038409378887 97x^3u^2 - 12939226340221196774 92x^2yu^2 +$$
$$13907536926901897677 06x^4v + 24643890801017127516 8x^3yv +$$
$$79369122220858397910 4x^4 + 49922327851425638277 8x^3y +$$
$$64525616777037225702 1x^3u + 98478614500010759892 9x^2yu -$$
$$28071852467374955669 7x^2u^2 + 77993302363668422379 9xyu^2 +$$
$$84218944649447106542 7x^3v + 55855144402200423378 0x^2yv +$$
$$91324189699423759343 1x^3 + 12449633635513429496 90x^2y +$$
$$72711776546004320792 6x^2u + 10124410309230281872 82xyu -$$
$$21753359867708939458xu^2 - 34494210636062588896 6yu^2 +$$
$$35302520023217058393 6x^2v - 21103312194862399145 5xyv -$$
$$16387578568385021983 2x^2 - 61719875462517417909 3xy +$$
$$59783013472835612282 9xu + 16990186180271683095 4yu -$$

$$822032246651072261 92u^2 + 8231045543079961 9016xv+$$
$$191169787322405231086yv + 341475392487935405751x+$$
$$350318508927358217032y - 210287318910739415 84u - 9558514495942700720v]$$

Here, we are working on $X \times X$ where the first copy of X has coordinates (x, y) and the second copy has coordinates (u, v).

The equation g_{P_0} is given by

$$\begin{aligned} g_{P_0} :=& 118016503u^{11} + 793929202u^{10} - 2478346563u^9 - 3325919630u^8 - \\ & 3561952636u^7 + 2886039937u^6 + 5879367604u^5 - 3830171961u^4 + \\ & 75101411u^3 + 2188669692u^2 - 697370245u + 85830184)/(338078160u^{14} + \\ & 1369216548u^{13} + 2510230338u^{12} + 2713077234u^{11} + 1318504824u^{10} - \\ & 3414589416u^9 - 135231264u^8 - 236654712u^7 - 6668591706u^6 + \\ & 1850977926u^5 + 3220194474u^4 - 1293148962u^3 + 397241838u^2 - \\ & 8451954u)v + (375507055u^{14} + 718827791u^{13} - 1351825398u^{12} - \\ & 3390292268u^{11} - 6705483125u^{10} + 42915092u^9 - 3840900734u^8 - \\ & 10868247049u^7 + 12659952140u^6 + 12198614901u^5 - 5503860549u^4 - \\ & 1083606073u^3 + 1748789999u^2 - 686641472u + 85830184)/(338078160u^{14} + \\ & 1369216548u^{13} + 2510230338u^{12} + 2713077234u^{11} + 1318504824u^{10} - \\ & 3414589416u^9 - 135231264u^8 - 236654712u^7 - 6668591706u^6 + \\ & 1850977926u^5 + 3220194474u^4 - 1293148962u^3 + 397241838u^2 - 8451954u) \end{aligned} \tag{9.12}$$

where u, v are elements of the function field of X satisfying $v^2 + (u^3 + u + 1) = u^5 - u$.

The equation g_{P_1} is given by

$$g_{P_1} := (9192u^{12} + 11490u^{11} + 10341u^{10} + 104559u^9 + 116049u^8 + 189585u^7 + \tag{9.13}$$

$$24129u^6 - 659526u^5 - 335508u^4 + 291846u^3 + 135582u^2 + 34470u +$$
$$1149)/(17360u^{11} + 35588u^{10} + 40362u^9 + 23002u^8 - 18662u^7 -$$
$$161014u^6 + 333746u^5 - 518630u^4 + 361088u^3 - 108500u^2 + 21266u -$$
$$434)v + (-9192u^{14} - 2298u^{13} - 8043u^{12} - 118347u^{11} - 181542u^{10} -$$
$$351594u^9 - 2298u^8 + 689400u^7 - 13788u^6 - 476835u^5 + 65493u^4 +$$
$$167754u^3 + 52854u^2 - 13788u + 2298)/(17360u^{11} + 35588u^{10} +$$
$$40362u^9 + 23002u^8 - 18662u^7 - 161014u^6 + 333746u^5 - 518630u^4 +$$
$$361088u^3 - 108500u^2 + 21266u - 434)$$

where u, v are elements of the function field of X satisfying $v^2 + (u^3 + u + 1) = u^5 - u$.

References

[ABB+] Eran Assaf, Angelica Babei, Ben Breen, Sara Chari, Edgar Costa, Juanita Duque-Rosero, Avinash Kulkarni, Grant Molnar, Michael Musty, Sam Schiavone, Shikhin Sethi, Samuel Tripp, and John Voight. *Hilbert modular forms, Magma code*. https://github.com/edgarcosta/hilbertmodularforms. ↑47.

[BGJGP05] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen. Finiteness results for modular curves of genus at least 2. *American Journal of Mathematics*, 127(6):1325–1387, 2005. ↑21 and 26.

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Annals of Mathematics. Second Series*, 189(3):885–944, 2019. ↑84.

[Bal] Jennifer S. Balakrishnan. *Sage code*. https://github.com/jbalakrishnan/AWS. ↑89, 129, and 133.

[Bal13] Jennifer S. Balakrishnan. Iterated Coleman integration for hyperelliptic curves. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Series*, pages 41–61. Mathematical Sciences Publishers, Berkeley, CA, 2013. ↑76.

[Bal15a] Jennifer S. Balakrishnan. Coleman integration for even-degree models of hyperelliptic curves. *London Mathematical Society Journal of Computation and Mathematics*, 18(1):258–265, 2015. ↑16.

[Bal15b] Jennifer S. Balakrishnan. Explicit p-adic methods for elliptic and hyperelliptic curves. In *Advances on superelliptic curves and their applications*, volume 41 of *NATO Science for Peace and Security Series D: Information and Communication Security*, pages 260–285. IOS, Amsterdam, 2015. ↑13 and 17.

[BB12] Jennifer S. Balakrishnan and Amnon Besser. Computing local p-adic height pairings on hyperelliptic curves. *International Mathematics Research Notices. IMRN*, (11):2405–2444, 2012. ↑9, 87, 120, and 122.

[BB15] Jennifer S. Balakrishnan and Amnon Besser. Coleman-Gross height pairings and the p-adic sigma function. *Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]*, 698:89–104, 2015. ↑9, 10, and 76.

[BBM16] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller. Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves. *Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]*, 720:51–79, 2016. ↑10, 18, 72, and 73.

[BBM17] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller. Computing integral points on hyperelliptic curves using quadratic Chabauty. *Mathematics of Computation*, 86(305):1403–1434, 2017. ↑76.

[BBB+21] Jennifer S. Balakrishnan, Alex J. Best, Francesca Bianchi, Brian Lawrence, J. Steffen Müller, Nicholas Triantafillou, and Jan Vonk. Two recent p-adic approaches towards the (effective) Mordell conjecture. *Arithmetic L-functions and differential geometric methods*, pages 31–74, 2021. ↑8, 86, 93, 96, 101, 128, 130, and 131.

[BBK10] Jennifer S. Balakrishnan, Robert W. Bradshaw, and Kiran S. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Computer Science*, pages 16–31. Springer, Berlin, 2010. ↑16 and 76.

[BD18] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Mathematical Journal*, 167(11):1981–2038, 2018. With an appendix by J. Steffen Müller. ↑3, 71, 74, 78, 82, 95, and 129.

[BD21] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and Rational Points II: Generalised Height Functions on Selmer Varieties. *International Mathematics Research Notices. IMRN*, (15):11923–12008, 2021. ↑3, 71, 82, 95, and 129.

[BDM+21] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Quadratic Chabauty for modular curves: Algorithms and examples, 2021. Preprint, `arXiv:1501.04657`. ↑8, 74, 82, 84, and 93.

[BKK11] Jennifer S. Balakrishnan, Kiran S. Kedlaya, and Minhyong Kim. Appendix and erratum to "Massey products for elliptic curves of rank 1". *Journal of the American Mathematical Society*, 24(1):281–291, 2011. ↑76.

[BM] Jennifer S. Balakrishnan and J. Steffen Müller. *Computational Tools for Quadratic Chabauty*. http://math.bu.edu/people/jbala/2020BalakrishnanMuellerNotes.pdf. ↑77.

[BMS16] Jennifer S. Balakrishnan, J. Steffen Müller, and William A. Stein. A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties. *Mathematics of Computation*, 85(298):983–1016, 2016. ↑65 and 89.

[BMTV] Jennifer S. Balakrishnan, Steffen J. Müller, Jan Tuitman, and Jan Vonk. *Magma code*. https://github.com/steffenmueller/QCMod. ↑85, 86, 89, 92, and 129.

[BT20] Jennifer S. Balakrishnan and Jan Tuitman. Explicit Coleman integration for curves. *Mathematics of Computation*, 89(326):2965–2984, 2020. ↑16.

[BGX21] Francesc Bars, Josep González, and Xavier Xarles. Hyperelliptic parametrizations of $\mathbb{Q}$ curves. *The Ramanujan Journal*, 56(1):103–120, 2021. ↑8 and 93.

[BCD+14] Massimo Bertolini, Francesc Castella, Henri Darmon, Samit Dasgupta, Kartik Prasanna, and Victor Rotger. p-adic L-functions and Euler systems: a tale in two trilogies. In *Automorphic forms and Galois representations. Vol. 1*, volume 414 of *London Mathematical Society Lecture Note Seres*, pages 52–101. Cambridge University Press, Cambridge, 2014. ↑38.

[BDP13] Massimo Bertolini, Henri Darmon, and Kartik Prasanna. Generalized Heegner cycles and p-adic Rankin L-series. *Duke Mathematical Journal*, 162(6):1033–1148, 2013. With an appendix by Brian Conrad. ↑6, 21, 22, 30, 34, 36, 37, 38, 39, 40, and 42.

[BDP17] Massimo Bertolini, Henri Darmon, and Kartik Prasanna. p-adic L-functions and the coniveau filtration on Chow groups. *Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]*, 731:21–86, 2017. With an appendix by Brian Conrad. ↑29, 45, and 46.

[Bes02] Amnon Besser. Coleman integration using the Tannakian formalism. *Mathematische Annalen*, 322(1):19–48, 2002. ↑18.

[Bes04] Amnon Besser. The p-adic height pairings of Coleman-Gross and of Nekovář. In *Number theory*, volume 36 of *CRM Proceedings Lecture Notes*, pages 13–25. American Mathematical Society, Providence, RI, 2004. ↑74.

[Bes05] Amnon Besser. p-adic Arakelov theory. *Journal of Number Theory*, 111(2):318–371, 2005. ↑73.

[Bes12] Amnon Besser. Heidelberg lectures on Coleman integration. In *The arithmetic of fundamental groups—PIA 2010*, volume 2 of *Contributions in Mathematical and Compututational Sciences*, pages 3–52. Springer, Heidelberg, 2012. ↑14 and 75.

[Bia20] Francesca Bianchi. Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture. *Algebra & Number Theory*, 14(9):2369–2416, 2020. ↑77, 79, 80, and 81.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004. ↑115.

[Cha41] Claude Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, 212:882–885, 1941. ↑2.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993. ↑66.

[Col82] Robert F. Coleman. Dilogarithms, regulators and p-adic L-functions. *Inventiones Mathematicae*, 69(2):171–208, 1982. ↑18.

[Col85a] Robert F. Coleman. Effective Chabauty. *Duke Mathematical Journal*, 52(3):765–770, 1985. ↑2 and 16.

[Col85b] Robert F. Coleman. Torsion points on curves and p-adic abelian integrals. *Annals of Mathematics. Second Series*, 121(1):111–168, 1985. ↑14 and 15.

[Col91] Robert F. Coleman. The universal vectorial bi-extension and p-adic heights. *Inventiones Mathematicae*, 103(3):631–650, 1991. ↑58.

[CG89] Robert F. Coleman and Benedict H. Gross. p-adic heights on curves. In *Algebraic number theory*, volume 17 of *Advanced Studies Pure Mathematics*, pages 73–81. Academic Press, Boston, MA, 1989. ↑6, 9, 10, 58, and 106.

[Col18] Dan J Collins. Numerical computation of Petersson inner products and q-expansions, 2018. Preprint, `arXiv:1802.09740`. ↑63 and 91.

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Mathematics of Computation*, 88(317):1303–1339, 2019. ↑114, 115, and 132.

[Cre95] J. E. Cremona. Computing the degree of the modular parametrization of a modular elliptic curve. *Mathematics of Computation*, 64(211):1235–1250, 1995. ↑67.

[dS87] Ehud de Shalit. *Iwasawa theory of elliptic curves with complex multiplication*, volume 3 of *Perspectives in Mathematics*. Academic Press, Inc., Boston, MA, 1987. p-adic L functions. ↑49 and 50.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proceedings International Summer School University of Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349, 1973. ↑45.

[DLF21] Netan Dogra and Samuel Le Fourn. Quadratic Chabauty for modular curves and modular forms of rank one. *Mathematische Annalen*, 380(1-2):393–448, 2021. ↑26 and 32.

[Dok04] Tim Dokchitser. Computing special values of motivic L-functions. *Experimental Mathematics*, 13(2):137–149, 2004. ↑63 and 66.

[EL21] Bas Edixhoven and Guido Lido. Geometric quadratic Chabauty. *Journal of the Institute of Mathematics of Jussieu*, page 1–55, 2021. ↑6, 95, 96, 97, 99, 100, 101, 104, 105, 106, 107, 108, 109, 111, 114, 115, 117, 118, 125, 126, 127, 129, 137, 138, and 139.

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones Mathematicae*, 73(3):349–366, 1983. ↑1.

[Fly97] E. V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Mathematica*, 105(1):79–94, 1997. ↑96.

[FvdP04] Jean Fresnel and Marius van der Put. *Rigid analytic geometry and its applications*, volume 218 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 2004. ↑14.

[Gal96] Steven D. Galbraith. Equations for modular curves, 1996. Ph.D. Thesis, University of Oxford. ↑86.

[GKZ87] B. Gross, W. Kohnen, and D. Zagier. Heegner points and derivatives of L-series. II. *Mathematische Annalen*, 278(1-4):497–562, 1987. ↑28.

[Gro78] Benedict H. Gross. On the periods of abelian integrals and a formula of Chowla and Selberg. *Inventiones Mathematicae*, 45(2):193–211, 1978. With an appendix by David E. Rohrlich. ↑30.

[Gro84] Benedict H. Gross. Heegner points on $X_0(N)$. In *Modular forms (Durham, 1983)*, Ellis Horwood Series in Mathematics and its Applications: Statistics, Operational Research, pages 87–105. Horwood, Chichester, 1984. ↑28 and 32.

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Inventiones Mathematicae*, 84(2):225–320, 1986. ↑5, 20, 28, and 31.

[GRR72] Alexander Grothendieck, Michel Raynaud, and Dock Sang Rim. *Groupes de monodromie en géométrie algébrique. I.* Lecture Notes in Mathematics, Vol. 288. Springer-Verlag, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I). ↑102.

[HS22] Sachi Hashimoto and Pim Spelier. A geometric linear Chabauty comparison theorem. *Acta Arithmetica*, 202(1):67–88, 2022. ↑109, 129, and 131.

[Kat76] Nicholas M. Katz. p-adic interpolation of real analytic Eisenstein series. *Annals of Mathematics. Second Series*, 104(3):459–571, 1976. ↑76.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16(4):323–338, 2001. ↑17.

[Ked03] Kiran S. Kedlaya. Errata for: "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology" [J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338; mr1877805]. volume 18, pages 417–418. 2003. Dedicated to Professor K. S. Padmanabhan. ↑17.

[KM04] Kamal Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Mathematics of Computation*, 73(245):333–357, 2004. ↑110.

[Kim09] Minhyong Kim. The unipotent Albanese map and Selmer varieties for curves. *Kyoto University. Research Institute for Mathematical Sciences. Publications*, 45(1):89–133, 2009. ↑3 and 72.

[Kim10] Minhyong Kim. Massey products for elliptic curves of rank 1. *Journal of the American Mathematical Society*, 23(3):725–747, 2010. ↑76.

[KT08] Minhyong Kim and Akio Tamagawa. The l-component of the unipotent Albanese map. *Mathematische Annalen*, 340(1):223–235, 2008. ↑82.

[Li75] Wen Ch'ing Winnie Li. Newforms and functional equations. *Mathematische Annalen*, 212:285–315, 1975. ↑25.

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2022. [Online; accessed 21 February 2022]. ↑32.

[Mas20] Nicolas Mascot. Hensel-lifting torsion points on Jacobians and Galois representations. *Mathematics of Computation*, 89(323):1417–1455, 2020. ↑110.

[MST06] Barry Mazur, William Stein, and John Tate. Computation of p-adic heights and log convergence. *Documenta Mathematica*, (Extra Vol.):577–614, 2006. ↑76.

[MT83] Barry Mazur and John Tate. Canonical height pairings via biextensions. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progress in Mathematics*, pages 195–237. Birkhäuser Boston, Boston, MA, 1983. ↑6, 9, 30, 58, 59, 60, and 61.

[MTT86] Barry Mazur, John Tate, and Jeremy Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Inventiones Mathematicae*, 84(1):1–48, 1986. ↑61, 62, 64, 65, and 77.

[MB85] Laurent Moret-Bailly. Pinceaux de variétés abéliennes. *Astérisque*, (129):266, 1985. ↑102.

[Nek93] Jan Nekovář. On p-adic height pairings. In *Séminaire de Théorie des Nombres, Paris, 1990–91*, volume 108 of *Progress in Mathematics*, pages 127–202. Birkhäuser Boston, Boston, MA, 1993. ↑3 and 74.

[Par00] Pierre Parent. Torsion des courbes elliptiques sur les corps cubiques. *Université de Grenoble. Annales de l'Institut Fourier*, 50(3):723–749, 2000. ↑99.

[PR87] Bernadette Perrin-Riou. Points de Heegner et dérivées de fonctions L p-adiques. *Inventiones Mathematicae*, 89(3):455–510, 1987. ↑5, 56, 59, 61, and 62.

[Pol14] Robert Pollack. Overconvergent modular symbols. In *Computations with modular forms*, volume 6 of *Contributions in Mathematical and Computational Sciences*, pages 69–105. Springer, Cham, 2014. ↑64.

[PS11] Robert Pollack and Glenn Stevens. Overconvergent modular symbols and p-adic L-functions. *Annales Scientifiques de l'École Normale Supérieure. Quatrième Série*, 44(1):1–42, 2011. ↑56, 63, 64, and 66.

[Rib80] Kenneth A. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Mathematische Annalen*, 253(1):43–62, 1980. ↑25.

[Rub81] Karl Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. *Inventiones Mathematicae*, 64(3):455–470, 1981. ↑36.

[Rub94] Karl Rubin. p-adic variants of the Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication. In *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991)*, volume 165 of *Contemporary Mathematics*, pages 71–80. American Mathematical Society, Providence, RI, 1994. ↑49, 50, and 51.

[Sch82] Peter Schneider. p-adic height pairings. I. *Inventiones Mathematicae*, 69(3):401–409, 1982. ↑6 and 58.

[Shi73] Goro Shimura. On the factors of the jacobian variety of a modular function field. *Journal of the Mathematical Society of Japan*, 25:523–544, 1973. ↑25 and 38.

[Shi75] Goro Shimura. On some arithmetic properties of modular forms of one and several variables. *Annals of Mathematics. Second Series*, 102(3):491–515, 1975. ↑42.

[Shi77] Goro Shimura. On the periods of modular forms. *Mathematische Annalen*, 229(3):211–221, 1977. ↑65.

[Sma94] N. P. Smart. S-integral points on elliptic curves. *Mathematical Proceedings of the Cambridge Philosophical Society*, 116(3):391–399, 1994. ↑74.

[Smi05] Benjamin Smith. *Explicit endomorphisms and correspondences*. PhD thesis, University of Sydney, 2005. ↑114 and 115.

[Spe20] Pim Spelier. *A geometric approach to linear Chabauty*, 2020. https://www.universiteitleiden.nl/en/science/mathematics/education/theses#master-theses-mathematics, Master's thesis, Leiden University. ↑12, 96, 109, and 111.

[Sta18] Giovanni Staglianò. A Macaulay2 package for computations with rational maps. *Journal of Software for Algebra and Geometry*, 8:61–70, 2018. ↑116.

[Sta96] H. M. Stark. Counting points on CM elliptic curves. volume 26, pages 1115–1138. 1996. Symposium on Diophantine Problems (Boulder, CO, 1994). ↑29.

[Ste07] William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells. ↑52.

[SW13] William Stein and Christian Wuthrich. Algorithms for the arithmetic of elliptic curves using Iwasawa theory. *Mathematics of Computation*, 82(283):1757–1792, 2013. ↑62 and 63.

[Ste00] William Arthur Stein. Explicit approaches to modular abelian varieties, 2000. Ph.D. Thesis, UC Berkeley. ↑65.

[Sut19] Andrew V. Sutherland. Fast Jacobian arithmetic for hyperelliptic curves of genus 3. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Series*, pages 425–442. Mathematical Sciences Publishers, Berkeley, CA, 2019. ↑121.

[Tui16] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$. *Mathematics of Computation*, 85(298):961–981, 2016. ↑17.

[Tui17] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields and their Applications*, 45:301–322, 2017. ↑17.

[Urb14] Eric Urban. Nearly overconvergent modular forms. In *Iwasawa theory 2012*, volume 7 of *Contributions in Mathematical and Computational Sciences*, pages 401–441. Springer, Heidelberg, 2014. ↑41.

[vBHM20] Raymond van Bommel, David Holmes, and J. Steffen Müller. Explicit arithmetic intersection theory and computation of Néron-Tate heights. *Mathematics of Computation*, 89(321):395–410, 2020. ↑87 and 123.

[VZ93] Fernando Rodriguez Villegas and Don Zagier. Square roots of central values of Hecke L-series. In *Advances in number theory (Kingston, ON, 1991)*, Oxford Science Publications, pages 81–99. Oxford University Press, New York, 1993. ↑43 and 44.

[VZB19] John Voight and David Zureick-Brown. The canonical ring of a stacky curve, 2019. Preprint, `arXiv:2101.01862`. ↑47.

[Zag94] Don Zagier. Modular forms and differential operators. volume 104, pages 57–75. 1994. K. G. Ramanathan memorial issue. ↑44.

[Zag08] Don Zagier. Elliptic modular forms and their applications. In *The 1-2-3 of modular forms*, Universitext, pages 1–103. Springer, Berlin, 2008. ↑42, 43, 44, and 45.

Curriculum Vitae